



Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 9.0.3.13, Rules: 18533
Scan started: 4/25/2020 9:41:34 PM

Table of Contents

Introduction

- General Information
- Login Settings

Summary

- Issue Types
- Vulnerable URLs
- Fix Recommendations
- Security Risks
- Causes
- WASC Threat Classification

Issues Sorted by Issue Type

- Cross-Site Request Forgery 50
- Missing Secure Attribute in Encrypted Session (SSL) Cookie 5
- Archive File Download 20
- Cacheable SSL Page Found 39
- Compressed Directory Found 140
- Hidden Directory Detected 1190
- Missing or insecure "Content-Security-Policy" header 5
- Missing or insecure "X-Content-Type-Options" header 5
- Missing or insecure "X-XSS-Protection" header 5
- Missing or insecure Cross-Frame Scripting Defence 5
- Missing or insecure HTTP Strict-Transport-Security Header 5
- Oracle Log File Information Disclosure 20
- Potential Order Information Found 6
- Query Parameter in SSL Request 52
- Temporary File Download 20
- Application Error 9
- Application Test Script Detected 28
- Client-Side (JavaScript) Cookie References 7
- Email Address Pattern Found 14

- Integer Overflow 7
- Internal IP Disclosure Pattern Found 3
- Link to unclassified site 4
- Possible Server Path Disclosure Pattern Found 13
- SHA-1 cipher suites were detected 1

Introduction

This report contains the results of a web application security scan performed by IBM Security AppScan Standard.

Medium severity issues: 55
Low severity issues: 1512
Informational severity issues: 86
Total security issues included in the report: 1653
Total security issues discovered in the scan: 1653

General Information

Scan file name: test426

Scan started: 4/25/2020 9:41:34 PM

Test policy: Default

Host portal-ippe1.eniot.io

Port 443

Operating system: Unknown

Web server: Unknown

Application server: JavaAppServer

Login Settings

Login method: Recorded login
Concurrent logins: Enabled
JavaScript execution: Disabled
In-session detection: Enabled
In-session pattern: Envision_CLP
Tracked or session ID cookies:
837cbf2c4037d0ea9e37c5df2937b9c2
42dea464b09cd2371e151241b10bd05b
JSESSIONID
JSESSIONID
global_id
JSESSIONID
8142657bb99ce5d47beb6ebdabe5671b
_ga
_gid
JSESSIONID
0b68a657f24d12cce48ed4247bcc86d0
JSESSIONID

```
33296aa8a77f7e6d9209cc11b282bf5c  
4bfff685a1f608acedeac059cb0cf3236  
149118e82bd3db8f33f21b97080c04f  
061609d4b398ee03ad76311f6534dd7  
tempoSessionId  
4ccbdc795fbfb26b13bb45b228a8153ff
```

Tracked or session ID parameters: ->"credentials"

Login sequence:

https://portal-ippe1.eniot.io/
https://portal-ippe1.eniot.io/navigator/config/getloginstyle
https://portal-ippe1.eniot.io/navigator/navigator/getoldmenus?
lang=en-US
https://portal-ippe1.eniot.io/iam-
web/organization/security/setting/info?subject_type=org&subject_id=
https://portal-ippe1.eniot.io/portal/
https://portal-ippe1.eniot.io/iam/api/v2/session/get
https://portal-ippe1.eniot.io/devportal/home.html?appId=167
https://portal-ippe1.eniot.io/navigator/navigator/getmenus
https://portal-ippe1.eniot.io/portal-web/config/customStyle
https://portal-ippe1.eniot.io/portal-web/config/docurl?key=devcenter
https://portal-ippe1.eniot.io/iam-web/logout
https://portal-ippe1.eniot.io/devportal/login.html
https://portal-ippe1.eniot.io/devportal/login.html
https://portal-ippe1.eniot.io/portal-web/config/customStyle
https://portal-ippe1.eniot.io/portal-web/config/docurl?key=devcenter
https://portal-ippe1.eniot.io/iam-web/v1/encrypt/publicKey
https://redirector.gvt1.com/edged1/chrome/dict/en-us-8-0.bdic
https://portal-ippe1.eniot.io/iam/api/v3/login
https://portal-ippe1.eniot.io/iam/api/v2/user/organization/list
https://portal-ippe1.eniot.io/iam-web/session/set
https://portal-ippe1.eniot.io/iam-web/security/mfa/status?
user_id=u15877199768991&org_id=o15790616298731
https://portal-ippe1.eniot.io/portal/
https://portal-
ippe1.eniot.io/iam/api/v2/authorization/listBySubject?
subjectType=USER&resourceTypes=menu,menu_v1&subjectId=u1587719976899
1&organizationId=o15790616298731
https://portal-ippe1.eniot.io/navigator/navigator/platform/getmenus
https://portal-ippe1.eniot.io/portal-web/config/docurl?key=devcenter
https://portal-ippe1.eniot.io/portal-web/config/help?keys=about

```
https://portal-ippe1.eniot.io/portal-web/config/customStyle
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-dm/tslmodel.html?
__ts__=1587875295990
https://portal-ippe1.eniot.io/dm-bff/rest/model/getSystemOU
https://portal-ippe1.eniot.io/iam-web/user/authorization/check
https://portal-ippe1.eniot.io/dm-
bff/rest/model/queryTSLModelSummaryByOU
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-dm/overview.html?
__ts__=1587875304449
https://portal-ippe1.eniot.io/dm-
bff/rest/product/queryProductListAll?currentPage=1&pageSize=200
https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics?
productKey=all&now=1587875304973&zero=1587798000000
https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues?
productKey=all&timePeriod=hour&currentTs=1587875304973
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-dm/logicasset.html?
__ts__=1587875313318
https://portal-ippe1.eniot.io/dm-
bff/rest/model/queryTSLModelSummaryByOU
https://portal-ippe1.eniot.io/dm-bff/logicasset/search?
pageNo=1&pageSize=10&expression=
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-dm/simulator.html?
__ts__=1587875316717
https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices
https://portal-ippe1.eniot.io/iam-web/user/authorization/check
https://portal-ippe1.eniot.io/dm-
bff/rest/product/queryProductListAll?currentPage=1&pageSize=200
https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-dm/integration.html?
__ts__=1587875318434
https://portal-ippe1.eniot.io/dm-
bff/rest/product/queryProductListAll?currentPage=1&pageSize=200
https://portal-ippe1.eniot.io/dm-bff/inte/queryChannels
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-dm/firmware.html?
__ts__=1587875329998
https://portal-ippe1.eniot.io/dm-
bff/rest/product/queryProductListAll?currentPage=1&pageSize=200
https://portal-ippe1.eniot.io/iam-web/user/authorization/check
https://portal-ippe1.eniot.io/dm-bff/ota/queryFws?productKey=
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-dm/simulator.html?
__ts__=1587875331107
https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices
https://portal-ippe1.eniot.io/iam-web/user/authorization/check
https://portal-ippe1.eniot.io/dm-
bff/rest/product/queryProductListAll?currentPage=1&pageSize=200
https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/orginfo.html?
__ts__=1587875348818
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/iam-web/organization/info?
id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/organization/transfer/info?
org_id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?
__ts__=1587875358762
https://portal-ippe1.eniot.io/audit/duration?serviceName=audit-
service
https://portal-ippe1.eniot.io/audit/search?
```

```

offset=0&limit=10&startTime=1587270559107&endTime=1587875359107&query={"userName":""}&service=iam&query->"userName"
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/marsweb/main.html?__ts__=1587875385962
https://dashboard-ppe1.envisioniot.com/login/
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-data/storagepolicy.html?
__ts__=1587875419217
https://portal-ippe1.eniot.io/api/archive/resources/isOpen
https://portal-ippe1.eniot.io/api/archive/strategies
https://portal-ippe1.eniot.io/iam-web/user/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/dataide/index.html?
__ts__=1587875425922
https://portal-ippe1.eniot.io/ide/user/getUsername
https://portal-ippe1.eniot.io/ide/datasource/pagingInfo?
dataSourceType=&dataSourceName=
https://portal-ippe1.eniot.io/ide/datasource/query?
pageNum=1&dataSourceType=&dataSourceName=
https://portal-ippe1.eniot.io/ide/datasource/pagingInfo?
dataSourceType=&dataSourceName=
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal/enosapidoc.html?
__ts__=1587875454537
https://portal-ippe1.eniot.io/portal-web/config/docurl?key=apidoc
https://support-cn5.envisioniot.com/docs/api/en/2.1.0/overview.html
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/devportal/sdk_download.html?
__ts__=1587875463396
https://portal-ippe1.eniot.io/navigator/navigator/getSDKs?lang=en-US
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-api/apimanagement.html?
__ts__=1587875471588
https://portal-ippe1.eniot.io/enos-app-webservice/app/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/apim/agroup
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/apim/agroup
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/apim/agroup
https://portal-ippe1.eniot.io/apim/api
https://portal-ippe1.eniot.io/apim/api
https://portal-ippe1.eniot.io/apim/api
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/apim/api
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/enos-app-webservice/app/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-data/modeldeployment.html?
__ts__=1587875519827
https://portal-ippe1.eniot.io/ahs/get/models?pageNum=1&pageSize=10
https://mlide-ppe1.envisioniot.com/tempo/index.jsp
http://mlide-ppe1.envisioniot.com/tempo/login.jsp
https://mlide-ppe1.envisioniot.com/tempo/login.jsp
https://mlide-ppe1.envisioniot.com/tempo/i18nManager/loadI18n
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/dataide/index.html?
__ts__=1587875545355
https://portal-ippe1.eniot.io/ide/user/getAllUsers
https://portal-ippe1.eniot.io/ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
https://portal-ippe1.eniot.io/ide/user/getUsername
https://portal-ippe1.eniot.io/ide/flow/getTimeZone
https://portal-ippe1.eniot.io/ide/user/getAllUsers
https://portal-ippe1.eniot.io/ide/flow/list?
type=0&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&ord

```

```
erBy=update_time&isAsc=false
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/saturnweb/?__ts__=1587875606682
https://portal-ippe1.eniot.io/iam/api/v2/session/get
https://portal-ippe1.eniot.io/saturn/batch/ws/v1/cluster/scheduler
https://portal-ippe1.eniot.io/saturn/batch/ws/v1/cluster/apps?
user=data_o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-data/dataexplore.html?
__ts__=1587875610867
https://portal-ippe1.eniot.io/portal-web/dataex/list?
ouId=o15790616298731
https://portal-ippe1.eniot.io/portal-web/resmgnt/list/ou/service?
serviceName=dataexplorer
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/dataide/index.html?
__ts__=1587875621621
https://portal-ippe1.eniot.io/ide/user/getUsername
https://portal-ippe1.eniot.io/ide/datasource/pagingInfo?
dataSourceType=&dataSourceName=
https://portal-ippe1.eniot.io/ide/datasource/query?
pageNum=1&dataSourceType=&dataSourceName=
https://portal-ippe1.eniot.io/ide/datasource/pagingInfo?
dataSourceType=&dataSourceName=
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal/resourcemanagement.html?
__ts__=1587875625390
https://portal-ippe1.eniot.io/portal-web/resmgnt/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-web/resmgnt/template/streaming
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/serviceaccount.html?
__ts__=1587875645251
https://portal-ippe1.eniot.io/iam-web/appInstance/list
https://portal-ippe1.eniot.io/iam-web/policy/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/orginfo.html?
__ts__=1587875720211
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/iam-web/organization/info?
id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/organization/transfer/info?
org_id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/usermanagement.html?
__ts__=1587875726603
https://portal-ippe1.eniot.io/iam-web/user/list
https://portal-ippe1.eniot.io/iam-web/organization/info?
id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/orginfo.html?
__ts__=1587875760878
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/iam-web/organization/info?
id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/organization/transfer/info?
org_id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/organization/info?
id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/usermanagement.html?
__ts__=1587875820348
https://portal-ippe1.eniot.io/iam-web/user/list
https://portal-ippe1.eniot.io/iam-web/organization/info?
id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/adduser.html?
__ts__=1587875827476&page=1&userType=0
```

```
https://portal-ippe1.eniot.io/iam-web/user/list
https://portal-ippe1.eniot.io/iam-web/v1/encrypt/publicKey
https://portal-ippe1.eniot.io/iam-
web/organization/security/setting/info?
subject_type=org&subject_id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/usermanagement.html?
__ts__=1587875833651&userType=0
https://portal-ippe1.eniot.io/iam-web/user/list
https://portal-ippe1.eniot.io/iam-web/organization/info?
id=o15790616298731
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/authmanagement.html?
__ts__=1587875862413
https://portal-ippe1.eniot.io/iam-web/policy/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/addpolicy.html?
__ts__=1587875864635&isEdit=false&oId=o15790616298731&uId=u158771997
68991
https://portal-ippe1.eniot.io/iam-web/policy/list
https://portal-ippe1.eniot.io/iam-web/organization/resource/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/authmanagement.html?
__ts__=1587875870129&page=
https://portal-ippe1.eniot.io/iam-web/policy/list
https://portal-ippe1.eniot.io/iam-web/session/get
https://portal-ippe1.eniot.io/portal-iam/ldap.html?
__ts__=1587875870826
https://portal-ippe1.eniot.io/iam-web/ldapSource/list
```

Summary

Issue Types 24

TOC

Issue Type	Number of Issues
M Cross-Site Request Forgery	50 
M Missing Secure Attribute in Encrypted Session (SSL) Cookie	5
L Archive File Download	20 
L Cacheable SSL Page Found	39 
L Compressed Directory Found	140 
L Hidden Directory Detected	1190 
L Missing or insecure "Content-Security-Policy" header	5
L Missing or insecure "X-Content-Type-Options" header	5
L Missing or insecure "X-XSS-Protection" header	5
L Missing or insecure Cross-Frame Scripting Defence	5
L Missing or insecure HTTP Strict-Transport-Security Header	5
L Oracle Log File Information Disclosure	20 
L Potential Order Information Found	6
L Query Parameter in SSL Request	52 
L Temporary File Download	20 
I Application Error	9 
I Application Test Script Detected	28 
I Client-Side (JavaScript) Cookie References	7 
I Email Address Pattern Found	14 
I Integer Overflow	7 
I Internal IP Disclosure Pattern Found	3 
I Link to unclassified site	4 
I Possible Server Path Disclosure Pattern Found	13 
I SHA-1 cipher suites were detected	1 

Vulnerable URLs 1293

TOC

URL	Number of Issues
M https://portal-ippe1.eniot.io/apim/agroup	5 
M https://portal-ippe1.eniot.io/audit/duration	3 
M https://portal-ippe1.eniot.io/dataide/index.html	2 
M https://portal-ippe1.eniot.io/devportal/home.html	6 
M https://portal-ippe1.eniot.io/devportal/sdk_download.html	2 
M https://portal-ippe1.eniot.io/dm-bff/logicasset/search	10 
M https://portal-ippe1.eniot.io/dm-bff/rest/model/queryTSLModelSummaryByOU	3 
M https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll	8 
M https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices	3 
M https://portal-ippe1.eniot.io/iam-web/appInstance/list	3 
M https://portal-ippe1.eniot.io/iam-web/ldapSource/validateLinkName	3 
M https://portal-ippe1.eniot.io/iam-web/logout	3 
M https://portal-ippe1.eniot.io/iam-web/organization/info	4 
M https://portal-ippe1.eniot.io/iam-web/organization/resource/list	3 
M https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info	7 
M https://portal-ippe1.eniot.io/iam-web/organization/transfer/info	3 
M https://portal-ippe1.eniot.io/iam-web/policy/list	3 
M https://portal-ippe1.eniot.io/iam-web/security/mfa/status	4 
M https://portal-ippe1.eniot.io/iam-web/session/get	2 
M https://portal-ippe1.eniot.io/iam-web/session/set	3 
M https://portal-ippe1.eniot.io/iam-web/user/authorization/check	3 
M https://portal-ippe1.eniot.io/iam-web/user/list	4 
M https://portal-ippe1.eniot.io/iam/api/v2/authorization/listBySubject	6 
M https://portal-ippe1.eniot.io/ide/datasource/pagingInfo	4 
M https://portal-ippe1.eniot.io/ide/datasource/query	5 
M https://portal-ippe1.eniot.io/ide/flow/list	11 
M https://portal-ippe1.eniot.io/navigator/navigator/getoldmenus	5 
M https://portal-ippe1.eniot.io/navigator/navigator/getsdks	3 
M https://portal-ippe1.eniot.io/portal-api/apimanagement.html	2 
M https://portal-ippe1.eniot.io/portal-data/modeldeployment.html	1 
M https://portal-ippe1.eniot.io/portal-data/storagepolicy.html	1 
M https://portal-ippe1.eniot.io/portal-dm/firmware.html	1 
M https://portal-ippe1.eniot.io/portal-dm/integration.html	1 
M https://portal-ippe1.eniot.io/portal-dm/logicasset.html	1 
M https://portal-ippe1.eniot.io/portal-dm/overview.html	2 
M https://portal-ippe1.eniot.io/portal-dm/simulator.html	1 
M https://portal-ippe1.eniot.io/portal-dm/tslmodel.html	2 
M https://portal-ippe1.eniot.io/portal-iam/actionTrail.html	1 

M	https://portal-ippe1.eniot.io/portal-iam/addLdapService.html	1	
M	https://portal-ippe1.eniot.io/portal-iam/addpolicy.html	1	
M	https://portal-ippe1.eniot.io/portal-iam/adduser.html	1	
M	https://portal-ippe1.eniot.io/portal-iam/orginfo.html	1	
M	https://portal-ippe1.eniot.io/portal-iam/usermanagement.html	1	
M	https://portal-ippe1.eniot.io/portal-web/config/docurl	4	
M	https://portal-ippe1.eniot.io/portal-web/config/help	3	
M	https://portal-ippe1.eniot.io/portal-web/dataex/list	4	
M	https://portal-ippe1.eniot.io/portal-web/resmgnt/list/ou/service	4	
M	https://portal-ippe1.eniot.io/portal/enosapidoc.html	1	
M	https://portal-ippe1.eniot.io/saturn/batch/ws/v1/cluster/apps	2	
M	https://portal-ippe1.eniot.io/saturnweb/	2	
M	https://portal-ippe1.eniot.io/	5	
M	https://portal-ippe1.eniot.io/iam/api/v2/session/get	3	
M	https://portal-ippe1.eniot.io/navigator/config/getloginstyle	2	
L	https://portal-ippe1.eniot.io/audit/search	10	
L	https://portal-ippe1.eniot.io/dm-bff/inte/queryChannels	3	
L	https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues	7	
L	https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics	8	
L	https://portal-ippe1.eniot.io/dm-bff/rest/model/getSystemOU	3	
L	https://portal-ippe1.eniot.io/enos-app-webservice/app/list	3	
L	https://portal-ippe1.eniot.io/iam-web/v1/encrypt/publicKey	3	
L	https://portal-ippe1.eniot.io/api/archive/resources/isOpen	1	
L	https://portal-ippe1.eniot.io/api/archive/strategies	1	
L	https://portal-ippe1.eniot.io/dm-bff/ota/queryFws	2	
L	https://portal-ippe1.eniot.io/iam-web/ldapSource/list	1	
L	https://portal-ippe1.eniot.io/iam/api/v2/user/organization/list	1	
L	https://portal-ippe1.eniot.io/ide/flow/getTimeZone	1	
L	https://portal-ippe1.eniot.io/ide/user/getAllUsers	1	
L	https://portal-ippe1.eniot.io/ide/user/getUsername	1	
L	https://portal-ippe1.eniot.io/navigator/navigator/getmenus	4	
L	https://portal-ippe1.eniot.io/navigator/navigator/platform/getmenus	1	
L	https://portal-ippe1.eniot.io/portal-web/config/customStyle	1	
L	https://portal-ippe1.eniot.io/portal-web/resmgnt/list	1	
L	https://portal-ippe1.eniot.io/portal-web/resmgnt/template/streaming	1	
L	https://portal-ippe1.eniot.io/saturnweb/res/common/index.57829111.bundle.js	1	
L	https://portal-ippe1.eniot.io/dm-bff/	12	
L	https://portal-ippe1.eniot.io/dm-bff/inte/	17	
L	https://portal-ippe1.eniot.io/dm-bff/logicasset/	17	
L	https://portal-ippe1.eniot.io/dm-bff/overview/	17	

L	https://portal-ippe1.eniot.io/dm-bff/rest/	17	<div style="width: 100%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/dm-bff/rest/model/	17	<div style="width: 100%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/dm-bff/rest/product/	17	<div style="width: 100%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/dm-bff/simulator/	17	<div style="width: 100%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/enos-app-webservice/	29	<div style="width: 75%; background-color: yellow;"></div> <div style="width: 25%; background-color: #6f8ea9;"></div>
L	https://portal-ippe1.eniot.io/enos-app-webservice/app/	34	<div style="width: 100%; background-color: yellow;"></div> <div style="width: 100%; background-color: #6f8ea9;"></div>
L	https://portal-ippe1.eniot.io/.adm/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/.admin/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/.cobalt/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/.meta/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/.sploits/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/.web/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/364332/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/857583/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/874840/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/CF_MX_SERVER/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/Citrix/NFuse17/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/Citrix/NFuseAdmin/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/Citrix/NFuseEnterprise/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/DotNetNuke/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/Infrastructure/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/Msword/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/OMA/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC1/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC10/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC100/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC11/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC12/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC13/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC14/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC15/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC16/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC17/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC18/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC19/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC2/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC20/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC21/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC22/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC23/	1	<div style="width: 10%; background-color: yellow;"></div>
L	https://portal-ippe1.eniot.io/W3SVC24/	1	<div style="width: 10%; background-color: yellow;"></div>

L	https://portal-ippe1.eniot.io/W3SVC25/	1	
L	https://portal-ippe1.eniot.io/W3SVC26/	1	
L	https://portal-ippe1.eniot.io/W3SVC27/	1	
L	https://portal-ippe1.eniot.io/W3SVC28/	1	
L	https://portal-ippe1.eniot.io/W3SVC29/	1	
L	https://portal-ippe1.eniot.io/W3SVC3/	1	
L	https://portal-ippe1.eniot.io/W3SVC30/	1	
L	https://portal-ippe1.eniot.io/W3SVC31/	1	
L	https://portal-ippe1.eniot.io/W3SVC32/	1	
L	https://portal-ippe1.eniot.io/W3SVC33/	1	
L	https://portal-ippe1.eniot.io/W3SVC34/	1	
L	https://portal-ippe1.eniot.io/W3SVC35/	1	
L	https://portal-ippe1.eniot.io/W3SVC36/	1	
L	https://portal-ippe1.eniot.io/W3SVC37/	1	
L	https://portal-ippe1.eniot.io/W3SVC38/	1	
L	https://portal-ippe1.eniot.io/W3SVC39/	1	
L	https://portal-ippe1.eniot.io/W3SVC4/	1	
L	https://portal-ippe1.eniot.io/W3SVC40/	1	
L	https://portal-ippe1.eniot.io/W3SVC41/	1	
L	https://portal-ippe1.eniot.io/W3SVC42/	1	
L	https://portal-ippe1.eniot.io/W3SVC43/	1	
L	https://portal-ippe1.eniot.io/W3SVC44/	1	
L	https://portal-ippe1.eniot.io/W3SVC45/	1	
L	https://portal-ippe1.eniot.io/W3SVC46/	1	
L	https://portal-ippe1.eniot.io/W3SVC47/	1	
L	https://portal-ippe1.eniot.io/W3SVC48/	1	
L	https://portal-ippe1.eniot.io/W3SVC49/	1	
L	https://portal-ippe1.eniot.io/W3SVC5/	1	
L	https://portal-ippe1.eniot.io/W3SVC50/	1	
L	https://portal-ippe1.eniot.io/W3SVC51/	1	
L	https://portal-ippe1.eniot.io/W3SVC52/	1	
L	https://portal-ippe1.eniot.io/W3SVC53/	1	
L	https://portal-ippe1.eniot.io/W3SVC54/	1	
L	https://portal-ippe1.eniot.io/W3SVC55/	1	
L	https://portal-ippe1.eniot.io/W3SVC56/	1	
L	https://portal-ippe1.eniot.io/W3SVC57/	1	
L	https://portal-ippe1.eniot.io/W3SVC58/	1	
L	https://portal-ippe1.eniot.io/W3SVC59/	1	
L	https://portal-ippe1.eniot.io/W3SVC6/	1	
L	https://portal-ippe1.eniot.io/W3SVC60/	1	
L	https://portal-ippe1.eniot.io/W3SVC61/	1	

L	https://portal-ippe1.eniot.io/W3SVC62/	1	
L	https://portal-ippe1.eniot.io/W3SVC63/	1	
L	https://portal-ippe1.eniot.io/W3SVC64/	1	
L	https://portal-ippe1.eniot.io/W3SVC65/	1	
L	https://portal-ippe1.eniot.io/W3SVC66/	1	
L	https://portal-ippe1.eniot.io/W3SVC67/	1	
L	https://portal-ippe1.eniot.io/W3SVC68/	1	
L	https://portal-ippe1.eniot.io/W3SVC69/	1	
L	https://portal-ippe1.eniot.io/W3SVC7/	1	
L	https://portal-ippe1.eniot.io/W3SVC70/	1	
L	https://portal-ippe1.eniot.io/W3SVC71/	1	
L	https://portal-ippe1.eniot.io/W3SVC72/	1	
L	https://portal-ippe1.eniot.io/W3SVC73/	1	
L	https://portal-ippe1.eniot.io/W3SVC74/	1	
L	https://portal-ippe1.eniot.io/W3SVC75/	1	
L	https://portal-ippe1.eniot.io/W3SVC76/	1	
L	https://portal-ippe1.eniot.io/W3SVC77/	1	
L	https://portal-ippe1.eniot.io/W3SVC78/	1	
L	https://portal-ippe1.eniot.io/W3SVC79/	1	
L	https://portal-ippe1.eniot.io/W3SVC8/	1	
L	https://portal-ippe1.eniot.io/W3SVC80/	1	
L	https://portal-ippe1.eniot.io/W3SVC81/	1	
L	https://portal-ippe1.eniot.io/W3SVC82/	1	
L	https://portal-ippe1.eniot.io/W3SVC83/	1	
L	https://portal-ippe1.eniot.io/W3SVC84/	1	
L	https://portal-ippe1.eniot.io/W3SVC85/	1	
L	https://portal-ippe1.eniot.io/W3SVC86/	1	
L	https://portal-ippe1.eniot.io/W3SVC87/	1	
L	https://portal-ippe1.eniot.io/W3SVC88/	1	
L	https://portal-ippe1.eniot.io/W3SVC89/	1	
L	https://portal-ippe1.eniot.io/W3SVC9/	1	
L	https://portal-ippe1.eniot.io/W3SVC90/	1	
L	https://portal-ippe1.eniot.io/W3SVC91/	1	
L	https://portal-ippe1.eniot.io/W3SVC92/	1	
L	https://portal-ippe1.eniot.io/W3SVC93/	1	
L	https://portal-ippe1.eniot.io/W3SVC94/	1	
L	https://portal-ippe1.eniot.io/W3SVC95/	1	
L	https://portal-ippe1.eniot.io/W3SVC96/	1	
L	https://portal-ippe1.eniot.io/W3SVC97/	1	
L	https://portal-ippe1.eniot.io/W3SVC98/	1	
L	https://portal-ippe1.eniot.io/W3SVC99/	1	

L	https://portal-ippe1.eniot.io/WEB-INF/	1	
L	https://portal-ippe1.eniot.io/WEB-INF/cfclasses/	1	
L	https://portal-ippe1.eniot.io/WEB-INF/lib/	1	
L	https://portal-ippe1.eniot.io/_borders/	1	
L	https://portal-ippe1.eniot.io/_derived/	1	
L	https://portal-ippe1.eniot.io/_errors/	1	
L	https://portal-ippe1.eniot.io/_fpclass/	1	
L	https://portal-ippe1.eniot.io/_include/	1	
L	https://portal-ippe1.eniot.io/_logs/	1	
L	https://portal-ippe1.eniot.io/_mem_bin/	1	
L	https://portal-ippe1.eniot.io/_mMDBscripts/	1	
L	https://portal-ippe1.eniot.io/_MMServerscripts/	1	
L	https://portal-ippe1.eniot.io/_objects/	1	
L	https://portal-ippe1.eniot.io/_overlay/	1	
L	https://portal-ippe1.eniot.io/_pages/	1	
L	https://portal-ippe1.eniot.io/_passwords/	1	
L	https://portal-ippe1.eniot.io/_private/	1	
L	https://portal-ippe1.eniot.io/_scriptlibrary/	1	
L	https://portal-ippe1.eniot.io/_scripts/	1	
L	https://portal-ippe1.eniot.io/_sharedtemplates/	1	
L	https://portal-ippe1.eniot.io/_tests/	1	
L	https://portal-ippe1.eniot.io/_themes/	1	
L	https://portal-ippe1.eniot.io/_vti_adm/	1	
L	https://portal-ippe1.eniot.io/_vti_aut/	1	
L	https://portal-ippe1.eniot.io/_vti_bin/	1	
L	https://portal-ippe1.eniot.io/_vti_bin/_vti_adm/	1	
L	https://portal-ippe1.eniot.io/_vti_bin/_vti_aut/	1	
L	https://portal-ippe1.eniot.io/_vti_bot/	1	
L	https://portal-ippe1.eniot.io/_vti_cnf/	1	
L	https://portal-ippe1.eniot.io/_vti_log/	1	
L	https://portal-ippe1.eniot.io/_vti_pvt/	1	
L	https://portal-ippe1.eniot.io/_vti_script/	1	
L	https://portal-ippe1.eniot.io/_vti_shm/	1	
L	https://portal-ippe1.eniot.io/_vti_txt/	1	
L	https://portal-ippe1.eniot.io/abc/	1	
L	https://portal-ippe1.eniot.io/about/	1	
L	https://portal-ippe1.eniot.io/acart2_0/	1	
L	https://portal-ippe1.eniot.io/acartpath/	1	
L	https://portal-ippe1.eniot.io/acceso/	1	
L	https://portal-ippe1.eniot.io/access-log/	1	
L	https://portal-ippe1.eniot.io/access/	1	

L	https://portal-ippe1.eniot.io/accessinglog/	1	
L	https://portal-ippe1.eniot.io/accesslog/	1	
L	https://portal-ippe1.eniot.io/accesswatch/	1	
L	https://portal-ippe1.eniot.io/acciones/	1	
L	https://portal-ippe1.eniot.io/account/	1	
L	https://portal-ippe1.eniot.io/accounting/	1	
L	https://portal-ippe1.eniot.io/accounts/	1	
L	https://portal-ippe1.eniot.io/activex/	1	
L	https://portal-ippe1.eniot.io/actuate/	1	
L	https://portal-ippe1.eniot.io/acweb/	1	
L	https://portal-ippe1.eniot.io/adcycle/	1	
L	https://portal-ippe1.eniot.io/add/	1	
L	https://portal-ippe1.eniot.io/address/	1	
L	https://portal-ippe1.eniot.io/adm/	1	
L	https://portal-ippe1.eniot.io/admcgi/	1	
L	https://portal-ippe1.eniot.io/admentor/	1	
L	https://portal-ippe1.eniot.io/admentor/admin/	1	
L	https://portal-ippe1.eniot.io/admin-serv/	1	
L	https://portal-ippe1.eniot.io/admin/	1	
L	https://portal-ippe1.eniot.io/admin_/_	1	
L	https://portal-ippe1.eniot.io/admin_files/	1	
L	https://portal-ippe1.eniot.io/admincp/	1	
L	https://portal-ippe1.eniot.io/administration/	1	
L	https://portal-ippe1.eniot.io/administrator/	1	
L	https://portal-ippe1.eniot.io/adminsample/	1	
L	https://portal-ippe1.eniot.io/adminuser/	1	
L	https://portal-ippe1.eniot.io/admisapi/	1	
L	https://portal-ippe1.eniot.io/admission/	1	
L	https://portal-ippe1.eniot.io/adsamples/	1	
L	https://portal-ippe1.eniot.io/advwebadmin/	1	
L	https://portal-ippe1.eniot.io/advworks/	1	
L	https://portal-ippe1.eniot.io/affiliates/	1	
L	https://portal-ippe1.eniot.io/agencies/	1	
L	https://portal-ippe1.eniot.io/agent/	1	
L	https://portal-ippe1.eniot.io/agentes/	1	
L	https://portal-ippe1.eniot.io/agents/	1	
L	https://portal-ippe1.eniot.io/akopia/	1	
L	https://portal-ippe1.eniot.io/album/	1	
L	https://portal-ippe1.eniot.io/alias/	1	
L	https://portal-ippe1.eniot.io/allaire/	1	
L	https://portal-ippe1.eniot.io/analog-5.1/	1	

L	https://portal-ippe1.eniot.io/analog/	1	
L	https://portal-ippe1.eniot.io/analyze/	1	
L	https://portal-ippe1.eniot.io/apache/	1	
L	https://portal-ippe1.eniot.io/app/	1	
L	https://portal-ippe1.eniot.io/application/	1	
L	https://portal-ippe1.eniot.io/application_assemblies/	1	
L	https://portal-ippe1.eniot.io/application_browsers/	1	
L	https://portal-ippe1.eniot.io/application_code/	1	
L	https://portal-ippe1.eniot.io/application_data/	1	
L	https://portal-ippe1.eniot.io/application_globalresources/	1	
L	https://portal-ippe1.eniot.io/application_localresources/	1	
L	https://portal-ippe1.eniot.io/application_themes/	1	
L	https://portal-ippe1.eniot.io/application_webreferences/	1	
L	https://portal-ippe1.eniot.io/applications/	1	
L	https://portal-ippe1.eniot.io/apps/	1	
L	https://portal-ippe1.eniot.io/appweb/	1	
L	https://portal-ippe1.eniot.io/apt/	1	
L	https://portal-ippe1.eniot.io/ar/	1	
L	https://portal-ippe1.eniot.io/archive/	1	
L	https://portal-ippe1.eniot.io/archives/	1	
L	https://portal-ippe1.eniot.io/art/	1	
L	https://portal-ippe1.eniot.io/asp.net/	1	
L	https://portal-ippe1.eniot.io/asp/	1	
L	https://portal-ippe1.eniot.io/aspnet/	1	
L	https://portal-ippe1.eniot.io/aspnet_client/	1	
L	https://portal-ippe1.eniot.io/aspsamp/	1	
L	https://portal-ippe1.eniot.io/aspx/	1	
L	https://portal-ippe1.eniot.io/assemblies/	1	
L	https://portal-ippe1.eniot.io/assets/	1	
L	https://portal-ippe1.eniot.io/atc/	1	
L	https://portal-ippe1.eniot.io/auth/	1	
L	https://portal-ippe1.eniot.io/authadmin/	1	
L	https://portal-ippe1.eniot.io/aux/	1	
L	https://portal-ippe1.eniot.io/aw/	1	
L	https://portal-ippe1.eniot.io/ayuda/	1	
L	https://portal-ippe1.eniot.io/azdlite/	1	
L	https://portal-ippe1.eniot.io/back/	1	
L	https://portal-ippe1.eniot.io/backdoor/	1	
L	https://portal-ippe1.eniot.io/backup/	1	
L	https://portal-ippe1.eniot.io/backups/	1	
L	https://portal-ippe1.eniot.io/bak/	1	

L	https://portal-ippe1.eniot.io/banca/	1	
L	https://portal-ippe1.eniot.io/banco/	1	
L	https://portal-ippe1.eniot.io/bank/	1	
L	https://portal-ippe1.eniot.io/banner/	1	
L	https://portal-ippe1.eniot.io/banner01/	1	
L	https://portal-ippe1.eniot.io/banners/	1	
L	https://portal-ippe1.eniot.io/bar/	1	
L	https://portal-ippe1.eniot.io/base/	1	
L	https://portal-ippe1.eniot.io/batch/	1	
L	https://portal-ippe1.eniot.io/bb-dnbd/	1	
L	https://portal-ippe1.eniot.io/bbv/	1	
L	https://portal-ippe1.eniot.io/bdata/	1	
L	https://portal-ippe1.eniot.io/bdatos/	1	
L	https://portal-ippe1.eniot.io/beta/	1	
L	https://portal-ippe1.eniot.io/billing/	1	
L	https://portal-ippe1.eniot.io/bin/	1	
L	https://portal-ippe1.eniot.io/binaries/	1	
L	https://portal-ippe1.eniot.io/bio/	1	
L	https://portal-ippe1.eniot.io/bios/	1	
L	https://portal-ippe1.eniot.io/biztalkserverdocs/	1	
L	https://portal-ippe1.eniot.io/biztalkserverrepository/	1	
L	https://portal-ippe1.eniot.io/bkup/	1	
L	https://portal-ippe1.eniot.io/blockquote/	1	
L	https://portal-ippe1.eniot.io/blog/	1	
L	https://portal-ippe1.eniot.io/boadmin/	1	
L	https://portal-ippe1.eniot.io/bob/	1	
L	https://portal-ippe1.eniot.io/body/	1	
L	https://portal-ippe1.eniot.io/book/	1	
L	https://portal-ippe1.eniot.io/boot/	1	
L	https://portal-ippe1.eniot.io/bottom.html	1	
L	https://portal-ippe1.eniot.io/btauxdir/	1	
L	https://portal-ippe1.eniot.io/budget/	1	
L	https://portal-ippe1.eniot.io/bug/	1	
L	https://portal-ippe1.eniot.io/bugs/	1	
L	https://portal-ippe1.eniot.io/bugzilla/	1	
L	https://portal-ippe1.eniot.io/buy/	1	
L	https://portal-ippe1.eniot.io/buynow/	1	
L	https://portal-ippe1.eniot.io/c/	1	
L	https://portal-ippe1.eniot.io/ca_icons/	1	
L	https://portal-ippe1.eniot.io/cache-stats/	1	
L	https://portal-ippe1.eniot.io/caja/	1	

L	https://portal-ippe1.eniot.io/card/	1	
L	https://portal-ippe1.eniot.io/cards/	1	
L	https://portal-ippe1.eniot.io/carellofdocs/	1	
L	https://portal-ippe1.eniot.io/cart/	1	
L	https://portal-ippe1.eniot.io/cash/	1	
L	https://portal-ippe1.eniot.io/casp401k/	1	
L	https://portal-ippe1.eniot.io/caspagent/	1	
L	https://portal-ippe1.eniot.io/caspclient/	1	
L	https://portal-ippe1.eniot.io/caspdoc/	1	
L	https://portal-ippe1.eniot.io/caspsamp/	1	
L	https://portal-ippe1.eniot.io/catalog/	1	
L	https://portal-ippe1.eniot.io/catinfo/	1	
L	https://portal-ippe1.eniot.io/cbi-bin/	1	
L	https://portal-ippe1.eniot.io/cc/	1	
L	https://portal-ippe1.eniot.io/ccard/	1	
L	https://portal-ippe1.eniot.io/ccbill/	1	
L	https://portal-ippe1.eniot.io/cd-cgi/	1	
L	https://portal-ippe1.eniot.io/cd/	1	
L	https://portal-ippe1.eniot.io/cdrom/	1	
L	https://portal-ippe1.eniot.io/ce_html/	1	
L	https://portal-ippe1.eniot.io/cert/	1	
L	https://portal-ippe1.eniot.io/certcontrol/	1	
L	https://portal-ippe1.eniot.io/certenroll/	1	
L	https://portal-ippe1.eniot.io/certificado/	1	
L	https://portal-ippe1.eniot.io/certificate/	1	
L	https://portal-ippe1.eniot.io/certsrv/	1	
L	https://portal-ippe1.eniot.io/cfappman/	1	
L	https://portal-ippe1.eniot.io/cfdocs/	1	
L	https://portal-ippe1.eniot.io/cfide/	1	
L	https://portal-ippe1.eniot.io/cfide/administrator/	1	
L	https://portal-ippe1.eniot.io/cgi-auth/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/.cobalt/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/calendar/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/carello/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/cgi-bin/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/cgi/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/csfaq/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/cssearch/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/cutecast/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/dasp/	1	

L	https://portal-ippe1.eniot.io/cgi-bin/dbman/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/dcforum/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/ews/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/excite/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/gbook/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/guestbook/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/gw5/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/hamweather/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/hwadmin5340/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/iisadmin/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/ikonboard/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/logs	1	
L	https://portal-ippe1.eniot.io/cgi-bin/mwf/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/news/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/openwebmail/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/pollit/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/powerup/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/rwcgi60/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/samples/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/search/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/ssi/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/suche/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/sws/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/templates/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/tools/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/w3-msql/	1	
L	https://portal-ippe1.eniot.io/cgi-bin/www-sql/	1	
L	https://portal-ippe1.eniot.io/cgi-bin2/	1	
L	https://portal-ippe1.eniot.io/cgi-db2/	1	
L	https://portal-ippe1.eniot.io/cgi-dos/	1	
L	https://portal-ippe1.eniot.io/cgi-forte/	1	
L	https://portal-ippe1.eniot.io/cgi-home/	1	
L	https://portal-ippe1.eniot.io/cgi-lib/	1	
L	https://portal-ippe1.eniot.io/cgi-local/	1	
L	https://portal-ippe1.eniot.io/cgi-scripts/	1	
L	https://portal-ippe1.eniot.io/cgi-shl/	1	
L	https://portal-ippe1.eniot.io/cgi-shop/	1	
L	https://portal-ippe1.eniot.io/cgi-source/	1	
L	https://portal-ippe1.eniot.io/cgi-sys/	1	
L	https://portal-ippe1.eniot.io/cgi-temp/	1	
L	https://portal-ippe1.eniot.io/cgi-weddico/	1	

L	https://portal-ippe1.eniot.io/cgi-win/	1	
L	https://portal-ippe1.eniot.io/cgi/	1	
L	https://portal-ippe1.eniot.io/cgibin/	1	
L	https://portal-ippe1.eniot.io/cgilib/	1	
L	https://portal-ippe1.eniot.io/cgis/	1	
L	https://portal-ippe1.eniot.io/cgiscritps/	1	
L	https://portal-ippe1.eniot.io/cgishl/	1	
L	https://portal-ippe1.eniot.io/cgiwin/	1	
L	https://portal-ippe1.eniot.io/chart/	1	
L	https://portal-ippe1.eniot.io/charting/	1	
L	https://portal-ippe1.eniot.io/charts/	1	
L	https://portal-ippe1.eniot.io/citrix/	1	
L	https://portal-ippe1.eniot.io/citrix/icaweb/	1	
L	https://portal-ippe1.eniot.io/citrix/pnagent/	1	
L	https://portal-ippe1.eniot.io/class/	1	
L	https://portal-ippe1.eniot.io/classcache/	1	
L	https://portal-ippe1.eniot.io/classes/	1	
L	https://portal-ippe1.eniot.io/client/	1	
L	https://portal-ippe1.eniot.io/cliente/	1	
L	https://portal-ippe1.eniot.io/clientes/	1	
L	https://portal-ippe1.eniot.io/clients/	1	
L	https://portal-ippe1.eniot.io/clocktower/	1	
L	https://portal-ippe1.eniot.io/cm/	1	
L	https://portal-ippe1.eniot.io/cmsample/	1	
L	https://portal-ippe1.eniot.io/cobalt-images/	1	
L	https://portal-ippe1.eniot.io/code/	1	
L	https://portal-ippe1.eniot.io/com1/	1	
L	https://portal-ippe1.eniot.io/com2/	1	
L	https://portal-ippe1.eniot.io/com3/	1	
L	https://portal-ippe1.eniot.io/common/	1	
L	https://portal-ippe1.eniot.io/communicator/	1	
L	https://portal-ippe1.eniot.io/compra/	1	
L	https://portal-ippe1.eniot.io/compras/	1	
L	https://portal-ippe1.eniot.io/compressed/	1	
L	https://portal-ippe1.eniot.io/conecta/	1	
L	https://portal-ippe1.eniot.io/conf/	1	
L	https://portal-ippe1.eniot.io/config/	1	
L	https://portal-ippe1.eniot.io/connect/	1	
L	https://portal-ippe1.eniot.io/connections/	1	
L	https://portal-ippe1.eniot.io/console/	1	
L	https://portal-ippe1.eniot.io/contact/	1	

L	https://portal-ippe1.eniot.io/content/	1	
L	https://portal-ippe1.eniot.io/contrib/	1	
L	https://portal-ippe1.eniot.io/controlpanel/	1	
L	https://portal-ippe1.eniot.io/cool-logs/	1	
L	https://portal-ippe1.eniot.io/corp/	1	
L	https://portal-ippe1.eniot.io/correo/	1	
L	https://portal-ippe1.eniot.io/counter/	1	
L	https://portal-ippe1.eniot.io/course_tools/	1	
L	https://portal-ippe1.eniot.io/cpanel/	1	
L	https://portal-ippe1.eniot.io/credit/	1	
L	https://portal-ippe1.eniot.io/creditcards/	1	
L	https://portal-ippe1.eniot.io/crypto/	1	
L	https://portal-ippe1.eniot.io/crystalreportviewers/	1	
L	https://portal-ippe1.eniot.io/csr/	1	
L	https://portal-ippe1.eniot.io/css/	1	
L	https://portal-ippe1.eniot.io/cuenta/	1	
L	https://portal-ippe1.eniot.io/cuentas/	1	
L	https://portal-ippe1.eniot.io/currency/	1	
L	https://portal-ippe1.eniot.io/current/	1	
L	https://portal-ippe1.eniot.io/custdata/	1	
L	https://portal-ippe1.eniot.io/customer/	1	
L	https://portal-ippe1.eniot.io/customers/	1	
L	https://portal-ippe1.eniot.io/cutenews/	1	
L	https://portal-ippe1.eniot.io/cvs/	1	
L	https://portal-ippe1.eniot.io/csvweb/	1	
L	https://portal-ippe1.eniot.io/cybercash/	1	
L	https://portal-ippe1.eniot.io/cybercrash/	1	
L	https://portal-ippe1.eniot.io/darkportal/	1	
L	https://portal-ippe1.eniot.io/dat/	1	
L	https://portal-ippe1.eniot.io/data/	1	
L	https://portal-ippe1.eniot.io/database/	1	
L	https://portal-ippe1.eniot.io/databases/	1	
L	https://portal-ippe1.eniot.io/datafiles/	1	
L	https://portal-ippe1.eniot.io/date/	1	
L	https://portal-ippe1.eniot.io/dato/	1	
L	https://portal-ippe1.eniot.io/datos/	1	
L	https://portal-ippe1.eniot.io/db/	1	
L	https://portal-ippe1.eniot.io/db2/	1	
L	https://portal-ippe1.eniot.io/dbase/	1	
L	https://portal-ippe1.eniot.io/dcforum/	1	
L	https://portal-ippe1.eniot.io/ddreport/	1	

L	https://portal-ippe1.eniot.io/ddrint/	1	█
L	https://portal-ippe1.eniot.io/defaultwebapp/	1	█
L	https://portal-ippe1.eniot.io/demo/	1	█
L	https://portal-ippe1.eniot.io/demoauct/	1	█
L	https://portal-ippe1.eniot.io/demomall/	1	█
L	https://portal-ippe1.eniot.io/demos/	1	█
L	https://portal-ippe1.eniot.io/deny/	1	█
L	https://portal-ippe1.eniot.io/department/	1	█
L	https://portal-ippe1.eniot.io/departments/	1	█
L	https://portal-ippe1.eniot.io/detail/	1	█
L	https://portal-ippe1.eniot.io/dev/	1	█
L	https://portal-ippe1.eniot.io/dev60cgi/rwcgi60/	1	█
L	https://portal-ippe1.eniot.io-devel/	1	█
L	https://portal-ippe1.eniot.io-developer/	1	█
L	https://portal-ippe1.eniot.io-development/	1	█
L	https://portal-ippe1.eniot.io-dir/	1	█
L	https://portal-ippe1.eniot.io-directory/	1	█
L	https://portal-ippe1.eniot.io-dist/	1	█
L	https://portal-ippe1.eniot.io-dlsym/	1	█
L	https://portal-ippe1.eniot.io-dm/	1	█
L	https://portal-ippe1.eniot.io-dm_jsp/	1	█
L	https://portal-ippe1.eniot.io-dmr/	1	█
L	https://portal-ippe1.eniot.io-dms/	1	█
L	https://portal-ippe1.eniot.io-doc-html/	1	█
L	https://portal-ippe1.eniot.io-doc/	1	█
L	https://portal-ippe1.eniot.io-doc/packages/	1	█
L	https://portal-ippe1.eniot.io-doc1/	1	█
L	https://portal-ippe1.eniot.io-doc11/	1	█
L	https://portal-ippe1.eniot.io-doc_Boa/	1	█
L	https://portal-ippe1.eniot.io-docroot/	1	█
L	https://portal-ippe1.eniot.io-docs/	1	█
L	https://portal-ippe1.eniot.io-docs1/	1	█
L	https://portal-ippe1.eniot.io-docucolor/	1	█
L	https://portal-ippe1.eniot.io-document/	1	█
L	https://portal-ippe1.eniot.io-documentation/	1	█
L	https://portal-ippe1.eniot.io-documents/	1	█
L	https://portal-ippe1.eniot.io-dom/	1	█
L	https://portal-ippe1.eniot.io-domain/	1	█
L	https://portal-ippe1.eniot.io-down/	1	█
L	https://portal-ippe1.eniot.io-download/	1	█
L	https://portal-ippe1.eniot.io-downloading/	1	█

L	https://portal-ippe1.eniot.io/downloads/	1	█
L	https://portal-ippe1.eniot.io/dropbox/	1	█
L	https://portal-ippe1.eniot.io/dscgi/	1	█
L	https://portal-ippe1.eniot.io/dump/	1	█
L	https://portal-ippe1.eniot.io/durep/	1	█
L	https://portal-ippe1.eniot.io/dyngb/	1	█
L	https://portal-ippe1.eniot.io/easylog/	1	█
L	https://portal-ippe1.eniot.io/easylogs/	1	█
L	https://portal-ippe1.eniot.io/ecartus/	1	█
L	https://portal-ippe1.eniot.io/ejemplo/	1	█
L	https://portal-ippe1.eniot.io/ejemplos/	1	█
L	https://portal-ippe1.eniot.io/email/	1	█
L	https://portal-ippe1.eniot.io/employees/	1	█
L	https://portal-ippe1.eniot.io/empbris/	1	█
L	https://portal-ippe1.eniot.io/en/	1	█
L	https://portal-ippe1.eniot.io/english/	1	█
L	https://portal-ippe1.eniot.io/envia/	1	█
L	https://portal-ippe1.eniot.io/enviamail/	1	█
L	https://portal-ippe1.eniot.io/error_log/	1	█
L	https://portal-ippe1.eniot.io/errorreporter/	1	█
L	https://portal-ippe1.eniot.io/errors/	1	█
L	https://portal-ippe1.eniot.io/es/	1	█
L	https://portal-ippe1.eniot.io/estore/	1	█
L	https://portal-ippe1.eniot.io/etc/	1	█
L	https://portal-ippe1.eniot.io/eupload/	1	█
L	https://portal-ippe1.eniot.io/exadmin/	1	█
L	https://portal-ippe1.eniot.io/exair/	1	█
L	https://portal-ippe1.eniot.io/example/	1	█
L	https://portal-ippe1.eniot.io/examples/	1	█
L	https://portal-ippe1.eniot.io/examples/web-inf/	1	█
L	https://portal-ippe1.eniot.io/excel/	1	█
L	https://portal-ippe1.eniot.io/exchange/	1	█
L	https://portal-ippe1.eniot.io/exchweb/	1	█
L	https://portal-ippe1.eniot.io/exe/	1	█
L	https://portal-ippe1.eniot.io/exec/	1	█
L	https://portal-ippe1.eniot.io/expeval/	1	█
L	https://portal-ippe1.eniot.io/explorer/	1	█
L	https://portal-ippe1.eniot.io/export/	1	█
L	https://portal-ippe1.eniot.io/external/	1	█
L	https://portal-ippe1.eniot.io/extras/	1	█
L	https://portal-ippe1.eniot.io/faq/	1	█

L	https://portal-ippe1.eniot.io/faqs/	1	
L	https://portal-ippe1.eniot.io/fbsd/	1	
L	https://portal-ippe1.eniot.io/fcgi-bin/	1	
L	https://portal-ippe1.eniot.io/features/	1	
L	https://portal-ippe1.eniot.io/file/	1	
L	https://portal-ippe1.eniot.io/fileadmin/	1	
L	https://portal-ippe1.eniot.io/files/	1	
L	https://portal-ippe1.eniot.io/foldoc/	1	
L	https://portal-ippe1.eniot.io/foo/	1	
L	https://portal-ippe1.eniot.io/footer/	1	
L	https://portal-ippe1.eniot.io/form-totaller/	1	
L	https://portal-ippe1.eniot.io/form/	1	
L	https://portal-ippe1.eniot.io/forms/	1	
L	https://portal-ippe1.eniot.io/formsmgr/	1	
L	https://portal-ippe1.eniot.io/forte/examples/	1	
L	https://portal-ippe1.eniot.io/forum/	1	
L	https://portal-ippe1.eniot.io/forums/	1	
L	https://portal-ippe1.eniot.io/forward/	1	
L	https://portal-ippe1.eniot.io/foto/	1	
L	https://portal-ippe1.eniot.io/fotos/	1	
L	https://portal-ippe1.eniot.io/fpadmin/	1	
L	https://portal-ippe1.eniot.io/fpdb/	1	
L	https://portal-ippe1.eniot.io/fpsample/	1	
L	https://portal-ippe1.eniot.io/framesets/	1	
L	https://portal-ippe1.eniot.io/frontend/	1	
L	https://portal-ippe1.eniot.io/ftp/	1	
L	https://portal-ippe1.eniot.io/ftproot/	1	
L	https://portal-ippe1.eniot.io/fun/	1	
L	https://portal-ippe1.eniot.io/fwd/	1	
L	https://portal-ippe1.eniot.io/g/	1	
L	https://portal-ippe1.eniot.io/gallery/	1	
L	https://portal-ippe1.eniot.io/gfx/	1	
L	https://portal-ippe1.eniot.io/girl/	1	
L	https://portal-ippe1.eniot.io/girls/	1	
L	https://portal-ippe1.eniot.io/glba/	1	
L	https://portal-ippe1.eniot.io/global/	1	
L	https://portal-ippe1.eniot.io/glossary/	1	
L	https://portal-ippe1.eniot.io/graphics/	1	
L	https://portal-ippe1.eniot.io/graphs/	1	
L	https://portal-ippe1.eniot.io/grocery/	1	
L	https://portal-ippe1.eniot.io/group/	1	

L	https://portal-ippe1.eniot.io/guest/	1	
L	https://portal-ippe1.eniot.io/guestbook/	1	
L	https://portal-ippe1.eniot.io/guests/	1	
L	https://portal-ippe1.eniot.io/guide/	1	
L	https://portal-ippe1.eniot.io/gxapp/	1	
L	https://portal-ippe1.eniot.io/h1/	1	
L	https://portal-ippe1.eniot.io/head/	1	
L	https://portal-ippe1.eniot.io/help/	1	
L	https://portal-ippe1.eniot.io/helpdesk/	1	
L	https://portal-ippe1.eniot.io/hidden/	1	
L	https://portal-ippe1.eniot.io/hippa/	1	
L	https://portal-ippe1.eniot.io/hire/	1	
L	https://portal-ippe1.eniot.io/history/	1	
L	https://portal-ippe1.eniot.io/hit_matic/	1	
L	https://portal-ippe1.eniot.io/hit_tracker/	1	
L	https://portal-ippe1.eniot.io/hitmatic/	1	
L	https://portal-ippe1.eniot.io/hlstats/	1	
L	https://portal-ippe1.eniot.io/home/	1	
L	https://portal-ippe1.eniot.io/homepage/	1	
L	https://portal-ippe1.eniot.io/horde/	1	
L	https://portal-ippe1.eniot.io/hostingcontroller/	1	
L	https://portal-ippe1.eniot.io/howitworks/	1	
L	https://portal-ippe1.eniot.io/howto/	1	
L	https://portal-ippe1.eniot.io/ht/	1	
L	https://portal-ippe1.eniot.io/htbin/	1	
L	https://portal-ippe1.eniot.io/htdocs/	1	
L	https://portal-ippe1.eniot.io/htm/	1	
L	https://portal-ippe1.eniot.io/html/	1	
L	https://portal-ippe1.eniot.io/htmldocs/	1	
L	https://portal-ippe1.eniot.io/httpacl/	1	
L	https://portal-ippe1.eniot.io/hyperstat/	1	
L	https://portal-ippe1.eniot.io/i-build/	1	
L	https://portal-ippe1.eniot.io/i-mall/	1	
L	https://portal-ippe1.eniot.io/ibi_html/	1	
L	https://portal-ippe1.eniot.io/ibill/	1	
L	https://portal-ippe1.eniot.io/ibmwebas/	1	
L	https://portal-ippe1.eniot.io/ibmwebas/infocenter/	1	
L	https://portal-ippe1.eniot.io/icons/	1	
L	https://portal-ippe1.eniot.io/icons/small/	1	
L	https://portal-ippe1.eniot.io/idea/	1	
L	https://portal-ippe1.eniot.io/ideas/	1	

L	https://portal-ippe1.eniot.io/iis/	1	
L	https://portal-ippe1.eniot.io/iisadmin/	1	
L	https://portal-ippe1.eniot.io/iisadmpwd/	1	
L	https://portal-ippe1.eniot.io/iishelp/	1	
L	https://portal-ippe1.eniot.io/iissamples/	1	
L	https://portal-ippe1.eniot.io/image/	1	
L	https://portal-ippe1.eniot.io/imagenes/	1	
L	https://portal-ippe1.eniot.io/images/	1	
L	https://portal-ippe1.eniot.io/img-sys/	1	
L	https://portal-ippe1.eniot.io/img/	1	
L	https://portal-ippe1.eniot.io/imgs/	1	
L	https://portal-ippe1.eniot.io/import/	1	
L	https://portal-ippe1.eniot.io/impreso/	1	
L	https://portal-ippe1.eniot.io/inbox/	1	
L	https://portal-ippe1.eniot.io/inc/	1	
L	https://portal-ippe1.eniot.io/include/	1	
L	https://portal-ippe1.eniot.io/includes/	1	
L	https://portal-ippe1.eniot.io/incoming/	1	
L	https://portal-ippe1.eniot.io/index.html/	1	
L	https://portal-ippe1.eniot.io/index/	1	
L	https://portal-ippe1.eniot.io/indy/	1	
L	https://portal-ippe1.eniot.io/info/	1	
L	https://portal-ippe1.eniot.io/information/	1	
L	https://portal-ippe1.eniot.io/ingresa/	1	
L	https://portal-ippe1.eniot.io/ingreso/	1	
L	https://portal-ippe1.eniot.io/instaboard/	1	
L	https://portal-ippe1.eniot.io/install/	1	
L	https://portal-ippe1.eniot.io/instantwebmail/	1	
L	https://portal-ippe1.eniot.io/interaction/	1	
L	https://portal-ippe1.eniot.io/interchange/	1	
L	https://portal-ippe1.eniot.io/internal/	1	
L	https://portal-ippe1.eniot.io/interscan/	1	
L	https://portal-ippe1.eniot.io/intranet/	1	
L	https://portal-ippe1.eniot.io/intranet_index/	1	
L	https://portal-ippe1.eniot.io/inventory/	1	
L	https://portal-ippe1.eniot.io/invitado/	1	
L	https://portal-ippe1.eniot.io/ipchat/	1	
L	https://portal-ippe1.eniot.io/isapi/	1	
L	https://portal-ippe1.eniot.io/ishttpd/	1	
L	https://portal-ippe1.eniot.io/sqlplus/	1	
L	https://portal-ippe1.eniot.io/issamples/	1	

L	https://portal-ippe1.eniot.io/java-sys/	1	
L	https://portal-ippe1.eniot.io/java/	1	
L	https://portal-ippe1.eniot.io/javavadoc/	1	
L	https://portal-ippe1.eniot.io/javascript/	1	
L	https://portal-ippe1.eniot.io/javasdk/	1	
L	https://portal-ippe1.eniot.io/javatest/	1	
L	https://portal-ippe1.eniot.io/javax/	1	
L	https://portal-ippe1.eniot.io/jave/	1	
L	https://portal-ippe1.eniot.io/jdbc/	1	
L	https://portal-ippe1.eniot.io/ji/	1	
L	https://portal-ippe1.eniot.io/jigsaw/	1	
L	https://portal-ippe1.eniot.io/job/	1	
L	https://portal-ippe1.eniot.io/join/	1	
L	https://portal-ippe1.eniot.io/joomla/	1	
L	https://portal-ippe1.eniot.io/jrun/	1	
L	https://portal-ippe1.eniot.io/jrunscripts/	1	
L	https://portal-ippe1.eniot.io/js/	1	
L	https://portal-ippe1.eniot.io/jsdirbrowser/	1	
L	https://portal-ippe1.eniot.io/jserv/	1	
L	https://portal-ippe1.eniot.io/jservdocs/	1	
L	https://portal-ippe1.eniot.io/jstlib/	1	
L	https://portal-ippe1.eniot.io/jsp/	1	
L	https://portal-ippe1.eniot.io/jspdocs/	1	
L	https://portal-ippe1.eniot.io/junk/	1	
L	https://portal-ippe1.eniot.io/kiva/	1	
L	https://portal-ippe1.eniot.io/kjva/	1	
L	https://portal-ippe1.eniot.io/knowledgebase/	1	
L	https://portal-ippe1.eniot.io/level/	1	
L	https://portal-ippe1.eniot.io/lib/	1	
L	https://portal-ippe1.eniot.io/libraries/	1	
L	https://portal-ippe1.eniot.io/library/	1	
L	https://portal-ippe1.eniot.io/libro/	1	
L	https://portal-ippe1.eniot.io/lincoln/	1	
L	https://portal-ippe1.eniot.io/linux/	1	
L	https://portal-ippe1.eniot.io/list/	1	
L	https://portal-ippe1.eniot.io/local/	1	
L	https://portal-ippe1.eniot.io/localhost/	1	
L	https://portal-ippe1.eniot.io/location/	1	
L	https://portal-ippe1.eniot.io/log/	1	
L	https://portal-ippe1.eniot.io/logfile/	1	

L	https://portal-ippe1.eniot.io/logfiles/	1	
L	https://portal-ippe1.eniot.io/logg/	1	
L	https://portal-ippe1.eniot.io/logger/	1	
L	https://portal-ippe1.eniot.io/logging/	1	
L	https://portal-ippe1.eniot.io/login/	1	
L	https://portal-ippe1.eniot.io/logs/	1	
L	https://portal-ippe1.eniot.io/lost%2bfound/	1	
L	https://portal-ippe1.eniot.io/lost+found/	1	
L	https://portal-ippe1.eniot.io/lpt/	1	
L	https://portal-ippe1.eniot.io/machine/	1	
L	https://portal-ippe1.eniot.io/mail/	1	
L	https://portal-ippe1.eniot.io/mail_log_files/	1	
L	https://portal-ippe1.eniot.io/mail_logs/	1	
L	https://portal-ippe1.eniot.io/mailman/	1	
L	https://portal-ippe1.eniot.io/mailroot/	1	
L	https://portal-ippe1.eniot.io/main/	1	
L	https://portal-ippe1.eniot.io/mall_log_files/	1	
L	https://portal-ippe1.eniot.io/mambo/	1	
L	https://portal-ippe1.eniot.io/man/	1	
L	https://portal-ippe1.eniot.io/manage/	1	
L	https://portal-ippe1.eniot.io/manager/	1	
L	https://portal-ippe1.eniot.io/mantis/	1	
L	https://portal-ippe1.eniot.io/manual/	1	
L	https://portal-ippe1.eniot.io/manuals/	1	
L	https://portal-ippe1.eniot.io/maps/	1	
L	https://portal-ippe1.eniot.io/market/	1	
L	https://portal-ippe1.eniot.io/marketing/	1	
L	https://portal-ippe1.eniot.io/mastergate/	1	
L	https://portal-ippe1.eniot.io/mc-icons/	1	
L	https://portal-ippe1.eniot.io/mcartfree/	1	
L	https://portal-ippe1.eniot.io/media/	1	
L	https://portal-ippe1.eniot.io/member/	1	
L	https://portal-ippe1.eniot.io/members/	1	
L	https://portal-ippe1.eniot.io/message/	1	
L	https://portal-ippe1.eniot.io/messaging/	1	
L	https://portal-ippe1.eniot.io/metacart/	1	
L	https://portal-ippe1.eniot.io/mib/	1	
L	https://portal-ippe1.eniot.io/mibs/	1	
L	https://portal-ippe1.eniot.io/microsoft-server-activesync/	1	
L	https://portal-ippe1.eniot.io/microsoft/	1	
L	https://portal-ippe1.eniot.io/midicart/	1	

L	https://portal-ippe1.eniot.io/ministats/	1	
L	https://portal-ippe1.eniot.io/misc/	1	
L	https://portal-ippe1.eniot.io/mkstats/	1	
L	https://portal-ippe1.eniot.io/modules/	1	
L	https://portal-ippe1.eniot.io/mon/	1	
L	https://portal-ippe1.eniot.io/movies/	1	
L	https://portal-ippe1.eniot.io/movimientos/	1	
L	https://portal-ippe1.eniot.io.mozilla/	1	
L	https://portal-ippe1.eniot.io/mp3/	1	
L	https://portal-ippe1.eniot.io/mp3s/	1	
L	https://portal-ippe1.eniot.io/mqseries/	1	
L	https://portal-ippe1.eniot.io/mrtg/	1	
L	https://portal-ippe1.eniot.io/ms/	1	
L	https://portal-ippe1.eniot.io/msadc/	1	
L	https://portal-ippe1.eniot.io/mspress30/	1	
L	https://portal-ippe1.eniot.io/msql/	1	
L	https://portal-ippe1.eniot.io/multimedia/	1	
L	https://portal-ippe1.eniot.io/my/	1	
L	https://portal-ippe1.eniot.io/mybb/	1	
L	https://portal-ippe1.eniot.io/mysql/	1	
L	https://portal-ippe1.eniot.io/mysql_admin/	1	
L	https://portal-ippe1.eniot.io/nada.html/	1	
L	https://portal-ippe1.eniot.io/ncadmin/	1	
L	https://portal-ippe1.eniot.io/nchelp/	1	
L	https://portal-ippe1.eniot.io/ncsample/	1	
L	https://portal-ippe1.eniot.io/net/	1	
L	https://portal-ippe1.eniot.io/netbasic/	1	
L	https://portal-ippe1.eniot.io/netbilling/	1	
L	https://portal-ippe1.eniot.io/netdetector/	1	
L	https://portal-ippe1.eniot.io/netdynamic/	1	
L	https://portal-ippe1.eniot.io/netdynamics/	1	
L	https://portal-ippe1.eniot.io/netmagstats/	1	
L	https://portal-ippe1.eniot.io/netperf/	1	
L	https://portal-ippe1.eniot.io/netpierce/	1	
L	https://portal-ippe1.eniot.io/netscape/	1	
L	https://portal-ippe1.eniot.io/netshare/	1	
L	https://portal-ippe1.eniot.io/nettracker/	1	
L	https://portal-ippe1.eniot.io/network/	1	
L	https://portal-ippe1.eniot.io/new%20folder%20(2)/	1	
L	https://portal-ippe1.eniot.io/new%20folder%20(3)/	1	
L	https://portal-ippe1.eniot.io/new%20folder/	1	

L	https://portal-ippe1.eniot.io/new/	1	
L	https://portal-ippe1.eniot.io/news/	1	
L	https://portal-ippe1.eniot.io/newsgroups/	1	
L	https://portal-ippe1.eniot.io/nextgeneration/	1	
L	https://portal-ippe1.eniot.io/nicklas/	1	
L	https://portal-ippe1.eniot.io/nl/	1	
L	https://portal-ippe1.eniot.io/noticias/	1	
L	https://portal-ippe1.eniot.io/notes/	1	
L	https://portal-ippe1.eniot.io/noticias/	1	
L	https://portal-ippe1.eniot.io/ns-icons/	1	
L	https://portal-ippe1.eniot.io/nsearch/	1	
L	https://portal-ippe1.eniot.io/nsn/	1	
L	https://portal-ippe1.eniot.io/number/	1	
L	https://portal-ippe1.eniot.io/objects/	1	
L	https://portal-ippe1.eniot.io/odbc/	1	
L	https://portal-ippe1.eniot.io/oekaki/	1	
L	https://portal-ippe1.eniot.io/of/	1	
L	https://portal-ippe1.eniot.io/officescan/	1	
L	https://portal-ippe1.eniot.io/old/	1	
L	https://portal-ippe1.eniot.io/old_files/	1	
L	https://portal-ippe1.eniot.io/oldfiles/	1	
L	https://portal-ippe1.eniot.io/online/	1	
L	https://portal-ippe1.eniot.io/oop/	1	
L	https://portal-ippe1.eniot.io/opendocman/	1	
L	https://portal-ippe1.eniot.io/opa/	1	
L	https://portal-ippe1.eniot.io/oracle/	1	
L	https://portal-ippe1.eniot.io/oradata/	1	
L	https://portal-ippe1.eniot.io/order/	1	
L	https://portal-ippe1.eniot.io/orders/	1	
L	https://portal-ippe1.eniot.io/other/	1	
L	https://portal-ippe1.eniot.io/oto/	1	
L	https://portal-ippe1.eniot.io/outgoing/	1	
L	https://portal-ippe1.eniot.io/owa/	1	
L	https://portal-ippe1.eniot.io/owls/	1	
L	https://portal-ippe1.eniot.io/owners/	1	
L	https://portal-ippe1.eniot.io/ows-bin/	1	
L	https://portal-ippe1.eniot.io/p0rn/	1	
L	https://portal-ippe1.eniot.io/pages/	1	
L	https://portal-ippe1.eniot.io/pass/	1	
L	https://portal-ippe1.eniot.io/password/	1	
L	https://portal-ippe1.eniot.io/passwords/	1	

L	https://portal-ippe1.eniot.io/patch/	1	
L	https://portal-ippe1.eniot.io/path/	1	
L	https://portal-ippe1.eniot.io/pay/	1	
L	https://portal-ippe1.eniot.io/payment/	1	
L	https://portal-ippe1.eniot.io/paymentmanager/	1	
L	https://portal-ippe1.eniot.io/payments/	1	
L	https://portal-ippe1.eniot.io/pbsdata/	1	
L	https://portal-ippe1.eniot.io/pbserver/	1	
L	https://portal-ippe1.eniot.io/pccsmysqadm/	1	
L	https://portal-ippe1.eniot.io/pdg_cart/	1	
L	https://portal-ippe1.eniot.io/pds/	1	
L	https://portal-ippe1.eniot.io/people/	1	
L	https://portal-ippe1.eniot.io/perl/	1	
L	https://portal-ippe1.eniot.io/perl5/	1	
L	https://portal-ippe1.eniot.io/personal/	1	
L	https://portal-ippe1.eniot.io/phone/	1	
L	https://portal-ippe1.eniot.io/phorum/	1	
L	https://portal-ippe1.eniot.io/photoads/	1	
L	https://portal-ippe1.eniot.io/photoalbum/	1	
L	https://portal-ippe1.eniot.io/photopost/	1	
L	https://portal-ippe1.eniot.io/photos/	1	
L	https://portal-ippe1.eniot.io/php/	1	
L	https://portal-ippe1.eniot.io/php_classes/	1	
L	https://portal-ippe1.eniot.io/phpbb/	1	
L	https://portal-ippe1.eniot.io/phpbb208/	1	
L	https://portal-ippe1.eniot.io/phpmyadmin/	1	
L	https://portal-ippe1.eniot.io/phpnuke/	1	
L	https://portal-ippe1.eniot.io/phpgadmin/	1	
L	https://portal-ippe1.eniot.io/phpprojekt/	1	
L	https://portal-ippe1.eniot.io/phpsecurepages/	1	
L	https://portal-ippe1.eniot.io/pics/	1	
L	https://portal-ippe1.eniot.io/pix/	1	
L	https://portal-ippe1.eniot.io/pl/	1	
L	https://portal-ippe1.eniot.io/plugins/	1	
L	https://portal-ippe1.eniot.io/policy/	1	
L	https://portal-ippe1.eniot.io/porn/	1	
L	https://portal-ippe1.eniot.io/porno/	1	
L	https://portal-ippe1.eniot.io/ppwb/	1	
L	https://portal-ippe1.eniot.io/ppwb/Temp/	1	
L	https://portal-ippe1.eniot.io/pr0n/	1	
L	https://portal-ippe1.eniot.io/pre/	1	

L	https://portal-ippe1.eniot.io/press/	1	█
L	https://portal-ippe1.eniot.io/printers/	1	█
L	https://portal-ippe1.eniot.io/priv/	1	█
L	https://portal-ippe1.eniot.io/privado/	1	█
L	https://portal-ippe1.eniot.io/private/	1	█
L	https://portal-ippe1.eniot.io/process/	1	█
L	https://portal-ippe1.eniot.io/prod/	1	█
L	https://portal-ippe1.eniot.io/productcart/	1	█
L	https://portal-ippe1.eniot.io/products/	1	█
L	https://portal-ippe1.eniot.io/programming/	1	█
L	https://portal-ippe1.eniot.io/programs/	1	█
L	https://portal-ippe1.eniot.io/pron/	1	█
L	https://portal-ippe1.eniot.io/protected/	1	█
L	https://portal-ippe1.eniot.io/prueba/	1	█
L	https://portal-ippe1.eniot.io/pruebas/	1	█
L	https://portal-ippe1.eniot.io/prv/	1	█
L	https://portal-ippe1.eniot.io/prxdocs/	1	█
L	https://portal-ippe1.eniot.io/psuser/	1	█
L	https://portal-ippe1.eniot.io/pub/	1	█
L	https://portal-ippe1.eniot.io/public/	1	█
L	https://portal-ippe1.eniot.io/publica/	1	█
L	https://portal-ippe1.eniot.io/publicar/	1	█
L	https://portal-ippe1.eniot.io/publico/	1	█
L	https://portal-ippe1.eniot.io/publish/	1	█
L	https://portal-ippe1.eniot.io/publisher/	1	█
L	https://portal-ippe1.eniot.io/purchase/	1	█
L	https://portal-ippe1.eniot.io/purchases/	1	█
L	https://portal-ippe1.eniot.io/pw/	1	█
L	https://portal-ippe1.eniot.io/python/	1	█
L	https://portal-ippe1.eniot.io/quickplace/	1	█
L	https://portal-ippe1.eniot.io/ramgen/	1	█
L	https://portal-ippe1.eniot.io/random_banner/	1	█
L	https://portal-ippe1.eniot.io/readme/	1	█
L	https://portal-ippe1.eniot.io/recent/	1	█
L	https://portal-ippe1.eniot.io/register/	1	█
L	https://portal-ippe1.eniot.io/registered/	1	█
L	https://portal-ippe1.eniot.io/report/	1	█
L	https://portal-ippe1.eniot.io/report_bin/rwcgi60/	1	█
L	https://portal-ippe1.eniot.io/reports/	1	█
L	https://portal-ippe1.eniot.io/repository/	1	█
L	https://portal-ippe1.eniot.io/research/	1	█

L	https://portal-ippe1.eniot.io/reseller/	1	
L	https://portal-ippe1.eniot.io/resource/	1	
L	https://portal-ippe1.eniot.io/resources/	1	
L	https://portal-ippe1.eniot.io/restricted/	1	
L	https://portal-ippe1.eniot.io/retail/	1	
L	https://portal-ippe1.eniot.io/reviews/	1	
L	https://portal-ippe1.eniot.io/rightfax/	1	
L	https://portal-ippe1.eniot.io/rksh/	1	
L	https://portal-ippe1.eniot.io/roads/	1	
L	https://portal-ippe1.eniot.io/root/	1	
L	https://portal-ippe1.eniot.io/rpc/	1	
L	https://portal-ippe1.eniot.io/sale/	1	
L	https://portal-ippe1.eniot.io/sales/	1	
L	https://portal-ippe1.eniot.io/sample/	1	
L	https://portal-ippe1.eniot.io/samples/	1	
L	https://portal-ippe1.eniot.io/samples/dbsamp/	1	
L	https://portal-ippe1.eniot.io/save/	1	
L	https://portal-ippe1.eniot.io/sbin/	1	
L	https://portal-ippe1.eniot.io/scans/	1	
L	https://portal-ippe1.eniot.io/scm/	1	
L	https://portal-ippe1.eniot.io/script/	1	
L	https://portal-ippe1.eniot.io/scripts/	1	
L	https://portal-ippe1.eniot.io/scripts/iisadmin/	1	
L	https://portal-ippe1.eniot.io/scripts/tools/	1	
L	https://portal-ippe1.eniot.io/sdk/	1	
L	https://portal-ippe1.eniot.io/search-ui/	1	
L	https://portal-ippe1.eniot.io/search/	1	
L	https://portal-ippe1.eniot.io/search97/	1	
L	https://portal-ippe1.eniot.io/secret/	1	
L	https://portal-ippe1.eniot.io/sections/	1	
L	https://portal-ippe1.eniot.io/secure/	1	
L	https://portal-ippe1.eniot.io/secured/	1	
L	https://portal-ippe1.eniot.io/sek-bin/	1	
L	https://portal-ippe1.eniot.io/selector/	1	
L	https://portal-ippe1.eniot.io/sell/	1	
L	https://portal-ippe1.eniot.io/server_stats/	1	
L	https://portal-ippe1.eniot.io/servers/	1	
L	https://portal-ippe1.eniot.io/serverstats/	1	
L	https://portal-ippe1.eniot.io/service/	1	
L	https://portal-ippe1.eniot.io/services/	1	
L	https://portal-ippe1.eniot.io/servicio/	1	

L	https://portal-ippe1.eniot.io/servicios/	1	
L	https://portal-ippe1.eniot.io/servlet/	1	
L	https://portal-ippe1.eniot.io/servlet/ssifilter/	1	
L	https://portal-ippe1.eniot.io/servlets/	1	
L	https://portal-ippe1.eniot.io/session/	1	
L	https://portal-ippe1.eniot.io/sessiondata/	1	
L	https://portal-ippe1.eniot.io/setup/	1	
L	https://portal-ippe1.eniot.io/sex/	1	
L	https://portal-ippe1.eniot.io/share/	1	
L	https://portal-ippe1.eniot.io/shell-cgi/	1	
L	https://portal-ippe1.eniot.io/shell/	1	
L	https://portal-ippe1.eniot.io/shipping/	1	
L	https://portal-ippe1.eniot.io/shop/	1	
L	https://portal-ippe1.eniot.io/shoponline/	1	
L	https://portal-ippe1.eniot.io/shopper/	1	
L	https://portal-ippe1.eniot.io/shopping_cart/	1	
L	https://portal-ippe1.eniot.io/shtml/	1	
L	https://portal-ippe1.eniot.io/signup/	1	
L	https://portal-ippe1.eniot.io/silverstream/	1	
L	https://portal-ippe1.eniot.io/site/	1	
L	https://portal-ippe1.eniot.io/site/iissamples/	1	
L	https://portal-ippe1.eniot.io/site_settings/	1	
L	https://portal-ippe1.eniot.io/siteadmin/	1	
L	https://portal-ippe1.eniot.io/siteman000510/	1	
L	https://portal-ippe1.eniot.io/sitemgr/	1	
L	https://portal-ippe1.eniot.io/siteminder/	1	
L	https://portal-ippe1.eniot.io/siteminderagent/	1	
L	https://portal-ippe1.eniot.io/siteminderagent/pw/	1	
L	https://portal-ippe1.eniot.io/sites/	1	
L	https://portal-ippe1.eniot.io/sites/samples/	1	
L	https://portal-ippe1.eniot.io/siteserver/	1	
L	https://portal-ippe1.eniot.io/sitestats/	1	
L	https://portal-ippe1.eniot.io/siteupdate/	1	
L	https://portal-ippe1.eniot.io/smallco/	1	
L	https://portal-ippe1.eniot.io/smreports/	1	
L	https://portal-ippe1.eniot.io/smreports/	1	
L	https://portal-ippe1.eniot.io/smreportsviewer/	1	
L	https://portal-ippe1.eniot.io/snmp/	1	
L	https://portal-ippe1.eniot.io/snort/	1	
L	https://portal-ippe1.eniot.io/soap/	1	
L	https://portal-ippe1.eniot.io/soapdocs/	1	

L	https://portal-ippe1.eniot.io/software/	1	
L	https://portal-ippe1.eniot.io/solaris/	1	
L	https://portal-ippe1.eniot.io/solution/	1	
L	https://portal-ippe1.eniot.io/solutions/	1	
L	https://portal-ippe1.eniot.io/sounds/	1	
L	https://portal-ippe1.eniot.io/source/	1	
L	https://portal-ippe1.eniot.io/sources/	1	
L	https://portal-ippe1.eniot.io/spool/	1	
L	https://portal-ippe1.eniot.io/sproot/	1	
L	https://portal-ippe1.eniot.io/sql/	1	
L	https://portal-ippe1.eniot.io/squid/	1	
L	https://portal-ippe1.eniot.io/src/	1	
L	https://portal-ippe1.eniot.io/srchadm/	1	
L	https://portal-ippe1.eniot.io/srcview/	1	
L	https://portal-ippe1.eniot.io/ssi/	1	
L	https://portal-ippe1.eniot.io/ssl/	1	
L	https://portal-ippe1.eniot.io/sslkeys/	1	
L	https://portal-ippe1.eniot.io/staff/	1	
L	https://portal-ippe1.eniot.io/staging/	1	
L	https://portal-ippe1.eniot.io/stat/	1	
L	https://portal-ippe1.eniot.io/static/	1	
L	https://portal-ippe1.eniot.io/statistic/	1	
L	https://portal-ippe1.eniot.io/statistics/	1	
L	https://portal-ippe1.eniot.io/stats-bin-p/	1	
L	https://portal-ippe1.eniot.io/stats-bin-p/reports/	1	
L	https://portal-ippe1.eniot.io/stats/	1	
L	https://portal-ippe1.eniot.io/stats_old/	1	
L	https://portal-ippe1.eniot.io/status/	1	
L	https://portal-ippe1.eniot.io/storage/	1	
L	https://portal-ippe1.eniot.io/store/	1	
L	https://portal-ippe1.eniot.io/storedb/	1	
L	https://portal-ippe1.eniot.io/storemgr/	1	
L	https://portal-ippe1.eniot.io/strategy/	1	
L	https://portal-ippe1.eniot.io/string/	1	
L	https://portal-ippe1.eniot.io/stuff/	1	
L	https://portal-ippe1.eniot.io/style/	1	
L	https://portal-ippe1.eniot.io/styles/	1	
L	https://portal-ippe1.eniot.io/stylesheet/	1	
L	https://portal-ippe1.eniot.io/stylesheets/	1	
L	https://portal-ippe1.eniot.io subdir/	1	
L	https://portal-ippe1.eniot.io subir/	1	

L	https://portal-ippe1.eniot.io/sun/	1	
L	https://portal-ippe1.eniot.io/sup/	1	
L	https://portal-ippe1.eniot.io/super_stats/	1	
L	https://portal-ippe1.eniot.io/support/	1	
L	https://portal-ippe1.eniot.io/surf/	1	
L	https://portal-ippe1.eniot.io/survey/	1	
L	https://portal-ippe1.eniot.io/sys/	1	
L	https://portal-ippe1.eniot.io/sysadmin/	1	
L	https://portal-ippe1.eniot.io/sysbackup/	1	
L	https://portal-ippe1.eniot.io/system/	1	
L	https://portal-ippe1.eniot.io/tar/	1	
L	https://portal-ippe1.eniot.io/tarjetas/	1	
L	https://portal-ippe1.eniot.io/tasks/	1	
L	https://portal-ippe1.eniot.io/te_html/	1	
L	https://portal-ippe1.eniot.io/technote/	1	
L	https://portal-ippe1.eniot.io/temp/	1	
L	https://portal-ippe1.eniot.io/template/	1	
L	https://portal-ippe1.eniot.io/templates/	1	
L	https://portal-ippe1.eniot.io/temporal/	1	
L	https://portal-ippe1.eniot.io/test-cgi/	1	
L	https://portal-ippe1.eniot.io/test/	1	
L	https://portal-ippe1.eniot.io/testdir/	1	
L	https://portal-ippe1.eniot.io/testing/	1	
L	https://portal-ippe1.eniot.io/tests/	1	
L	https://portal-ippe1.eniot.io/testweb/	1	
L	https://portal-ippe1.eniot.io/text/	1	
L	https://portal-ippe1.eniot.io/themes/	1	
L	https://portal-ippe1.eniot.io/ticket/	1	
L	https://portal-ippe1.eniot.io/tickets/	1	
L	https://portal-ippe1.eniot.io/tmp/	1	
L	https://portal-ippe1.eniot.io/tmplogs/	1	
L	https://portal-ippe1.eniot.io/todo/	1	
L	https://portal-ippe1.eniot.io/tomcat-docs/	1	
L	https://portal-ippe1.eniot.io/tools/	1	
L	https://portal-ippe1.eniot.io/top_list_/_	1	
L	https://portal-ippe1.eniot.io/tpv/	1	
L	https://portal-ippe1.eniot.io/trabajo/	1	
L	https://portal-ippe1.eniot.io/tradetheme/	1	
L	https://portal-ippe1.eniot.io/trafficlog/	1	
L	https://portal-ippe1.eniot.io/training/	1	
L	https://portal-ippe1.eniot.io/transactional/	1	

L	https://portal-ippe1.eniot.io/transito/	1	
L	https://portal-ippe1.eniot.io/transpolar/	1	
L	https://portal-ippe1.eniot.io/tree/	1	
L	https://portal-ippe1.eniot.io/trees/	1	
L	https://portal-ippe1.eniot.io/tsweb/	1	
L	https://portal-ippe1.eniot.io/ttweb/	1	
L	https://portal-ippe1.eniot.io/turba/	1	
L	https://portal-ippe1.eniot.io/tutorial/	1	
L	https://portal-ippe1.eniot.io/tutos/	1	
L	https://portal-ippe1.eniot.io/tuxedo/	1	
L	https://portal-ippe1.eniot.io/uddi/uddilistusersservlet/	1	
L	https://portal-ippe1.eniot.io/update/	1	
L	https://portal-ippe1.eniot.io/updated/	1	
L	https://portal-ippe1.eniot.io/updates/	1	
L	https://portal-ippe1.eniot.io/upload/	1	
L	https://portal-ippe1.eniot.io/uploads/	1	
L	https://portal-ippe1.eniot.io/urlresult/	1	
L	https://portal-ippe1.eniot.io/us/	1	
L	https://portal-ippe1.eniot.io/usage/	1	
L	https://portal-ippe1.eniot.io/user/	1	
L	https://portal-ippe1.eniot.io/userdb/	1	
L	https://portal-ippe1.eniot.io/userlog/	1	
L	https://portal-ippe1.eniot.io/users/	1	
L	https://portal-ippe1.eniot.io/usr/	1	
L	https://portal-ippe1.eniot.io/ustats/	1	
L	https://portal-ippe1.eniot.io/usuario/	1	
L	https://portal-ippe1.eniot.io/usuarios/	1	
L	https://portal-ippe1.eniot.io/util/	1	
L	https://portal-ippe1.eniot.io/utils/	1	
L	https://portal-ippe1.eniot.io/vfs/	1	
L	https://portal-ippe1.eniot.io/vignette/	1	
L	https://portal-ippe1.eniot.io/w3perl/	1	
L	https://portal-ippe1.eniot.io/w3perl/admin/	1	
L	https://portal-ippe1.eniot.io/w3svc101/	1	
L	https://portal-ippe1.eniot.io/warez/	1	
L	https://portal-ippe1.eniot.io/way-board/	1	
L	https://portal-ippe1.eniot.io/wconnect/	1	
L	https://portal-ippe1.eniot.io/web/	1	
L	https://portal-ippe1.eniot.io/web800fo/	1	
L	https://portal-ippe1.eniot.io/web_store/	1	
L	https://portal-ippe1.eniot.io/web_usage/	1	

L	https://portal-ippe1.eniot.io/webaccess/	1	
L	https://portal-ippe1.eniot.io/webadmin/	1	
L	https://portal-ippe1.eniot.io/webagent/	1	
L	https://portal-ippe1.eniot.io/webalizer/	1	
L	https://portal-ippe1.eniot.io/webapplication1/	1	
L	https://portal-ippe1.eniot.io/webapplication2/	1	
L	https://portal-ippe1.eniot.io/webapps/	1	
L	https://portal-ippe1.eniot.io/webbank/	1	
L	https://portal-ippe1.eniot.io/webboard/	1	
L	https://portal-ippe1.eniot.io/webcart-lite/	1	
L	https://portal-ippe1.eniot.io/webcart/	1	
L	https://portal-ippe1.eniot.io/webcash/	1	
L	https://portal-ippe1.eniot.io/webdata/	1	
L	https://portal-ippe1.eniot.io/webdb/	1	
L	https://portal-ippe1.eniot.io/webdev/	1	
L	https://portal-ippe1.eniot.io/weblog/	1	
L	https://portal-ippe1.eniot.io/weblogs/	1	
L	https://portal-ippe1.eniot.io/webmail/	1	
L	https://portal-ippe1.eniot.io/webmaster/	1	
L	https://portal-ippe1.eniot.io/webmaster_logs/	1	
L	https://portal-ippe1.eniot.io/webnews/	1	
L	https://portal-ippe1.eniot.io/webobjects/	1	
L	https://portal-ippe1.eniot.io/webpub-ui/	1	
L	https://portal-ippe1.eniot.io/webpub/	1	
L	https://portal-ippe1.eniot.io/webreports/	1	
L	https://portal-ippe1.eniot.io/webreps/	1	
L	https://portal-ippe1.eniot.io/webservice/	1	
L	https://portal-ippe1.eniot.io/webshare/	1	
L	https://portal-ippe1.eniot.io/webshop/	1	
L	https://portal-ippe1.eniot.io/website/	1	
L	https://portal-ippe1.eniot.io/webspheresamples/	1	
L	https://portal-ippe1.eniot.io/websql/	1	
L	https://portal-ippe1.eniot.io/webstat/	1	
L	https://portal-ippe1.eniot.io/webstats/	1	
L	https://portal-ippe1.eniot.io/webtrace/	1	
L	https://portal-ippe1.eniot.io/webtrend/	1	
L	https://portal-ippe1.eniot.io/webtrends/	1	
L	https://portal-ippe1.eniot.io/whatsnew/	1	
L	https://portal-ippe1.eniot.io/wikihome/	1	
L	https://portal-ippe1.eniot.io/windows/	1	
L	https://portal-ippe1.eniot.io/word/	1	

L	https://portal-ippe1.eniot.io/wordpress/	1	
L	https://portal-ippe1.eniot.io/work/	1	
L	https://portal-ippe1.eniot.io/working/	1	
L	https://portal-ippe1.eniot.io/wsdl/	1	
L	https://portal-ippe1.eniot.io/wsdocs/	1	
L	https://portal-ippe1.eniot.io/wssamples/	1	
L	https://portal-ippe1.eniot.io/wstats/	1	
L	https://portal-ippe1.eniot.io/wusage/	1	
L	https://portal-ippe1.eniot.io/wwthreads/	1	
L	https://portal-ippe1.eniot.io/www-sql/	1	
L	https://portal-ippe1.eniot.io/www/	1	
L	https://portal-ippe1.eniot.io/wwwjoin/	1	
L	https://portal-ippe1.eniot.io/wwwlog/	1	
L	https://portal-ippe1.eniot.io/wwwroot/	1	
L	https://portal-ippe1.eniot.io/wwwstat/	1	
L	https://portal-ippe1.eniot.io/wwwstats/	1	
L	https://portal-ippe1.eniot.io/wx/	1	
L	https://portal-ippe1.eniot.io/xdk/	1	
L	https://portal-ippe1.eniot.io/xml/	1	
L	https://portal-ippe1.eniot.io/xss/	1	
L	https://portal-ippe1.eniot.io/xtemp/	1	
L	https://portal-ippe1.eniot.io/yabbse/	1	
L	https://portal-ippe1.eniot.io/zentrack/	1	
L	https://portal-ippe1.eniot.io/zip/	1	
L	https://portal-ippe1.eniot.io/zipfiles/	1	
L	https://portal-ippe1.eniot.io/zipped/	1	
L	https://portal-ippe1.eniot.io/zips/	1	
L	https://portal-ippe1.eniot.io/zos/	1	
L	https://portal-ippe1.eniot.io/~admin/	1	
L	https://portal-ippe1.eniot.io/~bin/	1	
L	https://portal-ippe1.eniot.io/~dev/	1	
L	https://portal-ippe1.eniot.io/~etc/	1	
L	https://portal-ippe1.eniot.io/~ftp/	1	
L	https://portal-ippe1.eniot.io/~guest/	1	
L	https://portal-ippe1.eniot.io/~home/	1	
L	https://portal-ippe1.eniot.io/~log/	1	
L	https://portal-ippe1.eniot.io/~mnt/	1	
L	https://portal-ippe1.eniot.io/~nobody/	1	
L	https://portal-ippe1.eniot.io/~nobody/etc/	1	
L	https://portal-ippe1.eniot.io/~root/	1	
L	https://portal-ippe1.eniot.io/~sbin/	1	

L	https://portal-ippe1.eniot.io/~stats/	1	
L	https://portal-ippe1.eniot.io/~tmp/	1	
L	https://portal-ippe1.eniot.io/~usr/	1	
L	https://portal-ippe1.eniot.io/~uucp/	1	
L	https://portal-ippe1.eniot.io/~var/	1	
L	https://portal-ippe1.eniot.io/~webstats/	1	
L	https://portal-ippe1.eniot.io/~wsdocs/	1	
L	https://portal-ippe1.eniot.io/devportal/login.html	4	
L	https://portal-ippe1.eniot.io/portal/	4	
I	https://portal-ippe1.eniot.io/devportal/res/common/index_445fadca.js	2	
I	https://portal-ippe1.eniot.io/portal-api/res/apimanagement/index_f20f1232.js	3	
I	https://portal-ippe1.eniot.io/portal-data/res/commons/index_16eaf087.js	3	
I	https://portal-ippe1.eniot.io/portal-dm/res/commons/index_67ac1ffc.js	3	
I	https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js	8	
I	https://portal-ippe1.eniot.io/portal/res/commons/index_6b2dae79.js	4	
I	https://portal-ippe1.eniot.io/saturnweb/res/index/index.57829111.bundle.js	2	
I	https://portal-ippe1.eniot.io/devportal/res/home/index_57c2c951.js	1	
I	https://portal-ippe1.eniot.io/devportal/res/index/index_6ef3d11b.js	2	
I	https://portal-ippe1.eniot.io/devportal/res/login/index_df108705.js	2	
I	https://portal-ippe1.eniot.io/iam/api/v3/login	1	
I	https://portal-ippe1.eniot.io/portal/res/homepage/index_09e65fab.js	1	
I	https://portal-ippe1.eniot.io/dataide/0.39453f26.chunk.js	1	
I	https://portal-ippe1.eniot.io/dataide/bundle.8d1d5153eebcba2626de.js	1	
I	https://portal-ippe1.eniot.io/devportal/res/sdk_download/index_60ae01311.js	1	
I	https://portal-ippe1.eniot.io/portal-api/res/vendor/index_183eb259.js	1	
I	https://portal-ippe1.eniot.io/portal-data/res/modeldeployment/index_2c95a1f5.js	1	

Fix Recommendations 22

TOC

Remediation Task	Number of Issues
M Add the 'Secure' attribute to all sensitive cookies	5
M Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form	50 
L Always use SSL and POST (body) parameters when sending sensitive information.	52 

L	Change server's supported ciphersuites	1
L	Config your server to use the "Content-Security-Policy" header with secure policies	5
L	Config your server to use the "X-Content-Type-Options" header with "nosniff" value	5
L	Config your server to use the "X-Frame-Options" header with DENY or SAMEORIGIN value	5
L	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)	5
L	Do not keep sensitive information in easy to guess file names, or restrict access to them	6
L	Download the relevant security patch for your web server or web application.	13
L	Examine the link to determine whether it is indeed supposed to be included in the web application	4
L	Implement the HTTP Strict-Transport-Security policy with a long "max-age"	5
L	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely	1190
L	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	39
L	Remove business and security logic from the client side	7
L	Remove e-mail addresses from the website	14
L	Remove internal IP addresses from your website	3
L	Remove old versions of files from the virtual directory	40
L	Remove or restrict access to the compressed directory file	140
L	Remove test scripts from the server	28
L	Turn off tracing, restrict access to the log file, or remove it.	20
L	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	16

Security Risks 12

TOC

Risk	Number of Issues
M	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
M	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
L	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

L	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords	140	<div style="width: 100%;"><div style="width: 10%;">10%</div></div>
L	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site	1190	<div style="width: 100%;"><div style="width: 100%;">100%</div></div>
L	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	25	<div style="width: 100%;"><div style="width: 5%;">5%</div></div>
L	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted	52	<div style="width: 100%;"><div style="width: 10%;">10%</div></div>
I	It is possible to gather sensitive debugging information	16	<div style="width: 100%;"><div style="width: 2%;">2%</div></div>
I	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side	7	<div style="width: 100%;"><div style="width: 1%;">1%</div></div>
I	N/A	4	<div style="width: 100%;"><div style="width: 1%;">1%</div></div>
I	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application	13	<div style="width: 100%;"><div style="width: 1%;">1%</div></div>

Causes 12

TOC

Cause	Number of Issues	
M	Insufficient authentication method was used by the application	50 <div style="width: 100%;"><div style="width: 10%;">10%</div></div>
M	The web application sends non-secure cookies over SSL	5 <div style="width: 100%;"><div style="width: 1%;">1%</div></div>
L	Temporary files were left in production environment	68 <div style="width: 100%;"><div style="width: 10%;">10%</div></div>
L	Sensitive information might have been cached by your browser	39 <div style="width: 100%;"><div style="width: 5%;">5%</div></div>
L	Insecure web application programming or configuration	188 <div style="width: 100%;"><div style="width: 15%;">15%</div></div>
L	The web server or application server are configured in an insecure way	1211 <div style="width: 100%;"><div style="width: 100%;">100%</div></div>
L	Query parameters were passed over SSL, and may contain sensitive information	52 <div style="width: 100%;"><div style="width: 10%;">10%</div></div>
I	Proper bounds checking were not performed on incoming parameter values	16 <div style="width: 100%;"><div style="width: 2%;">2%</div></div>
I	No validation was done in order to make sure that user input matches the data type expected	16 <div style="width: 100%;"><div style="width: 2%;">2%</div></div>
I	Cookies are created at the client side	7 <div style="width: 100%;"><div style="width: 1%;">1%</div></div>
I	N/A	4 <div style="width: 100%;"><div style="width: 1%;">1%</div></div>
I	Latest patches or hotfixes for 3rd. party products were not installed	13 <div style="width: 100%;"><div style="width: 1%;">1%</div></div>

WASC Threat Classification

TOC

Threat	Number of Issues	
--------	------------------	--

Cross-site Request Forgery	50	
Information Leakage	1523	
Integer Overflows	7	
Malicious Content Tests	4	
Predictable Resource Location	68	
Server Misconfiguration	1	

Issues Sorted by Issue Type

M

Cross-Site Request Forgery 50

TOC

Issue 1 of 50

TOC

Cross-Site Request Forgery

Severity: Medium

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/search>

Entity: search (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 2 of 50

TOC

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/user/authorization/check>

Entity: check (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 3 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/devportal/home.html>

Entity: home.html (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 4 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices>

Entity: queryMockDevices (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 5 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/audit/duration>

Entity: duration (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 6 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-web/config/docurl>

Entity: docurl (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 7 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getsdks>

Entity: getsdks (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 8 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: list (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 9 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/ldapSource/validateLinkName>

Entity: validateLinkName (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 10 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/appInstance/list>

Entity: list (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 11 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/organization/info>

Entity: info (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 12 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-web/resmgnt/list/ou/service>

Entity: service (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 13 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/ide/datasource/pagingInfo>

Entity: pagingInfo (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 14 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/saturn/batch/ws/v1/cluster/apps>

Entity: apps (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 15 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/ide/datasource/query>

Entity: query (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 16 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/user/list>

Entity: list (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 17 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-web/dataex/list>

Entity: list (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 18 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/organization/transfer/info>

Entity: info (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 19 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-web/config/help>

Entity: help (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 20 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getoldmenus>

Entity: getoldmenus (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 21 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/policy/list>

Entity: list (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 22 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/queryTSLModelSummaryByOU>

Entity: queryTSLModelSummaryByOU (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 23 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam/api/v2/authorization/listBySubject>

Entity: listBySubject (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 24 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/organization/resource/list>

Entity: list (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 25 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-data/modeldeployment.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 26 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-dm/logicasset.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 27 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-dm/overview.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 28 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-dm/simulator.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 29 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-iam/usermanagement.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 30 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-iam/adduser.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 31 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-api/apimanagement.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 32 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/dataide/index.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 33 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: https://portal-ippe1.eniot.io/devportal/sdk_download.html

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 34 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/saturnweb/>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 35 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-iam/addLdapService.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 36 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info>

Entity: info (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 37 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/apim/agroup>

Entity: agroup (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 38 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-dm/tslmodel.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 39 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-iam/addpolicy.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 40 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-dm/integration.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 41 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-dm/firmware.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 42 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-iam/orginfo.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 43 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-data/storagepolicy.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 44 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal-iam/actionTrail.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 45 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/portal/enosapidoc.html>

Entity: __ts__ (Parameter)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a manipulated CSRF-token.

Issue 46 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/logout>

Entity: logout (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 47 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/security/mfa/status>

Entity: status (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 48 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/session/get>

Entity: get (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 49 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam-web/session/set>

Entity: set (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Issue 50 of 50

[TOC](#)

Cross-Site Request Forgery

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll>

Entity: queryProductListAll (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: Insufficient authentication method was used by the application

Fix: Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

M

Missing Secure Attribute in Encrypted Session (SSL) Cookie 5

TOC

Issue 1 of 5

TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/>

Entity: 837cbf2c4037d0ea9e37c5df2937b9c2 (Cookie)

Risk: It may be possible to steal user and session information (cookies) that was sent during an encrypted session

Causes: The web application sends non-secure cookies over SSL

Fix: Add the 'Secure' attribute to all sensitive cookies

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Original Response

```
HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Accept-Ranges: bytes
```

```

Content-Length: 462
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: "5e02ecff-1ce"
Set-Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:03:01 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>EnOS</title>
    <script type="text/javascript" src="/navigator/config/getloginstyle?"></script>
...

```

Issue 2 of 5

TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Severity: Medium

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/navigator/config/getloginstyle>

Entity: 54e50ebe879a92d35e3acc94c2ba7606 (Cookie)

Risk: It may be possible to steal user and session information (cookies) that was sent during an encrypted session

Causes: The web application sends non-secure cookies over SSL

Fix: Add the 'Secure' attribute to all sensitive cookies

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Original Response

```

...
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 0
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: loginStyle=enos; Max-Age=2592000; Expires=Thu, 28-May-2020 03:27:10 GMT; Path=/
Set-Cookie: 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; path=/; HttpOnly
Date: Tue, 28 Apr 2020 03:27:10 GMT
...

```

Issue 3 of 5

TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Severity:	Medium
CVSS Score:	6.4
URL:	https://portal-ippe1.eniot.io/navigator/config/getloginstyle
Entity:	loginStyle (Cookie)
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Original Response

```
...
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 0
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: loginStyle=enos; Max-Age=2592000; Expires=Thu, 28-May-2020 03:27:10 GMT; Path=/
Set-Cookie: 54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; path=/; HttpOnly
Date: Tue, 28 Apr 2020 03:27:10 GMT
...
...
```

Issue 4 of 5

TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Severity:	Medium
CVSS Score:	6.4
URL:	https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info
Entity:	42dea464b09cd2371e151241b10bd05b (Cookie)
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Original Response

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4eba1; path=/; HttpOnly
Date: Tue, 28 Apr 2020 03:27:11 GMT
Content-Type: application/json; charset=UTF-8

{
  "status": 404,
  "message": "securitySetting.not.exist",
  "data": null,
  "success": false,
  "fail": true
}
```

Issue 5 of 5

TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Severity: **Medium**

CVSS Score: 6.4

URL: <https://portal-ippe1.eniot.io/iam/api/v2/session/get>

Entity: 48a7cc09a4a7ce6e3cb4774f8375cca6 (Cookie)

Risk: It may be possible to steal user and session information (cookies) that was sent during an encrypted session

Causes: The web application sends non-secure cookies over SSL

Fix: Add the 'Secure' attribute to all sensitive cookies

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Original Response

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
```

```
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 48a7cc09a4a7ce6e3cb4774f8375cca6=19100327c0969385538ec45876d7af38; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:56:58 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "message": "User login session expired",
  "fail": true,
  "failed": true,
  "success": false,
  "successful": false
}

...
```

Issue 1 of 20

TOC

Archive File Download

Severity: Low**CVSS Score:** 5.0**URL:** <https://portal-ippe1.eniot.io/navigator/navigator/getoldmenus>**Entity:** getoldmenus (Page)**Risk:** It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords**Causes:** Temporary files were left in production environment**Fix:** Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Referer: https://portal-ippe1.eniot.io/
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; loginStyle=enos
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Accept: /*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: application/json; charset=UTF-8

{
  "code": 30000,
  "msg": "",
  "data": null
}
...
```

Issue 2 of 20

TOC

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info>

Entity: info (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Referer: https://portal-ippe1.eniot.io/
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50be879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; loginStyle=enos
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Accept: */
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 52
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4eba1; path=/; HttpOnly
Date: Tue, 28 Apr 2020 05:53:05 GMT
Content-Type: application/json

{
  "status": 51,
  "message": "User login session expired"
}
...
```

Issue 3 of 20

TOC

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/iam-web/v1/encrypt/publicKey
Entity:	publicKey (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Accept: /*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 52
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:32 GMT
Content-Type: application/json

{
  "status": 51,
  "message": "User login session expired"
}
...
```

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/session/set>

Entity: set (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
AM_S_RKH5UeYn6zUEwYXzTcCDawBjpnjdyctjq6G86PU8HyC9VqYy5ptJpxQQphpsxkayV2BkTuEkhUEqQjw6GmwTgEpqKaCt
VcCgWLVZTJxh9scr7YkesegFdJCJBE4NXU7U;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Origin: https://portal-ippe1.eniot.io
Accept: */*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "fail": true,
  "success": false
}
...
```

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/model/getSystemOU
Entity:	getSystemOU (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /dm-bff/rest/model/getSystemOU.arc HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/tslmodel.html?__ts__=1587876208642&&
Cookie: lang=en-US; locale=en-US;
837cbf2c4037de0a9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
8142657bb99ce5d47beb6ebda5671b=7249efda1c32d9b86f368cf91fd8b7de;
global_id=IAM_S_wcUH9dpScRgLYbzhG2qFst9uzW9FZ3CADv5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMLy
YWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSAgzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616
...
...
```

Issue 6 of 20

TOC

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/model/queryTSLModelSummaryByOU
Entity:	queryTSLModelSummaryByOU (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /dm-bff/rest/model/queryTSLModelSummaryByOU.arc HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/tslmodel.html?__ts__=1587876208642&&
Cookie: lang=en-US; locale=en-US;
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
8142657bb9ce5d47beb6ebdbabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
global_id=IAM_S_wcUH9dpScURgLYbzhG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMjj9DddBfhksUqcSpZwL3dmSaHc4EMLy
YWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616
...
...
```

Issue 7 of 20

TOC

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/user/authorization/check>

Entity: check (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9
...
...
```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json; charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "fail": true,
  "success": false
}
...

```

Issue 8 of 20

TOC

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll>

Entity: queryProductListAll (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
GET /dm-bff/rest/product/queryProductListAll.arc?currentPage=1&pageSize=200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876212059&&
Cookie: lang=en-US; locale=en-US; JSESSIONID=1775EDCDD10CCB2EF1691AAA917B2F6B;
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
203d16c4c34b4d37cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
8142657bb9ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
global_id=IAM_S_wCUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMLY
YWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io

```

```

eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616
...

```

Issue 9 of 20

[TOC](#)

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics>

Entity: queryStatistics (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
GET /dm-bff/overview/queryStatistics.arc?productKey=all&now=1588053509168&zero=1587798000000
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?_ts_=1587876212059&&
Cookie: lang=en-US; locale=en-US; JSESSIONID=1775EDCDD10CCB2EF1691AAA917B2F6B;
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdf61f683ce3be3d9cd9e;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
global_id=IAM_S_wcUH9dpScURgLYbzrhG2qFst9uzW9FZ3CADv5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMLy
YWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEVsGaDsmgDGg3;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616
...

```

Issue 10 of 20

[TOC](#)

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues
Entity:	getMetricValues (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /dm-bff/overview/getMetricValues.arc?productKey=all&timePeriod=hour&currentTs=1588053509168
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876212059&&
Cookie: lang=en-US; locale=en-US; JSESSIONID=1775EDCD10CCB2F1691AAA917B2F6B;
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b98443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
global_id=IAM_S_wcUH9dpScURgLYbzhG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMjj9DddBfhksUqcSpZwL3dmSaHc4EMLy
YWgnjqaXAgzLqW8hw8jTmU6dEaq0bPsazTEvsGaDsmgDGg3;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616
...
...
```

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/logicasset/search
Entity:	search (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /dm-bff/logicasset/search.ARC?pageNo=1&pageSize=10&expression= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/logicasset.html?__ts__=1587876217997&&
Cookie: __ga=GA1.2.610865653.1587876213; __gat_gtag_UA_110195466_1=1; locale=en-US; lang=en-US;
__gid=GA1.2.1711793339.1587876213; __gat_gtag_UA_110195466_2=1;
JSESSIONID=1775EDCDD10CCB2EF1691AAA917B2F6B;
global_id=IAM_S_wcUH9dpScURgLYbzhG2qFst9uzWFZ3CADv5AfAucCynec9DnMjJ9DddBfhksUqcSpZwL3dmSaHc4EMLy
YWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3;
8142657bb9ce5d47beb6ebab5671b=7249efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
54e50be879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
837cbf2c4037de9e37c5df2937b9c2=a7251de0c2fdf61f683ce3be3d9cd9e; loginStyle=enos;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices
Entity:	queryMockDevices (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /dm-bff/simulator/queryMockDevices.arc HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/simulator.html?__ts__=1587876219549&&
Cookie: __gat_gtag_UA_110195466_1=1; __gid=GA1.2.1711793339.1587876213;
         __ga=GA1.2.610865653.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; lang=en-US;
JSESSIONID=1775EDCDD10CCB2EF1691AAA917B2F6B;
global_id=IAM_S_wcUH9dpScURgLYbzhG2qFst9uzWFZ3CADv5AfAucCynec9DnMjJ9DddBfhksUqcSpZwL3dmSaHc4EMLy
YWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3;
8142657bb9ce5d47beb6ebab5671b=7249efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
837cbf2c4037de9e37c5df2937b9c2=a7251de0c2fdf61f683ce3be3d9cd9e; loginStyle=enos;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/inte/queryChannels
Entity:	queryChannels (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /dm-bff/inte/queryChannels.arc HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/integration.html?__ts__=1587876220608&&
Cookie: _gid=GA1.2.1711793339.1587876213; _ga=GA1.2.610865653.1587876213; lang=en-US; locale=en-US; _gat_gtag_UA_110195466_1=1; _gat_gtag_UA_110195466_2=1;
JSESSIONID=1775EDCDD10CCB2EF1691AAA917B2F6B;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
8142657bb99ce5d47beb6ebda5671b=7249fdalc32d9b86f368cf91fd8b7de;
global_id=IAM_S_wcUH9dpScURgLYbzhG2qFst9uzW9FZ3CADV5AfAucCynec9DnMJJj9DddBfhksUqcSpzwL3dmSaHc4EMLy
YWgnjqaXAgzLqW8hw8jTmU6dEaqQbPsazTEvsGaDsmgDGg3;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/audit/search
Entity:	search (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /audit/search.arc?
offset=0&limit=10&startTime=1587449509611&endTime=1588054309611&query=%7B%22userName%22%3A%22%22%
7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1;
__ga=GA1.2.610865653.1587876213; __gat_gtag_UA_110195466_1=1;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
8142657bb9ce5d47beb6ebabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
global_id=IAM_S_CEZJQVH3zteSzxXyheDkT6MmRBYxdYmjX5PPQaSaeEPTQewSqnPBygSWDXmu5hbxRgBEU4mhT72ey5Luc
SkDzSEwLzmJsuFNgWYJR8QUMB8RM64WV4t8E5bPkTNZQSfr;
0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500; loginStyle=enos
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Archive File Download

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/user/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json; charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "success": false,
  "fail": true
}
...
```

Archive File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/enos-app-webservice/app/list
Entity:	list (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
GET /enos-app-webservice/app/list.arc HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: _gat_gtag_UA_110195466_1=1; _ga=GA1.2.61086563.1587876213; lang=en-US;
_gid=GA1.2.1711793339.1587876213; locale=en-US; _gat_gtag_UA_110195466_2=1;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
0b68a657f24d12cce48ed4247bcc86d0=352d6229764949a7eae62da3419c0f1c4;
33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f;
4bff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fd8f;
global_id=IAM_S_CEZJQVH3zteSzxXyheDkT6MmRBYXdYmjX5PPQaSaeEPTQewSqnPBygSWDXmu5hbxRgBEU4mhT72ey5Luc
SkDz8EWL2mJsuFnqWYJR8QUMB8RM64WV4t8E5bPkTNZQSfr;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4eba1; loginStyle=enos;
061609d44b398ee03ad76311f6534dd7=580ff856a53d3823b619922623f730d5;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
JSESSIONID=A5B04F75F3ACBC3EAE224BF0FE530969;
e9dc754e254cef59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
48a7cc09ada7ce6e3cb4774f8375cca6=8368
...
```

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/policy/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
GET /iam-web/policy/list.arc HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/serviceaccount.html?__ts__=1587876399694&&
Cookie: lang=en-US; locale=en-US; __ga=GA1.2.610865653.1587876213;
_gid=GA1.2.1711793339.1587876213; JSESSIONID=8DAB31BE074803E24AF4DCD7F918FB4B;
d1d736358848df1792c8a926c47ba864=699d293f17bdc607d65f688e3d8d7cecc;
50ea23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4;
33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f;
4bff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf;
global_id=IAM_S_CE2ZJQVH3ztesZxxYhebKT6MmRBYXdymjX5PPQaSaeEPTQewSqnpyBygSWDXmu5hbxRgBEU4mhT72ey5Luc
SkDzsEwLZmJsuFNqWYJR8QUMb8RM64WV4t8E5bPkTNZQSfr;
8142657bb99ce5d47beb6ebda5671b=7249efdal1c32d9886f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal; loginStyle=enos;
9dc22c3867b96443dd332ac8e31ba30=0a1fcfa09465bf34beeedacee49efaa9;
JSESSIONID=A5B04F75F3ACBC3EAE224BF0FE530969;
e9dc754e254cfe59b74a9c413b3c49a=c856bc06c5587b4275472696a7fe613;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
149118e82bd3db1f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
e6c982c2af8fea3b4dddd995510bccce=3c55dd8c6c72bbec3a8d6c3dc7c40e;
7d1ffbf2f004d3ac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
061609d44b398ee03ad76311f6534dd7=580ff56a53d3823b619922623f730d5;
4cbbec795fb26b13bb45b228a8153ff=5b06b0f4b34a370e60d6ba4458d079a7;
48a7cc09a4a7ce6e3cb4774f83375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fwwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json;charset=UTF-8
{
```

```
        "status": 500,
        "message": "system error",
        "data": null,
        "success": false,
        "fail": true
    }
```

Issue 18 of 20

TOC

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/appInstance/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json; charset=UTF-8

{
    "status": 500,
    "message": "system error",
    "data": null,
    "success": false,
    "fail": true
}
...
```

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/resource/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

GET /iam-web/organization/resource/list.arc HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/addpolicy.html?
__ts__=1587876415042&isEdit=false&id=o15790616298731&uId=u15877199768991&
Cookie: __gid=GA1.2.1711793339.1587876213; __ga=GA1.2.610865653.1587876213; locale=en-US; lang=en-US; __gat_gtag_UA_110195466_1=1; __gat_gtag_UA_110195466_2=1;
JSESSIONID=8DAB31BE074803E24AF4CD7F918FB4B;
e9dc754e254cfe9b74a9c4131b3c49a=c856bc06c5587b4275472696a7fe613;
33296aa8a77f7e6d9209cc1b282bf5c=29583daf49f8c47f70937b3e6464d67f;
061609d44b398ee03ad76311f6534dd7=580ffb56a53d3823b619922623f730d5;
4ccbfb795bf26b13bb45b228a8153ff=5b06b0f4b34a370e60d6ba4458d079a7;
48a7cc09a4a7ce63cb4774f8375cca6=836861ced028279968e30876217a4500;
203d16c43c34b4d73cbe8d13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
d1d736358848df1792c8a926c47ba864=699d293f17bdc607d65f688e3d8d7ceec; loginStyle=enos;
0b68a657f24d12cce48ed4247bcc86d0=352d62297649a7eae62da3419c0f1c4;
8142657bb99ce5d47beb6ebdbabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31;
e6c982c2af8fea3b4ddd995510bccce=3c55ddb8c6c72bbec3a8d6c3cd7c40e;
JSESSIONID=A5B04F75F3ACBC3EAE224BF0FE530969;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
4bfff685a1f608aceced059cb0cf3236=30c82d07997f54b264a0d1bc9c26fdbf;
9dc22c38677b964a43dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9;
50eaad23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
global_id=IAM_S_CEZJQVH3zteSzxxYheDkT6MmRBYxdYmjX5PPQaSaeEPTQewSqnPBygSWDXmu5hbxRgBEU4mhT72ey5Luc
SkDzsEwLzmJsuFnGwYJR8QUMb8RM64WV4t8E5bPktNZQSfr;
54e50be879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "success": false,
  "fail": true
}

```

Issue 20 of 20

[TOC](#)

Archive File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/logout>

Entity: logout (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
3dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4eb1; loginStyle=enos;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Origin: https://portal-ippe1.eniot.io
Accept: /*
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json;charset=UTF-8

{

```

```

        "status": 500,
        "message": "system error",
        "data": null,
        "success": false,
        "fail": true
    }
    ...
}

```

L

Cacheable SSL Page Found 39

TOC

Issue 1 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/queryChannels>

Entity: queryChannels (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=EF54141901C9FF8BD9915A9B26F2E374; Path=/dm-bff; HttpOnly
Date: Mon, 27 Apr 2020 03:49:38 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Request Success",
    "data": [
        ],
        "subMsg": null,
        "requestId": null,
        "retCode": 10000
    }...
}

```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues>

Entity: getMetricValues (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5FBB9D7135CC57A9D4826BC702C96FFF; Path=/dm-bff; HttpOnly
Date: Mon, 27 Apr 2020 03:47:21 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Request Success",
  "data": {
    "deviceRegisterCount": {
      "precision": {
        "minPrecision": 60000
      },
      "values": {
        "1587959040000": 10,
        ...
      }
    }
  }
}

```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/api/archive/strategies>

Entity: strategies (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept=Encoding
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 3fe8ef195d77afaeca93685b8f336acc=c94a5e50aef67bdd765c95a93660a9d; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:32:59 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "message": "",
  "data": [
    ...
  ]
}...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/duration>

Entity: duration (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 59
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 50eaa23de448b610a687b0e42bab51f=96ce1ab32224c4d6f39eb475596cac05; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:03:04 GMT
Content-Type: application/json

{
  "msg": "session not exists, please login in",
  "retCode": 401
}...
```

Issue 5 of 39

[TOC](#)

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: search (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached,

but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 59
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 50eaa23de448b610a687b0e42babb51f=0d269ec330206b966f847c4eaafb00be; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:03:04 GMT
Content-Type: application/json

{
  "msg": "session not exists, please login in",
  "retCode": 401
}...
```

Issue 6 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/config/docurl>

Entity: docurl (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:04:56 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": null,
  "data": "https://support-cn5.envisioniot.com/docs/api/en/2.1.0/overview.html",
  "subMsg": null,
  "requestId": null,
  "retCode": 10000
}...
```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getsdks>

Entity: getsdks (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:06:35 GMT
Content-Type: application/json; charset=UTF-8

{
  "code": 10000,
  "msg": null,
  "data": [
    {
      "level": 1,
      "name": "EnOS IoT Hub SDK",
      "key": "sdk8",
      "children": [
        ...
      ]
    }
  ]
}

```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getoldmenus>

Entity: getoldmenus (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:08:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "msg": null,
  "data": [
    {
      "appKey": "165",
      "appName": "Console",
      "checkSession": true,
      "appIcon": "icon_icon",
      "replaceTop": true,
      ...
    }
  ]
}
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/list>

Entity: list (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1125
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:08:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 0,
  "msg": null,
  "subMsg": null,
  "data": [
    {
      "id": "2ede5e33-b5e0-4e08-8c91-2e305bc81b6d",
      ...
    }
  ]
}
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/getTimeZone>

Entity: getTimeZone (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:11:43 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "message": "",
  "data": {
    "timezone": "GMT+0"
  }
}...
```

Issue 11 of 39

TOC

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: list (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:11:43 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "message": "",
  "data": {
    "flows": [
      ...
    ],
    "count": 0
  }
}...
```

Issue 12 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/user/getAllUsers>

Entity: getAllUsers (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:11:43 GMT
Content-Type: application/json;charset=UTF-8
```

```
{
  "code": 10000,
  "message": "",
  "data": [
    "security_scan",
    "xinyu.fan",
    "ziming.xu",
    "ning.wang",
    "weiyong.sun",
    "jian.tang",
    ...
  ]
}
```

Issue 13 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam/api/v2/session/get>

Entity: get (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 48a7cc09a4a7ce6e3cb4774f8375cca6=7e47171c9b10870fb0d3163a093b7252; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:13:27 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 0,
  "message": "",
  "sessionId": "IAM_S_HFN2qKMBFVa9qWNhQx8EURF6E6UqSW8jC2qTUymQfQDjKgMynk36BaQjMgWAHa75hB3LsQPKB8tB7z7AXEbpgYe7B
KtrS6NXK79cYME3BjrCyD7s3HSTBjsanD4pAUT",
  "user": {
    "id": "u15877199768991",
    "organizationId": "o15790616298731",
    ...
  }
}
```

Cacheable SSL Page Found**Severity:** Low**CVSS Score:** 5.0**URL:** <https://portal-ippe1.eniot.io/portal-web/dataex/list>**Entity:** list (Page)**Risk:** It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations**Causes:** Sensitive information might have been cached by your browser**Fix:** Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:15:12 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": null,
  "data": null,
  "subMsg": null,
  "requestId": null,
  "retCode": 10000
}...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/resmgnt/list/ou/service>

Entity: service (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:15:12 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": null,
  "data": [
    ,
    "subMsg": null,
    "requestId": null,
    "retCode": 10000
  ...
}
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/user/getUsername>

Entity: getUsername (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:17:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "message": "",
  "data": {
    "username": "security_scan"
  }
}...
```

Issue 17 of 39

TOC

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/resmgnt/template/streaming>

Entity: streaming (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:17:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": null,
  "data": {
    "serviceName": "streaming",
    "docUrl": "resource_management_streaming",
    "types": [
      {
        "type": 1,
        "name": null,
        "enabled": true,
      ...
    }
}
```

Issue 18 of 39

[TOC](#)

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/resmgnt/list>

Entity: list (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:17:26 GMT
```

```

Content-Type: application/json;charset=UTF-8

{
  "msg": null,
  "data": [
    {
      "id": "data-asset",
      "name": {
        "en-US": "Data Asset Management",
        "zh-CN": "数据资产管理"
      }
    },
    "services": [
      ...
    ]
  ]
}

```

Issue 19 of 39

[TOC](#)

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/datasource/pagingInfo>

Entity: pagingInfo (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:17:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "message": "",
  "data": {
    "perPageCount": 10,
    "totalCount": 0
  }
}...

```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/datasource/query>

Entity: query (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:17:26 GMT
Content-Type: application/json; charset=UTF-8

{
  "code": 10000,
  "message": "",
  "data": [
    ...
  ]
}...

```

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/info>

Entity: info (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:19:22 GMT
Content-Type: application/json; charset=UTF-8

{
  "status": 0,
  "message": null,
  "data": {
    "register_id": "o15790616298731",
    "id": "o15790616298731",
    "name": "Envision_CLP",
    "domain": "data_o15790616298731",
    "owner": {
      "is_phone_verified": false,
    ...
  }
}
```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/saturnweb/res/common/index.57829111.bundle.js
Entity:	index.57829111.bundle.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

HTTP/1.1 200
Last-Modified: Thu, 02 Jan 2020 07:51:19 GMT
Connection: keep-alive
Server: nginx
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 295830
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: W/"295830-1577951479000"
Date: Mon, 27 Apr 2020 10:43:37 GMT
Content-Type: application/javascript

```
!function(t){function e(n){if(r[n])return r[n].exports;var o=r[n]={i:n,l:!1,exports:{}};return t[n].call(o.exports,o,o.exports,e),o.l=!0,o.exports}var n=window.webpackJsonp>window.webpackJsonp=function(r,i,a){for(var u,c,s,l=0,f=[];l<r.length;l++)c=r[l],o[c]&&f.push(o[c][0]),o[c]=0;for(u in i)Object.prototype.hasOwnProperty.call(i,u)&&(t[u]=i[u]);for(n&&n.r,i,a);f.length;)f.shift();if(a)for(l=0;l<a.length;l++)s=e({e.s=a[l]});return s};var r={},o={3:0};e.m+=e.c=r,e.d=function(t,n,r){e.o(t,n)||Object.defineProperty(t,n,{configurable:!1,enumerable:!0,get:undefined});e.n=function(t){var n=t&&t._esModule?function(){return t.default}:function(){return t};return e.d(n,"a",n),e.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e),e.p=="/sturnweb/",e.oe=function(t){throw console.error(t,t),e.e.s=914}};([function(t,e,n){"use strict";t.exports=n(242)},function(t,e,n){t.exports=n(1210)()}],function(t,e,n){var r=n(20),o=n(99),i=n(81),a=n(82),u=n(100),c=function(t,e,n){var s,l,f,p,d=t&c.F,h=t&c.G,v=t&c.S,m=t&c.P,g=t&c.B,y=h?r:v?r[e]||[r[e]=={}]:{r[e]||{}}.prototype,b=h;o:o[e]||{o[e]={}},_=b.prototype||(b.prototype={});h&&(n=e);for(s in n)l!=d&&y&&void 0==y[s],f=(l?y:n)[s],p=g&&l?u(f,r):m&&"function"==typeof f?u(Function.call,f):f,y&&a(y,s,f,t&c.U),b[s]!=f&&i(b,s,p),m&&_[s]!=f&&_[s]=f});r.core=o,c.F=1,c.G=2,c.S=4,c.P=8,c.B=16,c.W=32,c.U=64,c.R=128,t.exports=c},function(t,e,n){"use..."}
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/api/archive/resources/isOpen>

Entity: isOpen (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:32:59 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "message": "",
  "data": {
    "isOpen": false
  }
}...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/transfer/info>

Entity: info (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:45:59 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 403,
  "message": "No permission to get information of the organization transfer",
  "data": null,
  "success": false,
  "fail": true
}...
```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/v1/encrypt/publicKey>

Entity: publicKey (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:22 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 0,
  "message": null,
  "data": {
    "key_id": "FIXED_KEY_ID",
    "public_key": "-----BEGIN PUBLIC KEY-----\n'nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKB87CRMTufaNoG/EaHx\n\\nb5/rBan6g5sta1Yg6UFZ0t1o4HMd\nYVR40oTYjuJzNoCvjaco+LWNbcOCioTKpto\\nb4PCb/cXCZmXs6WsZSIt0iLVwm3aufkVuEpeqGf5H8CeTcytGAzI3qKQ8Pyy\nWM8F\\nwdCDTLWP1Tqt4e8EncC5z8ja8hrkqdwVovLCNr3z3KSMc8rnLfOWidqmR4hIhA\\nFe4YscD8GddEkI32i02TAG2L1\n95+DxvLmncFAUyUFWbybe5gvOD5C1CAx1Im+/p\\nfq9ILeruu/FJ74ycp3/jNhBjiOxRrqa4NkJPbeaBIIIE0sRNw4gpchmtf\n... PUBLIC KEY-----",
  },
  "success": true,
  ...
}
```

Issue 26 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/config/help>

Entity: help (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
```

```

Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": null,
  "data": {
    "about": {
      "product": {
        "zh-CN": "Envision Enos™ 2.0",
        "en-US": "Envision Enos™ 2.0"
      },
      "copyright": {
        "zh-CN": "© 2019 Envision Digital. 保留所有权利.",
        ...
      }
    }
  }
}

```

Issue 27 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/config/customStyle>

Entity: customStyle (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": null,
  "data": {
    "copyright": {
      "text": {
        "zh-CN": "© 2019 Envision Digital. 保留所有权利.",
        "en-US": "© 2019 Envision Digital. All Rights Reserved."
      },
      "links": {
        "zh-CN": [
          ...
        ]
      }
    }
  }
}

```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/iam/api/v2/authorization/listBySubject
Entity:	listBySubject (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 48a7cc09a4a7ce6e3cb4774f8375cca6=fcf06b15ed4bb6dabb8fee09aab0f422; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 0,
  "message": "",
  "rules": [
    {
      "resourceId": "r15790608556141",
      "resourceType": "menu",
      ...
    }
  ]
}

```

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/getSystemOU>

Entity: getSystemOU (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:58:34 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Request Success",
  "data": "sysenos2018",
  "subMsg": null,
  "requestId": null,
  "retCode": 10000
}...
```

Issue 30 of 39

TOC

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/platform/getmenus>

Entity: getmenus (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 10000,
  "msg": null,
  "data": {
    "commonModules": [
      ...
    ],
    "topModules": [
      ...
    ],
    ...
  }
}
```

Issue 31 of 39

[TOC](#)

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/ldapSource/list>

Entity: list (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:50:05 GMT
```

```

Content-Type: application/json;charset=UTF-8

{
  "status": 0,
  "message": null,
  "data": {
    "total": 0,
    "offset": 0,
    "open": 0,
    "list": [
    ]
  }
...

```

Issue 32 of 39

[TOC](#)

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/ldapSource/validateLinkName>

Entity: validateLinkName (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:56:53 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 0,
  "message": null,
  "data": true,
  "success": true,
  "fail": false
}...

```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/ota/queryFws
Entity:	queryFws (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 59
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 10:14:20 GMT
Content-Type: application/json

{
  "msg": "session not exists, please login in",
  "retCode": 401
}...

```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/navigator/navigator/getmenus
Entity:	getmenus (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 30000,
  "msg": "",
  "data": null
}...
```

Issue 35 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info>

Entity: info (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:09:44 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 404,
  "message": "securitySetting.not.exist",
  "data": null,
  "success": false,
```

```
        "fail": true
    }...
```

Issue 36 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam/api/v2/user/organization/list>

Entity: list (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:12:04 GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 0,
  "message": "",
  "organizations": [
    {
      "id": "o15790616298731",
      "domain": "data_o15790616298731",
      "name": "Envision_CLP",
      "description": ""
    }
  ]
}
```

Issue 37 of 39

TOC

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/security/mfa/status>

Entity: status (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:12:06 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 0,
  "message": null,
  "data": 0,
  "success": true,
  "fail": false
}...
```

Issue 38 of 39

TOC

Cacheable SSL Page Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll>

Entity: queryProductListAll (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=28232C55BFC550E665CD57922C145A9F; Path=/dm-bff; HttpOnly
Date: Sun, 26 Apr 2020 05:13:17 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Request Success",
  "data": {
    "record": [
      {
        "id": "4YW3PlZD",
        "name": "CLP_Wind_Turbine",
        "key": "4YW3PlZD",
        "secret": "9FciljOOnQ8",
        ...
      }
    ]
  }
}
```

Issue 39 of 39

TOC

Cacheable SSL Page Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics>

Entity: queryStatistics (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Sensitive information might have been cached by your browser

Fix: Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Raw Test Response:

```
HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=AFF551542252D3664A095ACCC3174045; Path=/dm-bff; HttpOnly
```

```

Date: Sun, 26 Apr 2020 05:13:57 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Request Success",
  "data": {
    "deviceTotalCount": 10,
    "mqttBytesDaily": 0,
    "mqttNumberDaily": 0
  },
  "subMsg": null,
  "requestId": null,
  ...
}

```

L

Compressed Directory Found 140

TOC

Issue 1 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.zip (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwU$zbYesMFjMvbak5FCUgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding

```

```

Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=6DBD0C5F799A61EB9731909D44DA4777; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=6DBD0C5F799A61EB9731909D44DA4777; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:22 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 2 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fwwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json

```

```

Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=7D0AA705E13C421ADA7C9021C6B07474; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=7D0AA705E13C421ADA7C9021C6B07474; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 3 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.zip (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

...

```

Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=18C14027000DAF002C5131EFFB5D2CFA; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=18C14027000DAF002C5131EFFB5D2CFA; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 4 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=CB5BB611EFFFCAA5688C33A20EA44439; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=CB5BB611EFFFCAA5688C33A20EA44439; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:24 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/model/
Entity:	model.zip (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E48CE50713BA8E2CFD75D1605611369C; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E48CE50713BA8E2CFD75D1605611369C; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=45382B9275CABD9C71AF9A67CC06F29B; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=45382B9275CABD9C71AF9A67CC06F29B; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:24 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
    "retCode": 404
}
...

```

Issue 7 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=110194BCAFEA935225F9AF9BC1DDE7E7; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=110194BCAFEA935225F9AF9BC1DDE7E7; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly

```

```

Date: Tue, 28 Apr 2020 04:32:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 8 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E0851455ECA89F7205DC971CD8F67BF5; Path=/dm-bff; HttpOnly
...
...

```

```

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E0851455ECA89F7205DC971CD8F67BF5; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:24 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 9 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgtqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private

```

```

Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8311882385D046B8AC958FDCAF036EDB4; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8311882385D046B8AC958FDCAF036EDB4; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:24 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 10 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbAK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=02BD4EB4334EF0154740931362B092CA; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=02BD4EB4334EF0154740931362B092CA; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:24 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 11 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io

```

```

eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3823B7B0AF44B8BD9EED8DEC920CF576; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3823B7B0AF44B8BD9EED8DEC920CF576; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 12 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=901E7C9CEB3ABDAE61B2092FEEBBE153; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=901E7C9CEB3ABDAE61B2092FEEBBE153; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/
Entity:	rest.lha (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=245E680F99033F2A447AE198C2C67BD0; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=245E680F99033F2A447AE198C2C67BD0; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.lha (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2AD6331445105B38E0019F0EE01234CE; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2AD6331445105B38E0019F0EE01234CE; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
    "retCode": 404
}
...

```

Issue 15 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.lha (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=DFEDEDD7CFCAA03D49F2EAE4BC00EEF65; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=DFEDEDD7CFCAA03D49F2EAE4BC00EEF65; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly

```

```

Date: Tue, 28 Apr 2020 04:32:26 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 16 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=223D856E12C416A9D1AD1AF8C82B6ECA; Path=/dm-bff; HttpOnly
...
...
```

```

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=223D856E12C416A9D1AD1AF8C82B6ECA; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 17 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgtqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private

```

```

Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=49D9955F1BD433C0B382C9993EBC7F2E; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=49D9955F1BD433C0B382C9993EBC7F2E; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:27 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 18 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E41C77C3318564AB90E1F7665FC2DA65; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E41C77C3318564AB90E1F7665FC2DA65; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:27 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 19 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io

```

```

eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2E0E6655079DCC47FD1A3105D6816CA0; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2E0E6655079DCC47FD1A3105D6816CA0; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 20 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=93592A2577B2A371E4C25238DC86A192; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=93592A2577B2A371E4C25238DC86A192; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/model/
Entity:	model.tar (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=DF5101C243814B6AB31C288FDC0C6410; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=DF5101C243814B6AB31C288FDC0C6410; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.ajr (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=9C72635DA10B0D480D6989481CE2FDC7; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=9C72635DA10B0D480D6989481CE2FDC7; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
    "retCode": 404
}
...

```

Issue 23 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5B3EA47C9DA6CA026DAF082D5E65DA56; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5B3EA47C9DA6CA026DAF082D5E65DA56; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly

```

```

Date: Tue, 28 Apr 2020 04:32:29 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 24 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8E3F4F62F4A73F0F3184AEEEEE95D02F; Path=/dm-bff; HttpOnly
...
...

```

```

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8E3F4F62F4A73F0F3184AEEE95D02F; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 25 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgtqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private

```

```

Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8056DC2EDBE6B9B8474527F03DF80055; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8056DC2EDBE6B9B8474527F03DF80055; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 26 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbAK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=441A1043B12331018847AF8AF5DF8B64; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=441A1043B12331018847AF8AF5DF8B64; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:31 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 27 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io

```

```

eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2684F37A4FD26543A1883992B733F23A; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2684F37A4FD26543A1883992B733F23A; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 28 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: dm-bff.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=0422C11A7D60ACD875EAC0230D0121B8; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=0422C11A7D60ACD875EAC0230D0121B8; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:32 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/model/
Entity:	model.arc (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=D53327CAB678A6B417CE8AD294368D28; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=D53327CAB678A6B417CE8AD294368D28; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:31 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=839CB672520B15766049F11907CA31D0; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=839CB672520B15766049F11907CA31D0; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:32 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
    "retCode": 404
}
...

```

Issue 31 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.tar.lzma (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsCjXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C6D2324FFB2894BF8914A2336A6B2F15; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C6D2324FFB2894BF8914A2336A6B2F15; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdःee; path=/; HttpOnly

```

```

Date: Tue, 28 Apr 2020 04:32:40 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 32 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=AA88B81C7B400F36BAF2DD24AB9169BB; Path=/dm-bff; HttpOnly
...
...

```

```

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=AA88B81C7B400F36BAF2DD24AB9169BB; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:41 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 33 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest>

Entity: rest.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgtqzbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private

```

```

Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=BE208436B5E4BA2995068F6CC1CC56A4; Path=/dm-bff; HttpOnly

...
...

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=BE208436B5E4BA2995068F6CC1CC56A4; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:41 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 34 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.tar.lzma (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8BCD63F9EC5480379FF7915F6C43CDDA; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8BCD63F9EC5480379FF7915F6C43CDDA; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:47 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 35 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io

```

```

eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=699BC81A3FA997EB9922FE8608DD8988; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=699BC81A3FA997EB9922FE8608DD8988; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 36 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8CD3E62CD15F0B7F228DC1905C0E65EA; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8CD3E62CD15F0B7F228DC1905C0E65EA; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:49 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/
Entity:	rest.ar (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=23CBD4F9D4FE50473CC673735891374; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=23CBD4F9D4FE50473CC673735891374; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:58 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: rest.ear (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8A067D1469EC93D3DE3494D673CC5716; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8A067D1469EC93D3DE3494D673CC5716; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:59 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
    "retCode": 404
}
...

```

Issue 39 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.ar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=55917AAE03A36ABE985BF13899FF9911; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=55917AAE03A36ABE985BF13899FF9911; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly

```

```

Date: Tue, 28 Apr 2020 04:33:01 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 40 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: model.ear (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E3FE6D34005F05219BA0E3D9E454EB30; Path=/dm-bff; HttpOnly
...
...

```

```

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E3FE6D34005F05219BA0E3D9E454EB30; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:33:02 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 41 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.zip (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSeMFjMvbak5FCJgtqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt

```

```

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=FA6CC52C14DCD3D467A5BD924586F790; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:10 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 42 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaKFCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3AAC8CACE75A98F0A68EF504ADB8C7F; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:12 GMT
Content-Type: application/json;charset=UTF-8

{

```

```

    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 43 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8F0CB055C0DFC7EFE8A30981279244BE; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:12 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.zip (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=CC5B893C1060F48BF80D1C12FA08065F; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:12 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=A66B9D518A6D27D285B2A544F7CF6916; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:13 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=4A98F954941A79283A62FFC761D81B12; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:13 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C1DDAF298D6E825835C872D6722E379F; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:13 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.lha (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=F15966A351AB41F99A222F777D6AC443; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:14 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=77E6D8B2CD70A35F71B982ED1F2C33BF; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:14 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/logicasset/
Entity:	logicasset.zip (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfkyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=278607E446D31293FDAA4A83E30BCB0A; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:14 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=00DD6927246377FD40D32CA4EF524751; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:15 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
    "retCode": 404
}
...
}
```

Issue 52 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.lha (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=724BA733CA2C21845EF3947C07A2E2E4; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:15 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=7DE4819B4304BC21C1CAA0EFFE4B7903; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:15 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=BCCD90C1EAF92B26A4402C4F9A4545C6; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:15 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=BE6FBA92FAE17F58386CA7D284E5A89E; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:16 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=30CAEA42644FF1B4B575EA82FCD370DB; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:16 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/logicasset/
Entity:	logicasset.ace (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfkyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5703E894761A222AC18D32BABF5812B5; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:17 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUzbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=A6E36DA3B48A4F5BE3594AE5A64E8E56; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:17 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/overview/
Entity:	overview.tar (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsCjXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8EAA7F1BF7C91E7634C86071708C75B6; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:18 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/logicasset/
Entity:	logicasset.lha (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfkyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=62D869A887B105D931A544681C489C63; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:18 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUzbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3CA650B320D24502595DD8212E960258; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:19 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/product/
Entity:	product.arc (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsCjXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E9069DA8AFFCEB85F21697C99E5CE13E; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:19 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=ABB7469C66F57AD453E40A29AD349F8E; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:20 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/simulator/
Entity:	simulator.zip (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfkyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=39EEB89AB1FD773B16227954BD677A7F; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:19 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=EE1CC3CEDD7A5E94B7DBB7F3673C2D49; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:19 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
    "retCode": 404
}
...

```

Issue 66 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSebYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=D0F8E1BDAA63433BBE5FBF5D054AE2F7; Path=/dm-bff; HttpOnly
```

```

Date: Tue, 28 Apr 2020 04:34:20 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 67 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=7F98F5CC3E6E8744B1B372C4D8048028; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:20 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,

```

```

        "subMsg": "Not Found",
        "requestId": null,
        "retCode": 404
    }
    ...

```

Issue 68 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=B184D8D967A098B77DD4AEFEB82B1CD; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:21 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKNOW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSebYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=1AF2BA728F37A7242FA254F49C047F8D; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:20 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
}
```

```

        "data": null,
        "subMsg": "Not Found",
        "requestId": null,
        "retCode": 404
    }
    ...

```

Issue 70 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCUgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin

```

```

Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=617719625B8136DBDFB47A9C4B9D6FDE; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:20 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 71 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.zip (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=50E667F41895553EA1C1DF72CF44A19; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:21 GMT
Content-Type: application/json;charset=UTF-8

```

```
{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
}
```

Issue 72 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=CCCCA024657AA5F0B2F6D48732967980; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:22 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
```

```
}
```

```
...
```

Issue 73 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=96D91C599A616FB71EAF0AC5DDE09A8A; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:21 GMT
```

```

Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 74 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...
Server: nginx

```

```

Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=7599AFA4317DFD8A134A2A91FD8BA654; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:21 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 75 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains

```

```

Set-Cookie: JSESSIONID=458A91416BC923FC6D26C8D7A36D5C4E; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:22 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 76 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.lha (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...
```

```

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=1E0DB1C3A63CA8E11D225D95DB38D1DE; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:22 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 77 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgtqzbLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io

```

```

Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=DC05EB25427F4866A57159906DCB0B6A; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:22 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 78 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=1923208D18A5A478234D865EB23180DC; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:24 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 79 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.ac (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive

```

```

Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2393149476C68B7A1767FB6018B8CA7D; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 80 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json

```

```

Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=16EB665EE2CB917E988F6C0A24D1C352; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:23 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 81 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.lha (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

...

```

Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2F39F31268790BFA704EA81EE0BC9B01; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:24 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 82 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}

```

```

Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5D1192D0BC39927405E1F03994539FD5; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 83 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=318D914275B96B7B76C7CC06A2B7F9B4; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 84 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=318D914275B96B7B76C7CC06A2B7F9B4; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:25 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

```

31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
...
...
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=87724D8B34F7C1A307FC7854688CD371; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 85 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=4138F06DA7B903EA5AA6E9E3D89EC518; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:27 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 86 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
```

```

AMSA2gzkwUzbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=4AA4669117206F7D7B7F875480654BB5; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:27 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 87 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=EBA60106B0F6C751E9755A9091E1F6BC; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=769599706DD31A2C72D70EEA10E3A8ED; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:28 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E2179597EEDFC57D6C60A628F2AAC76E; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C3A1165767DF9AC760923BF371094371; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.tar.lzma (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=08B54F915039FB8B3CA68EF760E85182; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5306DBDF1808F7F183C32739B45F717E; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=969250F712B5BF2730969105C9A10F7C; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.tar.lzma (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5CACEF1CC949335C5CFBFB0287A1007C; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=13A1342850B0EACC0E72F588A4F1EAA; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:31 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=4A6C01251F01391B17447FAE3F9FD1EA; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:31 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/logicasset/
Entity:	logicasset.tar.lzma (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfkyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=13F3112E28394B5B63DA8DA13C7F9E61; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:33 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=10145F4B2E1C8DCAC9C4F0079DBE5AAB; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:33 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
}
```

```
    "retCode": 404
}
...

```

Issue 99 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSebYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=671D35C45A738A57D16D36BA4F2564BA; Path=/dm-bff; HttpOnly
```

```

Date: Tue, 28 Apr 2020 04:34:34 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 100 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.ar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=5E9F848F9B85DE98E4C2F52A982D5239; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:38 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
}
```

```
        "subMsg": "Not Found",
        "requestId": null,
        "retCode": 404
    }
    ...
}
```

Issue 101 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.tar.lzma (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
```

```

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=7C5D8EE79C56405FFADBC42C8E4FD07A; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:38 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 102 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: product.ear (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaKFCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=B72ACB86F7E23ACB51A615DB7FAC4B52; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:39 GMT
Content-Type: application/json;charset=UTF-8

{

```

```

    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 103 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding

```

```

Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=D8DB68FF2879B2D76C985EEB71877A2C; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:39 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 104 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwU5bYesMFjMvbak5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

```

```

...
...
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept=Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=4B0F404C8A97D007EFC6490ACBBCD12C; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:39 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 105 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.ar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive

```

```

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=40BEC3DE9E55F1F9A4F481D610020DC2; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:40 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 106 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: overview.ear (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C12E12D95C965E293E570BA915B39F77; Path=/dm-bff; HttpOnly

```

```

Date: Tue, 28 Apr 2020 04:34:41 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 107 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.tar.lzma (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3DF2259E71CA5CFDBB91944A6D559418; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:43 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
}
```

```

    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 108 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=28BE777B142679B00D9E8661CF5329C8; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:44 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.ar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSebYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=0E5EE183CC4884A9C52F85103B4D7378; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:45 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
}
```

```

        "data": null,
        "subMsg": "Not Found",
        "requestId": null,
        "retCode": 404
    }
    ...

```

Issue 110 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=6FD84E058B10A7F5C953346ACBC41857; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:45 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKNOW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: logicasset.ear (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E6804F8DBF930DC7D1ABD55C07A0305A; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:46 GMT
Content-Type: application/json;charset=UTF-8
```

```
{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
}
```

Issue 112 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.ar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSebYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
```

```

Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=B73A9FDFF88E3518C115889C49CD8A24; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:50 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 113 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: simulator.ear (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

```

```

...
...
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=AAD6A2B8196442242D5B748A6C9B0550; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:50 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 114 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.ar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked

```

```

Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=9180A71CF0E984558693AC2DB433268F; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:54 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 115 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: inte.ear (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains

```

```

Set-Cookie: JSESSIONID=31BD1542719A3A2778790BC179D095D0; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:55 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 116 of 140

TOC

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.zip (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffb2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:47 GMT
Content-Type: application/json;charset=UTF-8

{
    "requestId": null,
    "status": 404,
}
```

```

    "msg": "not.exist",
    "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.zip",
    "data": null
}
...

```

Issue 117 of 140

[TOC](#)

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 141
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:47 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.gz",
  "data": null
}
...

```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:47 GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.rar",
  "data": null
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2zkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.ace",
  "data": null
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/enos-app-webservice/
Entity:	enos-app-webservice.lha (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.lha",
  "data": null
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.lzh",
  "data": null
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.tar",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.arj",
  "data": null
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 142
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.arc",
  "data": null
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: enos-app-webservice.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 145
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/enos-app-webservice.tar.gz",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.zip (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.zip",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 129
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.gz",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.rar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.rar",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.ace (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.ace",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.lha (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.lha",
  "data": null
}
...
```

Compressed Directory Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.lzh (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.lzh",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.tar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:48 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.tar",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.arj (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:49 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.arj",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.arc (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:49 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.arc",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.tar.gz (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 133
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:49 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/app.tar.gz",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.tar.lzma (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:11 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app.tar.lzma",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.war (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 126
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:12 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app.war",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.wim (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 126
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:13 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app.wim",
  "data": null
}
...
```

Compressed Directory Found

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: app.ar (Page)

Risk: It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Causes: Insecure web application programming or configuration

Fix: Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 125
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:22 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app.ar",
  "data": null
}
...
```

Compressed Directory Found

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/enos-app-webservice/app/
Entity:	app.ear (Page)
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 126
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:22 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app.ear",
  "data": null
}
...
```

L

Hidden Directory Detected 1190

TOC

Issue 1 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/domain/>

Entity: domain/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /domain/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 2 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/documentation/
Entity:	documentation/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /documentation/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 3 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dom/
Entity:	dom/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dom/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 4 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/downloading/>

Entity: downloading/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /downloading/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 5 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/banco/>

Entity: banco/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /banco/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 6 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dropbox/
Entity:	dropbox/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dropbox/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 7 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dscgi/
Entity:	dscgi/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dscgi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 8 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dump/>

Entity: dump/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dump/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 9 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/empris/>

Entity: empris/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /empris/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 10 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/easylogs/
Entity:	easylogs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /easylogs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 11 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ecartus/
Entity:	ecartus/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ecartus/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 12 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/english/>

Entity: english/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /english/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 13 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dyngb/>

Entity: dyngb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dyngb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 14 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/error_log/
Entity:	error_log/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /error_log/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 15 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/errorreporter/
Entity:	errorreporter/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /errorreporter/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 16 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/exadmin/>

Entity: exadmin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /exadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 17 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/estore/>

Entity: estore/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /estore/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 18 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/eupload/
Entity:	eupload/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /eupload/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 19 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/exair/
Entity:	exair/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /exair/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 20 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/examples/web-inf/>

Entity: web-inf/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /examples/web-inf/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 21 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bank/>

Entity: bank/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bank/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 22 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/exchange/
Entity:	exchange/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /exchange/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 23 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/banca/
Entity:	banca/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /banca/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 24 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/doc11/>

Entity: doc11/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /doc11/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 25 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cybercrash/>

Entity: cybercrash/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cybercrash/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 26 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/en/
Entity:	en/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /en/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 27 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/docroot/
Entity:	docroot/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /docroot/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 28 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/darkportal/>

Entity: darkportal/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /darkportal/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 29 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/backups/>

Entity: backups/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /backups/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 30 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/date/
Entity:	date/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /date/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 31 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/db2/
Entity:	db2/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /db2/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 32 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dcforum/>

Entity: dcforum/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dcforum/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 33 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ddrint/>

Entity: ddrint/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ddrint/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 34 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/demoauct/
Entity:	demoauct/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /demoauct/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 35 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/defaultwebapp/
Entity:	defaultwebapp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /defaultwebapp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 36 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/demomall/>

Entity: demomall/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /demomall/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 37 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/deny/>

Entity: deny/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /deny/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 38 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/department/
Entity:	department/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /department/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 39 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/departments/
Entity:	departments/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /departments/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 40 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/album/>

Entity: album/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /album/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 41 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/detail/>

Entity: detail/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /detail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 42 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dev60cgi/rwsgi60/
Entity:	rwsgi60/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dev60cgi/rwsgi60/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 43 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dist/
Entity:	dist/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dist/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 44 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/developer/>

Entity: developer/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /developer/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 45 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bak/>

Entity: bak/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bak/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 46 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dlsym/
Entity:	dlsym/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dlsym/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 47 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm_jsp/
Entity:	dm_jsp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dm_jsp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 48 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm/>

Entity: dm/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 49 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dms/>

Entity: dms/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dms/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 50 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/explorer/
Entity:	explorer/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /explorer/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 51 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/exchweb/
Entity:	exchweb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /exchweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 52 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/banners/>

Entity: banners/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /banners/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 53 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/exec/>

Entity: exec/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /exec/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 54 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cvsweb/
Entity:	cvsweb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cvsweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 55 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/guide/
Entity:	guide/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /guide/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 56 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/h1/>

Entity: h1/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /h1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 57 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/head/>

Entity: head/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /head/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 58 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/hippa/
Entity:	hippa/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hippa/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 59 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/hostingcontroller/
Entity:	hostingcontroller/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hostingcontroller/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 60 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/horde/>

Entity: horde/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /horde/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 61 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/hire/>

Entity: hire/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hire/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 62 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/hit_matic/
Entity:	hit_matic/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hit_matic/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 63 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/history/
Entity:	history/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /history/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 64 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/howto/>

Entity: howto/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /howto/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 65 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/group/>

Entity: group/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /group/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 66 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/howitworks/
Entity:	howitworks/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /howitworks/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 67 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/htm/
Entity:	htm/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /htm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 68 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/htmldocs/>

Entity: htmldocs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /htmldocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 69 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/httpacl/>

Entity: httpacl/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /httpacl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 70 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ibmwebas/
Entity:	ibmwebas/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ibmwebas/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 71 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ibmwebas/infocenter/
Entity:	infocenter/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ibmwebas/infocenter/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 72 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/i-build/>

Entity: i-build/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /i-build/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 73 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/ibi_html/

Entity: ibi_html/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ibi_html/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 74 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/icons/
Entity:	icons/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /icons/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 75 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/bbv/
Entity:	bbv/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bbv/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 76 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/icons/small/>

Entity: small/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /icons/small/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 77 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/grocery/>

Entity: grocery/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /grocery/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 78 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/graphs/
Entity:	graphs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /graphs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 79 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/glossary/
Entity:	glossary/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /glossary/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 80 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/faq/>

Entity: faq/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /faq/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 81 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/external/>

Entity: external/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /external/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 82 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/extras/
Entity:	extras/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /extras/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 83 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/export/
Entity:	export/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /export/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 84 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/fcgi-bin/>

Entity: fcgi-bin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fcgi-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 85 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/faqs/>

Entity: faqs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /faqs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 86 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/features/
Entity:	features/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /features/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 87 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/banner/
Entity:	banner/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /banner/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 88 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/fileadmin/>

Entity: fileadmin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fileadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 89 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/foldoc/>

Entity: foldoc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /foldoc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 90 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/foo/
Entity:	foo/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /foo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 91 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/form-totaller/
Entity:	form-totaller/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /form-totaller/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 92 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/footer/>

Entity: footer/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /footer/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 93 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/forward/>

Entity: forward/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /forward/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 94 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/frontend/
Entity:	frontend/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /frontend/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 95 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/banner01/
Entity:	banner01/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /banner01/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 96 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ftproot/>

Entity: ftproot/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ftproot/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 97 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/g/>

Entity: g/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /g/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 98 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/fwd/
Entity:	fwd/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fwd/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 99 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/gallery/
Entity:	gallery/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /gallery/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 100 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/girl/>

Entity: girl/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /girl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 101 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/expeval/>

Entity: expeval/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /expeval/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 102 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/girls/
Entity:	girls/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /girls/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 103 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/glba/
Entity:	glba/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /glba/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 104 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bdata/>

Entity: bdata/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bdata/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 105 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cvs/>

Entity: cvs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cvs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 106 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/customer/
Entity:	customer/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /customer/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 107 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cfide/administrator/
Entity:	administrator/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cfide/administrator/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 108 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/certsrv/>

Entity: certsrv/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /certsrv/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 109 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-auth/>

Entity: cgi-auth/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-auth/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 110 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/calendar/
Entity:	calendar/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/calendar/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 111 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/auth/
Entity:	auth/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /auth/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 112 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/cgi/>

Entity: cgi/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/cgi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 113 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/carello/>

Entity: carello/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/carello/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 114 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/csfaq/
Entity:	csfaq/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/csfaq/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 115 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/cgi-bin/
Entity:	cgi-bin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/cgi-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 116 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/cssearch/>

Entity: cssearch/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/cssearch/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 117 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/certenroll/>

Entity: certenroll/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /certenroll/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 118 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/cutecast/
Entity:	cutecast/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/cutecast/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 119 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/dcforum/
Entity:	dcforum/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/dcforum/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 120 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/dbman/>

Entity: dbman/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/dbman/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 121 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/ews/>

Entity: ews/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/ews/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 122 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/authadmin/
Entity:	authadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /authadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 123 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/excite/
Entity:	excite/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/excite/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 124 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/gbook/>

Entity: gbook/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/gbook/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 125 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/guestbook/>

Entity: guestbook/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/guestbook/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 126 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/gw5/
Entity:	gw5/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/gw5/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 127 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/hamweather/
Entity:	hamweather/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/hamweather/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 128 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/hwadmin5340/>

Entity: hwadmin5340/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/hwadmin5340/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 129 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/dasp/>

Entity: dasp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/dasp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 130 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ce_html/
Entity:	ce_html/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ce_html/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 131 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/certcontrol/
Entity:	certcontrol/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /certcontrol/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 132 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cd-cgi/>

Entity: cd-cgi/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cd-cgi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 133 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/biztalkserverrepository/>

Entity: biztalkserverrepository/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /biztalkserverrepository/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 134 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/blockquote/
Entity:	blockquote/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /blockquote/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 135 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/boadmin/
Entity:	boadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /badmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 136 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bob/>

Entity: bob/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bob/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 137 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/blog/>

Entity: blog/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /blog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 138 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/body/
Entity:	body/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /body/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 139 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/book/
Entity:	book/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /book/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 140 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/asp/>

Entity: asp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /asp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 141 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/budget/>

Entity: budget/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /budget/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 142 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/btauxdir/
Entity:	btauxdir/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /btauxdir/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 143 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/agents/
Entity:	agents/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /agents/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 144 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bugzilla/>

Entity: bugzilla/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bugzilla/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 145 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/casp401k/>

Entity: casp401k/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /casp401k/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 146 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/caspagent/
Entity:	caspagent/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /caspagent/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 147 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ca_icons/
Entity:	ca_icons/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ca_icons/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 148 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/careollofdocs/>

Entity: careollofdocs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /careollofdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 149 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/caspclient/>

Entity: caspclient/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /caspclient/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 150 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/catinfo/
Entity:	catinfo/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /catinfo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 151 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/caspdoc/
Entity:	caspdoc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /caspdoc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 152 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/caspssamp/>

Entity: caspsamp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /caspssamp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 153 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/atc/>

Entity: atc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /atc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 154 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cc/
Entity:	cc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 155 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/iisadmin/
Entity:	iisadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/iisadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 156 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ccbill/>

Entity: ccbill/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ccbill/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 157 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cutenews/>

Entity: cutenews/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cutenews/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 158 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/ikonboard/
Entity:	ikonboard/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/ikonboard/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 159 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/news/
Entity:	news/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/news/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 160 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/charts/>

Entity: charts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /charts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 161 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/charting/>

Entity: charting/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /charting/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 162 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/chart/
Entity:	chart/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /chart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 163 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/citrix/
Entity:	citrix/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /citrix/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 164 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/classcache/>

Entity: classcache/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /classcache/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 165 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/backdoor/>

Entity: backdoor/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /backdoor/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 166 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/citrix/pnagent/
Entity:	pnagent/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /citrix/pnagent/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 167 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/citrix/icaweb/
Entity:	icaweb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /citrix/icaweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 168 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/client/>

Entity: client/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /client/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 169 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/clients/>

Entity: clients/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /clients/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 170 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/clocktower/
Entity:	clocktower/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /clocktower/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 171 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgiwin/
Entity:	cgiwin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgiwin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 172 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/console/>

Entity: console/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /console/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 173 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/connections/>

Entity: connections/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /connections/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 174 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/course_tools/
Entity:	course_tools/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /course_tools/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 175 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/contact/
Entity:	contact/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /contact/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 176 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/creditcards/>

Entity: creditcards/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /creditcards/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 177 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/crystalreportviewers/>

Entity: crystalreportviewers/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /crystalreportviewers/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 178 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/backup/
Entity:	backup/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /backup/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 179 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/currency/
Entity:	currency/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /currency/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 180 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/custdata/>

Entity: custdata/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /custdata/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 181 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/current/>

Entity: current/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /current/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 182 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-temp/
Entity:	cgi-temp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-temp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 183 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/common/
Entity:	common/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /common/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 184 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/openwebmail/>

Entity: openwebmail/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/openwebmail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 185 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/pollit/>

Entity: pollit/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/pollit/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 186 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-source/
Entity:	cgi-source/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-source/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 187 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-sys/
Entity:	cgi-sys/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-sys/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 188 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/aux/>

Entity: aux/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /aux/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 189 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/powerup/>

Entity: powerup/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/powerup/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 190 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/samples/
Entity:	samples/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/samples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 191 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/rwsgi60/
Entity:	rwsgi60/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/rw.cgi60/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 192 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/search/>

Entity: search/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/search/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 193 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/ssi/>

Entity: ssi/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/ssi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 194 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/sws/
Entity:	sws/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/sws/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 195 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/suche/
Entity:	suche/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/suche/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 196 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/templates/>

Entity: templates/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/templates/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 197 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/tools/>

Entity: tools/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/tools/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 198 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/aw/
Entity:	aw/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /aw/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 199 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/w3-msql/
Entity:	w3-msql/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/w3-msql/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/www-sql/>

Entity: www-sql/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/www-sql/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin2/
Entity:	cgi-bin2/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin2/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 202 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgilib/
Entity:	cgilib/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgilib/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 203 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-db2/>

Entity: cgi-db2/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-db2/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 204 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-lib/>

Entity: cgi-lib/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-lib/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 205 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-shop/
Entity:	cgi-shop/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-shop/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 206 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-scripts/
Entity:	cgi-scripts/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-scripts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 207 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgiscripts/>

Entity: cgiscripts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgiscripts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 208 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ayuda/>

Entity: ayuda/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ayuda/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 209 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-bin/mwfp/
Entity:	mwf/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/mwfp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 210 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/iishelp/
Entity:	iishelp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /iishelp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 211 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iis/>

Entity: iis/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /iis/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 212 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iisadmpwd/>

Entity: iisadmpwd/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /iisadmpwd/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 213 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/kjva/
Entity:	kjva/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /kjva/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 214 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/jspdocs/
Entity:	jspdocs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jspdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 215 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/level/>

Entity: level/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /level/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 216 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bin/>

Entity: bin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 217 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/lincoln/
Entity:	lincoln/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /lincoln/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 218 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/list/
Entity:	list/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /list/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 219 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/local/>

Entity: local/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /local/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 220 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/localhost/>

Entity: localhost/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /localhost/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 221 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mail_logs/
Entity:	mail_logs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mail_logs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 222 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/location/
Entity:	location/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /location/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 223 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/jservdocs/>

Entity: jservdocs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jservdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 224 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mailman/>

Entity: mailman/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mailman/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 225 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/main/
Entity:	main/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /main/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 226 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/boot/
Entity:	boot/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /boot/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 227 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/man/>

Entity: man/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /man/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 228 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/manager/>

Entity: manager/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /manager/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 229 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/manuals/
Entity:	manuals/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /manuals/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 230 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/maps/
Entity:	maps/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /maps/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 231 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mailroot/>

Entity: mailroot/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mailroot/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 232 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/jsdirbrowser/>

Entity: jsdirbrowser/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jsdirbrowser/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 233 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/join/
Entity:	join/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /join/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 234 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/jrunscripts/
Entity:	jrunscripts/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jrunscripts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 235 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/i-mail/>

Entity: i-mail/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /i-mail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 236 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/img-sys/>

Entity: img-sys/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /img-sys/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 237 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/inbox/
Entity:	inbox/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /inbox/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 238 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/index/
Entity:	index/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /index/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 239 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/indy/>

Entity: indy/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /indy/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 240 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/instaboard/>

Entity: instaboard/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /instaboard/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 241 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/instantwebmail/
Entity:	instantwebmail/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /instantwebmail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 242 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/bdatos/
Entity:	bdatos/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bdatos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 243 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/interaction/>

Entity: interaction/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /interaction/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 244 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/interscan/>

Entity: interscan/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /interscan/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 245 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/interchange/
Entity:	interchange/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /interchange/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 246 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ipchat/
Entity:	ipchat/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ipchat/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 247 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/isapi/>

Entity: isapi/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /isapi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 248 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/issamples/>

Entity: issamples/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /issamples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 249 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/javadoc/
Entity:	javadoc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /javadoc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 250 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/isqlplus/
Entity:	isqlplus/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /isqlplus/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 251 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ishttpd/>

Entity: ishttpd/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ishttpd/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 252 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/java-sys/>

Entity: java-sys/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /java-sys/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 253 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dmr/
Entity:	dmr/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dmr/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 254 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/beta/
Entity:	beta/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /beta/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 255 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/javax/>

Entity: javax/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /javax/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 256 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ji/>

Entity: ji/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ji/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 257 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/jigsaw/
Entity:	jigsaw/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jigsaw/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 258 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/biztalkserverdocs/
Entity:	biztalkserverdocs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /biztalkserverdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 259 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/archives/>

Entity: archives/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /archives/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 260 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bio/>

Entity: bio/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bio/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 261 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/bios/
Entity:	bios/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bios/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 262 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webnews/
Entity:	webnews/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webnews/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 263 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webobjects/>

Entity: webobjects/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webobjects/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 264 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webservice/>

Entity: webservice/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webservice/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 265 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webshare/
Entity:	webshare/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webshare/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 266 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webspheresamples/
Entity:	webspheresamples/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webspheressamples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 267 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/websql/>

Entity: websql/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /websql/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 268 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wikihome/>

Entity: wikihome/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wikihome/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 269 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/working/
Entity:	working/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /working/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 270 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cfappman/
Entity:	cfappman/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cfappman/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 271 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wsdl/>

Entity: wsdl/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wsdl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 272 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wssamples/>

Entity: wssamples/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wssamples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 273 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webmail/
Entity:	webmail/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webmail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 274 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/wwwroot/
Entity:	wwwroot/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wwwroot/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 275 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wx/>

Entity: wx/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wx/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 276 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/xdk/>

Entity: xdk/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /xdk/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 277 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/yabbse/
Entity:	yabbse/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /yabbse/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 278 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/xss/
Entity:	xss/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /xss/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 279 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/zentrack/>

Entity: zentrack/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /zentrack/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 280 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/zip/>

Entity: zip/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /zip/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 281 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cfdocs/
Entity:	cfdocs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cfdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 282 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/zipped/
Entity:	zipped/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /zipped/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 283 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/zips/>

Entity: zips/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /zips/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 284 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wwthreads/>

Entity: wwthreads/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wwthreads/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 285 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webdev/
Entity:	webdev/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webdev/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 286 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webcash/
Entity:	webcash/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webcash/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 287 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/certificate/>

Entity: certificate/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /certificate/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 288 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/.cobalt/>

Entity: .cobalt/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /.cobalt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 289 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/gxapp/
Entity:	gxapp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /gxapp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 290 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/certificado/
Entity:	certificado/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /certificado/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 291 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/vignette/>

Entity: vignette/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /vignette/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 292 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/w3perl/admin/>

Entity: admin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /w3perl/admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 293 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/way-board/
Entity:	way-board/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /way-board/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 294 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/w3svc101/
Entity:	w3svc101/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /w3svc101/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 295 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wconnect/>

Entity: wconnect/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wconnect/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 296 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webagent/>

Entity: webagent/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webagent/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 297 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webapplication1/
Entity:	webapplication1/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webapplication1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 298 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webapplication2/
Entity:	webapplication2/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webapplication2/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 299 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webapps/>

Entity: webapps/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webapps/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 300 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webbank/>

Entity: webbank/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webbank/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 301 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/zos/
Entity:	zos/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /zos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 302 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/signup/
Entity:	signup/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /signup/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 303 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/forte/examples/>

Entity: examples/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /forte/examples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 304 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mybb/>

Entity: mybb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mybb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 305 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/doc_Boa/
Entity:	doc_Boa/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /doc_Boa/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 306 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/lost%2bfound/
Entity:	lost%2bfound/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /lost%2bfound/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 307 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/new%20folder/>

Entity: new%20folder/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /new%20folder/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 308 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: [https://portal-ippe1.eniot.io/new%20folder%20\(2\)/](https://portal-ippe1.eniot.io/new%20folder%20(2)/)

Entity: new%20folder%20(2)/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /new%20folder%20(2)/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 309 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ppwb(Temp/
Entity:	Temp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ppwb(Temp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 310 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/new%20folder%20(3)/
Entity:	new%20folder%20(3)/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /new%20folder%20(3) HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 311 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/samples/dbsamp/>

Entity: dbsamp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /samples/dbsamp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 312 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/scripts/tools/>

Entity: tools/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /scripts/tools/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 313 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-forте/
Entity:	cgi-forте/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-forте/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 314 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-dos/
Entity:	cgi-dos/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-dos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 315 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/staging/>

Entity: staging/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /staging/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 316 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sites/samples/>

Entity: samples/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sites/samples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 317 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/stats-bin-p/reports/
Entity:	reports/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stats-bin-p/reports/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 318 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/top_list_/
Entity:	top_list_/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /top_list_ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 319 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tradetheme/>

Entity: tradetheme/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tradetheme/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 320 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tsweb/>

Entity: tsweb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tsweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 321 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/Infrastructure/
Entity:	Infrastructure/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /Infrastructure/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 322 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/market/
Entity:	market/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /market/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 323 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mastergate/>

Entity: mastergate/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mastergate/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 324 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mcartfree/>

Entity: mcartfree/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mcartfree/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 325 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mc-icons/
Entity:	mc-icons/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mc-icons/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 326 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/srcview/
Entity:	srcview/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /srcview/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 327 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/logs>

Entity: logs (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/logs HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 328 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/.cobalt/>

Entity: .cobalt/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/.cobalt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 329 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mambo/
Entity:	mambo/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mambo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 330 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/bottom.html
Entity:	bottom.html (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bottom.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 331 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/DotNetNuke/>

Entity: DotNetNuke/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /DotNetNuke/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 332 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wordpress/>

Entity: wordpress/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wordpress/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 333 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cfide/
Entity:	cfide/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cfide/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 334 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/joomla/
Entity:	joomla/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /joomla/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 335 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cpanel/>

Entity: cpanel/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cpanel/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 336 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mantis/>

Entity: mantis/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mantis/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 337 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/.adm/
Entity:	.adm/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /.adm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 338 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/.admin/
Entity:	.admin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /.admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 339 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/.splorts/>

Entity: .splorts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /.splorts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 340 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/CF_MX_SERVER/

Entity: CF_MX_SERVER/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /CF_MX_SERVER/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 341 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/Citrix/NFuse17/
Entity:	NFuse17/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /Citrix/NFuse17/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 342 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/Citrix/NFuseAdmin/
Entity:	NFuseAdmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /Citrix/NFuseAdmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 343 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/Citrix/NFuseEnterprise/>

Entity: NFuseEnterprise/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /Citrix/NFuseEnterprise/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 344 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-bin/>

Entity: cgi-bin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 345 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/WEB-INF/
Entity:	WEB-INF/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /WEB-INF/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 346 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/OMA/
Entity:	OMA/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /OMA/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 347 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/WEB-INF/cfclasses/>

Entity: cfclasses/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /WEB-INF/cfclasses/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 348 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/analog-5.1/>

Entity: analog-5.1/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /analog-5.1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 349 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/WEB-INF/lib/
Entity:	lib/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /WEB-INF/lib/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 350 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/assets/
Entity:	assets/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /assets/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 351 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/asp.net/>

Entity: asp.net/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /asp.net/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 352 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bkup/>

Entity: bkup/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bkup/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 353 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/usage/
Entity:	usage/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /usage/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 354 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/media/
Entity:	media/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /media/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 355 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/member/>

Entity: member/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /member/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 356 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/metacart/>

Entity: metacart/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /metacart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 357 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/bug/
Entity:	bug/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bug/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 358 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_vti_shm/
Entity:	_vti_shm/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_shm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 359 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/prueba/>

Entity: prueba/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /prueba/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 360 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pub/>

Entity: pub/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pub/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 361 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/pruebas/
Entity:	pruebas/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pruebas/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 362 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/public/
Entity:	public/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /public/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 363 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/publica/>

Entity: publica/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /publica/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 364 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/publicar/>

Entity: publicar/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /publicar/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 365 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/publico/
Entity:	publico/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /publico/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 366 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/publisher/
Entity:	publisher/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /publisher/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 367 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/publish/>

Entity: publish/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /publish/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 368 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/protected/>

Entity: protected/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /protected/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 369 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/purchase/
Entity:	purchase/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /purchase/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 370 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/purchases/
Entity:	purchases/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /purchases/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 371 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pw/>

Entity: pw/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pw/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 372 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/register/>

Entity: register/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /register/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 373 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/python/
Entity:	python/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /python/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 374 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/registered/
Entity:	registered/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /registered/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 375 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/report/>

Entity: report/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /report/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 376 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/reports/>

Entity: reports/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /reports/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 377 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/reseller/
Entity:	reseller/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /reseller/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 378 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/restricted/
Entity:	restricted/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /restricted/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 379 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/retail/>

Entity: retail/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /retail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 380 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/prod/>

Entity: prod/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /prod/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 381 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_vti_txt/
Entity:	_vti_txt/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_txt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 382 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/private/
Entity:	private/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /private/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 383 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/privado/>

Entity: privado/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /privado/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 384 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/objects/>

Entity: objects/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /objects/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 385 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/odbc/
Entity:	odbc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /odbc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 386 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/old/
Entity:	old/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /old/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 387 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/old_files/

Entity: old_files/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /old_files/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 388 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/oldfiles/>

Entity: oldfiles/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /oldfiles/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 389 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_vti_bot/
Entity:	_vti_bot/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_bot/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 390 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/oracle/
Entity:	oracle/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /oracle/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 391 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/oradata/>

Entity: oradata/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /oradata/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 392 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/order/>

Entity: order/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /order/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 393 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/orders/
Entity:	orders/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /orders/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 394 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/outgoing/
Entity:	outgoing/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /outgoing/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 395 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/owners/>

Entity: owners/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /owners/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 396 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pages/>

Entity: pages/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pages/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 397 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/passwords/
Entity:	passwords/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /passwords/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 398 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/perl/
Entity:	perl/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /perl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 399 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/personal/>

Entity: personal/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /personal/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_vti_log/

Entity: _vti_log/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_log/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/php/
Entity:	php/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /php/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 402 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/php_classes/
Entity:	php_classes/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /php_classes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 403 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pics/>

Entity: pics/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pics/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 404 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pix/>

Entity: pix/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pix/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 405 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/printers/
Entity:	printers/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /printers/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 406 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/priv/
Entity:	priv/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /priv/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 407 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/acceso/>

Entity: acceso/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /acceso/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 408 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/noticias/>

Entity: noticias/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /noticias/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 409 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/root/
Entity:	root/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /root/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 410 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sample/
Entity:	sample/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sample/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 411 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/siteminder/>

Entity: siteminder/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /siteminder/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 412 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/siteman000510/>

Entity: siteman000510/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /siteman000510/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 413 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/accesslog/
Entity:	accesslog/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /accesslog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 414 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/siteminderagent/
Entity:	siteminderagent/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /siteminderagent/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 415 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sites/>

Entity: sites/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sites/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 416 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sitestats/>

Entity: sitestats/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sitestats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 417 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/siteupdate/
Entity:	siteupdate/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /siteupdate/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 418 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/smreports/
Entity:	smreports/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /smreports/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 419 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/smreportsviewer/>

Entity: smreportsviewer/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /smreportsviewer/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 420 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/siteadmin/>

Entity: siteadmin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /siteadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 421 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/software/
Entity:	software/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /software/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 422 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/solaris/
Entity:	solaris/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /solaris/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 423 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sql/>

Entity: sql/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sql/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 424 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/accesswatch/>

Entity: accesswatch/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /accesswatch/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 425 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/squid/
Entity:	squid/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /squid/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 426 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/src/
Entity:	src/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /src/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 427 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/srchadm/>

Entity: srchadm/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /srchadm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 428 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ssl/>

Entity: ssl/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ssl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 429 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ssi/
Entity:	ssi/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ssi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 430 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/stat/
Entity:	stat/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stat/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 431 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/staff/>

Entity: staff/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /staff/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 432 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sslkeys/>

Entity: sslkeys/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sslkeys/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 433 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/source/
Entity:	source/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /source/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 434 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/site/
Entity:	site/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /site/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 435 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/shtml/>

Entity: shtml/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shtml/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 436 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/shopper/>

Entity: shopper/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shopper/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 437 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/samples/
Entity:	samples/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /samples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 438 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/save/
Entity:	save/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /save/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 439 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/script/>

Entity: script/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /script/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 440 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/scripts/>

Entity: scripts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /scripts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 441 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/search/
Entity:	search/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /search/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 442 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/search-ui/
Entity:	search-ui/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /search-ui/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 443 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/secret/>

Entity: secret/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /secret/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 444 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/access-log/>

Entity: access-log/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /access-log/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 445 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/secure/
Entity:	secure/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /secure/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 446 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/secured/
Entity:	secured/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /secured/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 447 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sell/>

Entity: sell/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sell/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 448 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/server_stats/

Entity: server_stats/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /server_stats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 449 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/serverstats/
Entity:	serverstats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /serverstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 450 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/service/
Entity:	service/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /service/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 451 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/services/>

Entity: services/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /services/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 452 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/servicio/>

Entity: servicio/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /servicio/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 453 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/servicios/
Entity:	servicios/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /servicios/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 454 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/servlet/
Entity:	servlet/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /servlet/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 455 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/servlets/>

Entity: servlets/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /servlets/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 456 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/access/>

Entity: access/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /access/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 457 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/setup/
Entity:	setup/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /setup/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 458 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/share/
Entity:	share/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /share/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 459 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/shop/>

Entity: shop/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shop/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 460 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sales/>

Entity: sales/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sales/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 461 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/statistic/
Entity:	statistic/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /statistic/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 462 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/nl/
Entity:	nl/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 463 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/new/>

Entity: new/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /new/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 464 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/import/>

Entity: import/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /import/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 465 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/inc/
Entity:	inc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /inc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 466 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/impreso/
Entity:	impreso/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /impreso/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 467 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/include/>

Entity: include/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /include/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 468 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/includes/>

Entity: includes/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /includes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 469 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/incoming/
Entity:	incoming/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /incoming/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 470 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/index.html/
Entity:	index.html/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 471 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_objects/

Entity: _objects/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_objects/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 472 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/info/>

Entity: info/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /info/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 473 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/information/
Entity:	information/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /information/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 474 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/imgs/
Entity:	imgs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /imgs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 475 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ingresa/>

Entity: ingresa/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ingresa/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 476 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/install/>

Entity: install/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /install/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 477 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/internal/
Entity:	internal/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /internal/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 478 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/intranet/
Entity:	intranet/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /intranet/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 479 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/inventory/>

Entity: inventory/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /inventory/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 480 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/invitado/>

Entity: invitado/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /invitado/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 481 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_passwords/
Entity:	_passwords/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_passwords/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 482 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/java/
Entity:	java/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /java/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 483 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/japidoc/>

Entity: japidoc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /japidoc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 484 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/javascript/>

Entity: javascript/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /javascript/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 485 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ingreso/
Entity:	ingreso/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ingreso/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 486 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/javasdk/
Entity:	javasdk/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /javasdk/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 487 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/img/>

Entity: img/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /img/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 488 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/images/>

Entity: images/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /images/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 489 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/imagenes/
Entity:	imagenes/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /imagenes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 490 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_errors/
Entity:	_errors/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_errors/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 491 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/guest/>

Entity: guest/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /guest/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 492 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/guests/>

Entity: guests/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /guests/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 493 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/guestbook/
Entity:	guestbook/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /guestbook/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 494 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/help/
Entity:	help/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /help/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 495 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/helpdesk/>

Entity: helpdesk/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /helpdesk/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 496 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/hidden/>

Entity: hidden/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hidden/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 497 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/hit_tracker/
Entity:	hit_tracker/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hit_tracker/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 498 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/hitmatic/
Entity:	hitmatic/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hitmatic/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 499 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/hlstats/>

Entity: hlstats/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hlstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 500 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/home/>

Entity: home/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /home/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 501 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_fpclass/
Entity:	_fpclass/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_fpclass/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 502 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ht/
Entity:	ht/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ht/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 503 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/homepage/>

Entity: homepage/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /homepage/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 504 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/htbin/>

Entity: htbin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /htbin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 505 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/htdocs/
Entity:	htdocs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /htdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 506 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/html/
Entity:	html/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /html/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 507 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/hyperstat/>

Entity: hyperstat/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /hyperstat/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 508 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ibill/>

Entity: ibill/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ibill/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 509 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/idea/
Entity:	idea/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /idea/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 510 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ideas/
Entity:	ideas/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ideas/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 511 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/image/>

Entity: image/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /image/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 512 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/javatest/>

Entity: javatest/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /javatest/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 513 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_mem_bin/
Entity:	_mem_bin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_mem_bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 514 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/news/
Entity:	news/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /news/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 515 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/jave/>

Entity: jave/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jave/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 516 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/job/>

Entity: job/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /job/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 517 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/manual/
Entity:	manual/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /manual/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 518 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/manage/
Entity:	manage/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /manage/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 519 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/members/>

Entity: members/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /members/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 520 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/marketing/>

Entity: marketing/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /marketing/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 521 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/message/
Entity:	message/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /message/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 522 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/messaging/
Entity:	messaging/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /messaging/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 523 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ministats/>

Entity: ministats/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ministats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 524 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/misc/>

Entity: misc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /misc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 525 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_themes/
Entity:	_themes/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_themes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 526 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mkstats/
Entity:	mkstats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mkstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 527 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/mysql_admin/

Entity: mysql_admin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mysql_admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 528 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/msql/>

Entity: msql/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /msql/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 529 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mall_log_files/
Entity:	mall_log_files/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mall_log_files/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 530 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/movimientos/
Entity:	movimientos/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /movimientos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 531 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mysql/>

Entity: mysql/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mysql/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 532 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/nada.html/>

Entity: nada.html/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nada.html/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 533 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/netmagstats/
Entity:	netmagstats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netmagstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 534 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/netscape/
Entity:	netscape/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netscape/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 535 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/netshare/>

Entity: netshare/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netshare/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 536 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/.web/>

Entity: .web/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /.web/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 537 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mqseries/
Entity:	mqseries/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mqseries/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 538 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/nettracker/
Entity:	nettracker/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nettracker/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 539 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_vti_bin/

Entity: _vti_bin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 540 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/mail_log_files/

Entity: mail_log_files/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mail_log_files/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 541 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_tests/
Entity:	_tests/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_tests/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 542 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mail/
Entity:	mail/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 543 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/jrun/>

Entity: jrun/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jrun/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 544 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/js/>

Entity: js/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /js/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 545 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_private/
Entity:	_private/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_private/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 546 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/jserv/
Entity:	jserv/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jserv/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 547 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/jslib/>

Entity: jslib/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jslib/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 548 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/library/>

Entity: library/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /library/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 549 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/junk/
Entity:	junk/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /junk/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 550 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/kiva/
Entity:	kiva/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /kiva/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 551 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/libro/>

Entity: libro/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /libro/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 552 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/jsp/>

Entity: jsp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jsp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 553 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/lib/
Entity:	lib/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /lib/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 554 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/linux/
Entity:	linux/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /linux/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 555 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/log/>

Entity: log/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /log/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 556 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_scripts/

Entity: _scripts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_scripts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 557 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/login/
Entity:	login/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /login/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 558 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/logs/
Entity:	logs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /logs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 559 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/logg/>

Entity: logg/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /logg/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 560 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/logfile/>

Entity: logfile/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /logfile/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 561 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/logging/
Entity:	logging/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /logging/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 562 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/logfiles/
Entity:	logfiles/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /logfiles/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 563 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/logger/>

Entity: logger/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /logger/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 564 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/lost+found/>

Entity: lost+found/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /lost+found/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 565 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/jdbc/
Entity:	jdbc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /jdbc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 566 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/lpt/
Entity:	lpt/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /lpt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 567 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/statistics/>

Entity: statistics/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /statistics/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 568 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/graphics/>

Entity: graphics/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /graphics/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 569 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mon/
Entity:	mon/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mon/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 570 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/acciones/
Entity:	acciones/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /acciones/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 571 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_include/

Entity: _include/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_include/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 572 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_logs/

Entity: _logs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_logs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 573 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_borders/
Entity:	_borders/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_borders/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 574 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/snort/
Entity:	snort/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /snort/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 575 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_mmdbscripts/

Entity: _mmdbscripts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_mmdbscripts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 576 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_mmserverscripts/

Entity: _mmserverscripts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_mmserverscripts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 577 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_overlay/
Entity:	_overlay/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_overlay/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 578 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_pages/
Entity:	_pages/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_pages/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 579 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/apache/>

Entity: apache/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /apache/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 580 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_scriptlibrary/

Entity: _scriptlibrary/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_scriptlibrary/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 581 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_vti_bin/_vti_adm/
Entity:	_vti_adm/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_bin/_vti_adm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 582 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/app/
Entity:	app/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /app/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 583 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_vti_adm/

Entity: _vti_adm/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_adm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 584 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_vti_aut/

Entity: _vti_aut/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_aut/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 585 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_vti_cnf/
Entity:	_vti_cnf/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_cnf/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 586 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_vti_bin/_vti_aut/
Entity:	_vti_aut/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_bin/_vti_aut/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 587 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_vti_pvt/

Entity: _vti_pvt/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_pvt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 588 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/_vti_script/

Entity: _vti_script/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_vti_script/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 589 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/application/
Entity:	application/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 590 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_sharedtemplates/
Entity:	_sharedtemplates/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_sharedtemplates/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 591 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~log/>

Entity: ~log/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~log/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 592 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/binaries/>

Entity: binaries/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /binaries/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 593 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/364332/
Entity:	364332/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /364332/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 594 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/base/
Entity:	base/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /base/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 595 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/apt/>

Entity: apt/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /apt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 596 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~etc/>

Entity: ~etc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~etc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 597 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~guest/
Entity:	~guest/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~guest/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 598 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~ftp/
Entity:	~ftp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~ftp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 599 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~home/>

Entity: ~home/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~home/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/agentes/>

Entity: agentes/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /agentes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~stats/
Entity:	~stats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~stats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 602 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~sbin/
Entity:	~sbin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~sbin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 603 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~nobody/>

Entity: ~nobody/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~nobody/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 604 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~mnt/>

Entity: ~mnt/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~mnt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 605 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~root/
Entity:	~root/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~root/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 606 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/agent/
Entity:	agent/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /agent/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 607 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~tmp/>

Entity: ~tmp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~tmp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 608 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~usr/>

Entity: ~usr/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~usr/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 609 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~uucp/
Entity:	~uucp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~uucp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 610 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~var/
Entity:	~var/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~var/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 611 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/contrib/>

Entity: contrib/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /contrib/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 612 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/doc/packages/>

Entity: packages/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /doc/packages/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 613 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/analog/
Entity:	analog/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /analog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 614 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~wsdocs/
Entity:	~wsdocs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~wsdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 615 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~webstats/>

Entity: ~webstats/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~webstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 616 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~nobody/etc/>

Entity: etc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~nobody/etc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 617 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/machine/
Entity:	machine/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /machine/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 618 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/net/
Entity:	net/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /net/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 619 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/857583/>

Entity: 857583/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /857583/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 620 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/about/>

Entity: about/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /about/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 621 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~dev/
Entity:	~dev/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~dev/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 622 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/analyze/
Entity:	analyze/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /analyze/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 623 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/874840/>

Entity: 874840/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /874840/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 624 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ar/>

Entity: ar/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ar/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 625 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/application_assemblies/
Entity:	application_assemblies/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_assemblies/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 626 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/application_browsers/
Entity:	application_browsers/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_browsers/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 627 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/application_code/

Entity: application_code/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_code/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 628 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/application_data/

Entity: application_data/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_data/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 629 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/application_globalresources/
Entity:	application_globalresources/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_globalresources/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 630 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/application_localresources/
Entity:	application_localresources/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_localresources/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 631 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/application_themes/

Entity: application_themes/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_themes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 632 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/application_webreferences/

Entity: application_webreferences/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /application_webreferences/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 633 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/appweb/
Entity:	appweb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /appweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 634 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/aspnet/
Entity:	aspnet/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /aspnet/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 635 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/allaire/>

Entity: allaire/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /allaire/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 636 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/archive/>

Entity: archive/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /archive/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 637 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/aspsamp/
Entity:	aspsamp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /aspsamp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 638 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/assemblies/
Entity:	assemblies/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /assemblies/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 639 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/azdlite/>

Entity: azdlite/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /azdlite/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 640 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/back/>

Entity: back/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /back/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 641 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/bar/
Entity:	bar/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bar/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 642 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/batch/
Entity:	batch/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /batch/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 643 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/bb-dnbd/>

Entity: bb-dnbd/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bb-dnbd/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 644 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/billing/>

Entity: billing/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /billing/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 645 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/art/
Entity:	art/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /art/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 646 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/alias/
Entity:	alias/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /alias/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 647 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/agencies/>

Entity: agencies/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /agencies/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 648 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/akopia/>

Entity: akopia/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /akopia/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 649 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/acart2_0/
Entity:	acart2_0/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /acart2_0/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 650 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/acartpath/
Entity:	acartpath/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /acartpath/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 651 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/accessinglog/>

Entity: accessinglog/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /accessinglog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 652 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/accounts/>

Entity: accounts/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /accounts/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 653 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/applications/
Entity:	applications/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /applications/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 654 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/adcycle/
Entity:	adcycle/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /adcycle/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 655 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/acweb/>

Entity: acweb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /acweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 656 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/actuate/>

Entity: actuate/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /actuate/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 657 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/add/
Entity:	add/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /add/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 658 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/address/
Entity:	address/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /address/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 659 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/admcgi/>

Entity: admcgi/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admcgi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 660 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/admentor/admin/>

Entity: admin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admentor/admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 661 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/admincp/
Entity:	admincp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admincp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 662 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/admin_/
Entity:	admin_/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admin_ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 663 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/adminsample/>

Entity: adminsample/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /adminsample/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 664 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/admin-serv/>

Entity: admin-serv/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admin-serv/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 665 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/admisapi/
Entity:	admisapi/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admisapi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 666 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/apps/
Entity:	apps/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /apps/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 667 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/admission/>

Entity: admission/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admission/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 668 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/adsamples/>

Entity: adsamples/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /adsamples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 669 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/advwebadmin/
Entity:	advwebadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /advwebadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 670 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/advworks/
Entity:	advworks/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /advworks/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 671 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/abc/>

Entity: abc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /abc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 672 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/affiliates/>

Entity: affiliates/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /affiliates/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 673 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/admin_files/
Entity:	admin_files/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admin_files/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 674 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/zipfiles/
Entity:	zipfiles/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /zipfiles/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 675 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/~bin/>

Entity: ~bin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 676 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/test/>

Entity: test/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /test/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 677 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/testing/
Entity:	testing/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /testing/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 678 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/tests/
Entity:	tests/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tests/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 679 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ticket/>

Entity: ticket/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ticket/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 680 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/activex/>

Entity: activex/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /activex/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 681 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/tickets/
Entity:	tickets/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tickets/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 682 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/tmp/
Entity:	tmp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tmp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 683 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tpv/>

Entity: tpv/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tpv/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 684 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tools/>

Entity: tools/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tools/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 685 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/trabajo/
Entity:	trabajo/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /trabajo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 686 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/test-cgi/
Entity:	test-cgi/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /test-cgi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 687 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/trafficlog/>

Entity: trafficlog/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /trafficlog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 688 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/transpolar/>

Entity: transpolar/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /transpolar/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 689 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/tree/
Entity:	tree/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tree/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 690 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/adm/
Entity:	adm/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /adm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 691 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/update/>

Entity: update/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /update/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 692 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/updates/>

Entity: updates/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /updates/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 693 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/trees/
Entity:	trees/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /trees/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 694 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/upload/
Entity:	upload/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /upload/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 695 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/uploads/>

Entity: uploads/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /uploads/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 696 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/user/>

Entity: user/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /user/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 697 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/transito/
Entity:	transito/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /transito/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 698 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/temporal/
Entity:	temporal/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /temporal/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 699 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/template/>

Entity: template/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /template/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 700 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/stats/>

Entity: stats/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 701 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/stats_old/
Entity:	stats_old/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stats_old/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 702 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/templates/
Entity:	templates/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /templates/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 703 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/status/>

Entity: status/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /status/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 704 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/storage/>

Entity: storage/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /storage/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 705 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/store/
Entity:	store/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /store/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 706 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/styles/
Entity:	styles/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /styles/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 707 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/stuff/>

Entity: stuff/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stuff/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 708 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/style/>

Entity: style/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /style/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 709 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/stylesheets/
Entity:	stylesheet/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stylesheet/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 710 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/subir/
Entity:	subir/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /subir/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 711 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/stylesheets/>

Entity: stylesheets/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stylesheets/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 712 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/account/>

Entity: account/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /account/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 713 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sun/
Entity:	sun/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sun/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 714 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/super_stats/
Entity:	super_stats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /super_stats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 715 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/support/>

Entity: support/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /support/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 716 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sysadmin/>

Entity: sysadmin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sysadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 717 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sysbackup/
Entity:	sysbackup/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sysbackup/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 718 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sys/
Entity:	sys/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sys/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 719 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/system/>

Entity: system/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /system/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 720 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tarjetas/>

Entity: tarjetas/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tarjetas/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 721 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/tar/
Entity:	tar/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tar/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 722 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/temp/
Entity:	temp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /temp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 723 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/accounting/>

Entity: accounting/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /accounting/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 724 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/users/>

Entity: users/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /users/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 725 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/~admin/
Entity:	~admin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /~admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 726 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/usr/
Entity:	usr/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /usr/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 727 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/usuario/>

Entity: usuario/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /usuario/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 728 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webreps/>

Entity: webreps/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webreps/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 729 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/website/
Entity:	website/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /website/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 730 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webstats/
Entity:	webstats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 731 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webstat/>

Entity: webstat/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webstat/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 732 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webtrends/>

Entity: webtrends/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webtrends/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 733 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webtrace/
Entity:	webtrace/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webtrace/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 734 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/windows/
Entity:	windows/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /windows/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 735 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/administrator/>

Entity: administrator/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /administrator/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 736 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/word/>

Entity: word/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /word/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 737 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/work/
Entity:	work/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /work/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 738 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webreports/
Entity:	webreports/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webreports/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 739 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wsdocs/>

Entity: wsdocs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wsdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 740 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/www-sql/>

Entity: www-sql/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /www-sql/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 741 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/wusage/
Entity:	wusage/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wusage/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 742 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/wwwlog/
Entity:	wwwlog/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wwwlog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 743 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/wwwjoin/>

Entity: wwwjoin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wwwjoin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 744 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/www/>

Entity: www/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /www/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 745 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/wwwstat/
Entity:	wwwstat/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wwwstat/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 746 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/wwwstats/
Entity:	wwwstats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wwwstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 747 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/xml/>

Entity: xml/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /xml/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 748 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/adminuser/>

Entity: adminuser/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /adminuser/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 749 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/xtemp/
Entity:	xtemp/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /xtemp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 750 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/wstats/
Entity:	wstats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /wstats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 751 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webpub/>

Entity: webpub/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webpub/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 752 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/administration/>

Entity: administration/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /administration/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 753 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webpub-ui/
Entity:	webpub-ui/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webpub-ui/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 754 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/usuarios/
Entity:	usuarios/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /usuarios/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 755 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/admentor/>

Entity: admentor/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admentor/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 756 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/util/>

Entity: util/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /util/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 757 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/utils/
Entity:	utils/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /utils/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 758 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/vfs/
Entity:	vfs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /vfs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 759 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/w3perl/>

Entity: w3perl/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /w3perl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 760 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/warez/>

Entity: warez/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /warez/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 761 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/web/
Entity:	web/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /web/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 762 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/web_usage/
Entity:	web_usage/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /web_usage/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 763 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webaccess/>

Entity: webaccess/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webaccess/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 764 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/web800fo/>

Entity: web800fo/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /web800fo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 765 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webadmin/
Entity:	webadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 766 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/admin/
Entity:	admin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 767 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webcart-lite/>

Entity: webcart-lite/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webcart-lite/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 768 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webalizer/>

Entity: webalizer/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webalizer/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 769 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webboard/
Entity:	webboard/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webboard/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 770 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webcart/
Entity:	webcart/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webcart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 771 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/weblogs/>

Entity: weblogs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /weblogs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 772 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webdata/>

Entity: webdata/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webdata/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 773 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webdb/
Entity:	webdb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webdb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 774 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/weblog/
Entity:	weblog/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /weblog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 775 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webmaster/>

Entity: webmaster/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webmaster/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 776 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/webmaster_logs/

Entity: webmaster_logs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webmaster_logs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 777 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/global/
Entity:	global/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /global/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 778 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ustats/
Entity:	ustats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ustats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 779 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/gfx/>

Entity: gfx/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /gfx/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 780 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sex/>

Entity: sex/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sex/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 781 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/shell/
Entity:	shell/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shell/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 782 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/shipping/
Entity:	shipping/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shipping/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 783 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/shell-cgi/>

Entity: shell-cgi/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shell-cgi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 784 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/fun/>

Entity: fun/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fun/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 785 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/shoponline/
Entity:	shoponline/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shoponline/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 786 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/shopping_cart/
Entity:	shopping_cart/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /shopping_cart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 787 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/site_settings/

Entity: site_settings/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /site_settings/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 788 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sitemgr/>

Entity: sitemgr/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sitemgr/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 789 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/siteminderagent/pw/
Entity:	pw/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /siteminderagent/pw/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 790 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/smallco/
Entity:	smallco/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /smallco/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 791 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/snmp/>

Entity: snmp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /snmp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 792 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/soap/>

Entity: soap/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /soap/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 793 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cbi-bin/
Entity:	cbi-bin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cbi-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 794 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/soapdocs/
Entity:	soapdocs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /soapdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 795 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ccard/>

Entity: ccard/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ccard/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 796 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/solution/>

Entity: solution/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /solution/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 797 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/solutions/
Entity:	solutions/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /solutions/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 798 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sounds/
Entity:	sounds/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sounds/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 799 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sources/>

Entity: sources/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sources/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sproot/>

Entity: sproot/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sproot/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/spool/
Entity:	spool/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /spool/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 802 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/smereports/
Entity:	smereports/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /smereports/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 803 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cd/>

Entity: cd/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cd/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 804 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/session/>

Entity: session/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /session/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 805 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sessiondata/
Entity:	sessiondata/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sessiondata/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 806 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/servlet/ssifilter/
Entity:	ssifilter/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /servlet/ssifilter/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 807 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/recent/>

Entity: recent/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /recent/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 808 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/repository/>

Entity: repository/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /repository/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 809 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/report_bin/rwsgi60/
Entity:	rwsgi60/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /report_bin/rwsgi60/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 810 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cash/
Entity:	cash/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cash/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 811 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/research/>

Entity: research/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /research/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 812 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/resource/>

Entity: resource/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /resource/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 813 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/resources/
Entity:	resources/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /resources/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 814 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/reviews/
Entity:	reviews/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /reviews/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 815 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/rightfax/>

Entity: rightfax/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /rightfax/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 816 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/rksh/>

Entity: rksh/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /rksh/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 817 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/rpc/
Entity:	rpc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /rpc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 818 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sale/
Entity:	sale/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sale/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 819 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/roads/>

Entity: roads/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /roads/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 820 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/scans/>

Entity: scans/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /scans/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 821 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/catalog/
Entity:	catalog/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /catalog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 822 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sdk/
Entity:	sdk/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sdk/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 823 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/scm/
Entity:	scm/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /scm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 824 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sbin/>

Entity: sbin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sbin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 825 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/search97/
Entity:	search97/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /search97/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 826 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/sections/
Entity:	sections/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sections/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 827 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/servers/>

Entity: servers/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /servers/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 828 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sek-bin/>

Entity: sek-bin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sek-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 829 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/selector/
Entity:	selector/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /selector/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 830 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/string/
Entity:	string/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /string/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 831 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/readme/>

Entity: readme/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /readme/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 832 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/stats-bin-p/>

Entity: stats-bin-p/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /stats-bin-p/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 833 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/userlog/
Entity:	userlog/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /userlog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 834 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/Msword/
Entity:	Msword/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /Msword/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 835 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/storemgr/>

Entity: storemgr/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /storemgr/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 836 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC98/>

Entity: W3SVC98/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC98/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 837 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC16/
Entity:	W3SVC16/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC16/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 838 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/iisadmin/
Entity:	iisadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /iisadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 839 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC99/>

Entity: W3SVC99/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC99/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 840 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iissamples/>

Entity: iissamples/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /iissamples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 841 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/userdb/
Entity:	userdb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /userdb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 842 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/scripts/iisadmin/
Entity:	iisadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /scripts/iisadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 843 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/aspx/>

Entity: aspx/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /aspx/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 844 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/siteserver/>

Entity: siteserver/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /siteserver/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 845 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/site/iissamples/
Entity:	iissamples/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /site/iissamples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 846 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC19/
Entity:	W3SVC19/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC19/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 847 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC2/>

Entity: W3SVC2/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC2/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 848 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC18/>

Entity: W3SVC18/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC18/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 849 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC20/
Entity:	W3SVC20/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC20/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 850 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC22/
Entity:	W3SVC22/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC22/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 851 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC21/>

Entity: W3SVC21/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC21/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 852 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC23/>

Entity: W3SVC23/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC23/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 853 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC24/
Entity:	W3SVC24/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC24/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 854 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC1/
Entity:	W3SVC1/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 855 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC25/>

Entity: W3SVC25/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC25/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 856 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/updated/>

Entity: updated/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /updated/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 857 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/us/
Entity:	us/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /us/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 858 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC17/
Entity:	W3SVC17/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC17/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 859 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/urlresult/>

Entity: urlresult/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /urlresult/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 860 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/subdir/>

Entity: subdir/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /subdir/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 861 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/surf/
Entity:	surf/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /surf/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 862 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/survey/
Entity:	survey/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /survey/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 863 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/sup/>

Entity: sup/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /sup/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 864 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/technote/>

Entity: technote/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /technote/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 865 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/te_html/
Entity:	te_html/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /te_html/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 866 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cdrom/
Entity:	cdrom/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cdrom/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 867 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/testweb/>

Entity: testweb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /testweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 868 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/testdir/>

Entity: testdir/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /testdir/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 869 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/text/
Entity:	text/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /text/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 870 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/tomcat-docs/
Entity:	tomcat-docs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tomcat-docs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 871 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tmplogs/>

Entity: tmplogs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tmplogs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 872 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/todo/>

Entity: todo/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /todo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 873 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/training/
Entity:	training/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /training/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 874 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/transactional/
Entity:	transactional/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /transactional/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 875 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/themes/>

Entity: themes/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /themes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 876 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tutorial/>

Entity: tutorial/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tutorial/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 877 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/turba/
Entity:	turba/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /turba/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 878 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ttweb/
Entity:	ttweb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ttweb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 879 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cert/>

Entity: cert/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cert/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 880 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tutos/>

Entity: tutos/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tutos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 881 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/uddi/uddilistusersservlet/
Entity:	uddilistusersservlet/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /uddi/uddilistusersservlet/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 882 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/strategy/
Entity:	strategy/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /strategy/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 883 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/random_banner/

Entity: random_banner/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /random_banner/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 884 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC26/>

Entity: W3SVC26/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC26/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 885 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/tuxedo/
Entity:	tuxedo/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tuxedo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 886 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/quickplace/
Entity:	quickplace/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /quickplace/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 887 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/nextgeneration/>

Entity: nextgeneration/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nextgeneration/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 888 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/nicklas/>

Entity: nicklas/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nicklas/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 889 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/newsroups/
Entity:	newsroups/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /newsroups/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 890 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/notcias/
Entity:	notcias/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /notcias/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 891 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/buynow/>

Entity: buynow/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /buynow/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 892 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/nsearch/>

Entity: nsearch/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nsearch/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 893 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/notes/
Entity:	notes/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /notes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 894 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ns-icons/
Entity:	ns-icons/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ns-icons/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 895 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/nsn/>

Entity: nsn/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nsn/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 896 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/network/>

Entity: network/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /network/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 897 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/number/
Entity:	number/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /number/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 898 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/oekaki/
Entity:	oekaki/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /oekaki/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 899 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/officescan/>

Entity: officescan/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /officescan/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 900 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/online/>

Entity: online/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /online/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 901 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/opendocman/
Entity:	opendocman/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /opendocman/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 902 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/oop/
Entity:	oop/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /oop/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 903 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/c/>

Entity: c/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /c/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 904 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/other/>

Entity: other/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /other/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 905 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ope/
Entity:	ope/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ope/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 906 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/oto/
Entity:	oto/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /oto/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 907 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/owa/>

Entity: owa/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /owa/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 908 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/of/>

Entity: of/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /of/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 909 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/owl/
Entity:	owl/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /owl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 910 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/netperf/
Entity:	netperf/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netperf/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 911 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/netpierce/>

Entity: netpierce/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netpierce/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 912 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mib/>

Entity: mib/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mib/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 913 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/netdetector/
Entity:	netdetector/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netdetector/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 914 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mibs/
Entity:	mibs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mibs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 915 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/microsoft/>

Entity: microsoft/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /microsoft/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 916 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/microsoft-server-activesync/>

Entity: microsoft-server-activesync/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /microsoft-server-activesync/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 917 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/midicart/
Entity:	midicart/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /midicart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 918 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/modules/
Entity:	modules/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /modules/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 919 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/movies/>

Entity: movies/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /movies/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 920 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mp3/>

Entity: mp3/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mp3/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 921 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/bugs/
Entity:	bugs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /bugs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 922 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mozilla/
Entity:	mozilla/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mozilla/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 923 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mp3s/>

Entity: mp3s/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mp3s/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 924 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ms/>

Entity: ms/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ms/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 925 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/mrtg/
Entity:	mrtg/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mrtg/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 926 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/msadc/
Entity:	msadc/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /msadc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 927 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/mspress30/>

Entity: mspress30/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /mspress30/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 928 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/my/>

Entity: my/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /my/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 929 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/multimedia/
Entity:	multimedia/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /multimedia/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 930 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/buy/
Entity:	buy/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /buy/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 931 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/netbilling/>

Entity: netbilling/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netbilling/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 932 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ncadmin/>

Entity: ncadmin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ncadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 933 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ncsample/
Entity:	ncsample/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ncsample/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 934 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/netbasic/
Entity:	netbasic/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netbasic/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 935 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/nchelp/>

Entity: nchelp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /nchelp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 936 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ows-bin/>

Entity: ows-bin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ows-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 937 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ramgen/
Entity:	ramgen/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ramgen/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 938 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/p0rn/
Entity:	p0rn/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /p0rn/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 939 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/password/>

Entity: password/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /password/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 940 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/phpprojekt/>

Entity: phpprojekt/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phpprojekt/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 941 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/phpsecurepages/
Entity:	phpsecurepages/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phpsecurepages/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 942 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/pl/
Entity:	pl/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 943 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/plugins/>

Entity: plugins/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /plugins/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 944 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/policy/>

Entity: policy/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /policy/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 945 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/porn/
Entity:	porn/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /porn/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 946 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/porno/
Entity:	porno/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /porno/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 947 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ppwb/>

Entity: ppwb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ppwb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 948 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cards/>

Entity: cards/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cards/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 949 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/pr0n/
Entity:	pr0n/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pr0n/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 950 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/phppgadmin/
Entity:	phppgadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phppgadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 951 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/process/>

Entity: process/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /process/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 952 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/products/>

Entity: products/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /products/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 953 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/productcart/
Entity:	productcart/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /productcart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 954 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/pre/
Entity:	pre/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pre/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 955 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/programming/>

Entity: programming/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /programming/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 956 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pron/>

Entity: pron/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pron/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 957 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/programs/
Entity:	programs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /programs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 958 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cart/
Entity:	cart/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 959 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/prv/>

Entity: prv/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /prv/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 960 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/prxdocs/>

Entity: prxdocs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /prxdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 961 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/psuser/
Entity:	psuser/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /psuser/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 962 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/press/
Entity:	press/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /press/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 963 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/phpnuke/>

Entity: phpnuke/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phpnuke/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 964 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/card/>

Entity: card/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /card/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 965 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/docucolor/
Entity:	docucolor/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /docucolor/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 966 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/pay/
Entity:	pay/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pay/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 967 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/patch/>

Entity: patch/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /patch/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 968 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/path/>

Entity: path/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /path/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 969 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cache-stats/
Entity:	cache-stats/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cache-stats/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 970 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/payment/
Entity:	payment/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /payment/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 971 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/payments/>

Entity: payments/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /payments/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 972 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/paymentmanager/>

Entity: paymentmanager/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /paymentmanager/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 973 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/pbsdata/
Entity:	pbsdata/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pbsdata/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 974 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/pbserver/
Entity:	pbserver/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pbserver/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 975 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pccsmysqladm/>

Entity: pccsmysqladm/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pccsmysqladm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 976 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pds/>

Entity: pds/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pds/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 977 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/caja/
Entity:	caja/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /caja/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 978 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/perl5/
Entity:	perl5/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /perl5/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 979 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/people/>

Entity: people/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /people/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 980 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/phone/>

Entity: phone/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phone/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 981 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/photoads/
Entity:	photoads/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /photoads/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 982 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/phorum/
Entity:	phorum/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phorum/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 983 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/photos/>

Entity: photos/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /photos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 984 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/photopost/>

Entity: photopost/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /photopost/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 985 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/photoalbum/
Entity:	photoalbum/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /photoalbum/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 986 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/phpbb/
Entity:	phpbb/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phpbb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 987 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/phpbb208/>

Entity: phpbb208/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phpbb208/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 988 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/pass/>

Entity: pass/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pass/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 989 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/phpmyadmin/
Entity:	phpmyadmin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /phpmyadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 990 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC28/
Entity:	W3SVC28/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC28/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 991 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC27/>

Entity: W3SVC27/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC27/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 992 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC29/>

Entity: W3SVC29/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC29/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 993 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/correos/
Entity:	correo/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /correo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 994 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/silverstream/
Entity:	silverstream/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /silverstream/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 995 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/counter/>

Entity: counter/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /counter/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 996 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/crypto/>

Entity: crypto/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /crypto/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 997 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/credit/
Entity:	credit/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /credit/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 998 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/csr/
Entity:	csr/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /csr/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 999 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/css/>

Entity: css/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /css/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cuentas/>

Entity: cuentas/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cuentas/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cuenta/
Entity:	cuenta/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cuenta/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1002 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/customers/
Entity:	customers/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /customers/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1003 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/corp/>

Entity: corp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /corp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1004 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/storedb/>

Entity: storedb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /storedb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1005 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cybercash/
Entity:	cybercash/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cybercash/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1006 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/data/
Entity:	data/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /data/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1007 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/database/>

Entity: database/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /database/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 1008 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/databases/>

Entity: databases/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /databases/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 1009 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/datafiles/
Entity:	datafiles/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /datafiles/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1010 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dato/
Entity:	dato/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dato/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1011 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/db/>

Entity: db/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /db/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1012 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/datos/>

Entity: datos/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /datos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1013 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ddreport/
Entity:	ddreport/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ddreport/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1014 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dat/
Entity:	dat/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dat/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1015 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dbase/>

Entity: dbase/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dbase/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1016 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cool-logs/>

Entity: cool-logs/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cool-logs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1017 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/controlpanel/
Entity:	controlpanel/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /controlpanel/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1018 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgibin/
Entity:	cgibin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgibin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1019 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/connect/>

Entity: connect/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /connect/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 1020 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/class/>

Entity: class/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /class/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

```
...
```

Issue 1021 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgishl/
Entity:	cgishl/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgishl/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1022 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgis/
Entity:	cgis/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgis/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1023 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/classes/>

Entity: classes/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /classes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1024 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cliente/>

Entity: cliente/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cliente/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1025 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/netdynamics/
Entity:	netdynamics/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netdynamics/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1026 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/clientes/
Entity:	clientes/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /clientes/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1027 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cobalt-images/>

Entity: cobalt-images/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cobalt-images/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1028 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cm/>

Entity: cm/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cm/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1029 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cmsample/
Entity:	cmsample/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cmsample/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1030 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/com2/
Entity:	com2/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /com2/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1031 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/code/>

Entity: code/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /code/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1032 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/com1/>

Entity: com1/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /com1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1033 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/communicator/
Entity:	communicator/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /communicator/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1034 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/com3/
Entity:	com3/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /com3/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1035 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/compra/>

Entity: compra/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /compra/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1036 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/pdg_cart/

Entity: pdg_cart/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /pdg_cart/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1037 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/compressed/
Entity:	compressed/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /compressed/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1038 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/compras/
Entity:	compras/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /compras/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1039 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/conecta/>

Entity: conecta/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /conecta/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1040 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/conf/>

Entity: conf/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /conf/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1041 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/config/
Entity:	config/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /config/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1042 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi/
Entity:	cgi/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1043 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/demo/>

Entity: demo/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /demo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1044 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dev/>

Entity: dev/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dev/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1045 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/webshop/
Entity:	webshop/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webshop/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1046 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/example/
Entity:	example/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /example/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1047 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/examples/>

Entity: examples/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /examples/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1048 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/whatsnew/>

Entity: whatsnew/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /whatsnew/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1049 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/excel/
Entity:	excel/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /excel/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1050 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/exe/
Entity:	exe/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /exe/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1051 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/form/>

Entity: form/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /form/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1052 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/files/>

Entity: files/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /files/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1053 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/forms/
Entity:	forms/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /forms/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1054 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/file/
Entity:	file/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /file/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1055 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/fbsd/>

Entity: fbsd/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fbsd/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1056 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/etc/>

Entity: etc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /etc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1057 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/forums/
Entity:	forums/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /forums/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1058 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/foto/
Entity:	foto/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /foto/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1059 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/formsmgr/>

Entity: formsmgr/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /formsmgr/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1060 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/.meta/>

Entity: .meta/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /.meta/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1061 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/_derived/
Entity:	_derived/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /_derived/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1062 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/fotos/
Entity:	fotos/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fotos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1063 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/fpdb/>

Entity: fpdb/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fpdb/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1064 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/fpadmin/>

Entity: fpadmin/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fpadmin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1065 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/fpsample/
Entity:	fpsample/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /fpsample/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1066 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/forum/
Entity:	forum/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /forum/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1067 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ftp/>

Entity: ftp/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ftp/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1068 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/es/>

Entity: es/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /es/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1069 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/framesets/
Entity:	framesets/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /framesets/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1070 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/errors/
Entity:	errors/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /errors/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1071 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enviamail/>

Entity: enviamail/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /enviamail/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1072 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/development/>

Entity: development/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /development/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1073 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/directory/
Entity:	directory/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /directory/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1074 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dir/
Entity:	dir/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /dir/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1075 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devel/>

Entity: devel/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /devel/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1076 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/doc1/>

Entity: doc1/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /doc1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1077 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/docs/
Entity:	docs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /docs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1078 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/doc-html/
Entity:	doc-html/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /doc-html/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1079 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/doc/>

Entity: doc/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /doc/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1080 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/webtrend/>

Entity: webtrend/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /webtrend/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1081 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/docs1/
Entity:	docs1/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /docs1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1082 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/document/
Entity:	document/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /document/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1083 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/download/>

Entity: download/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /download/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1084 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/down/>

Entity: down/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /down/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1085 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/documents/
Entity:	documents/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /documents/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1086 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/durep/
Entity:	durep/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /durep/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1087 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/downloads/>

Entity: downloads/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /downloads/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1088 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ejemplo/>

Entity: ejemplo/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ejemplo/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1089 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/easylog/
Entity:	easylog/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /easylog/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1090 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/ejemplos/
Entity:	ejemplos/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /ejemplos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1091 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/web_store/

Entity: web_store/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /web_store/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1092 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/employees/>

Entity: employees/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /employees/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1093 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/demos/
Entity:	demos/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /demos/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1094 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/envia/
Entity:	envia/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /envia/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1095 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/email/>

Entity: email/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /email/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1096 of 1190

TOC

Hidden Directory Detected

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-win/>

Entity: cgi-win/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-win/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1097 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-weddico/
Entity:	cgi-weddico/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-weddico/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1098 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-shl/
Entity:	cgi-shl/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-sh1/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1099 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC11/>

Entity: W3SVC11/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC11/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1100 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC52/>

Entity: W3SVC52/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC52/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1101 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC53/
Entity:	W3SVC53/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC53/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1102 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC55/
Entity:	W3SVC55/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC55/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1103 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC54/>

Entity: W3SVC54/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC54/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1104 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC56/>

Entity: W3SVC56/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC56/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1105 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC57/
Entity:	W3SVC57/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC57/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1106 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC58/
Entity:	W3SVC58/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC58/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1107 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC59/>

Entity: W3SVC59/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC59/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1108 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC51/>

Entity: W3SVC51/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC51/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1109 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC6/
Entity:	W3SVC6/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC6/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1110 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC60/
Entity:	W3SVC60/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC60/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1111 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC61/>

Entity: W3SVC61/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC61/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1112 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC65/>

Entity: W3SVC65/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC65/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1113 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC63/
Entity:	W3SVC63/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC63/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1114 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC64/
Entity:	W3SVC64/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC64/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1115 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC62/>

Entity: W3SVC62/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC62/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1116 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC66/>

Entity: W3SVC66/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC66/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1117 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC67/
Entity:	W3SVC67/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC67/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1118 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC69/
Entity:	W3SVC69/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC69/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1119 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC68/>

Entity: W3SVC68/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC68/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1120 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC7/>

Entity: W3SVC7/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC7/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1121 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC12/
Entity:	W3SVC12/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC12/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1122 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC49/
Entity:	W3SVC49/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC49/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1123 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC5/>

Entity: W3SVC5/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC5/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1124 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC50/>

Entity: W3SVC50/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC50/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1125 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC3/
Entity:	W3SVC3/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC3/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1126 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC30/
Entity:	W3SVC30/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC30/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1127 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC33/>

Entity: W3SVC33/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC33/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1128 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC31/>

Entity: W3SVC31/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC31/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1129 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC32/
Entity:	W3SVC32/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC32/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1130 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC10/
Entity:	W3SVC10/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC10/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1131 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC34/>

Entity: W3SVC34/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC34/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1132 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC35/>

Entity: W3SVC35/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC35/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1133 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC39/
Entity:	W3SVC39/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC39/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1134 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC37/
Entity:	W3SVC37/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC37/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1135 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC36/>

Entity: W3SVC36/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC36/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1136 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC38/>

Entity: W3SVC38/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC38/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1137 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC4/
Entity:	W3SVC4/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC4/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1138 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC41/
Entity:	W3SVC41/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC41/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1139 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC40/>

Entity: W3SVC40/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC40/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1140 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC42/>

Entity: W3SVC42/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC42/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1141 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC100/
Entity:	W3SVC100/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC100/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1142 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC44/
Entity:	W3SVC44/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC44/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1143 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC45/>

Entity: W3SVC45/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC45/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1144 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC46/>

Entity: W3SVC46/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC46/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1145 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC47/
Entity:	W3SVC47/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC47/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1146 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC43/
Entity:	W3SVC43/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC43/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1147 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC48/>

Entity: W3SVC48/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC48/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1148 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC70/>

Entity: W3SVC70/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC70/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1149 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC13/
Entity:	W3SVC13/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC13/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1150 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC71/
Entity:	W3SVC71/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC71/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1151 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC72/>

Entity: W3SVC72/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC72/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1152 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC96/>

Entity: W3SVC96/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC96/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1153 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/aspnet_client/
Entity:	aspnet_client/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /aspnet_client/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1154 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/content/
Entity:	content/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /content/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1155 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC97/>

Entity: W3SVC97/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC97/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1156 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/intranet_index/

Entity: intranet_index/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /intranet_index/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1157 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/knowledgebase/
Entity:	knowledgebase/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /knowledgebase/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1158 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/cgi-home/
Entity:	cgi-home/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-home/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1159 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/libraries/>

Entity: libraries/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /libraries/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1160 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/tasks/>

Entity: tasks/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /tasks/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1161 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/static/
Entity:	static/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /static/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1162 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC95/
Entity:	W3SVC95/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC95/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1163 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/netdynamic/>

Entity: netdynamic/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /netdynamic/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1164 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/cgi-local/>

Entity: cgi-local/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /cgi-local/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1165 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC94/
Entity:	W3SVC94/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC94/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1166 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC92/
Entity:	W3SVC92/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC92/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1167 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC73/>

Entity: W3SVC73/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC73/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1168 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC74/>

Entity: W3SVC74/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC74/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1169 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC75/
Entity:	W3SVC75/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC75/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1170 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC77/
Entity:	W3SVC77/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC77/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1171 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC76/>

Entity: W3SVC76/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC76/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1172 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC14/>

Entity: W3SVC14/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC14/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1173 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC78/
Entity:	W3SVC78/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC78/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1174 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC79/
Entity:	W3SVC79/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC79/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1175 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC8/>

Entity: W3SVC8/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC8/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1176 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC80/>

Entity: W3SVC80/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC80/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1177 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC81/
Entity:	W3SVC81/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC81/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1178 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC82/
Entity:	W3SVC82/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC82/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1179 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC83/>

Entity: W3SVC83/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC83/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1180 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC88/>

Entity: W3SVC88/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC88/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1181 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC85/
Entity:	W3SVC85/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC85/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1182 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC84/
Entity:	W3SVC84/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC84/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1183 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC15/>

Entity: W3SVC15/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC15/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1184 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC86/>

Entity: W3SVC86/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC86/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1185 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC87/
Entity:	W3SVC87/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC87/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1186 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC89/
Entity:	W3SVC89/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC89/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1187 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC9/>

Entity: W3SVC9/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC9/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
```

```
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1188 of 1190

TOC

Hidden Directory Detected

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/W3SVC90/>

Entity: W3SVC90/ (Page)

Risk: It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Causes: The web server or application server are configured in an insecure way

Fix: Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC90/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html
```

...

Issue 1189 of 1190

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC93/
Entity:	W3SVC93/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC93/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

Issue 1190 of 1190

[TOC](#)

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/W3SVC91/
Entity:	W3SVC91/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...
GET /W3SVC91/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx
Content-Length: 146
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:02:46 GMT
Content-Type: text/html

...
```

L

Missing or insecure "Content-Security-Policy" header 5

TOC

Issue 1 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```

...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Accept-Ranges: bytes
Content-Length: 462
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: "5e02ecff-1ce"
Set-Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:03:02 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>EnOS</title>
    <script type="text/javascript" src="/navigator/config/getloginstyle?"></script>
    <link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
    ...

```

Issue 2 of 5

[TOC](#)

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```

...
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f477...

```

```

Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Wed, 26 Feb 2020 01:04:24 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1331
Cache-control: private
Cache-control: no-store,no-cache
ETag: "5e55c418-533"
Set-Cookie: 9dc22c38677b96443dd332ac8e31ba30=0a1fca109465bf34beeedacee49efaa9; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html><html lang="zh-CN"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title>Envision</title>
<link rel="shortcut icon" href="/portal/envision.ico" type="image/x-icon" />
<link href="/portal/res/css/commons_124e0ac581550e321145.css" rel="stylesheet" />
<link href="/portal/res/css/homepage_21e4f52815ee33.css" rel="stylesheet" />
<script>
    window.location.pathname = window.location.pathname.replace(/homepage.html$/, '');
}</script>

```

Issue 3 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getmenus>

Entity: getmenus (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":null,"token":null,"orgCode":null,"userName":null,"locale":"en-US","isAdmin":false}

```

```

Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
Content-Type: application/json; charset=UTF-8

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 30000,
  "msg": "",
  "data": null
}
...

```

Issue 4 of 5

[TOC](#)

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/home.html>

Entity: home.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```

...
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebai; loginStyle=enos;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK

```

```

Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1135
Cache-Control: no-store,no-cache
ETag: "5e02ecff-46f"
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <title>EnOS Home</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="远景能源是最牛逼的。">
    <meta name="keywords" content="远景, 远景能源, Envision, 风机, 光伏, 物联网">
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
...

```

Issue 5 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/login.html>

Entity: login.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```

...
9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50be879a92d35e3acc94c2ba7606=4b8017b396a20ea33fb812287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Content-Length: 843
Cache-Control: no-store,no-cache
ETag: "5e02ecff-34b"
Date: Sun, 26 Apr 2020 05:09:44 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title></title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
    <div id="container">
    </div>
<script>
...

```

L

Missing or insecure "X-Content-Type-Options" header 5

TOC

Issue 1 of 5

TOC

Missing or insecure "X-Content-Type-Options" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Raw Test Response:

```

...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive

```

```

Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Accept-Ranges: bytes
Content-Length: 462
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: "5e02ecff-1ce"
Set-Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:03:02 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>EnOS</title>
    <script type="text/javascript" src="/navigator/config/getloginstyle?"></script>
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
...

```

Issue 2 of 5

TOC

Missing or insecure "X-Content-Type-Options" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Raw Test Response:

```

...
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f477...
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

```

```

Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Last-Modified: Wed, 26 Feb 2020 01:04:24 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1331
Cache-control: private
Cache-control: no-store,no-cache
ETag: "5e55c418-533"
Set-Cookie: 9dc22c38677b96443dd332ac8e31ba30=0alfca109465bf34beeedacee49efaa9; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html><html lang="zh-CN"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title>Envision</title>
<link rel="shortcut icon" href="/portal/envision.ico" type="image/x-icon" />
<link href="/portal/res/css/commons_124e0ac581550e321145.css" rel="stylesheet" />
<link href="/portal/res/css/homepage_21e4f52815ee33.css" rel="stylesheet" />
...

```

Issue 3 of 5

TOC

Missing or insecure "X-Content-Type-Options" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getmenus>

Entity: getmenus (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":null,"token":null,"orgCode":null,"userName":null,"locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
Content-Type: application/json; charset=UTF-8

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 30000,
  "msg": "",
  "data": null
}
...

```

Issue 4 of 5

[TOC](#)

Missing or insecure "X-Content-Type-Options" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/home.html>

Entity: home.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Raw Test Response:

```

...
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal; loginStyle=enos;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache

```

```

Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1135
Cache-Control: no-store,no-cache
ETag: "5e02ecff-46f"
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <title>EnOS Home</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="远景能源是最牛逼的。">
    <meta name="keywords" content="远景, 远景能源, Envision, 风机, 光伏, 物联网">
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
...

```

Issue 5 of 5

TOC

Missing or insecure "X-Content-Type-Options" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/login.html>

Entity: login.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Raw Test Response:

```

...
9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4eb1;
48a7cc09a4a7ce6e3cb4774f8375ccaa=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive

```

```

Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Content-Length: 843
Cache-Control: no-store,no-cache
ETag: "5e02ecff-34b"
Date: Sun, 26 Apr 2020 05:09:44 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title></title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
    <div id="container">
    </div>
<script>
...

```

L

Missing or insecure "X-XSS-Protection" header 5

TOC

Issue 1 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Raw Test Response:

```

...
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Accept-Ranges: bytes
Content-Length: 462
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: "5e02ecff-1ce"
Set-Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:03:02 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>EnOS</title>
    <script type="text/javascript" src="/navigator/config/getloginstyle?"></script>
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
...

```

Issue 2 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Raw Test Response:

```

...
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f477...
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

HTTP/1.1 200 OK

```

Last-Modified: Wed, 26 Feb 2020 01:04:24 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1331
Cache-control: private
Cache-control: no-store,no-cache
ETag: "5e55c418-533"
Set-Cookie: 9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html><html lang="zh-CN"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<title>EnVision</title>
<link rel="shortcut icon" href="/portal/envision.ico" type="image/x-icon" />
<link href="/portal/res/css/commons_124e0ac581550e321145.css" rel="stylesheet" />
<link href="/portal/res/css/homepage_21e4f52815ee33.css" rel="stylesheet" />
...

```

Issue 3 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getmenus>

Entity: getmenus (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":null,"token":null,"orgCode":null,"userName":null,"locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
Content-Type: application/json; charset=UTF-8

```

HTTP/1.1 200

Transfer-Encoding: chunked

```

Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 30000,
  "msg": "",
  "data": null
}
...

```

Issue 4 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/home.html>

Entity: home.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Raw Test Response:

```

...
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal; loginStyle=enos;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1135

```

```

Cache-Control: no-store,no-cache
ETag: "5e02ecff-46f"
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <title>EnOS Home</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="远景能源是最牛逼的。">
    <meta name="keywords" content="远景, 远景能源, Envision, 风机, 光伏, 物联网">
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
...

```

Issue 5 of 5

[TOC](#)

Missing or insecure "X-XSS-Protection" header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/login.html>

Entity: login.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Reasoning: AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow Cross-Site Scripting attacks

Raw Test Response:

```

...
9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Content-Length: 843

```

```

Cache-Control: no-store,no-cache
ETag: "5e02ecff-34b"
Date: Sun, 26 Apr 2020 05:09:44 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title></title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
    <div id="container">
    </div>
<script>
...

```

L

Missing or insecure Cross-Frame Scripting Defence 5

TOC

Issue 1 of 5

TOC

Missing or insecure Cross-Frame Scripting Defence

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/home.html>

Entity: home.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Frame-Options" header with DENY or SAMEORIGIN value

Reasoning: AppScan detected that the X-Frame-Options response header is missing or with insecure value, which may allow Cross-Frame Scripting attacks

Raw Test Response:

```

...
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-encoding
Content-Length: 1135
Cache-Control: no-store,no-cache
ETag: "5e02ecff-46f"
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

```

```

<!DOCTYPE html>
<html lang="en">
<head>
    <title>EnOS Home</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="远景能源是最牛逼的。">
    <meta name="keywords" content="远景, 远景能源, Envision, 风机, 光伏, 物联网">
...

```

Issue 2 of 5

TOC

Missing or insecure Cross-Frame Scripting Defence

Severity: Low

CVSS Score: 5.0

URL: https://portal-ippe1.eniot.io/devportal/sdk_download.html

Entity: sdk_download.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Frame-Options" header with DENY or SAMEORIGIN value

Reasoning: AppScan detected that the X-Frame-Options response header is missing or with insecure value, which may allow Cross-Frame Scripting attacks

Raw Test Response:

```

...
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Content-Length: 860
Cache-Control: no-store,no-cache
ETag: "5e02ecff-35c"
Date: Mon, 27 Apr 2020 10:42:05 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title>SDK下载</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
...

```

Missing or insecure Cross-Frame Scripting Defence

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-api/apimanagement.html>

Entity: apimanagement.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Frame-Options" header with DENY or SAMEORIGIN value

Reasoning: AppScan detected that the X-Frame-Options response header is missing or with insecure value, which may allow Cross-Frame Scripting attacks

Raw Test Response:

```
...
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1274
Cache-control: private
Cache-control: no-store,no-cache
ETag: "5e54fe6a-4fa"
Set-Cookie: e9dc754e254cfef59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:42:09 GMT
Content-Type: text/html

<!DOCTYPE html><html lang="zh-CN"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1"><meta http-equiv="pragma" content="no-cache"><meta http-equiv="cache-control" content="no-cache, no-store, max-age=0, private"><meta http-equiv="expires" content="0"><meta name="_csrfname_" content="#{_csrfname_}#"><meta name="_csrftoken_" content="#{_csrftoken_}#"><title></title>
<script>window.isCsrfDisabled="#{_iscsrfdisabled_}#";</script><script type="text/javascript">if(/\/\/.*\/homepage.html$/){ window.location.pathname = window.location.pathname.replace('/homepage.html$', ''); }</script><link rel="shortcut icon" href="/portal-api/envision.ico"><link href="/portal-api/res/css/vendor_cc5b223144890e94fc57.css" rel="stylesheet"><link href="/portal-api/res/css/apimanagement_cb5136c61fb5e1240f22.css" rel="stylesheet"></head><body><div id="container" style="height: 100%; min-width: 1024px;"></div><script type="text/javascript" src="/portal-api/res/vendor/index_183eb259.js"></script><script type="text/javascript" src="/portal-api/res/apimanagement/index_f20f1232.js"></script></body></html>
...
```

Missing or insecure Cross-Frame Scripting Defence

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dataide/index.html>

Entity: index.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Frame-Options" header with DENY or SAMEORIGIN value

Reasoning: AppScan detected that the X-Frame-Options response header is missing or with insecure value, which may allow Cross-Frame Scripting attacks

Raw Test Response:

```
...
Connection: keep-alive
Server: nginx
Accept-Ranges: bytes
Content-Length: 739
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: "5e54e008-2e3"
Set-Cookie: 4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:04:56 GMT
Content-Type: text/html

<!DOCTYPE HTML>
<html>
<head>
  <title>Envision Scheduler</title>
  <meta charset="utf-8" />
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
  <meta name="viewport" content="width=device-width, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no" />
...
...
```

Missing or insecure Cross-Frame Scripting Defence

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/saturnweb/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Config your server to use the "X-Frame-Options" header with DENY or SAMEORIGIN value

Reasoning: AppScan detected that the X-Frame-Options response header is missing or with insecure value, which may allow Cross-Frame Scripting attacks

Raw Test Response:

```
...
Server: nginx
Accept-Ranges: bytes
Content-Length: 603
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: W/"603-157795147900"
Set-Cookie: 4cbecc795bfb26b13bb45b228a8153ff=85cfac3476b54b38732205b5ec1113e5; path=/; HttpOnly
Date: Mon, 27 Apr 2020 10:43:31 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Space Monitor</title>
    <link rel="shortcut icon" href="/saturnweb/envision.ico"></head>
<body>
<div id="container" style='height: 100%; width:100%; min-width: 1186px;overflow: auto;'>
</div>
...
...
```

L

Missing or insecure HTTP Strict-Transport-Security Header 5

TOC

Issue 1 of 5

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal/>

Entity: (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 26 Feb 2020 01:04:24 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1331
Cache-control: private
Cache-control: no-store,no-cache
ETag: "5e55c418-533"
Set-Cookie: 9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html><html lang="zh-CN"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1"><meta http-equiv="pragma" content="no-cache"><meta http-equiv="cache-control" content="no-cache, no-store, max-age=0, private"><meta http-equiv="expires" content="0"><meta name="_csrfname_" content="#{_csrfname_}"><meta name="_csrftoken_" content="#{_csrftoken_}"><title></title>
<script>window.isCsrfDisabled="#{_iscsrfdisabled_}"</script><script type="text/javascript">if(/.*\/homepage.html$/ .test(window.location.pathname)) {
...
}
```

Issue 2 of 5

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/home.html>

Entity: home.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1135
Cache-Control: no-store,no-cache
ETag: "5e02ecff-46f"
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
    <title>EnOS Home</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    ...

```

Issue 3 of 5

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/devportal/login.html>

Entity: login.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 25 Dec 2019 05:00:47 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Content-Length: 843
Cache-Control: no-store,no-cache
ETag: "5e02ecff-34b"
Date: Sun, 26 Apr 2020 05:09:44 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title></title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <link rel="shortcut icon" href="/devportal/enos.ico"></head>
<body>
    <div id="container">
        ...
    </div>
</body>
</html>
```

Missing or insecure HTTP Strict-Transport-Security Header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-dm/tslmodel.html>

Entity: tslmodel.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 02 Mar 2020 06:51:50 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1349
Cache-control: private
Cache-control: no-store,no-cache
ETag: "5e5cad06-545"
Set-Cookie: 8142657bb99ce5d47beb6ebdabe5671b=ac0b924be4eb0af6a328b7e869e7e50c; path=/; HttpOnly
Date: Sun, 26 Apr 2020 05:12:04 GMT
Content-Type: text/html

<!DOCTYPE html><html lang="zh-CN"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1"><meta http-equiv="pragma" content="no-cache"><meta http-equiv="cache-control" content="no-cache, no-store, max-age=0, private"><meta http-equiv="expires" content="0"><meta name="_csrfname_" content="#{_csrfname_}"><meta name="_csrftoken_" content="#{_csrftoken_}"><title></title><script>window.isCsrfDisabled="#{_iscsrfdisabled_}"</script><script type="text/javascript">if(/\/.*\/homepage.html$/ .test(window.location.pathname)) {
...
}
```

Missing or insecure HTTP Strict-Transport-Security Header

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-dm/overview.html>

Entity: overview.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Causes: Insecure web application programming or configuration

Fix: Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Raw Test Response:

```
HTTP/1.1 200 OK
Last-Modified: Mon, 02 Mar 2020 06:51:50 GMT
Connection: keep-alive
Server: nginx
Pragma: no-cache
Accept-Ranges: bytes
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Length: 1349
Cache-Control: no-store,no-cache
ETag: "5e5cad06-545"
Date: Sun, 26 Apr 2020 05:12:58 GMT
Content-Type: text/html

<!DOCTYPE html><html lang="zh-CN"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1"><meta http-equiv="pragma" content="no-cache"><meta http-equiv="cache-control" content="no-cache, no-store, max-age=0, private"><meta http-equiv="expires" content="0"><meta name="csrfname" content="#_csrfname_"><meta name="_csrfname_" content="#_csrfname_#"><meta name="_csrftoken_" content="#_csrftoken_#"><title></title>
<script>window.isCsrfDisabled="#_iscsrfdisabled_#"</script><script type="text/javascript">if(/\/\/.*\/homepage.html$/_.test(window.location.pathname)) {
    window.location.pathname = window.location.pathname.replace(/homepage.html$/, '');
}</script><link rel="shortcut icon" href="/portal-dm/envision.ico"><link href="/portal-dm/res/css/commons_bcle6d5ab87d8626e54c.css" rel="stylesheet"><link href="/portal-dm/res/css/overview_6e095d...">
```

L

Oracle Log File Information Disclosure 20

TOC

Issue 1 of 20

TOC

Oracle Log File Information Disclosure

Severity:	Low
CVSS Score:	5.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/
Entity:	sqlnet.log (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	The web server or application server are configured in an insecure way
Fix:	Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3D3782011ABB6E8E8CA44DC618377405; Path=/dm-bff; HttpOnly
...
...
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3D3782011ABB6E8E8CA44DC618377405; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:02 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2s
AMSA2zkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8C7FB883251AA8A401865758348C7230; Path=/dm-bff; HttpOnly
...
...
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=8C7FB883251AA8A401865758348C7230; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:02 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
```

```
}
```

```
...
```

Issue 3 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sv2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=586FD56FA7DF183E81A5C1BB685DC2FA; Path=/dm-bff; HttpOnly
...
...
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=586FD56FA7DF183E81A5C1BB685DC2FA; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:03 GMT
Content-Type: application/json;charset=UTF-8
```

```
{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 4 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=D580ED8150BA00AA6CA30EF11D2AA1F2; Path=/dm-bff; HttpOnly

...
...
Vary: Accept-Encoding
```

```

Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSID=D580ED8150BA00AA6CA30EFL1D2AA1F2; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:03 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 5 of 20

[TOC](#)

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWOkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains

```

```

Set-Cookie: JSESSIONID=DA495EAECBCBAD5353A41F529A4C93B5; Path=/dm-bff; HttpOnly
...
...
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=DA495EAECBCBAD5353A41F529A4C93B5; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:03 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 6 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

HTTP/1.1 200

Transfer-Encoding: chunked

```

Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=0596526CC52538506ECA748D7C18F3FC; Path=/dm-bff; HttpOnly

...
...

Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=0596526CC52538506ECA748D7C18F3FC; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 04:32:04 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 7 of 20

[TOC](#)

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
```

```

Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=417552A287BB64BBFD4E308B8CFBA6F4; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:33:55 GMT
Content-Type: application/json;charset=UTF-8

{
    "msg": "Not Found; UNKONW_CODE: 404",
    "data": null,
    "subMsg": "Not Found",
    "requestId": null,
    "retCode": 404
}
...

```

Issue 8 of 20

[TOC](#)

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=014D8CC4ACDEAB34F59FCE29B62AC0B1; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:33:55 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 9 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQEJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgtqzbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx

```

```

Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=071262DD0BCC7FEB79156A63EDB52630; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:33:56 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 10 of 20

[TOC](#)

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=289CB40D52F209398C36A51A16DB7ED9; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:33:57 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 11 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive

```

```

Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=2C27DCA2F654150BFADD73936ABC3B1; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:33:57 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 12 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/>

Entity: sq|net.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWOkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding

```

```

Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E44318493E1C35CF5D7F47FBE6CAC7F5; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:33:58 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 13 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

```

HTTP/1.1 200

```

Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=E8BA17FC05ED77DDA4F6FE8EF3035428; Path=/dm-bff; HttpOnly
Date: Tue, 28 April 2020 04:33:58 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 14 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2zkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
```

```

Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=A30873C3DA0AB418BFF03626E031EA28; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:33:59 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 15 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUusbYesMFjMvbaK5FCJgTqbZLsJcXjfjyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=818CBD87805DFD03D97B511E29C7EC3C; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:00 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 16 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:

```

```

{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=08DFBD46B0C048D8F5A11BB8E530F3EB; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:34:01 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Issue 17 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json

```

```

Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 129
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/sqlnet.log",
  "data": null
}
...

```

Issue 18 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx

```

```

Content-Length: 129
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/sqlnet.trc",
  "data": null
}
...

```

Issue 19 of 20

[TOC](#)

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: sqlnet.log (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkWUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWOkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 133
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:29 GMT

```

```

Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/sqlnet.log",
  "data": null
}
...

```

Issue 20 of 20

TOC

Oracle Log File Information Disclosure

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: sqlnet.trc (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: The web server or application server are configured in an insecure way

Fix: Turn off tracing, restrict access to the log file, or remove it.

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 133
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  ...
}
```

```
"subMsg": "No handler found for GET /enos-app-webservice/app/sqlnet.trc",
"data": null
}
...
}
```

L

Potential Order Information Found 6

TOC

Issue 1 of 6

TOC

Potential Order Information Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: order.txt (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Do not keep sensitive information in easy to guess file names, or restrict access to them

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/order.t  
xt HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows  
NT 6.1; WOW64; Trident/7.0; rv:1
```

```

1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5ee; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; 0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bfff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgzLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0

```

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 128
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:35
GMT
Content-Type: application/json; charset=UTF-8

```

```

...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:35
GMT
Content-Type: application/json; charset=UTF-8

```

```

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/order.txt",
  "data": null
}
...

```

```
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

Issue 2 of 6

TOC

Potential Order Information Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: order.htm (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Do not keep sensitive information in easy to guess file names, or restrict access to them

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/order.h  
tm HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows  
NT 6.1; WOW64; Trident/7.0; rv:1  
1.0) like Gecko  
Referer: https://portal-ippe1.en  
iot.io/portal-api/apimanagement.  
html?__ts__=1587876282201&&  
Cookie: __gat_gtag_UA_110195466_1  
=1; __ga=GA1.2.610865653.15878762  
13; lang=en-US; __gid=GA1.2.17117  
93339.1587876213; locale=en-US;  
__gat_gtag_UA_110195466_2=1; 203d  
16c4c34b4d73cbe8d8ad13e35fee=828  
c5a658f7338cd2e39be4d51cfbd5e; 5  
0eaa23de448b610a687b0e42bab51f=  
0d269ec330206b966f847c4eaaf00be  
; 0b68a657f24d12cce48ed4247bcc86  
d0=352d622976494a7eae62da3419c0f  
1c4; 33296aa8a77f7e6d9209cc11b28  
2bf5c=29583daf49f8c47f70937b3e64  
64d67f; 4bf685a1f608acedeac059c  
b0cf3236=30c82d07997c54b264a0d1b  
c9c26fdbf; global_id=IAM_S_wcUH9  
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A  
fAucCynec9DnMJj9DddBfhksUqcSpZwL  
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT  
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814  
2657bb99ce5d47beb6ebdabe5671b=72  
49efda1c32d9b86f368cf91fd8b7de;  
42dea464b09cd2371e151241b10bd05b  
=bb630ba83d88f1a7ac7eaf4447f0a12  
6; loginStyle=enos; 061609d44b39  
8ee03ad76311f6534dd7=580fffb56a53  
d3823b619922623f730d5; 9dc22c386  
77b96443dd332ac8e31ba30=oalfca10  
9465bf34beeedacee49efaa9; 837cbf  
2c4037d0ea9e37c5df2937b9c2=a7251  
de0c2fdcf61f683ce3be3d9cd9e; JSE  
SSIONID=6193E8AF84785D4A135BCB96  
675B31C3; e9dc754e254cfe59b74a9c  
4131b3c49a=c856bc06c55877b427547  
2696a7fe613; 54e50ebe879a92d35e3  
acc94c2ba7606=4b8017b396a20ea33f  
8b12287962fe46; 2913cd5e4f9e0128  
15fa8ec11b6f36ea=6942da86168ec38  
34e85ca4ff9374f1d; 149118e82bd3d  
b81f33f21b97080c04f=30f016a0a0a5  
958add68aac97cce8796; 3fe8ef195d  
77afaeca93685b8f336acc=7531cac53  
1eb2b86ee84ca46c3920ce4; 48a7cc0  
9a4a7ce6e3cb4774f8375cca6=836861  
ced028279968e30876217a4500  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

```
...  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS  
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200  
Connection: keep-alive  
Server: nginx  
Content-Length: 128  
Cache-control: private  
Content-Disposition: inline;file  
name=f.txt  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fce=d41361c030cb24ef9ed  
fe1e31d899a31; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:03:35  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

```
...  
...  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fce=d41361c030cb24ef9ed  
fe1e31d899a31; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:03:35  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

```
{  
  "requestId": null,  
  "status": 404,  
  "msg": "not.exist",  
  "subMsg": "No handler found for  
GET /enos-app-webservice/order.h  
tm",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 3 of 6

TOC

Potential Order Information Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: order.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Do not keep sensitive information in easy to guess file names, or restrict access to them

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/order.h  
tml HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows  
NT 6.1; WOW64; Trident/7.0; rv:1  
1.0) like Gecko  
Referer: https://portal-ippe1.en  
iot.io/portal-api/apimanagement.  
html?__ts__=1587876282201&&  
Cookie: __gat_gtag_UA_110195466_1  
=1; __ga=GA1.2.610865653.15878762  
13; lang=en-US; __gid=GA1.2.17117  
93339.1587876213; locale=en-US;  
__gat_gtag_UA_110195466_2=1; 203d  
16c4c34b4d73cbe8d8ad13e35fee=828  
c5a658f7338cd2e39be4d51cfbd5e; 5  
0eaa23de448b610a687b0e42bab51f=  
0d269ec330206b966f847c4eaaf00be  
; 0b68a657f24d12cce48ed4247bcc86  
d0=352d622976494a7eae62da3419c0f  
1c4; 33296aa8a77f7e6d9209cc11b28  
2bf5c=29583daf49f8c47f70937b3e64  
64d67f; 4bf685a1f608acedeac059c  
b0cf3236=30c82d07997c54b264a0d1b  
c9c26fdbf; global_id=IAM_S_wcUH9  
dpScURgLYbzG2qFst9uzW9FZ3CADv5A  
fAucCynec9DnMJj9DddBfhksUqcSpZwL  
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT  
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814  
2657bb99ce5d47beb6ebdabe5671b=72  
49efda1c32d9b86f368cf91fd8b7de;  
42dea464b09cd2371e151241b10bd05b  
=bb630ba83d88f1a7ac7eaf4447f0a12  
6; loginStyle=enos; 061609d44b39  
8ee03ad76311f6534dd7=580fffb56a53  
d3823b619922623f730d5; 9dc22c386  
77b96443dd332ac8e31ba30=oalfca10  
9465bf34beeedacee49efaa9; 837cbf  
2c4037d0ea9e37c5df2937b9c2=a7251  
de0c2fdcf61f683ce3be3d9cd9e; JSE  
SSIONID=6193E8AF84785D4A135BCB96  
675B31C3; e9dc754e254cfe59b74a9c  
4131b3c49a=c856bc06c55877b427547  
2696a7fe613; 54e50ebe879a92d35e3  
acc94c2ba7606=4b8017b396a20ea33f  
8b12287962fe46; 2913cd5e4f9e0128  
15fa8ec11b6f36ea=6942da86168ec38  
34e85ca4ff9374f1d; 149118e82bd3d  
b81f33f21b97080c04f=30f016a0a0a5  
958add68aac97cce8796; 3fe8ef195d  
77afaeca93685b8f336acc=7531cac53  
1eb2b86ee84ca46c3920ce4; 48a7cc0  
9a4a7ce6e3cb4774f8375cca6=836861  
ced028279968e30876217a4500  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

```
...  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS  
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200  
Connection: keep-alive  
Server: nginx  
Content-Length: 129  
Cache-control: private  
Content-Disposition: inline;file  
name=f.txt  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fece=45b7075c35491e93b05  
a563912b65508; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:03:35  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

```
...  
...  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fece=45b7075c35491e93b05  
a563912b65508; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:03:35  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

```
{  
  "requestId": null,  
  "status": 404,  
  "msg": "not.exist",  
  "subMsg": "No handler found for  
GET /enos-app-webservice/order.h  
tml",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 4 of 6

TOC

Potential Order Information Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: order.txt (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Do not keep sensitive information in easy to guess file names, or restrict access to them

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

GET /enos-app-webservice/app/order.txt HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1

```

1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5ee; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; 0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bfff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgzLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0

```

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 132
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:35
GMT
Content-Type: application/json; charset=UTF-8

```

```

...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:35
GMT
Content-Type: application/json; charset=UTF-8

```

```

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/order.txt",
  "data": null
}
...

```

```
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

Issue 5 of 6

TOC

Potential Order Information Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: order.htm (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Do not keep sensitive information in easy to guess file names, or restrict access to them

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/order.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYBzhG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfc109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 132
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:36
GMT
Content-Type: application/json; charset=UTF-8
```

```
...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:36
GMT
Content-Type: application/json; charset=UTF-8
```

```
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/app/order.htm",}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 6 of 6

TOC

Potential Order Information Found

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: order.html (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Do not keep sensitive information in easy to guess file names, or restrict access to them

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/order.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYBzhG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfc109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 133
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:36
GMT
Content-Type: application/json; charset=UTF-8
```

```
...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:03:36
GMT
Content-Type: application/json; charset=UTF-8
```

```
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/order.html",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 1 of 52

TOC

Query Parameter in SSL Request**Severity:** Low**CVSS Score:** 5.0**URL:** <https://portal-ippe1.eniot.io/dm-bff/logicasset/search>**Entity:** pageNo (Parameter)**Risk:** It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted**Causes:** Query parameters were passed over SSL, and may contain sensitive information**Fix:** Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
POST /dm-bff/logicasset/search?pageNo=1&pageSize=10&expression= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/logicasset.html?__ts__=1587876217997&&
Cookie: JSESSIONID=9E6B2903FDD0748A5EFF2BE8D407DF8;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcxjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll>

Entity: currentPage (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/rest/product/queryProductListAll?currentPage=1&pageSize=200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&&
Cookie: JSESSIONID=9E6E2903FFDD0748A5EFF2BE8D407F8;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZlsJcxJfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebab5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/search>

Entity: pageSize (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
POST /dm-bff/logicasset/search?pageNo=1&pageSize=10&expression= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/logicasset.html?__ts__=1587876217997&&
Cookie: JSESSIONID=9E6E2903FFDD0748A5EFF2BE8D407DF8;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083bd5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7acf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics>

Entity: now (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/overview/queryStatistics?productKey=all&now=1587876217305&zero=1587798000000 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&&
Cookie: JSESSIONID=9E6E2903FFDD0748A5EFF2BE8D407DF8;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=83e861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics>

Entity: zero (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/overview/queryStatistics?productKey=all&now=1587876217305&zero=1587798000000 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&&
Cookie: JSESSIONID=9E6E2903FFDD0748A5EFF2BE8D407DF8;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7acf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=83e8661ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics>

Entity: productKey (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/overview/queryStatistics?productKey=all&now=1587876217305&zero=1587798000000 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&&
Cookie: JSESSIONID=9E6E2903FFDD0748A5EFF2BE8D407DF8;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7acf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/search>

Entity: expression (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
POST /dm-bff/logicasset/search?pageNo=1&pageSize=10&expression= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/logicasset.html?__ts__=1587876217997&&
Cookie: JSESSIONID=9E6E2903FFDD0748A5EFF2BE8D407DF8;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083bd45108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7acf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: service (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /audit/search?
offset=0&limit=10&startTime=1587271459563&endTime=1587876259563&query=%7B%22userName%22%3A%22%22%
7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33fb8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info>

Entity: subject_id (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam-web/organization/security/setting/info?subject_type=org&subject_id=o15790616298731
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/adduser.html?
_ts_=1587876405578&page=1&userType=0&
Cookie: JSESSIONID=F777866680F7050A40936778BDEA71B9;
837cbf2c4037d0ea9e37c5df2937b9c2=4bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce63cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbaK5
FCJgTqpbZLsJckJfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdbae5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50ea23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info>

Entity: subject_type (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam-web/organization/security/setting/info?subject_type=org&subject_id=o15790616298731
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/adduser.html?
_ts_=1587876405578&page=1&userType=0&
Cookie: JSESSIONID=F777866680F7050A40936778BDEA71B9;
837cbf2c4037d0ea9e37c5df2937b9c2=4bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce63cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11bf36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbaK5
FCJgTqpbZLsJckJfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdbae5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50ea23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/config/docurl>

Entity: key (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /portal-web/config/docurl?key=devcenter& HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal/
Cookie: JSESSIONID=A05E8D4A4D2C8B5BF10B302F1CEFA0FA;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebdabe5671b=7249efd1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0ce59203b8da772f33eeff2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254fce59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getoldmenus>

Entity: lang (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /navigator/navigator/getoldmenus?lang=en-US HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=da7250dd9604ecff7581423749e426e4;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Accept: */*
...
...
```

Issue 13 of 52

TOC

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: query->"userName" (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over

SSL.

Original Request

```
GET /audit/search?
offset=0&limit=10&startTime=1587271459563&endTime=1587876259563&query=%7B%22userName%22%3A%22%22%
7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; _gat_gtag_UA_110195466_2=1;
_ga=GA1.2.610865653.1587876213; _gat_gtag_UA_110195466_1=1;
203d16c4c34b4d73cbe8d8ad1e3e35fee=828c5a658f7338cd2e39be4d51cfbdee;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
8142657bb99ce5d47beb6ebab65671b=7249efda1c32d9b86f368cf91fd8b7de;
global_id=IAM_S_zvGC2jdEYl6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSeYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500; loginStyle=enos
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEYl6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSeYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
Content-Type: application/json;charset=UTF-8
```

Issue 14 of 52

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/navigator/navigator/getsdks>

Entity: lang (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /navigator/navigator/getsdks?lang=en-US HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/devportal/sdk_download.html?__ts__=1587876280536&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
```

```

42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab851f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeccfc0d4319ff8148138482f0f24
...

```

Issue 15 of 52

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: searchValue (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?_ts_=1587876338578&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33fb812287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;

```

```
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
```

Issue 16 of 52

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: orderBy (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedace49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168e3c3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbfUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSeYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AuwUZ;
8142657bb9ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.61086563.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: type (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET
/ide/flow/list?type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUUsbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebda5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db1f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254fce59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: owner (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332aca8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6bdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0d0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: cycle (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33fb8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6bdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0d0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: pageCount (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efd1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0d0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: isAsc (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332aca8e31ba30=0a1fc109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6bdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0d0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: pageNum (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332aca8e31ba30=0a1fc109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6bdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0d0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/saturn/batch/ws/v1/cluster/apps>

Entity: user (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /saturn/batch/ws/v1/cluster/apps?user=data_o15790616298731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/saturnweb/?_ts_=1587876377813&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50abe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc1b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/flow/list>

Entity: status (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/flow/list?
type=1&pageNum=1&pageCount=10&searchValue=&owner=&cycle=&status=&orderBy=update_time&isAsc=false
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876338578&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0d0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/resmgnt/list/ou/service>

Entity: serviceName (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /portal-web/resmgnt/list/ou/service?serviceName=dataexplorer HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-data/dataexplore.html?__ts__=1587876379783&&
Cookie: JSESSIONID=A05E8D4A4D2C8B5BF10B302F1CEFA0FA;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0ce59203b8da772f33eeff2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad7631f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254fce59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/datasource/pagingInfo>

Entity: dataSourceName (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/datasource/pagingInfo?dataSourceType=&dataSourceName= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/ide/index.html?__ts__=1587876381294&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c3867b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4FbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc1b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/dataex/list>

Entity: Old (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /portal-web/dataex/list?ouId=o15790616298731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-data/dataexplore.html?__ts__=1587876379783&&
Cookie: JSESSIONID=A05E8D4A4D2C8B5BF10B302F1CEFA0FA;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35eacc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebab5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0fce59203b8da772f33eeff2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad7631f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/datasource/pagingInfo>

Entity: dataSourceType (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/datasource/pagingInfo?dataSourceType=&dataSourceName= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/ide/index.html?__ts__=1587876381294&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c3867b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4FbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc1b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/datasource/query>

Entity: dataSourceName (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/datasource/query?pageNum=1&dataSourceType=&dataSourceName= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876381294&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4FbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc1b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/datasource/query>

Entity: pageNum (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/datasource/query?pageNum=1&dataSourceType=&dataSourceName= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876381294&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50abe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4FbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc1b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/transfer/info>

Entity: org_id (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam-web/organization/transfer/info?org_id=o15790616298731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/orginfo.html?__ts__=1587876401455&&
Cookie: JSESSIONID=F77786680F7050A40936778BDEA71B9;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedace49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTs2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0fce59203b8da772f33eeff2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad7631f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/ide/datasource/query>

Entity: dataSourceType (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /ide/datasource/query?pageNum=1&dataSourceType=&dataSourceName= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/dataide/index.html?__ts__=1587876381294&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4FbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc1b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 7d1ffb2f2f004d3aac9506740a8
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/info>

Entity: id (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam-web/organization/info?id=o15790616298731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/orginfo.html?__ts__=1587876401455&&
Cookie: JSESSIONID=F77786680F7050A40936778BDEA71B9;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35eacc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedace49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=83e861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0fce59203b8da772f33eeff2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad7631f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254fce59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues>

Entity: productKey (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/overview/getMetricValues?productKey=all&timePeriod=hour&currentTs=1587876217305
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&&
Cookie: JSESSIONID=9E6B2903FDD0748A5EFF2BE8D407DF8;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam/api/v2/authorization/listBySubject>

Entity: subjectType (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET
/iam/api/v2/authorization/listBySubject?subjectType=USER&resourceTypes=menu%2Cmenu_v1&subjectId=u
15877199768991&organizationId=o15790616298731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal/
Cookie: JSESSIONID=6ADB00E83B2911C8EF16FB0377D1892;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce61ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbaK5
FCJgTqbZLsJckJfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdbabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce4bed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50ea23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam/api/v2/authorization/listBySubject>

Entity: resourceTypes (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam/api/v2/authorization/listBySubject?
subjectType=USER&resourceTypes=menu%2Cmenu_v1&subjectId=u15877199768991&organizationId=o157906162
98731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal/
Cookie: JSESSIONID=6ADB00E83B2911C8FEF16FB0377D1892;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce61ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbaK5
FCJgTqpbZLsJcKjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdbabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce4bed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50ea23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll>

Entity: pageSize (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/rest/product/queryProductListAll?currentPage=1&pageSize=200 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&
Cookie: JSESSIONID=9E6E2903FFDD0748A5EFF2BE8D407DF8;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7acf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebabe5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues>

Entity: currentTs (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/overview/getMetricValues?productKey=all&timePeriod=hour&currentTs=1587876217305
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&&
Cookie: JSESSIONID=9E6B2903FDD0748A5EFF2BE8D407DF8;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues>

Entity: timePeriod (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /dm-bff/overview/getMetricValues?productKey=all&timePeriod=hour&currentTs=1587876217305
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/overview.html?__ts__=1587876216889&&
Cookie: JSESSIONID=9E6B2903FDD0748A5EFF2BE8D407DF8;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: startTime (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /audit/search?
offset=0&limit=10&startTime=1587271459563&endTime=1587876259563&query=%7B%22userName%22%3A%22%22%
7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: endTime (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /audit/search?
offset=0&limit=10&startTime=1587271459563&endTime=1587876259563&query=%7B%22userName%22%3A%22%22%
7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: offset (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET
/audit/search?offset=0&limit=10&startTime=1587271459563&endTime=1587876259563&query=%7B%22userName%22%3A%22%22%7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371le151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcxJfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: limit (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /audit/search?
offset=0&limit=10&startTime=1587271459563&endTime=1587876259563&query=%7B%22userName%22%3A%22%22%
7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: query (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /audit/search?
offset=0&limit=10&startTime=1587271459563&endTime=1587876259563&query=%7B%22userName%22%3A%22%22%
7D&service=iam HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587876259198&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33fb8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTgbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f
Connection: keep-alive
Host: portal-ippe1.eniot.io
...
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam/api/v2/authorization/listBySubject>

Entity: organizationId (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam/api/v2/authorization/listBySubject?
subjectType=USER&resourceTypes=menu%2Cmenu_v1&subjectId=u15877199768991&organizationId=o157906162
98731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal/
Cookie: JSESSIONID=6ADB00E83B2911C8FEF16FB0377D1892;
837cbf2c4037d0ea9e37c5df2937b9c2=4bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
48a7cc09a4a7ce61ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbaK5
FCJgTqpbZLsJcKjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdbabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce4bed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50ea23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam/api/v2/authorization/listBySubject>

Entity: subjectId (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam/api/v2/authorization/listBySubject?
subjectType=USER&resourceTypes=menu%2Cmenu_v1&subjectId=u15877199768991&organizationId=o157906162
98731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal/
Cookie: JSESSIONID=6ADB00E83B2911C8FEF16FB0377D1892;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce61ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbaK5
FCJgTqpbZLsJckJfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdbae5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce4bed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50ea23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bfff685a1f608acedeac059cb0cf3236=fd0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeecfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/portal-web/config/help>

Entity: keys (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /portal-web/config/help?keys=about& HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal/
Cookie: JSESSIONID=A05E8D4A4D2C8B5BF10B302F1CEFA0FA;
837cf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
54e50ebe879a92d35eacc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0afca109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvbaK5
FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb9ce5d47beb6ebda5671b=7249efdal1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0ce59203b8da772f33eeff2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad7631f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254fce59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/ldapSource/validateLinkName>

Entity: link_name (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam-web/ldapSource/validateLinkName?link_name**CONFIDENTIAL 1** HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/addLdapService.html?
_ts_=1587876442467&oId=o15790616298731&uId=u15877199768991&
Cookie: JSESSIONID=F777866680F705040936778BDEA71B9;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFrw3sV2SAMSAgzkwUSbYesMFjMvbaK5
FCJgTgbZlsJcxJfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ;
8142657bb99ce5d47beb6ebdabe5671b=7249efdalc32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
_ga=GA1.2.610865653.1587876213; _gid=GA1.2.1711793339.1587876213;
0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f;
JSESSIONID=0FB74735B8C7521CE8F3BD61C508D8ED;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
33296aa8a77f7e6d9209cc11b282bf5c=7e1ee36d5b3f36c7e4e26f2a182f6661;
3fe8ef195d77afacea93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
4bff685a1f608acedeac059cb0cf3236=f0d0ce59203b8da772f33eef2f6b6207d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
061609d44b398ee03ad76311f6534dd7=4caebeccfc0d4319ff8148138482f0f24;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b
...
```

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/security/mfa/status>

Entity: org_id (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...
GET /iam-web/security/mfa/status?user_id=u15877199768991&org_id=o15790616298731 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.3578.98 Safari/537.36
Referer: https://portal-ippe1.eniot.io/devportal/login.html
Cookie: JSESSIONID=4784D83521ADBA5A791A92506016A96E;
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
9dc22c38677b96443dd332ac8e31ba30=0a1fcac109465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_EsVzLfTwBTkCmgfJa7uUQEjC69wzfeClfVnrz3jqCdts5FVPAuZKynVK8VvbnZhbQcnNxkH9U6RCH3byV
XWJFbnJdD6vHndjkXQ7zt7a8VbWWTeewJfVcXTBYJZB2mM9
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US

...
```

Issue 50 of 52

TOC

Query Parameter in SSL Request

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/security/mfa/status>

Entity: user_id (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...  
GET /iam-web/security/mfa/status?user_id=u15877199768991&org_id=o15790616298731 HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/71.0.3578.98 Safari/537.36  
Referer: https://portal-ippe1.eniot.io/devportal/login.html  
Cookie: JSESSIONID=47F4D83521ADBA5A791A92506016A96E;  
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;  
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;  
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;  
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;  
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;  
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;  
lang=en-US;  
global_id=IAM_S_EsVzLffTwBTkCmgfJa7uUQEjC69wzfeCLfVnrz3jqCdt5FVPAPuZKynVK8VvbnZhbQcnNXkH9U6RCH3byV  
XWJFbnJdD6vHndjkXQ7zt7a8VbWWTewnJfVcXTBYJZBzmM9  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
locale: en-US  
...
```

Issue 51 of 52

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/ota/queryFws>

Entity: productKey (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```
...  
GET /dm-bff/ota/queryFws?productKey= HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/71.0.3578.98 Safari/537.36  
Referer: https://portal-ippe1.eniot.io/portal-dm/firmware.html?__ts__=1587877129478&&  
Cookie: JSESSIONID=37A90DCE9218B6BD0AE3CEC1CE0B7917;  
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;  
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;  
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;  
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;  
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;  
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
```

```

lang=en-US;
global_id=IAM_S_EsVzLfTwBTkCmgfJa7uUQEjC69wzfeCLfVnrz3jqCdts5FVPAuZKynVK8VvbnZhbQcnNXkH9U6RCH3byV
XWJFbnJdD6vHndjkXQ7zt7a8VbWWTewnJfVcXTBYJZBzmM9;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763;
_ga=GA1.2.1155129914.1587877118; _gid=GA1.2.1178620164.1587877118; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1
Connection: keep-alive
Host: portal-ippe1.eniot.io

...

```

Issue 52 of 52

TOC

Query Parameter in SSL Request

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/duration>

Entity: serviceName (Parameter)

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Original Request

```

...
GET /audit/duration?serviceName=audit-service HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.3578.98 Safari/537.36
Referer: https://portal-ippe1.eniot.io/portal-iam/actionTrail.html?__ts__=1587877132445&&
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; locale=en-US; loginStyle=enos;
lang=en-US;
global_id=IAM_S_EsVzLfTwBTkCmgfJa7uUQEjC69wzfeCLfVnrz3jqCdts5FVPAuZKynVK8VvbnZhbQcnNXkH9U6RCH3byV
XWJFbnJdD6vHndjkXQ7zt7a8VbWWTewnJfVcXTBYJZBzmM9;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763;
_ga=GA1.2.1155129914.1587877118; _gid=GA1.2.1178620164.1587877118; _gat_gtag_UA_110195466_1=1;
_gat_gtag_UA_110195466_2=1; 0b68a657f24d12cce48ed4247bcc86d0=a901f52b9d65f07e999e9696f586eb7f
Connection: keep-alive
Host: portal-ippe1.eniot.io

...

```

Issue 1 of 20

TOC

Temporary File Download**Severity:** Low**CVSS Score:** 5.0**URL:** <https://portal-ippe1.eniot.io/navigator/navigator/getoldmenus>**Entity:** getoldmenus (Page)**Risk:** It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords**Causes:** Temporary files were left in production environment**Fix:** Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Referer: https://portal-ippe1.eniot.io/
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; loginStyle=enos
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Accept: /*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Sun, 26 Apr 2020 05:09:43 GMT
Content-Type: application/json; charset=UTF-8

{
  "code": 30000,
  "msg": "",
  "data": null
}
...
```

Issue 2 of 20

TOC

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/security/setting/info>

Entity: info (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Referer: https://portal-ippe1.eniot.io/
Cookie: 837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; loginStyle=enos
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Accept: /*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 52
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; path=/; HttpOnly
Date: Tue, 28 Apr 2020 05:53:07 GMT
Content-Type: application/json

{
  "status": 51,
  "message": "User login session expired"
}
...
```

Issue 3 of 20

TOC

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/session/set>

Entity: set (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: The test tried to retrieve a source code file. The fact that the response did not yield an error, and contained non-HTML contents, indicates that the source code retrieval succeeded.

Raw Test Response:

```
...
AM_S_RKH5UeYn6zUEwYXzTcCdawBjpnjdyctjq6G86PU8HyC9VqYy5ptJpxQQphpsxkayV2BkTuEkhUEqQjw6GmwTgEpqKaCt
VcCgWLVZTJxh9scr7YkesegFdJCJBE4NXU7U;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Origin: https://portal-ippe1.eniot.io
Accept: /*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "fail": true,
  "success": false
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/v1/encrypt/publicKey>

Entity: publicKey (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
54e50eb879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9; loginStyle=enos;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Accept: /*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 52
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:32 GMT
Content-Type: application/json

{
  "status": 51,
  "message": "User login session expired"
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/user/authorization/check>

Entity: check (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: The test tried to retrieve a source code file. The fact that the response did not yield an error, and contained non-HTML contents, indicates that the source code retrieval succeeded.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:48:26 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "fail": true,
  "success": false
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/getSystemOU>

Entity: getSystemOU (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C4C2932D0CD8BCC8D38ECD4FCC665B85; Path=/dm-bff; HttpOnly
...
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C4C2932D0CD8BCC8D38ECD4FCC665B85; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 05:59:54 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/model/queryTSLModelSummaryByOU>

Entity: queryTSLModelSummaryByOU (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Cache-control: private

...
...

Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=F2C55103D5216C68117CEC785FFCF590; Path=/dm-bff; HttpOnly
Set-Cookie: 203d16c4c34b4d73cbe8d8ad13e35fee=052e1d9db6d2357e2ad4d7072abe7763; path=/; HttpOnly
Date: Tue, 28 Apr 2020 05:59:54 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
```

```
        "retCode": 404
    }
    ...
}
```

Issue 8 of 20

TOC

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll>

Entity: queryProductListAll (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=1137566B0CBE055E4607F6FE35572CA1; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 05:59:55 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics>

Entity: queryStatistics (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=B3DE615284F7FD8728E85C8E577C270; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 05:59:57 GMT
Content-Type: application/json; charset=UTF-8

{
  "msg": "Not Found; UNKONW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...

```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues>

Entity: getMetricValues (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=EE3DAB1B7276455FD641DAF6728F2CD2; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 06:00:29 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/search>

Entity: search (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfkyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=BC01F262CBDB059A3B20024DB6DC4F44; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 06:00:32 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/simulator/queryMockDevices>

Entity: queryMockDevices (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt

...
...

Server: nginx
Access-Control-Allow-Origin: https://portal-ippe1.eniot.io
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=4BDCC72FDBE65A662B2C8EF80E37D3E; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 06:00:33 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
}
```

```
    "retCode": 404
}
...
}
```

Issue 13 of 20

TOC

Temporary File Download

Severity: **Low**

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/dm-bff/inte/queryChannels>

Entity: queryChannels (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=33902724E7B087EB25CFEE5ED395CDB0; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 06:00:33 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Not Found; UNKNOW_CODE: 404",
  "data": null,
  "subMsg": "Not Found",
  "requestId": null,
  "retCode": 404
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/audit/search>

Entity: search (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: The test tried to retrieve a source code file. The fact that the response did not yield an error, and contained non-HTML contents, indicates that the source code retrieval succeeded.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSAgzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=285BD1AF9D2DD28167C59F06BA28EA2F; Path=/; HttpOnly
...
...
Vary: Accept-Encoding
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=285BD1AF9D2DD28167C59F06BA28EA2F; Path=/; HttpOnly
Set-Cookie: 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:13:19 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Success",
  "data": {
    "total": 872,
    "offset": 0,
```

```
"list": [
{
  "userIdentity": {
    "userId": "u15877199768991",
    "email": null,
    ...
}
```

Issue 15 of 20

TOC

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/user/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "success": false,
  "fail": true
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 132
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:14:57 GMT
Content-Type: application/json;charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/list.lzma",
  "data": null
}
...
```

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/policy/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

GET /iam-web/policy/list.lzma HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/serviceaccount.html?__ts__=1587876399694&&
Cookie: lang=en-US; locale=en-US; _ga=GA1.2.610865653.1587876213; JSESSIONID=8DAB31BE074803E24AF4DCD7F918FB4B;
_d1d736358848df1792c8a926c47ba864=699d293f17bdc607d65f688e3d8d7cec;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4;
33296aa8a77f7e6d9209cc1b282bf5c=29583daf49f8c47f70937b3e6464d67f;
4bff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf;
global_id=IAM_S_CEZZQVH3zteSzxYheDkT6MmRBYXdymjX5PPQaSaeEPTQewSqnpyBygSWDXmu5hbxRgBEU4mhT72ey5Luc
SkDZsEWL2mJsuFNgWYJR8QUMB8RM64WV4t8E5bPKTNZQSfr;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal; loginStyle=enos;
9dc22c38677b96443dd332ac8e31ba30=0a1fc1a09465bf34beeedacee49efaa9;
JSESSIONID=A5B04F75F3ACBC3EAE224BF0FE530969;
e9dc754e254cfe9b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
203d16c4c34b4d473cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbddee;
3fe8ef195d77afaea93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
e6c982c2af8fea3b4ddd995510bccce=3c55ddb8c6c72bbec3a8d6c3cd7c40e;
7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10df3e083b4d5108ce32;
061609d44b398ee03ad76311f6534dd7=580ffb56a53d3823b619922623f730d5;
4cbcbe795fb26b13bb45b228a8153ff=5b06b0f4b34a370e60d6ba4458d079a7;
48a7cc09a4a7ce6e3cb4774f8375cca=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6FwwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSAgzkwUsbYesMFjMvbak5FCJgTqbZLsCjxjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains

```

```

Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json; charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "success": false,
  "fail": true
}

```

Issue 18 of 20

[TOC](#)

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/appInstance/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
Host: portal-ippe1.eniot.io
eos_auth:
{"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ","orgCode":"o157906162987
31","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json; charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "success": false,
  "fail": true
}

```

```
}
```

```
...
```

Issue 19 of 20

TOC

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/organization/resource/list>

Entity: list (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Raw Test Response:

```
GET /iam-web/organization/resource/list.lzma HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-iam/addpolicy.html?
__ts__=1587876415042&isEdit=false&oId=o15790616298731&uId=u15877199768991&
Cookie: __gclid=GAI.2.1.21711793339.1587876213; __ga=GAI.2.610865653.1587876213; locale=en-US; lang=en-US; __gat_gtag_UA_110195466_1=1; __gat_gtag_UA_110195466_2=1;
JSESSIONID=8DAB31BE074803E24AF4CD7F918FB4B;
e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613;
33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f;
061609d44b398ee03ad7631f6534dd7=580fffb56a53d3823b61922623f730d5;
4cbbec795bf26b13bb45b228a1853ff=5b06b0f4b3a4370e60d6ba4458d079a7;
48a7cc09a4a7ce6e3cb4774f8375cc46=836861ced028279968e30876217a4500;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4eba1;
149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796;
d1d736358848df1792c8a926c47ba864=699d293f17bcd607d65f688e3d8d7cec; loginStyle=enos;
0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
7d1ffb2f004d3ac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31;
e6c982c2af8fea3b4ddd995510bccce=3c55ddb8c6c72bbec3a8d6c3cd7c40e;
JSESSIONID=A5B04F75F3ACBC3EAE224BF0FE530969;
3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32;
4bfff685alf608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf;
9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedace49efaa9;
50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaafb00be;
global_id=IAM_S_CEZJQVH3zteSzxXyheDkT6MmRBYxdYmjX5PPQaSaeEPTQewSqnPBygSWDXmu5hbxBgBEU4mhT72ey5Luc
SkDZsEwLZmJsuFnNgWYJR8QUMB8RM64WV4t8E5bPktNZQSfr;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NhAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
```

```

Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json;charset=UTF-8

{
  "status": 500,
  "message": "system error",
  "data": null,
  "success": false,
  "fail": true
}

```

Issue 20 of 20

[TOC](#)

Temporary File Download

Severity: Low

CVSS Score: 5.0

URL: <https://portal-ippe1.eniot.io/iam-web/logout>

Entity: logout (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove old versions of files from the virtual directory

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.

Raw Test Response:

```

...
3dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4eb1; loginStyle=enos;
48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
locale: en-US
Origin: https://portal-ippe1.eniot.io
Accept: /*
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding

```

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:46:02 GMT
Content-Type: application/json;charset=UTF-8

{
    "status": 500,
    "message": "system error",
    "data": null,
    "success": false,
    "fail": true
}

...
...
```

Issue 1 of 9

TOC

Application Error**Severity:** Informational**CVSS Score:** 0.0**URL:** <https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll>**Entity:** currentPage (Parameter)**Risk:** It is possible to gather sensitive debugging information**Causes:** Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected**Fix:** Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions**Reasoning:** The application has responded with an error message, indicating an undefined state that may expose sensitive information.**Raw Test Response:**

```
...
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:58:37 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
  "data": null,
  "subMsg": "errorcode.500",
  "requestId": null,
  "retCode": 99500
}
...
```

Issue 2 of 9

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/dm-bff/logicasset/search
Entity:	pageSize (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
POST /dm-bff/logicasset/search?pageNo=1&pageSize=10XYZ&expression= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/logicasset.html?__ts__=1587876217997&
Cookie: _ga=GA1.2.610865653.1587876213; _gat_gtag_UA_110195466_1=1; locale=en-US; lang=en-US;
_gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_2=1;
JSESSIONID=CA59A32FD9222E34FF5E0DF43BF08992;
global_id=IAM_S_Tdgv9KNqpfYms2rRDKTY76U2qSaxm6XTuBwqXYSzhLf3QN462Rm6dmHFFCyykATPRjpyAtbjqkacM678
BEyBvBVLCESSub4WhcrkXt9sz7dL5FBBuJB3vyNkLHfs9JG;
8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b=0941003bc28d1a3ea773f47748f4ebal;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34abeeedacee49efaa9;
54e50ebe879a92d35eacc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
837cbf2c4037d0ea9e37c5df2937b9c2=8bb8ca7d0ae10d5f3e083b4d5108ce32; loginStyle=enos;
48a7cc09a4a7ce63cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fwwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Content-Length: 0
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9
Content-Type: application/json;charset=UTF-8

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:58:37 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
  "data": null,
  "subMsg": "errorcode.500",
  "requestId": null,
  "retCode": 99500
}
```

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/dm-bff/logicasset/search
Entity:	expression (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```

POST /dm-bff/logicasset/search?pageNo=1&pageSize=10&expression=%27 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-dm/logicasset.html?__ts__=1587876217997&
Cookie: _ga=GA1.2.610865653.1587876213; _gat_gtag_UA_110195466_1=1; locale=en-US; lang=en-US;
_gid=GA1.2.1711793339.1587876213; _gat_gtag_UA_110195466_2=1;
JSESSIONID=5925094306742A0B229A68B2E363D60D;
global_id=IAM_S_HfHdmxRN7mqkKES7MbBmG9w5F3PWCbhKtU6yga9RSCMTXpeEttMnqZkGHwVHTazqngu4NhvB9DJVCGLM
pnuWXVuLsWHnqlcFsmsX4qXc3hKefjNs3zku9aVV4jchFVz;
8142657bb99ce5d47beb6ebdabe5671b=7249efd1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126;
9dc22c38677b96443dd332ac8e31ba30=0a1fcfa109465bf34beeedacee49efaa9;
54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46;
2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d;
203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbdee;
837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; loginStyle=enos;
48a7cc09a4a7ce63cb4774f8375cca6=836861ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth:
{"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2S
AMSA2gzkwUSbYesMFjMvbaK5FCJgTqbZLsJcXjfyK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o157906162987
31", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Content-Length: 0
Cache-Control: max-age=0
Accept: application/json
Origin: https://portal-ippe1.eniot.io
Accept-Language: en-US,en;q=0.9
Content-Type: application/json;charset=UTF-8

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Mon, 27 Apr 2020 10:58:37 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
}

```

```
        "data": null,
        "subMsg": "errorcode.500",
        "requestId": null,
        "retCode": 99500
    }
```

Issue 4 of 9

TOC

Application Error

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/portal-web/config/docurl>

Entity: key (Parameter)

Risk: It is possible to gather sensitive debugging information

Causes: Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

Fix: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 03:53:29 GMT
Content-Type: application/json; charset=UTF-8

{
    "msg": "Server_Error",
    "data": null,
    "subMsg": "Required String parameter 'key' is not present",
    "requestId": null,
    "retCode": 500
}
...
```

Issue 5 of 9

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/apim/agroup
Entity:	->"limit" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 04:09:04 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 500,
  "message": "Internal Server Error",
  "data": null
}
...
```

Issue 6 of 9

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/apim/agroup
Entity:	->"offset" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that

may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 04:09:04 GMT
Content-Type: application/json;charset=UTF-8

{
  "code": 500,
  "message": "Internal Server Error",
  "data": null
}
...
```

Issue 7 of 9

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-web/resmgnt/list/ou/service
Entity:	serviceName (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 04:10:09 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Server Error",
  "data": null,
  "subMsg": "Required String parameter 'serviceName' is not present",
  "requestId": null,
  "retCode": 500
}
...
```

Issue 8 of 9

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-web/dataex/list
Entity:	ould (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Connection: keep-alive
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 04:10:13 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Server Error",
  "data": null,
  "subMsg": "Required String parameter 'ouId' is not present",
  "requestId": null,
  "retCode": 500
}
...
```

Issue 9 of 9

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/dm-bff/overview/getMetricValues
Entity:	productKey (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=05F0CC3ACB68226D6C9B88D80C299510; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 04:41:05 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
  "data": null,
  "subMsg": "internal service error",
  "requestId": null,
  "retCode": 99500
}
...
```



Application Test Script Detected 28

TOC

Issue 1 of 28

TOC

Application Test Script Detected

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/enos-app-webservice/
Entity:	test (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test HT  
TP/1.1  
User-Agent: Mozilla/5.0 (Windows  
NT 6.1; WOW64; Trident/7.0; rv:1  
1.0) like Gecko  
Referer: https://portal-ippe1.en  
iot.io/portal-api/apimanagement.  
html?__ts__=1587876282201&&  
Cookie: __gat_gtag_UA_110195466_1  
=1; __ga=GA1.2.610865653.15878762  
13; lang=en-US; __gid=GA1.2.17117  
93339.1587876213; locale=en-US;  
__gat_gtag_UA_110195466_2=1; 203d  
16c4c34b4d73cbe8d8ad13e35fee=828  
c5a658f7338cd2e39be4d51cfbd5e; 5  
0eaa23de448b610a687b0e42bab51f=  
0d269ec330206b966f847c4eaaf00be  
; Ob68a657f24d12cce48ed4247bcc86  
d0=352d622976494a7eae62da3419c0f  
1c4; 33296aa8a77f7e6d9209cc11b28  
2bf5c=29583daf49f8c47f70937b3e64  
64d67f; 4bf685a1f608acedeac059c  
b0cf3236=30c82d07997c54b264a0d1b  
c9c26fdbf; global_id=IAM_S_wcUH9  
dpScURgLYBzhG2qFst9uzW9FZ3CADv5A  
fAucCynec9DnMJj9DddBfhksUqcSpZwL  
3dmSaHc4EMLyYWgnjqAXAgZLqW8hw8jT  
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814  
2657bb99ce5d47beb6ebdabe5671b=72  
49efda1c32d9b86f368cf91fd8b7de;  
42dea464b09cd2371e151241b10bd05b  
=bb630ba83d88f1a7ac7eaf4447f0a12  
6; loginStyle=enos; 061609d44b39  
8ee03ad76311f6534dd7=580ffb56a53  
d3823b619922623f730d5; 9dc22c386  
77b96443dd332ac8e31ba30=oalfca10  
9465bf34beeedacee49efaa9; 837cbf  
2c4037d0ea9e37c5df2937b9c2=a7251  
de0c2fdcf61f683ce3be3d9cd9e; JSE  
SSIONID=6193E8AF84785D4A135BCB96  
675B31C3; e9dc754e254cfe59b74a9c  
4131b3c49a=c856bc06c55877b427547  
2696a7fe613; 54e50ebe879a92d35e3  
acc94c2ba7606=4b8017b396a20ea33f  
8b12287962fe46; 2913cd5e4f9e0128  
15fa8ec11b6f36ea=6942da86168ec38  
34e85ca4ff9374f1d; 149118e82bd3d  
b81f33f21b97080c04f=30f016a0a0a5  
958add68aac97cce8796; 3fe8ef195d  
77afaeca93685b8f336acc=7531cac53  
1eb2b86ee84ca46c3920ce4; 48a7cc0  
9a4a7ce6e3cb4774f8375cca6=836861  
ced028279968e30876217a4500  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

...

```
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS  
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200  
Connection: keep-alive  
Server: nginx  
Content-Length: 123  
Cache-control: private  
Strict-Transport-Security: max-a  
ge=3153600; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fce=45b7075c35491e93b05  
a563912b65508; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:04:39  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

...

```
...
```

Strict-Transport-Security: max-a
ge=3153600; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fce=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json;c
harset=UTF-8

{
 "requestId": null,
 "status": 404,
 "msg": "not.exist",
 "subMsg": "No handler found for
GET /enos-app-webservice/test",
 "data": null

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
}  
...
```

Issue 2 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.php (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8

...
...

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/test.php",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 3 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.php3 (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.php3 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 128
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8
```

```
...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/test.php3",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 4 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.asp (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.asp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8

...
...

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/test.asp",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 5 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.aspx (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5ee; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; 0b68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfca10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 128
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
...
...
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/test.aspx",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 6 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.cgi (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.cgi HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8

...
...

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/test.cgi"
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 7 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.htm (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.htm  
m HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1  
1.0) like Gecko  
Referer: https://portal-ippe1.en  
iot.io/portal-api/apimanagement.  
html?__ts__=1587876282201&&  
Cookie: __gat_gtag_UA_110195466_1  
=1; __ga=GA1.2.610865653.15878762  
13; lang=en-US; __gid=GA1.2.17117  
93339.1587876213; locale=en-US;  
__gat_gtag_UA_110195466_2=1; 203d  
16c4c34b4d73cbe8d8ad13e35fee=828  
c5a658f7338cd2e39be4d51cfbd5e; 5  
0eaa23de448b610a687b0e42bab51f=  
0d269ec330206b966f847c4eaaf00be  
; 0b68a657f24d12cce48ed4247bcc86  
d0=352d622976494a7eae62da3419c0f  
1c4; 33296aa8a77f7e6d9209cc11b28  
2bf5c=29583daf49f8c47f70937b3e64  
64d67f; 4bf685a1f608acedeac059c  
b0cf3236=30c82d07997c54b264a0d1b  
c9c26fdbf; global_id=IAM_S_wcUH9  
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A  
fAucCynec9DnMJj9DddBfhksUqcSpZwL  
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT  
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814  
2657bb99ce5d47beb6ebdabe5671b=72  
49efda1c32d9b86f368cf91fd8b7de;  
42dea464b09cd2371e151241b10bd05b  
=bb630ba83d88f1a7ac7eaf4447f0a12  
6; loginStyle=enos; 061609d44b39  
8ee03ad76311f6534dd7=580fffb56a53  
d3823b619922623f730d5; 9dc22c386  
77b96443dd332ac8e31ba30=oalfc10  
9465bf34beeedacee49efaa9; 837cbf  
2c4037d0ea9e37c5df2937b9c2=a7251  
de0c2fdcf61f683ce3be3d9cd9e; JSE  
SSIONID=6193E8AF84785D4A135BCB96  
675B31C3; e9dc754e254cfe59b74a9c  
4131b3c49a=c856bc06c55877b427547  
2696a7fe613; 54e50ebe879a92d35e3  
acc94c2ba7606=4b8017b396a20ea33f  
8b12287962fe46; 2913cd5e4f9e0128  
15fa8ec11b6f36ea=6942da86168ec38  
34e85ca4ff9374f1d; 149118e82bd3d  
b81f33f21b97080c04f=30f016a0a0a5  
958add68aac97cce8796; 3fe8ef195d  
77afaeca93685b8f336acc=7531cac53  
1eb2b86ee84ca46c3920ce4; 48a7cc0  
9a4a7ce6e3cb4774f8375cca6=836861  
ced028279968e30876217a4500  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

```
...  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS  
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200  
Connection: keep-alive  
Server: nginx  
Content-Length: 127  
Cache-control: private  
Content-Disposition: inline;file  
name=f.txt  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fece=45b7075c35491e93b05  
a563912b65508; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:04:39  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

```
...  
...  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fece=45b7075c35491e93b05  
a563912b65508; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:04:39  
GMT  
Content-Type: application/json;c  
harset=UTF-8  
  
{  
  "requestId": null,  
  "status": 404,  
  "msg": "not.exist",  
  "subMsg": "No handler found for  
GET /enos-app-webservice/test.ht  
m",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 8 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.html (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 128
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8
```

```
...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:39
GMT
Content-Type: application/json; charset=UTF-8
```

```
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/test.html,"}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 9 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.cfm (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.cf
m HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.en
iot.io/portal-api/apimanagement.
html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1
=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; 0b68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYBzhG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfca10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fce=d41361c030cb24ef9ed
fe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
...
...
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fce=d41361c030cb24ef9ed
fe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/test.cf
m",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 10 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.pl (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.pl
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.en
iot.io/portal-api/apimanagement.
html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1
=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; Ob68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfca10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 126
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
...
...
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/test.pl
",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 11 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.dbf (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.db
f HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.en
iot.io/portal-api/apimanagement.
html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1
=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; 0b68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYBzhG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfca10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fce=d41361c030cb24ef9ed
fe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
...
...
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fce=d41361c030cb24ef9ed
fe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/test.db
f",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 12 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.shtml (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.sh  
tml HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows  
NT 6.1; WOW64; Trident/7.0; rv:1  
1.0) like Gecko  
Referer: https://portal-ippe1.en  
iot.io/portal-api/apimanagement.  
html?__ts__=1587876282201&&  
Cookie: __gat_gtag_UA_110195466_1  
=1; __ga=GA1.2.610865653.15878762  
13; lang=en-US; __gid=GA1.2.17117  
93339.1587876213; locale=en-US;  
__gat_gtag_UA_110195466_2=1; 203d  
16c4c34b4d73cbe8d8ad13e35fee=828  
c5a658f7338cd2e39be4d51cfbd5e; 5  
0eaa23de448b610a687b0e42bab51f=  
0d269ec330206b966f847c4eaaf00be  
; 0b68a657f24d12cce48ed4247bcc86  
d0=352d622976494a7eae62da3419c0f  
1c4; 33296aa8a77f7e6d9209cc11b28  
2bf5c=29583daf49f8c47f70937b3e64  
64d67f; 4bf685a1f608acedeac059c  
b0cf3236=30c82d07997c54b264a0d1b  
c9c26fdbf; global_id=IAM_S_wcUH9  
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A  
fAucCynec9DnMJj9DddBfhksUqcSpZwL  
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT  
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814  
2657bb99ce5d47beb6ebdabe5671b=72  
49efda1c32d9b86f368cf91fd8b7de;  
42dea464b09cd2371e151241b10bd05b  
=bb630ba83d88f1a7ac7eaf4447f0a12  
6; loginStyle=enos; 061609d44b39  
8ee03ad76311f6534dd7=580fffb56a53  
d3823b619922623f730d5; 9dc22c386  
77b96443dd332ac8e31ba30=oalfca10  
9465bf34beeedacee49efaa9; 837cbf  
2c4037d0ea9e37c5df2937b9c2=a7251  
de0c2fdcf61f683ce3be3d9cd9e; JSE  
SSIONID=6193E8AF84785D4A135BCB96  
675B31C3; e9dc754e254cfe59b74a9c  
4131b3c49a=c856bc06c55877b427547  
2696a7fe613; 54e50ebe879a92d35e3  
acc94c2ba7606=4b8017b396a20ea33f  
8b12287962fe46; 2913cd5e4f9e0128  
15fa8ec11b6f36ea=6942da86168ec38  
34e85ca4ff9374f1d; 149118e82bd3d  
b81f33f21b97080c04f=30f016a0a0a5  
958add68aac97cce8796; 3fe8ef195d  
77afaeca93685b8f336acc=7531cac53  
1eb2b86ee84ca46c3920ce4; 48a7cc0  
9a4a7ce6e3cb4774f8375cca6=836861  
ced028279968e30876217a4500  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

```
...  
Connection: keep-alive  
Host: portal-ippe1.eniot.io  
eos_auth: {"uid":"u1587719976899  
1","token":"IAM_S_zvGC2jdEyL6Qzd  
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S  
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb  
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS  
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200  
Connection: keep-alive  
Server: nginx  
Content-Length: 129  
Cache-control: private  
Content-Disposition: inline;file  
name=f.txt  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fece=45b7075c35491e93b05  
a563912b65508; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:04:40  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

```
...  
...  
Strict-Transport-Security: max-a  
ge=31536000; includeSubDomains  
Set-Cookie: 7d1ffbf2f004d3aac950  
6740a8c2fece=45b7075c35491e93b05  
a563912b65508; path=/; HttpOnly  
Date: Tue, 28 Apr 2020 06:04:40  
GMT  
Content-Type: application/json;c  
harset=UTF-8
```

```
{  
  "requestId": null,  
  "status": 404,  
  "msg": "not.exist",  
  "subMsg": "No handler found for  
GET /enos-app-webservice/test.sh  
tml",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 13 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.txt (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

GET /enos-app-webservice/test.tx
t HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1

```

1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5ee; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; 0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bfff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0

```

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

```

```

...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

```

```

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/test.txt",
  "data": null
}
...

```

```
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

Issue 14 of 28

TOC

Application Test Script Detected

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/>

Entity: test.jsp (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/test.js
p HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; 0b68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfca10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

...

```
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8

...

```
...
```

Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8

{
"requestId": null,
"status": 404,
"msg": "not.exist",
"subMsg": "No handler found for
GET /enos-app-webservice/**test**.js
p",

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 15 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/tes  
t HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows  
NT 6.1; WOW64; Trident/7.0; rv:1
```

```

1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5ee; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; 0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bfff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0

```

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 127
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

```

```

...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

```

```

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test",
  "data": null
}
...

```

```
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

Issue 16 of 28

TOC

Application Test Script Detected

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.php (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

...
Content-Type: application/json; charset=UTF-8

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.php",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 17 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.php3 (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.php3 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 132
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

...
...

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.php3",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 18 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.asp (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.asp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

...
Content-Type: application/json; charset=UTF-8

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.asp",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 19 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.aspx (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/tes
t.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.en
iot.io/portal-api/apimanagement.
html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1
=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; Ob68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYBzhG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580ffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfc10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 132
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fce=d41361c030cb24ef9ed
fe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8

...
...

Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fce=d41361c030cb24ef9ed
fe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/app/tes
t.aspx",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 20 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.cgi (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/tes
t.cgi HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.en
iot.io/portal-api/apimanagement.
html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1
=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; Ob68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfc10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
...
...
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json;c
harset=UTF-8
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/app/tes
t.cgi",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 21 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.htm (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

...
Content-Type: application/json; charset=UTF-8

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:40
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.htm",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 22 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.html (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580ffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 132
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

...
...

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.html",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 23 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.cfm (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.cfm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzH2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

...
Content-Type: application/json; charset=UTF-8

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=45b7075c35491e93b05a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.cfm",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 24 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.pl (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.pl HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 130
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

...
...

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.pl",
}
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 25 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.dbf (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/test.dbf HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; Ob68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bf685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzH2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efda1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=oalfca109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u15877199768991","token":"IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o15790616298731","userName":"security_scan","locale":"en-US","isAdmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;filename=f.txt
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

...
...

Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fce=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.dbf",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 26 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.shtml (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/tes
t.shtml HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.en
iot.io/portal-api/apimanagement.
html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1
=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; Ob68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfc10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 133
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json;c
harset=UTF-8
```

```
...
...
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json;c
harset=UTF-8
{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/app/tes
t.shtml",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```

Issue 27 of 28

TOC

Application Test Script Detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.txt (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/tes  
t.txt HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows  
NT 6.1; WOW64; Trident/7.0; rv:1
```

```

1.0) like Gecko
Referer: https://portal-ippe1.eniot.io/portal-api/apimanagement.html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1=1; __ga=GA1.2.610865653.1587876213; lang=en-US; __gid=GA1.2.1711793339.1587876213; locale=en-US; __gat_gtag_UA_110195466_2=1; 203d16c4c34b4d73cbe8d8ad13e35fee=828c5a658f7338cd2e39be4d51cfbd5ee; 50eaa23de448b610a687b0e42bab51f=0d269ec330206b966f847c4eaaf00be; 0b68a657f24d12cce48ed4247bcc86d0=352d622976494a7eae62da3419c0f1c4; 33296aa8a77f7e6d9209cc11b282bf5c=29583daf49f8c47f70937b3e6464d67f; 4bfff685a1f608acedeac059cb0cf3236=30c82d07997c54b264a0d1bc9c26fdbf; global_id=IAM_S_wcUH9dpScURgLYbzG2qFst9uzW9FZ3CAdV5AfAucCynec9DnMJj9DddBfhksUqcSpZwL3dmSaHc4EMlyYWgnjqAXAgZLqW8hw8jTmU6dEaqQbPsAzTEvsGaDsmgDGg3; 8142657bb99ce5d47beb6ebdabe5671b=7249efdal1c32d9b86f368cf91fd8b7de; 42dea464b09cd2371e151241b10bd05b=bb630ba83d88f1a7ac7eaf4447f0a126; loginStyle=enos; 061609d44b398ee03ad76311f6534dd7=580fffb56a53d3823b619922623f730d5; 9dc22c38677b96443dd332ac8e31ba30=0a1fc109465bf34beeedacee49efaa9; 837cbf2c4037d0ea9e37c5df2937b9c2=a7251de0c2fdcf61f683ce3be3d9cd9e; JSESSIONID=6193E8AF84785D4A135BCB96675B31C3; e9dc754e254cfe59b74a9c4131b3c49a=c856bc06c55877b4275472696a7fe613; 54e50ebe879a92d35e3acc94c2ba7606=4b8017b396a20ea33f8b12287962fe46; 2913cd5e4f9e012815fa8ec11b6f36ea=6942da86168ec3834e85ca4ff9374f1d; 149118e82bd3db81f33f21b97080c04f=30f016a0a0a5958add68aac97cce8796; 3fe8ef195d77afaeca93685b8f336acc=7531cac531eb2b86ee84ca46c3920ce4; 48a7cc09a4a7ce6e3cb4774f8375cca6=836861ced028279968e30876217a4500Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0

```

```

...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid": "u15877199768991", "token": "IAM_S_zvGC2jdEyL6Qzd4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9Sp8ZFwr3sV2SAMSA2gzkwUsbYesMFjMvbak5FCJgTqbZLsJcXjfYK8NnAY5q2TuxSRXj3fpsWQkuRb3AwUZ", "orgCode": "o15790616298731", "userName": "security_scan", "locale": "en-US", "isAdmin": false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

```

```

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

```

```

...
...
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac9506740a8c2fece=d41361c030cb24ef9edfe1e31d899a31; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json; charset=UTF-8

```

```

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for GET /enos-app-webservice/app/test.txt",
  "data": null
}
...

```

```
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

Issue 28 of 28

TOC

Application Test Script Detected

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/enos-app-webservice/app/>

Entity: test.jsp (Page)

Risk: It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Causes: Temporary files were left in production environment

Fix: Remove test scripts from the server

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Request:

Test Response

```
GET /enos-app-webservice/app/tes
t.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: https://portal-ippe1.en
iot.io/portal-api/apimanagement.
html?__ts__=1587876282201&&
Cookie: __gat_gtag_UA_110195466_1
=1; __ga=GA1.2.610865653.15878762
13; lang=en-US; __gid=GA1.2.17117
93339.1587876213; locale=en-US;
__gat_gtag_UA_110195466_2=1; 203d
16c4c34b4d73cbe8d8ad13e35fee=828
c5a658f7338cd2e39be4d51cfbd5e; 5
0eaa23de448b610a687b0e42bab51f=
0d269ec330206b966f847c4eaaf00be
; Ob68a657f24d12cce48ed4247bcc86
d0=352d622976494a7eae62da3419c0f
1c4; 33296aa8a77f7e6d9209cc11b28
2bf5c=29583daf49f8c47f70937b3e64
64d67f; 4bf685a1f608acedeac059c
b0cf3236=30c82d07997c54b264a0d1b
c9c26fdbf; global_id=IAM_S_wcUH9
dpScURgLYbzG2qFst9uzW9FZ3CAdV5A
fAucCynec9DnMJj9DddBfhksUqcSpZwL
3dmSaHc4EMLyWgnjqAXAgZLqW8hw8jT
mU6dEaqQbPsAzTEvsGaDsmgDGg3; 814
2657bb99ce5d47beb6ebdabe5671b=72
49efda1c32d9b86f368cf91fd8b7de;
42dea464b09cd2371e151241b10bd05b
=bb630ba83d88f1a7ac7eaf4447f0a12
6; loginStyle=enos; 061609d44b39
8ee03ad76311f6534dd7=580fffb56a53
d3823b619922623f730d5; 9dc22c386
77b96443dd332ac8e31ba30=oalfca10
9465bf34beeedacee49efaa9; 837cbf
2c4037d0ea9e37c5df2937b9c2=a7251
de0c2fdcf61f683ce3be3d9cd9e; JSE
SSIONID=6193E8AF84785D4A135BCB96
675B31C3; e9dc754e254cfe59b74a9c
4131b3c49a=c856bc06c55877b427547
2696a7fe613; 54e50ebe879a92d35e3
acc94c2ba7606=4b8017b396a20ea33f
8b12287962fe46; 2913cd5e4f9e0128
15fa8ec11b6f36ea=6942da86168ec38
34e85ca4ff9374f1d; 149118e82bd3d
b81f33f21b97080c04f=30f016a0a0a5
958add68aac97cce8796; 3fe8ef195d
77afaeca93685b8f336acc=7531cac53
1eb2b86ee84ca46c3920ce4; 48a7cc0
9a4a7ce6e3cb4774f8375cca6=836861
ced028279968e30876217a4500
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9
```

```
...
Connection: keep-alive
Host: portal-ippe1.eniot.io
eos_auth: {"uid":"u1587719976899
1","token":"IAM_S_zvGC2jdEyL6Qzd
4PbDLrk7WM6fWwbUFxQFJJkTS2WxHt9S
p8ZFwr3sV2SAMSA2gzkwUSbYesMFjMvb
aK5FCJgTqbZLsJcXjfYK8NnAY5q2TuxS
RXj3fpsWQkuRb3AwUZ","orgCode":"o
15790616298731","userName":"secu
rity_scan","locale":"en-US","isA
dmin":false}
Cache-Control: max-age=0
Accept: application/json
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200
Connection: keep-alive
Server: nginx
Content-Length: 131
Cache-control: private
Content-Disposition: inline;file
name=f.txt
Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json;c
harset=UTF-8

...
...

Strict-Transport-Security: max-a
ge=31536000; includeSubDomains
Set-Cookie: 7d1ffbf2f004d3aac950
6740a8c2fece=45b7075c35491e93b05
a563912b65508; path=/; HttpOnly
Date: Tue, 28 Apr 2020 06:04:41
GMT
Content-Type: application/json;c
harset=UTF-8

{
  "requestId": null,
  "status": 404,
  "msg": "not.exist",
  "subMsg": "No handler found for
GET /enos-app-webservice/app/tes
t.jsp",
```

```
RXj3fpsWQkuRb3AwUZ","orgCode":"o  
15790616298731","userName":"secu  
rity_scan","locale":"en-US","isA  
dmin":false}  
Cache-Control: max-age=0  
Accept: application/json  
Accept-Language: en-US,en;q=0.9
```

```
"data": null  
}  
...
```



Client-Side (JavaScript) Cookie References 7

TOC

Issue 1 of 7

TOC

Client-Side (JavaScript) Cookie References

Severity: Informational

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/devportal/res/common/index_445fadca.js

Entity: (window.webpackJsonp=window.webpackJsonp||[]).push([[],[function(n,e,t){n.exports=t(1148)()},fun
cti... (Page)

Risk: The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side

Causes: Cookies are created at the client side

Fix: Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```
...  
...h>3&&void 0!==arguments[3]?arguments[3]:30,r=new  
Date;r.setTime(r.getTime()+24*o*60*60*1e3),document.cookie=(0,p.filterXSS)(n)+"="+  
(0,p.filterXSS)(e)+"";expires='"+r.toGMTString()+"'; path='"+t}function N(n){for(v...  
...
```

Issue 2 of 7

TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal/res/commons/index_6b2dae79.js
Entity:	(window.webpackJsonp=window.webpackJsonp []).push([[],function(e,t,n){e.exports=n(1057)()},f unct... (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Causes:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```
...
...h>3&&void 0!==arguments[3]?arguments[3]:30,o=new
Date;o.setTime(o.getTime()+24*r*60*60*1e3),document.cookie="" .concat(e,"=").concat(escape(t)," ;ex
pires=").concat(o.toGMTString(),"; path=").concat(n)},clearCook...
...
...
...
...pe);var s="";for(var u in i)i[u]&&(s+="; "+u,!0==i[u]&&(s+=""+i[u].split("; ")[0]));return
document.cookie+"="+n+s}function a(e,n){if("undefined"!=typeof document){for(var o=
{}},i=document.cookie?document.c...
...
...
```

Issue 3 of 7

[TOC](#)

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-dm/res/commons/index_67ac1ffc.js
Entity:	(window.webpackJsonp=window.webpackJsonp []).push([[],function(e,t,n>{"use strict";n.d(t,"a"),(fu ... (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Causes:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```

...
...h>3&&void 0!==arguments[3]?arguments[3]:30,o=new
Date;o.setTime(o.getTime()+24*r*60*60*1e3),document.cookie="" .concat(e,"") .concat(escape(t)," ;ex
pires=") .concat(o.toGMTString()," ; path=").concat(n)},clearCook...
...

...
...

...pe);var u="";for(var l in a)a[l]&&(u+="; "+l,!0!==a[l]&&(u+="+" +a[l].split(";") [0]));return
document.cookie=t+"="+n+u}function i(e,n){if("undefined"!=typeof document){for(var o=
{}),a=document.cookie?document.c...

```

Issue 4 of 7

[TOC](#)

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-data/res/commons/index_16eaf087.js
Entity:	(window.webpackJsonp=window.webpackJsonp []).push([[],function(e,t,n){e.exports=n(1396)()},f unct... (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Causes:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```

...
...h>3&&void 0!==arguments[3]?arguments[3]:30,o=new
Date;o.setTime(o.getTime()+24*r*60*60*1e3),document.cookie="" .concat(e,"") .concat(escape(t)," ;ex
pires=") .concat(o.toGMTString()," ; path=").concat(n)},clearCook...
...

...
...

...pe);var u="";for(var s in i)i[s]&&(u+="; "+s,!0!==i[s]&&(u+="+" +i[s].split(";") [0]));return
document.cookie=t+"="+n+u}function a(e,n){if("undefined"!=typeof document){for(var o=
{}),i=document.cookie?document.c...

```

Issue 5 of 7

[TOC](#)

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-api/res/apimanagement/index_f20f1232.js
Entity:	!function(e){function t(t){for(var r,i,s=t[0],u=t[1],c=t[2],l=0,p=[];l<s.length;l++)i=s[l],o[i]&&p.p... (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Causes:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```
...>3&&void 0!==arguments[3]?arguments[3]:30,i=new Date;i.setTime(i.getTime()+24*r*60*60*1e3),document.cookie="" .concat(e,"") .concat(escape(t)," ;expires=") .concat(i.toGMTString()," ; path=").concat(n)},clearCook...  
...  
...  
...pe);var s="";for(var u in o)o[u]&&(s+="; "+u,!0==o[u]&&(s+="="+o[u].split("; ")[0]));return document.cookie+=";"+n+s}function a(e,n){if("undefined"!=typeof document){for(var i={},o=document.cookie?document.c...  
...
```

Issue 6 of 7

[TOC](#)

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js
Entity:	(window.webpackJsonp=window.webpackJsonp []).push([[],function(e,t,n>{"use strict";function r(e,... (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Causes:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```

...
...h>3&&void 0!==arguments[3]?arguments[3]:30,o=new
Date();o.setTime(o.getTime()+24*x*60*60*1e3),document.cookie="" .concat(e,"") .concat(escape(t)," ;ex
pires=") .concat(o.toGMTString()," ; path=").concat(n)},clearCook...
...

...
...
...pe);var u="";for(var s in i)i[s]&&(u+="; "+s,!0==i[s]&&(u+="=i[s].split("; ")[0]));return
document.cookie=t+"=n+u}function a(e,n){if("undefined"!=typeof document){for(var o=
{},i=document.cookie?document.c...
...

```

Issue 7 of 7

[TOC](#)

Client-Side (JavaScript) Cookie References

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/saturnweb/res/index/index.57829111.bundle.js>

Entity: webpackJsonp([0],[.,function(e,t,n>{"use strict";t._esModule=!0;var a=n(266),o=function(e){return e.. (Page)

Risk: The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side

Causes: Cookies are created at the client side

Fix: Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```

...
...h>3&&void 0!==arguments[3]?arguments[3]:30,o=new
Date();o.setTime(o.getTime()+24*x*60*60*1e3),document.cookie=e+"=escape(t)+";expires="+o.toGMTStr
ing()+" ; path="+n},formatDate:function(e,t){var n=t,a={"M+":e.g...
...
```



Email Address Pattern Found 14

[TOC](#)

Issue 1 of 14

[TOC](#)

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/devportal/res/home/index_57c2c951.js
Entity:	index_57c2c951.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
...n.LABEL_HOME PAGE_FOOTER_CONTACT_US,info:[],allLink:
[ {type:s.i18n.LABEL_HOME PAGE_FOOTER_MAIL,mailto:"group.iotsupport@envisioncn.com"}, 
{type:s.i18n.LABEL_HOME PAGE_FOOTER_ADDRESS,desc:s.i18n.LABEL_HOME PAGE_FOOTER_ADDRESS_DETAIL}, 
{typ...
...
...
...
...{n.exports=t.p+"res/imgs/page2BgL_040682fd.jpg"},1344:function(n,e,t)
{n.exports=t.p+"res/imgs/Group 2@2x_f202cc0e.png"},1345:function(n,e,t)
{n.exports=t.p+"res/imgs/page2groupZh_a9306d74.png"},1346:function(n,e,t){n.e...
...
...
```

Issue 2 of 14

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-dm/res/commons/index_67ac1ffc.js
Entity:	index_67ac1ffc.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```

...
...k mode compatible with Dr Brian Gladman fileenc.c
 * derived from CryptoJS.mode.CTR
 * Jan Hruby jhruby.web@gmail.com
 */
r.mode.CTRGladman=function(){var e=r.lib.BlockCipherMode.extend();function t(e){if(255==(e>>24...
...

```

Issue 3 of 14

TOC

Email Address Pattern Found

Severity: Informational

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js

Entity: index_e1944614.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```

...
...}catch(e){}i(e.prototype,n)}));
/**
 * @fileOverview
 * @name asn1-1.0.js
 * @author Kenji Urushima kenji.urushima@gmail.com
 * @version asn1 1.0.13 (2017-Jun-02)
 * @since jsrsasign 2.1
 * @license <a href="https://kjur.git...
...

...
...

...k mode compatible with Dr Brian Gladman fileenc.c
 * derived from CryptoJS.mode.CTR
 * Jan Hruby jhruby.web@gmail.com
*/
r.mode.CTRGladman=function(){var e=r.lib.BlockCipherMode.extend();function t(e){if(255==(e>>24...
...

...
...

...eration in the next 24 hours before the confirmation.",FORMMSG_EMAIL:"Invalid email format
(must be example@example.com"),WINMSG_SUBMIT_SUCCESS:"Submitted
successfully",WINMSG_SUBMIT_FAILED:"Failed to submit",WINMSG_REV...
...

...
...

...账户转移",TXT_CHANGE_OWNER:"您将变更此组织的所有者,更改将在将成为所有者的用户确认后完成,您可以在确认前的24小
时内撤消操作。",FORMMSG_EMAIL:"邮件格式无效,必须是example@example.com",WINMSG_SUBMIT_SUCCESS:"提交成
功",WINMSG_SUBMIT_FAILED:"提交失败",WINMSG_REVOKE_SUCCESS:"撤销成功",WINMSG_REVOK...

```

...

Issue 4 of 14

TOC

Email Address Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/iam/api/v2/session/get>

Entity: get (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
{
  "message": "",
  "sessionId": "IAM_S_HFN2qKMBFVa9qWNhQx8EURF6E6UqSW8jC2qTUymQfQDjKgMynk36BaQjMgWAHa75hB3LsQPKB8tB7z7AXEbpgeYe7B
KtrS6NXK79cYME3BJrCyD7s3HSTBjsanD4pAUT",
  "user": {
    "id": "u15877199768991",
    "organizationId": "o15790616298731",
    "authType": 0,
    "name": "security_scan",
    "phoneArea": "",
    "phone": "",
    "email": "liying.liu@envision-digital.com",
    "description": "",
    "resourceId": "r15877199768992",
    "type": 1,
    "state": 0,
    "phoneVerifiedAt": null,
    "emailVerifiedAt": "2020-04-25 04:33:37.0",
    "extra": {
      "password_strength": "MEDIUM",
      "password_expire_time": 1.603341217E12,
    }
  },
  ...
  ...
  "id": "IAM_S_HFN2qKMBFVa9qWNhQx8EURF6E6UqSW8jC2qTUymQfQDjKgMynk36BaQjMgWAHa75hB3LsQPKB8tB7z7AXEbpgeYe7B
KtrS6NXK79cYME3BJrCyD7s3HSTBjsanD4pAUT",
  "expires": 7200,
  "user": {
    "id": "u15877199768991",
    "organizationId": "o15790616298731",
    "authType": 0,
    "name": "security_scan",
    "phoneArea": "",
```

```

"phone": "",
"email": "liying.liu@envision-digital.com",
"description": "",
"resourceId": "r15877199768992",
"type": 1,
"state": 0,
"phoneVerifiedAt": null,
"emailVerifiedAt": "2020-04-25 04:33:37.0",
"extra": {
    "password_strength": "MEDIUM",
    "password_expire_time": 1.603341217E12,
}
...

```

Issue 5 of 14

[TOC](#)

Email Address Pattern Found

Severity: Informational

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal-data/res/commons/index_16eaf087.js

Entity: index_16eaf087.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```

...
...k mode compatible with Dr Brian Gladman fileenc.c
 * derived from CryptoJS.mode.CTR
 * Jan Hruby jhruby.web@gmail.com
 */
r.mode.CTRGladman=function(){var e=r.lib.BlockCipherMode.extend();function t(e){if(255==(e>>24...
...

```

Issue 6 of 14

[TOC](#)

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/iam-web/organization/info
Entity:	info (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
{
  "domain": "data_o15790616298731",
  "owner": {
    "is_phone_verified": false,
    "is_email_verified": true,
    "id": "u15790616302751",
    "auth_type": 0,
    "link_name": null,
    "name": "yongjun.fan",
    "mobile": "-",
    "email": "yongjun.fan@envision-digital.com",
    "org_id": "",
    "org_name": "",
    "state": 1,
    "multiple_factor": 0,
    "organizations": [
      ...
    ],
    "user_groups": [
      ...
    ]
}
```

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-api/res/apimanagement/index_f20f1232.js
Entity:	index_f20f1232.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...  
...k mode compatible with Dr Brian Gladman fileenc.c  
* derived from CryptoJS.mode.CTR  
* Jan Hruby jhruby.web@gmail.com  
*/  
r.mode.CTRGladman=function(){var e=r.lib.BlockCipherMode.extend();function t(e){if(255==(e>>24...  
...  
...
```

Issue 8 of 14

[TOC](#)

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/iam-web/user/list
Entity:	list (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...  
...  
"list": [  
{  
"is_phone_verified": false,  
"is_email_verified": true,  
"id": "u15877199768991",  
...
```

```
"auth_type": 0,
"link_name": null,
"name": "security_scan",
"mobile": "-",
"email": "liying.liu@envision-digital.com",
"org_id": "o15790616298731",
"org_name": "Envision_CLP",
"state": 1,
"multiple_factor": 0,
"organizations": [
],
"user_groups": [
    ...
    ...
},
{
    "is_phone_verified": false,
    "is_email_verified": true,
    "id": "u15814904235601",
    "auth_type": 0,
    "link_name": null,
    "name": "ziming.xu",
    "mobile": "-",
    "email": "ziming.xu@envision-digital.com",
    "org_id": "o15790616298731",
    "org_name": "Envision_CLP",
    "state": 1,
    "multiple_factor": 0,
    "organizations": [
],
    "user_groups": [
]
},
{
    "is_phone_verified": true,
    "is_email_verified": false,
    "id": "u15814903655501",
    "auth_type": 0,
    "link_name": null,
    "name": "ning.wang",
    "mobile": "86-18238932179",
    "email": "ning.wang@envision-digital.com",
    "org_id": "o15790616298731",
    "org_name": "Envision_CLP",
    "state": 1,
    "multiple_factor": 0,
    "organizations": [
],
    "user_groups": [
]
},
{
    "is_phone_verified": false,
    "is_email_verified": true,
    "id": "u15791653311591",
    "auth_type": 0,
    "link_name": null,
    "name": "weiyong.sun",
    "mobile": "-",
    "email": "weiyong.sun2@envision-digital.com",
    "org_id": "o15790616298731",
    "org_name": "Envision_CLP",
    "state": 1,
    "multiple_factor": 0,
    "organizations": [
],
    "user_groups": [
]
```

```
        ],
    },
    {
        "is_phone_verified": false,
        "is_email_verified": false,
        "id": "u15790680838661",
        "auth_type": 0,
        "link_name": null,
        "name": "jian.tang",
        "mobile": "-",
        "email": "jian.tang@envision-digital.com",
        "org_id": "o15790616298731",
        "org_name": "Envision_CLP",
        "state": 1,
        "multiple_factor": 0,
        "organizations": [
            ],
        "user_groups": [
            ]
    },
    {
        "is_phone_verified": true,
        "is_email_verified": false,
        "id": "u15790680496341",
        "auth_type": 0,
        "link_name": null,
        "name": "chaoxu.zhang",
        "mobile": "86-18136480672",
        "email": "chaoxu.zhang@envision-digital.com",
        "org_id": "o15790616298731",
        "org_name": "Envision_CLP",
        "state": 1,
        "multiple_factor": 0,
        "organizations": [
            ],
        "user_groups": [
            ]
    },
    {
        "is_phone_verified": false,
        "is_email_verified": true,
        "id": "u15790679969531",
        "auth_type": 0,
        "link_name": null,
        "name": "siwei.pan",
        "mobile": "-",
        "email": "siwei.pan@envision-digital.com",
        "org_id": "o15790616298731",
        "org_name": "Envision_CLP",
        "state": 1,
        "multiple_factor": 0,
        "organizations": [
            ],
        "user_groups": [
            ]
    },
    {
        "is_phone_verified": false,
        "is_email_verified": true,
        "id": "u15790679596511",
        "auth_type": 0,
        "link_name": null,
        "name": "jian.cheng",
        "mobile": "-",
        "email": "jian.cheng@envision-digital.com",
        "org_id": "o15790616298731",
        "org_name": "Envision_CLP",
        "state": 1,
        "multiple_factor": 0,
        "organizations": [
            ],
        "user_groups": [
            ]
    }
]
```

```

"user_groups": [
],
{
  "is_phone_verified": false,
  "is_email_verified": true,
  "id": "u15790616302751",
  "auth_type": 0,
  "link_name": null,
  "name": "yongjun.fan",
  "mobile": "-",
  "email": "yongjun.fan@envision-digital.com",
  "org_id": "o15790616298731",
  "org_name": "Envision_CLP",
  "state": 1,
  "multiple_factor": 0,
  "organizations": [
    ],
  "user_groups": [
    ...
  ]
}

```

Issue 9 of 14

[TOC](#)

Email Address Pattern Found

Severity: Informational

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/devportal/res/login/index_df108705.js

Entity: index_df108705.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```

...
...k mode compatible with Dr Brian Gladman fileenc.c
 * derived from CryptoJS.mode.CTR
 * Jan Hruby jhruby.web@gmail.com
 */
a.mode.CTRGladman=function(){var n=a.lib.BlockCipherMode.extend();function t(n){if(255==(n>>24...
...
...
...}catch(n){o(n.prototype,e)}});
/***
 * @fileOverview
 * @name asn1-1.0.js
 * @author Kenji Urushima kenji.urushima@gmail.com

```

```
* @version asn1 1.0.13 (2017-Jun-02)
* @since jsrsasign 2.1
* @license <a href="https://kjur.git...
```

...

Issue 10 of 14

TOC

Email Address Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/devportal/res/index/index_6ef3d11b.js

Entity: index_6ef3d11b.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
...k mode compatible with Dr Brian Gladman fileenc.c
 * derived from CryptoJS.mode.CTR
 * Jan Hruby jhruby.web@gmail.com
 */
a.mode.CTRGladman=function(){var n=a.lib.BlockCipherMode.extend();function e(n){if(255==(n>>24...
...
...
```

Issue 11 of 14

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/iam/api/v3/login
Entity:	login (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
{
  "message": "",
  "sessionId": "IAM_S_JQ3anHWv4kbcxTVNjmpEsGEyQczGujwFKHHrSTb5mBVkkfYpCVFhgZtDb4y8KS42qQppCE62EzF2RXHuAkQV2hPMGtAV7U5srwRPsxbVamraGYTMzzfPxDujttYyZUxn",
  "user": {
    "id": "u15877199768991",
    "organizationId": "o15790616298731",
    "authType": 0,
    "name": "security_scan",
    "phoneArea": "",
    "phone": "",
    "email": "liying.liu@envision-digital.com",
    "description": "",
    "resourceId": "r15877199768992",
    "type": 1,
    "state": 0,
    "phoneVerifiedAt": null,
    "emailVerifiedAt": "2020-04-25 04:33:37.0",
    "extra": {
      "password_strength": 0,
      "password_expire_time": 1603341217000,
    }
  },
  ...
  ...
  "id": "IAM_S_JQ3anHWv4kbcxTVNjmpEsGEyQczGujwFKHHrSTb5mBVkkfYpCVFhgZtDb4y8KS42qQppCE62EzF2RXHuAkQV2hPMGtAV7U5srwRPsxbVamraGYTMzzfPxDujttYyZUxn",
  "expires": 3600,
  "user": {
    "id": "u15877199768991",
    "organizationId": "o15790616298731",
    "authType": 0,
    "name": "security_scan",
    "phoneArea": "",
    "phone": "",
    "email": "liying.liu@envision-digital.com",
    "description": "",
    "resourceId": "r15877199768992",
    "type": 1,
    "state": 0,
    "phoneVerifiedAt": null,
    "emailVerifiedAt": "2020-04-25 04:33:37.0",
    "extra": {
      "password_strength": 0,
      "password_expire_time": 1603341217000,
    }
  },
  ...
}
```

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal/res/homepage/index_09e65fab.js
Entity:	index_09e65fab.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
...}catch(e){o(e.prototype,n)}};
/**
 * @fileOverview
 * @name asn1-1.0.js
 * @author Kenji Urushima kenji.urushima@gmail.com
 * @version asn1 1.0.13 (2017-Jun-02)
 * @since jsrsasign 2.1
 * @license <a href="https://kjur.git...
...
```

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/iam-web/session/get
Entity:	get (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
{
  "id": "IAM_S_uweMXX48ke2GHt65xYYrrB7AfGLypTtuufrJk3UrVF6uGvRNXKfyPms8jgsQWERW6FZDyvHBVYZPkMAh4KqRKcXdYSxYR7XrJ5ynrkCDP9yg5RyKtKzwssPnbBkap6hq",
  "expires": 7200,
  "user": {
    "id": "u15877199768991",
    "organization_id": "o15790616298731",
    "auth_type": 0,
    "name": "security_scan",
    "phone_area": "",
    "phone": "",
    "email": "liying.liu@envision-digital.com",
    "description": "",
    "resource_id": "r15877199768992",
    "type": 1,
    "state": 0,
    "phone_verified_at": null,
    "email_verified_at": "2020-04-25 04:33:37.0",
    "extra": {
      "password_strength": "MEDIUM",
      "password_expire_time": 1.603341217E12,
    }
  }
}
```

Issue 14 of 14

TOC

Email Address Pattern Found

Severity: Informational

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal/res/commons/index_6b2dae79.js

Entity: index_6b2dae79.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...
...k mode compatible with Dr Brian Gladman fileenc.c
 * derived from CryptoJS.mode.CTR
 * Jan Hruby jhruby.web@gmail.com
 */
r.mode.CTRGladman=function(){var e=r.lib.BlockCipherMode.extend();function t(e){if(255==(e>>24...
...
```

```

...
...eration in the next 24 hours before the confirmation.",FORMMSG_EMAIL:"Invalid email format
(must be example@example.com)",WINMSG_SUBMIT_SUCCESS:"Submitted
successfully",WINMSG_SUBMIT_FAILED:"Failed to submit",WINMSG_REV...
...

...
...账户转移",TXT_CHANGE_OWNER:"您将变更此组织的所有者,更改将在将成为所有者的用户确认后完成,您可以在确认前的24小
时内撤消操作。",FORMMSG_EMAIL:"邮件格式无效,必须是example@example.com",WINMSG_SUBMIT_SUCCESS:"提交成
功",WINMSG_SUBMIT_FAILED:"提交失败",WINMSG_REVOK_SUCCESS:"撤销成功",WINMSG_REVOK...
...

```

Integer Overflow 7

TOC

Issue 1 of 7

TOC

Integer Overflow

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/search>

Entity: pageNo (Parameter)

Risk: It is possible to gather sensitive debugging information

Causes: Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

Fix: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```

...
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=C36910A9675B9C0CED6C23F354FD1E8B; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 03:30:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
  "data": null,
  "subMsg": "errorcode.500",
  "requestId": null,
  "retCode": 99500
}

```

```
}
```

```
...
```

Issue 2 of 7

TOC

Integer Overflow

Severity:

Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/dm-bff/logicasset/search>

Entity: pageSize (Parameter)

Risk: It is possible to gather sensitive debugging information

Causes: Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

Fix: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=40A4091869FC779655BBDCFF5A8C219B; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 03:30:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
  "data": null,
  "subMsg": "errorcode.500",
  "requestId": null,
  "retCode": 99500
}
...
```

Issue 3 of 7

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/dm-bff/rest/product/queryProductListAll
Entity:	currentPage (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=56828B546E7763AEE82942FA65904DB5; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 03:30:30 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
  "data": null,
  "subMsg": "errorcode.500",
  "requestId": null,
  "retCode": 99500
}
...
```

Issue 4 of 7

[TOC](#)

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics
Entity:	now (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=3DA53D3B3315C336E842185C04D39C43; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 03:30:32 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
  "data": null,
  "subMsg": "errorcode.500",
  "requestId": null,
  "retCode": 99500
}
...
```

Issue 5 of 7

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/dm-bff/overview/queryStatistics
Entity:	zero (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=CDF848F583FCB84DAC6577D55C000F59; Path=/dm-bff; HttpOnly
Date: Tue, 28 Apr 2020 03:30:33 GMT
Content-Type: application/json;charset=UTF-8

{
  "msg": "Internal Server Error",
```

```
        "data": null,
        "subMsg": "errorcode.500",
        "requestId": null,
        "retCode": 99500
    }
    ...
}
```

Issue 6 of 7

TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/apim/agroup
Entity:	->"limit" (Parameter)
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 04:09:04 GMT
Content-Type: application/json;charset=UTF-8

{
    "code": 500,
    "message": "Internal Server Error",
    "data": null
}
...
```

Issue 7 of 7

TOC

Integer Overflow

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/apim/agroup>

Entity: ->"offset" (Parameter)

Risk: It is possible to gather sensitive debugging information

Causes: Proper bounds checking were not performed on incoming parameter values
No validation was done in order to make sure that user input matches the data type expected

Fix: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Raw Test Response:

```
...
Server: nginx
Vary: Accept-Encoding
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
Date: Tue, 28 Apr 2020 04:09:04 GMT
Content-Type: application/json; charset=UTF-8

{
  "code": 500,
  "message": "Internal Server Error",
  "data": null
}
...
```



Internal IP Disclosure Pattern Found 3

TOC

Issue 1 of 3

TOC

Internal IP Disclosure Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js

Entity: index_e1944614.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Raw Test Response:

```
...15 - 1440",HINT_IP_PLACEHOLDER:"Use ',' to seperate different IP addresses, support CIDR mode  
(e.g. 10.1.1.1/16)",WINMSG_MFA_FAILED:"Update Multi Factor Authentication  
failed",LABEL_ORG_ID:"Organization ID",T...  
  
...  
  
...度1024个字符",FORMMSG_EXPIRATION_TIME:"支持范围 15 - 1440 分钟",HINT_IP_PLACEHOLDER:'使用", "分隔不  
同的IP地址, 支持CIDR模式(如10.1.1.1/16)',WINMSG_MFA_FAILED:"更新双因子认证失败",LABEL_ORG_ID:"组织  
ID",TXT_ORG_TRANSFER:"所有者转移到 {0}",TXT_EMAIL_VALI...  
...
```

Issue 2 of 3

[TOC](#)

Internal IP Disclosure Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/saturnweb/res/index/index.57829111.bundle.js>

Entity: index.57829111.bundle.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Raw Test Response:

```
...  
...return","javascript:");case
```

```
4;if(!t.startsWith("http://")&&!t.startsWith("https://")||!t.includes("10.21.14.11:19890"))
{e.next=8;break}return e.abrupt("return",t.replace("https://
```

Issue 3 of 3

TOC

Internal IP Disclosure Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal/res/commons/index_6b2dae79.js

Entity: index_6b2dae79.js (Page)

Risk: It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Causes: Insecure web application programming or configuration

Fix: Remove internal IP addresses from your website

Reasoning: AppScan discovered what looks like an internal IP address in the response.

Raw Test Response:

```
...
...15 - 1440",HINT_IP_PLACEHOLDER:"Use ',' to separate different IP addresses, support CIDR mode
(e.g. 10.1.1.1/16)",WINMSG_MFA_FAILED:"Update Multi Factor Authentication
failed",LABEL_ORG_ID:"Organization ID",T...
...
...
...度1024个字符",FORMMSG_EXPIRATION_TIME:"支持范围 15 - 1440 分钟",HINT_IP_PLACEHOLDER:'使用', "分隔不
同的IP地址, 支持CIDR模式(如10.1.1.1/16)',WINMSG_MFA_FAILED:"更新双因子认证失败",LABEL_ORG_ID:"组织
ID",TXT_ORG_TRANSFER:"所有者转移到 {0}",TXT_EMAIL_VALI...
...
...
...ication/x-www-form-urlencoded方式提交数据",addressHint:"格式为: host(ip):port;host(ip):port,多台机
器请用分号(;)隔开。范例:10.2.3.4:8080;envisioncn.com:8080",apicreate:"API创建",apiedit:"编辑
API",basicInfo:"基本信息",defineApiRequest:"定义AP...
...
```



Link to unclassified site 4

TOC

Issue 1 of 4

TOC

Link to unclassified site

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js
Entity:	http://ÑÐµÑÑ/ (Link)
Risk:	N/A
Causes:	N/A
Fix:	Examine the link to determine whether it is indeed supposed to be included in the web application

Reasoning: The link is not listed in the IBM X-Force Exchange URL filter database as either safe or unsafe.



The Malware Link Analysis module could not classify this link

Issue 2 of 4

[TOC](#)

Link to unclassified site

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js
Entity:	http://a/ (Link)
Risk:	N/A
Causes:	N/A
Fix:	Examine the link to determine whether it is indeed supposed to be included in the web application

Reasoning: The link is not listed in the IBM X-Force Exchange URL filter database as either safe or unsafe.



The Malware Link Analysis module could not classify this link

Issue 3 of 4

[TOC](#)

Link to unclassified site

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js
Entity:	https://a:@b/ (Link)
Risk:	N/A
Causes:	N/A
Fix:	Examine the link to determine whether it is indeed supposed to be included in the web application

Reasoning: The link is not listed in the IBM X-Force Exchange URL filter database as either safe or unsafe.



The Malware Link Analysis module could not classify this link

Issue 4 of 4

[TOC](#)

Link to unclassified site

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js
Entity:	http://x/ (Link)
Risk:	N/A
Causes:	N/A
Fix:	Examine the link to determine whether it is indeed supposed to be included in the web application

Reasoning: The link is not listed in the IBM X-Force Exchange URL filter database as either safe or unsafe.



The Malware Link Analysis module could not classify this link

1

Possible Server Path Disclosure Pattern Found

13

[TOC](#)

Issue 1 of 13

[TOC](#)

Possible Server Path Disclosure Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal-dm/res/commons/index_67ac1ffc.js

Entity: index_67ac1ffc.js (Page)

Risk: It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes: Latest patches or hotfixes for 3rd. party products were not installed

Fix: Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...  
...-9]\d*)$/ ,qe=/[\xc0-\xd6\xd8-\xf6\xf8-\xff\u0100-  
\u017f]/g,Qe=/($^)/,Ze=['\n\r\u2028\u2029\\']/g,$e="\u0300-\u036f\ufe20-\ufe2f--end_high...  
...  
...  
... (?:(?:\d{1,2})|2[0-4]\d{5})|(?:\\.(?:[0-9]\d?|1\d\d|2[0-4]\d{4}))|(?:(?:[a-  
z]\u00a1--begin_highlight_tag---\uffff0-9]+?)|[a-z]\u00a1-\uffff0-9+)|(?:\\.(?:[a-z]\u00a1--  
b...  
...  
...
```

Issue 2 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal-iam/res/commons/index_e1944614.js

Entity: index_e1944614.js (Page)

Risk: It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes: Latest patches or hotfixes for 3rd. party products were not installed

Fix: Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...  
...-9]\d*)$/ ,ce=/[\xc0-\xd6\xd8-\xf6\xf8-\xff\u0100-  
\u017f]/g,le=/($^)/,fe=/['\n\r\u2028\u2029\\']/g,pe="\u0300-\u036f\\ufe20-\ufe2f--end_high...  
...  
...  
... (?1?\d{1,2}|2[0-4]\d{25[0-5]})(2)(?:\\.(?:[0-9]\d?1\\d\d{2[0-4]\d{25[0-4]}))|(?:(?:[a-  
z]\\u00a1--begin_highlight_tag---\\uffff0-9)+?)*(a-z\\u00a1-\\uffff0-9+)(?:\\.(?:[a-z]\\u00a1--  
b...  
...
```

Issue 3 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/dataide/bundle.8d1d5153eebcba2626de.js
Entity:	bundle.8d1d5153eebcba2626de.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...  
...ertyName=c[f]),l.hasOwnProperty(f)&&(h.mutationMethod=l[f]),u.properties[f]=h}})),a=":A-Z_a-  
z\\u00c0-\u00D6\\u00D8-\u00F6\\u00F8-\u02FF--e...  
...  
...  
...",DIR_OR_FILE_NAME:"Directory or File Name",HINT_INPUT_DIR_OR_FILE:"Enter directory or file  
name, eg--begin_highlight_tag--. /usr/clp/dim_xxx_xxx",HINT_INPUT_DIR_OR_FILE_ALERT:"Please enter  
directory or file name",HINT_SEARCH_RESO...  
...  
...  
..."\u00c7-",SELECT_COLUMN_DELIMITER:"\u00c7",IF_OTHERS:"\u00c7\u00c7",SELECT_ENCODING_FORMAT:"\u00c7\u00c7",  
ENCODING_FORMAT:"\u00c7\u00c7",COMPRESSION_FORMAT:"  
...  
...  
...isplay: block;\n font-family: \"anticon\" !important;\n}\n.anticon-step-forward:before {\n content: "\uE600";\n}\n.anticon-step-backward:before {\n content: "\uE601--end_highlight_tag...  
...  
...
```

```
...r {\n  color: #f04134;\n}\n.ant-notification-notice-close-x:after {\n  font-size: 12px;\n  content: --begin_highlight_tag--"\\"E633";\n  font-family: "anticon";\n  cursor:\n  pointer;\n}\n.ant-notification-notice-close {\n  position: ...\n...\n...\n.ng: antialiased;\n  -moz-osx-font-smoothing: grayscale;\n}\n.icon-icon_connect:before {\n  content: "\\"E97F";\n}\n.icon-icon_error:before {\n  content: "\\"E980";\n...\n...\n
```

Issue 4 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-data/res/commons/index_16eaf087.js
Entity:	index_16eaf087.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
z\\u00a1-\\ufff0-9]+-?) * [a-z\\u00a1-\\ufff0-9]+) (?:\\.(?:[a-z\\u00a1--b...
```

```
...
```

Issue 5 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: https://portal-ippe1.eniot.io/portal-data/res/modeldeployment/index_2c95a1f5.js

Entity: index_2c95a1f5.js (Page)

Risk: It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes: Latest patches or hotfixes for 3rd. party products were not installed

Fix: Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...
...)?([eE][-+]?\\d(_|\\d*)?",relevance:0},{className:"symbol",begin:"""+t},
{className:"title",begin:"(\\bwith\\s+)?(\\bprivate\\s+)?\\bpackage...
...
...
...import from interface abstract|0 try catch protected explicit",illegal:(^using\\s+[A-Za-z0-
9\\s]+;$--begin highlight_tag--|\\bfunctions*[^\\(|]",contains:
[{className:"string",begin:"",end:"",illegal:"\\n",contains:[e.BACKSLASH_ESCAPE...
...
...
...assName:"symbol",begin:"",contains:[1,{begin:a}],relevance:0},{className:"number",variants:
[{begin:"\\b0B([01_]+)"+"t"},{begin:"\\b0C([0-7_]+)"+"t"},{begin:--begin_h...
...
...
...-9][\\d_*)|0[bB][01_]+|0[xX]([\\da-fA-F][\\da-fA-F_]*|_[\\da-fA-F][\\da-fA-F_]*))",a="\\\\
(['"\\"?\\abfnrtv]|u[\\dA-Fa-f]{4}|[0-7]{1,3}|x[\\dA-Fa-f]{2}|U[\\dA-Fa-f]{8})|[a-zA-Z\\d]
{2,};",n={className:"numbe...
...
...
...vance:0},{className:"symbol",begin:t+:(!:)?",relevance:0},{className:"number",begin:"(\\b0[0-
7_]+)|\\b0x[0-9a-fA-F_]+|((\\b[1-9][0-9_]*\\.[0-9_]+)?|[0_]\\b",relevance:0},
{className:"variable",begin:"(\\...
...
...
...mbol",begin:":(?!\\s)",contains:[s,{begin:t}],relevance:0},{className:"number",begin:"(\\b0[0-
7_]+)|\\b0x[0-9a-fA-F_]+|((\\b[1-9][0-9_]*\\.[0-9_]+)?|[0_]\\b",relevance:0},{begin:"(\\$\\w|
```



```
...\\[\\:];return{aliases:["styl"],case_insensitive:!1,keywords:"if else for in",illegal:("+["\\?","(\\bReturn\\b)","(\\bEnd\\b)","
```

Issue 6 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity: **Informational**

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/dataide/0.39453f26.chunk.js>

Entity: 0.39453f26.chunk.js (Page)

Risk: It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes: Latest patches or hotfixes for 3rd. party products were not installed

Fix: Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...G[W]WWE",/\d{4}W\d{3}/],["GGGG[W]WW",/\d{4}W\d{2}/,!1],["YYYYDDD",/\d{7}/]],qr=[["HH:mm:ss.SSSS",/\d\:\d\:\d\:\d\d\.\d+/],["HH:mm:ss,SSSS",/\d--begin_highlight_ta...  
...  
...group {\n  font-size: 12px;\n}\n.ant-tree-checkbox-group-item {\n  display: inline-block;\n}\n@media \\"\\0screen {\n  .ant-tree-checkbox-checked .ant-tree-checkbox-inner:before,\n  .ant-tree-checkbox-checked .ant...  
...  
...  
...bility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\n  content: \"\\E6AE\";\n  -webkit-animation: loadingCircle 1s infinite linear;\n  animation: loadingCircle 1s i...  
...  
...  
...bility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\n  content: \"\\E606\";\n  font-weight: bold;\n  transition: -webkit-transform .3s;\n  transition: transform .3s;\n  tra...  
...  
...  
...bility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\n  content: \"\\E606\";\n  font-weight: bold;\n  transition: -webkit-transform .3s;\n  transition: transform .3s;\n  tra...  
...  
...bility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\n  content: \"\\E606\";\n  font-weight: bold;\n  transition: -webkit-transform .3s;\n  transition: transform .3s;\n  tra...
```

```

content: "\u2611";\n vertical-align: baseline;\n font-weight: normal;\n transition: -webkit-transform .3s;\n tr...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\n content: "\u2611";\n vertical-align: baseline;\n font-weight: normal;\n transition: -webkit-transform .3s;\n tr...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\n content: "\u2611";\n vertical-align: baseline;\n font-weight: normal;\n transition: -webkit-transform .3s;\n tr...
...
...
...kbox-group {\n font-size: 12px;\n}\n.ant-checkbox-group-item {\n display: inline-block;\n}\n\n@media \\\0screen {\n .ant-checkbox-checked .ant-checkbox-inner:before,\n .ant-checkbox-checked .ant-checkbox-inner...
...
...
...-category .ant-tree.ant-tree li span.ant-tree-switcher.ant-tree-switcher_open::after {\n content: "\u2611";\n font-size: 12px;\n color: #b8c2cf;\n transform: scale(1)\n rotate(0deg);\n zoom: 1;\n displ...
...
...
...height: 48px;\n line-height: 48px;\n font-size: 14px;\n}\n.ant-modal-close-x:before {\n content: "\u2611";\n display: block;\n font-family: "anticon" !important;\n}\n.ant-modal-close:focus,\n.ant-modal...
...
...
...n font-size: 12px;\n}\n.ant-select-tree-checkbox-group-item {\n display: inline-block;\n}\n\n@media \\\0screen {\n .ant-select-tree-checkbox-checked .ant-select-tree-checkbox-inner:before,\n .ant-select-tree-...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\n content: "\u2611";\n -webkit-animation: loadingCircle 1s infinite linear;\n animation: loadingCircle 1s i...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\n content: "\u2611";\n font-weight: bold;\n transition: -webkit-transform .3s;\n transition: transform .3s;\n tra...
...
...
...size: 12px;\n}\n.ant-select-arrow * {\n display: none;\n}\n\n.ant-select-arrow:before {\n content: "\u2611";\n transition: -webkit-transform 0.2s ease;\n transition: transform 0.2s ease;\n transition: t...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\n content: "\u2611";\n}\n\n.ant-select-selection__clear:hover {\n color: rgba(0, 0, 0,

```

```

0.43); \n} \n.ant-select-selection...
...
...
...040; \n} \n.ant-select-selection--multiple .ant-select-selection__choice__remove:before {\n content: "\u2022"; \n} \n.ant-select-selection--multiple .ant-select-selection__clear {\n top: 14px; \n} \n.ant-select...
...
...
...ibility; \n -webkit-font-smoothing: antialiased; \n -moz-osx-font-smooth...

```

Issue 7 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/devportal/res/common/index_445fadca.js
Entity:	index_445fadca.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```

...
...pertyName=l[p]), u.hasOwnProperty(p) && (h.mutationMethod=u[p]), s.properties[p]=h}}}, a=":A-Z_a-
z\\u00c0-\u00d6\\u00d8-\u00f6\\u00f8-\u02ff--e...
...
...
...isplay: block; \n font-family: "anticon" !important; \n anticon-step-forward:before {\n content: --begin_highlight_tag--"\u2022"; \n} \n anticon-step-backward:before {\n content: "\u2022--end_highlight_tag...
...
...
...1(\n font-size: 14px; \n) \n nbbody(\n font-family: Helvetica, Tahoma, Arial, "Microsoft YaHei", --begin_highlight_tag--"\u5fae\u8f6f\u96c5\u9ed1", "PingFang", "\u82f9\u65b9", STHeiti...
...
...
...iated; \n -moz-osx-font-smoothing: grayscale; \n) \n n.common_icon-maven_lftBB:before {\n content: "\u2022"; \n} \n n.common_icon-icon_1_8EoS:before {\n content: "\u2022--end_highlight...
...
...
... antialiased; \n -moz-osx-font-smoothing: grayscale; \n) \n n.dplicon_put_away:before {\n content: "\u2022"; \n} \n n.dplicon_put_away:after {\n content: "\u2022"; \n}

```

```

content: --begin_highlight_tag--"\u2022";\n  }\n\n.dplicon_expand:before {\n    content: "\u2022\u2022";
-end_highlight_tag...
...
...
... to help you send telemetry to the EnOS cloud and receive messages and commands from the EnOS
cloud.--begin_highlight_tag-- \nEnOS also provides service SDKs that you can use to interact
with your service configuration and data in...
...
...
...size: 12px;\n}\n.ant-select-arrow * {\n    display: none;\n}\n.ant-select-arrow:before {\n
content: "\u2022\u2022";\n    transition: transform 0.2s ease;\n}\n.ant-select-selection {\n    outline:
none;\n    user-select...
...
...
...ibility;\n    -webkit-font-smoothing: antialiased;\n    -moz-osx-font-smoothing: grayscale;\n
content: "\u2022\u2022";\n}\n.ant-select-selection__clear:hover {\n    color: rgba(0, 0, 0,
0.43);\n}\n.ant-select-selection...
...
...
...040;\n}\n.ant-select-selection--multiple .ant-select-selection__choice__remove:before {\n
content: "\u2022\u2022";\n}\n.ant-select-selection--multiple .ant-select-selection__clear {\n    top:
14px;\n}\n.ant-select...
...
...
...ibility;\n    -webkit-font-smoothing: antialiased;\n    -moz-osx-font-smoothing: grayscale;\n
content: "\u2022\u2022";\n    color: transparent;\n    display: inline-block;\n    font-size: 12px;\n    font-
size: 10px \u2022;\n    t...
...

```

Issue 8 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/devportal/res/sdk_download/index_60ae0311.js
Entity:	index_60ae0311.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```

...
...isplay: block;\n font-family: "anticon" !important;\n}\n.anticon-step-forward:before {\ncontent: "\\"E600";\n}\n.anticon-step-backward:before {\n content: "\\"E601--end_highlight_tag..."  

...
...
...size: 12px;\n}\n.ant-select-arrow * {\n display: none;\n}\n.ant-select-arrow:before {\ncontent: "--begin_highlight_tag--'\\E61D';\n -webkit-transition: -webkit-transform 0.2s ease;\ntransition: -webkit-transform 0.2s ease;\n...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\ncontent: "\\"E62E";\n}\n.ant-select-selection__clear:hover {\n color: rgba(0, 0, 0, 0.43);\n}\n.ant-select-selection...
...
...
...040;\n}\n.ant-select-selection--multiple .ant-select-selection__choice__remove:before {\ncontent: "\\"E633";\n}\n.ant-select-selection--multiple .ant-select-selection__clear {\n top: 14px;\n}\n.ant-select-...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\ncontent: "\\"E632";\n color: transparent;\n display: inline-block;\n font-size: 12px;\n font-size: 10px \\"9;\n ...
...
...
...n}\n.ant-carousel .slick-prev {\n left: -25px;\n}\n.ant-carousel .slick-prev:before {\ncontent: "\\"2190";\n}\n.ant-carousel .slick-next {\n right: -25px;\n}\n.ant-carousel .slick-next:before {\n conten...
...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\ncontent: "\\"E61F";\n display: inline-block;\n font-size: 12px;\n font-size: 8px \\"9;\n -webkit-transform: scale(...  

...
...
...bility;\n -webkit-font-smoothing: antialiased;\n -moz-osx-font-smoothing: grayscale;\ncontent: "\\"E64D";\n -webkit-animation: loadingCircle 1s infinite linear;\n animation: loadingCircle 1s in...
...
...
...in-right: 0;\n}\n.ant-checkbox-group-item + .ant-checkbox-group-item {\n margin-left: 0;\n}\n@media \\"@screen {\n .ant-checkbox-checked .ant-checkbox-inner:before,\n .ant-checkbox-checked .ant-checkbox-inner...
...
...
...mportant;\n}\n.ant-collapse > .ant-collapse-item > .ant-collapse-header .arrow:before {\ncontent: "\\"E61F";\n}\n.ant-collapse-anim-active {\n -webkit-transition: height 0.2s cubic-bezier(0.215, 0.61, 0.35...
...
...
...ndar-picker-icon {\n color: rgba(0, 0, 0, 0.43);\n}\n.ant-calendar-picker-icon:after {\ncontent: "\\"E6BB";\n font-family: "anticon";\n font-size: 12px;\n color: rgba(0, 0, 0, 0.43);\n display: inline-...
...
...
...nth-btn {\n left: 29px;\n}\n.ant-calendar-header .ant-calendar-prev-month-btn:after {\n

```

```

content: '\u2039';\n}.ant-calendar-header .ant-calendar-next-month-btn {\n  right:
29px;\n}.ant-calendar-header...
...
...
...ibility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\ncontent: "\uE62E";\n  font-size: 12px;\n  color: rgba(0, 0, 0, 0.25);\n  display: inline-block;\nline-height: 1;\n...
...
...
...\n}.ant-calendar-month-panel-header .ant-calendar-month-panel-prev-month-btn:after {\ncontent: '\u2039';\n}.ant-calendar-month-panel-header .ant-calendar-month-panel-next-month-
btn {\n  right: 29px;\n...
...
...
...x;\n}.ant-calendar-year-panel-header .ant-calendar-year-panel-prev-month-btn:after {\ncontent: '\u2039';\n}.ant-calendar-year-panel-header .ant-calendar-year-panel-next-month-
btn {\n  right: 29px;\n...
...
...
...}\n}.ant-calendar-decade-panel-header .ant-calendar-decade-panel-prev-month-btn:after {\ncontent: '\u2039';\n}.ant-calendar-decade-panel-header .ant-calendar-decade-panel-next-month-
btn {\n  right: 29px...
...
...
...ibility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\ncontent: "\uE62E";\n}.ant-time-picker-panel-clear-btn:hover:after {\n  color: rgba(0, 0, 0,
0.43);\n}.ant-time-p...
...
...
...gba(0, 0, 0, 0.43);\n  top: 50%;\n  margin-top: -6px;\n}.ant-time-picker-icon:after {\ncontent: "\uE641";\n  font-family: "anticon";\n  font-size: 12px;\n  color: rgba(0, 0, 0,
0.43);\n  display: block;\n...
...
...
...menu-submenu-title:after {\n  font-family: "anticon" !important;\n  positio...

```

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-api/res/apimanagement/index_f20f1232.js
Entity:	index_f20f1232.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...  
... (?:1?\d{1,2}|\d[0-4]\d|25[0-5])) {2} (?:\.\.(?:[0-9]\d?|1\d|\d2[0-4]\d|25[0-4])) | (?:(?:[a-  
z]\u00a1-\uffff0-9]+?)*)[a-z]\u00a1-\uffff0-9]+) (?:\.\.(?:[a-z]\u00a1--b...  
...
```

Issue 10 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/devportal/res/login/index_df108705.js
Entity:	index_df108705.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...G[W]WWE", /\d{4}W\d{3}/], ["GGGG[W]WW", /\d{4}W\d{2}/,!1], ["YYYYDDD", /\d{7}/]], Mt=  
[ "HH:mm:ss.SSSS", /\d:\d:\d\d\.\d+/], ["HH:mm:ss,SSSS", /\d--begin_highlight_ta...
```

...

...

```

...isplay: block;\n font-family: "anticon" !important;\n}.anticon-step-forward:before {\n content: "\u2022";\n}.anticon-step-backward:before {\n content: "\u2022--end_highlight_tag..."}
...
...
... (?::1?\d{1,2}|2[0-4]\d|25[0-5])){2} (?::\.(?:[0-9]\d?|1\d|\d|2[0-4]\d|25[0-4]))|(?:(?:[a-z]\u00a1--begin_highlight_tag---\uffff0-9]+?)*)[a-z]\u00a1-\uffff0-9]+)(?:\.(?:[a-z]\u00a1--b...
...
...
...height: 56px;\n line-height: 56px;\n font-size: 14px;\n}.ant-modal-close-x:before {\n content: "\u2022";\n display: block;\n font-family: "anticon" !important;\n}.ant-modal-close:focus,\n}.ant-modal...
...
...
...as-feedback .ant-form-item-children:after {\n animation-name: diffZoomIn1 !important;\n content: "\u2022";\n color: #52c41a;\n}.has-warning .ant-form-explain,\n.has-warning .ant-form-split {\n color:...
...
...
...ack {\n color: #faad14;\n}.has-warning.has-feedback .ant-form-item-children:after {\n content: "\u2022";\n color: #faad14;\n animation-name: diffZoomIn3 !important;\n}.has-warning .ant-select-select...
...
...
...dback {\n color: #f5222d;\n}.has-error.has-feedback .ant-form-item-children:after {\n content: "\u2022";\n color: #f5222d;\n animation-name: diffZoomIn2 !important;\n}.has-error .ant-select-select...
...
...
...ldren:after {\n display: inline-block;\n animation: loadingCircle 1s infinite linear;\n content: "\u2022";\n color: #0058FF;\n}.ant-advanced-search-form .ant-form-item {\n margin-bottom: 24px;\n}.ant...
...
...
... (?::1?\d{1,2}|2[0-4]\d|25[0-5])){2} (?::\.(?:[0-9]\d?|1\d|\d|2[0-4]\d|25[0-4]))|(?:(?:[a-z]\u00a1-\uffff0-9]+?)*)[a-z]\u00a1-\uffff0-9]+)(?:\.(?:[a-z]\u00a1--b...
...
...
...height: 48px;\n line-height: 48px;\n font-size: 14px;\n}.ant-modal-close-x:before {\n content: "\u2022";\n display: block;\n font-family: "anticon" !important;\n}.ant-modal-close:focus,\n}.ant-modal...
...
...
...ter {\n animation-name: diffZoomIn3 !important;\n}.has-success.has-feedback:after {\n content: "\u2022";\n color: #00a854;\n}.has-warning .ant-form-explain,\n.has-warning .ant-form-split {\n color:...
...
...
...n.has-warning.has-feedback {\n color: #ffbf00;\n}.has-warning.has-feedback:after {\n content: "\u2022";\n color: #ffbf00;\n}.has-warning .ant-select-selection {\n border-color: #ffbf00;\n}.has-w...
...
...
...\n}.has-error.has-feedback {\n color: #f04134;\n}.has-error.has-feedback:after {\n content: "\u2022";\n color: #f04134;\n}.has-error .ant-select-selection {\n border-color: #f04134;\n}.has-err...

```

```

...
...dback:after {\n  display: inline-block;\n  animation: loadingCircle 1s infinite linear;\n  content: "\u2196";\n  color: #108ee9;\n}\n.ant-advanced-search-form .ant-form-item {\n  margin-bottom: 16px;\n}\n.an...
...

```

Issue 11 of 13

[TOC](#)

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal-api/res/vendor/index_183eb259.js
Entity:	index_183eb259.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```

...
...G[W]WWE",/\d{4}W\d{3}/],["GGGG[W]WW",/\d{4}W\d{2}/,!1],["YYYYDDD",/\d{7}/]],bt=
[["HH:mm:ss.SSSS",/\d:\d:\d\d.\d+\d+],["HH:mm:ss,SSSS",/\d--begin_highlight_ta...
...
...
...-9]\d*)$/ ,Ke=/[\xc0-\xd6\xd8-\xf6\xf8-\xff\u0100-
\u017f]/g,Je=/($^)/,$e=['\n\r\u2028\u2029\\']/g,Xe="\u0300-\u036f\ufe20-\ufe2f--end_high...
...
...
...+(?:['â'](?:d|l|m|r|s|t|v)e))?",dt+"+(?:['â'](?:D|L|M|R|S|T|V)e))?", "\d*(?:1ST|2ND|3RD|(?!
[123]--begin_highlight_tag--)\dTH)(?=\\b|[a-z_])","\\d*(?:1st|2nd|3rd|(?![123])\\dth)(?=\\...
...

```

Issue 12 of 13

[TOC](#)

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/devportal/res/index/index_6ef3d11b.js
Entity:	index_6ef3d11b.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...
...G[W]WWE",/\d{4}W\d{3}/],["GGGG[W]WW",/\d{4}W\d{2}/,!1],["YYYYDDD",/\d{7}/]],ke=
[["HH:mm:ss.SSSS",/\d\:\d\:\d\:\d\.\d+/],["HH:mm:ss,SSSS",/\d--begin_highlight_ta...
...
...
...isplay: block;\n font-family: "anticon" !important;\n\n.anticon-step-forward:before {\n content: "\\"E600";\n}\n.anticon-step-backward:before {\n content: "\\"E601--end_highlight_tag...
...
...
... (?1?\d{1,2})2[0-4]\d{25[0-5])){2} (?:\.\.(?:[0-9]\d?1\d\d\d2[0-4]\d{25[0-4]}))|(?:(?:[a-z]\u00a1--begin_highlight_tag---\uffff0-9]+?)*[a-z]\u00a1-\uffff0-9+)(?:\.\.(?:[a-z]\u00a1--b...
...
...
...height: 56px;\n line-height: 56px;\n font-size: 14px;\n\n.ant-modal-close-x:before {\n content: "\\"E633";\n display: block;\n font-family: "anticon" !important;\n}\n.ant-modal-close:focus,\n.ant-modal...
...
...
...as-feedback .ant-form-item-children:after {\n animation-name: diffZoomIn1 !important;\n content: '\\"E630\\';\n color: #52c41a;\n}\n.has-warning .ant-form-explain,\n.has-warning .ant-form-split {\n color:...
...
...
...ack {\n color: #faad14;\n}\n.has-warning.has-feedback .ant-form-item-children:after {\n content: '\\"E62C\\';\n color: #faad14;\n animation-name: diffZoomIn3 !important;\n}\n.has-warning .ant-select-select...
...
...
...dback {\n color: #f5222d;\n}\n.has-error.has-feedback .ant-form-item-children:after {\n content: '\\"E62E\\';\n color: #f5222d;\n animation-name: diffZoomIn2 !important;\n}\n.has-error .ant-select-select...
...
...
...ldren:after {\n display: inline-block;\n animation: loadingCircle 1s infinite linear;\n content: "\\"E64D\\";\n color: #0058FF;\n}\n.ant-advanced-search-form .ant-form-item {\n margin-bottom: 24px;\n}\n.an...
```

```

...
...!important;\n}\n.ant-select-arrow * {\n  display: none;\n}\n.ant-select-arrow:before {\n  content: "\\\xE61D\";\n  transition: transform .3s;\n}\n.ant-select-selection {\n  outline: none;\n  user-select: none...
...

...
...ibility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\n  content: "\\\xE62E";\n}\n.ant-select-selection__clear:hover {\n  color: rgba(0, 0, 0, 0.45); \n}\n.ant-select-selection...
...

...
...040;\n}\n.ant-select-selection--multiple .ant-select-selection__choice__remove:before {\n  content: "\\\xE633";\n}\n.ant-select-selection--multiple .ant-select-selection__clear {\n  top: 16px; \n}\n.ant-select-...
...

...
...ibility;\n  -webkit-font-smoothing: antialiased;\n  -moz-osx-font-smoothing: grayscale;\n  content: "\\\xE632";\n  color: transparent;\n  display: inline-block;\n  font-size: 12px;\n  font-size: 10px \\\9;\n  t...
...

...
...menu-submenu-arrow:after {\n  font-family: "anticon" !important;\n  font-style: normal;\n  content: "\\\xE61F";\n  color: rgba(0, 0, 0, 0.45);\n  display: inline-block;\n  font-size: 12px;\n  font-size: 10px \...
...

```

Issue 13 of 13

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://portal-ippe1.eniot.io/portal/res/commons/index_6b2dae79.js
Entity:	index_6b2dae79.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```

...
...-9]\d*)$/ ,qe=/[\xc0-\xd6\xd8-\xf6\xf8-\xff\u0100-

```

```
\u017f]/g,Qe=/($^)/,ze=/^'\n\r\u2028\u2029\\]/g,Je="\u0300-\u036f\ufe20-\ufe2f--end_high...
```

```
...
```

```
... (?1?\d{1,2}2[0-4]\d{5}){2} (?\\.(?:[0-9]\d?1\d{2}[0-4]\d{4})|(?:(?:[az]\u00a1--begin_highlight_tag---\uffff0-9]+?)*(a-z\u00a1-\uffff0-9)+) (?\\.(?:[az]\u00a1--b...)
```

```
...
```

SHA-1 cipher suites were detected 1

TOC

Issue 1 of 1

TOC

SHA-1 cipher suites were detected

Severity: Informational

CVSS Score: 0.0

URL: <https://portal-ippe1.eniot.io/>

Entity: portal-ippe1.eniot.io (Page)

Risk: It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes: The web server or application server are configured in an insecure way

Fix: Change server's supported ciphersuites

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Verify that the site uses the cryptographically weak cipher suites listed here.

The following weak cipher suites are supported by the server:

Id	Name	SSL Version
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
53	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.2
65	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS 1.2
132	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS 1.2
49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.2