Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by HCL AppScan Standard 10.3.0
Scan started: 11/17/2023 6:30:04 PM

Table of Contents

Introduction

Summary

Issues Sorted by Issue Type

Introduction

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

High severity issues:	1
Medium severity issues:	23
Informational severity issues:	30
Total security issues included in the report:	55
Total security issues discovered in the scan:	55

General Information

Scan file name:	Untitled
Scan started:	11/17/2023 6:30:04 PM
Test policy:	Default
CVSS version:	3.1
Test optimization level:	Fast

Host	10.163.2.181
Port	8080
Operating system:	Unknown
Web server:	Oracle Web Listener
Application server:	PHP

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
In-session detection:	Enabled
In-session pattern:	
Tracked or session ID cookies:	
Tracked or session ID parameters:	
Login sequence:	

Summary

Issue Types 15

TOC

	Issue Type	Number of Issues
H	Unencrypted Login Request	1
M	Body Parameters Accepted in Query	5
M	Cookie with Insecure or Improper or Missing SameSite attribute	2
M	Directory Listing	1
M	Directory Listing Pattern Found	1
M	Missing "Content-Security-Policy" header	1
M	Missing or insecure "X-Content-Type-Options" header	1
M	Overly Permissive CORS Access Policy	1
M	Vulnerable Component	12
I	Client-Side (JavaScript) Cookie References	2
I	Email Address Pattern Found	1
I	Internal IP Disclosure Pattern Found	23
I	Missing "Referrer policy" Security Header	1
I	Possible Server Path Disclosure Pattern Found	1
I	Potential File Upload	2

Vulnerable URLs 34

TOC

	URL	Number of Issues
🟩	http://10.163.2.181:8080/sscsr_audit/dataentry/js/	12
H	http://10.163.2.181:8080/sscsr_audit/dataentry/login.php	2
M	http://10.163.2.181:8080/sscsr_audit/dataentry/admit_card_download_datatable.php	1
M	http://10.163.2.181:8080/sscsr_audit/dataentry/create_table.php	1
M	http://10.163.2.181:8080/sscsr_audit/dataentry/upload_admitcard_important_instructions.php	2
M	http://10.163.2.181:8080/sscsr_audit/dataentry/upload_excel_file.php	2
M	http://10.163.2.181:8080/	7
M	http://10.163.2.181:8080/sscsr_audit/dataentry/index.php	1
M	http://10.163.2.181:8080/sscsr_audit/dataentry/js/jquery.validate.min.js	2

I	http://10.163.2.181:8080/sscsr_audit/dataentry/js/jquery-ui.min.js	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/js/jquery.cookie.js	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/js/pdfmake.min.js	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/css/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/all.js	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/all.min.js	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/brands.js	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/brands.min.js	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/metadata/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/metadata/icon-families.json	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/metadata/icons.json	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/sprites/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/brands/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/regular/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/solid/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/webfonts/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/images/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/images/icons/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/images/logo/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/images/users/	1
I	http://10.163.2.181:8080/sscsr_audit/dataentry/log/	1

Fix Recommendations 14

TOC

	Remediation Task	Number of Issues
H	Always use SSL and POST (body) parameters when sending sensitive information.	1
H	Upgrade the component to the latest stable version	12
M	Config your server to use the "Content-Security-Policy" header with secure policies	1
M	Config your server to use the "X-Content-Type-Options" header with "nosniff" value	1
M	Do not accept body parameters that are sent in the query string	5
M	Modify the "Access-Control-Allow-Origin" header to contain only allowed sites	1
M	Modify the server configuration to deny directory listing, and install the latest security patches available	2
M	Review possible solutions for configuring SameSite Cookie attribute to recommended values	2
L	Config your server to use the "Referrer Policy" header with secure policies	1
L	Download the relevant security patch for your web server or web application.	1
L	Remove business and security logic from the client side	2

L	Remove e-mail addresses from the website	1
L	Remove internal IP addresses from your website	23
L	Restrict user capabilities and permissions during the file upload process	2

Security Risks 10

TOC

	Risk	Number of Issues
H	It may be possible to steal user login information such as usernames and passwords that are sent unencrypted	1
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	33
M	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	9
M	Prevent cookie information leakage by restricting cookies to first-party or same-site context, Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).	2
M	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files	2
I	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side	2
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	1
I	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents	2
I	It is possible to upload, modify or delete web pages, scripts and files on the web server	2

Causes 8

TOC

	Cause	Number of Issues
H	SSL (Secure Socket Layer) provides data confidentiality and integrity to HTTP. By encrypting HTTP messages, SSL protects from attackers eavesdropping or altering message contents. Login pages should always employ SSL to protect the user name and password while they are in transit from the client to the server. Lack of SSL use exposes the user credentials as clear text during transmission to the server and thus makes the credentials susceptible to eavesdropping.	1
M	Insecure web application programming or configuration	33
M	Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute	2
M	Directory browsing is enabled	2
🟩	A vulnerable component is used in the tested application.	12
I	Cookies are created at the client side	2
I	Latest patches or hotfixes for 3rd. party products were not installed	1
I	The software allows the attacker to upload or transfer files of dangerous types (for example, containing malicious code) and unlimited size that could be automatically processed within the product's environment.	2

WASC Threat Classification

TOC

Threat	Number of Issues
Abuse of Functionality	14
Directory Indexing	2
Information Leakage	36
Insufficient Transport Layer Protection	1
Server Misconfiguration	2

Issues Sorted by Issue Type

H Unencrypted Login Request 1 TOC

Issue 1 of 1 TOC

Unencrypted Login Request	
Severity:	High
CVSS Score:	8.2
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/login.php
Entity:	pass (Parameter)
Risk:	It may be possible to steal user login information such as usernames and passwords that are sent unencrypted
Cause:	SSL (Secure Socket Layer) provides data confidentiality and integrity to HTTP. By encrypting HTTP messages, SSL protects from attackers eavesdropping or altering message contents. Login pages should always employ SSL to protect the user name and password while they are in transit from the client to the server. Lack of SSL use exposes the user credentials as clear text during transmission to the server and thus makes the credentials susceptible to eavesdropping.
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Reasoning: AppScan identified a password parameter that was not sent over SSL.

Original Request

```
...

Content-Type: application/x-www-form-urlencoded
Cookie: name=value; PHPSESSID=5k44cos7uiiungervnu7rql1nb
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.181:8080/sscsr_audit/dataentry/login.php
Host: 10.163.2.181:8080
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 125

user=Exceluploader&pass=Admin%40123&csrf_token=c7e03885564ba36dd35c5727ba51d07ac3831d8df853c6cd2d5fa4a2bd2a8ae8&submit=Subm
it

HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 12:54:58 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 7311

...
```

M Body Parameters Accepted in Query 5

TOC

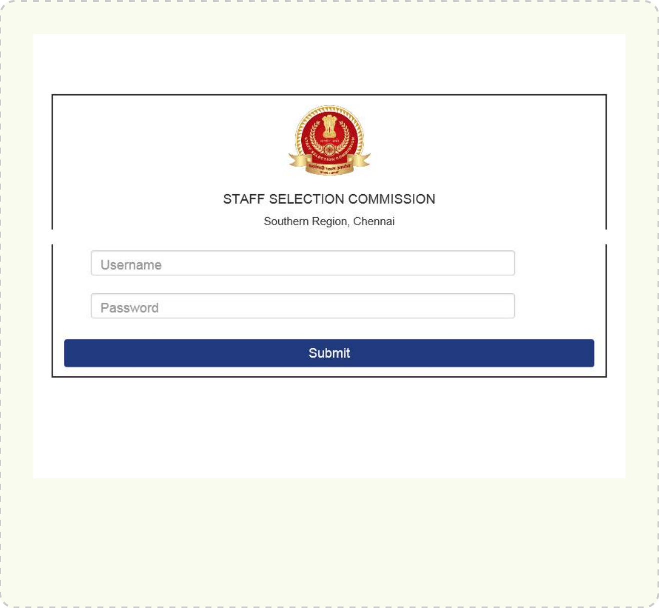
Issue 1 of 5

TOC

Body Parameters Accepted in Query	
Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/create_table.php
Entity:	create_table.php (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.
Cause:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

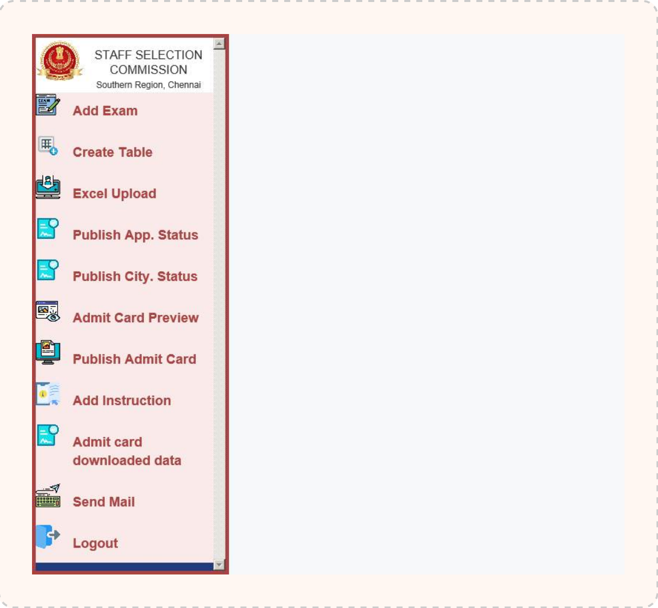
Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Original Response



≈

Test Response



Issue 2 of 5

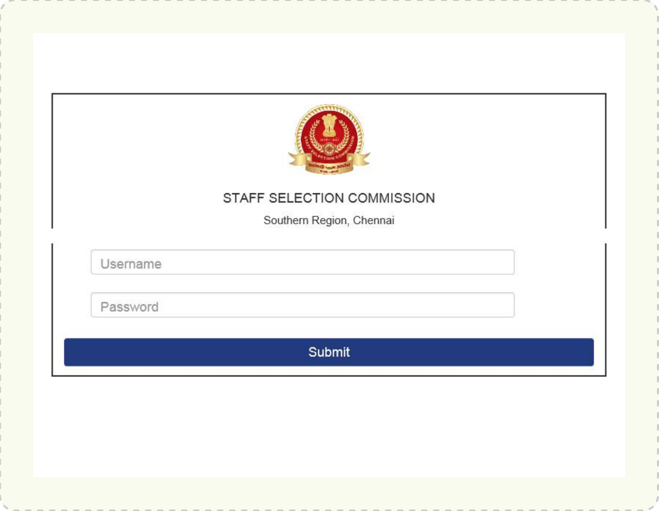
TOC

Body Parameters Accepted in Query

Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/login.php
Entity:	login.php (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.
Cause:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

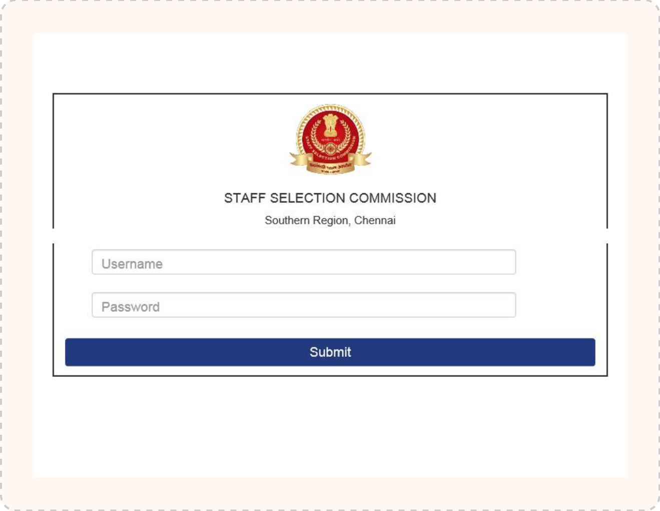
Original Response



STAFF SELECTION COMMISSION
Southern Region, Chennai

≈

Test Response



STAFF SELECTION COMMISSION
Southern Region, Chennai

Issue 3 of 5

TOC

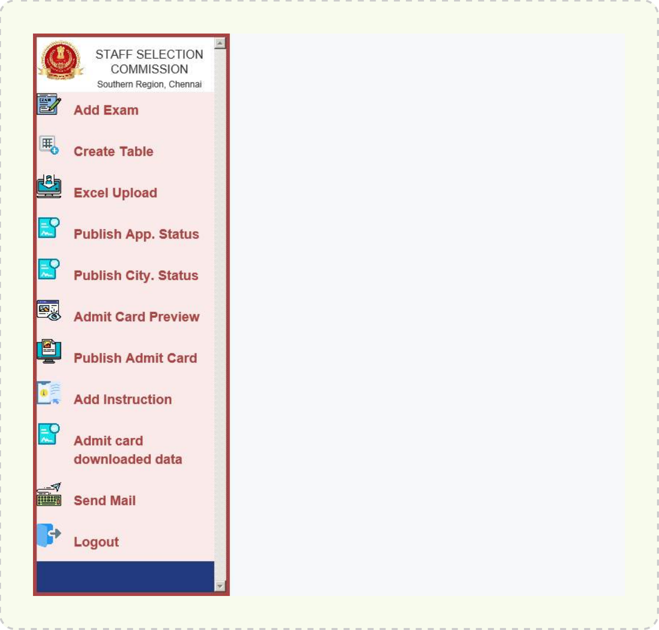
Body Parameters Accepted in Query

Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/admit_card_download_datatable.php
Entity:	admit_card_download_datatable.php (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.
Cause:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

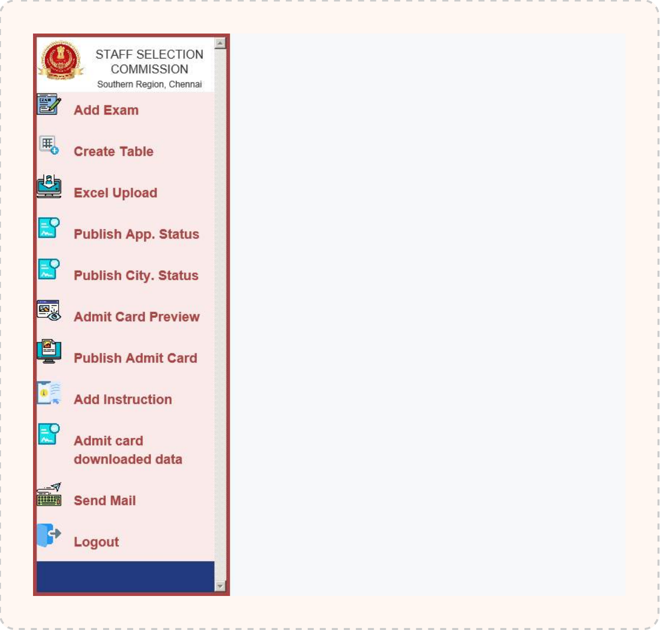
Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Original Response

Test Response



≈



Issue 4 of 5

TOC

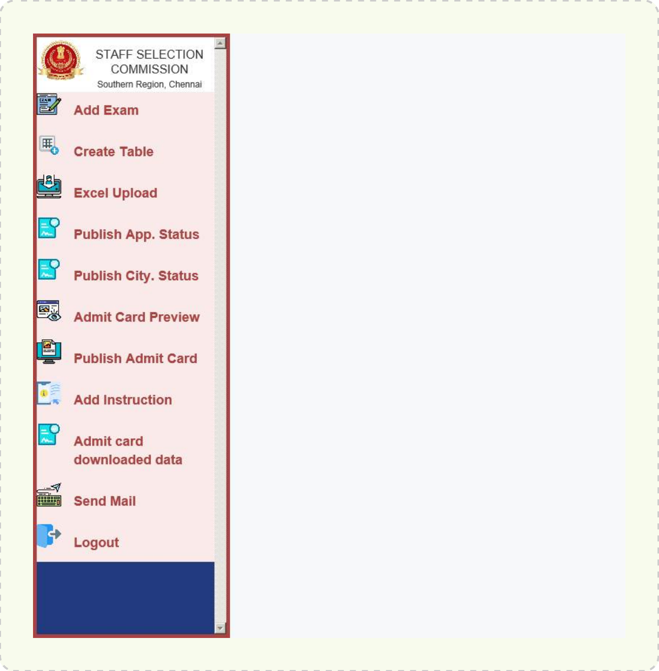
Body Parameters Accepted in Query

Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/upload_excel_file.php
Entity:	upload_excel_file.php (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.
Cause:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

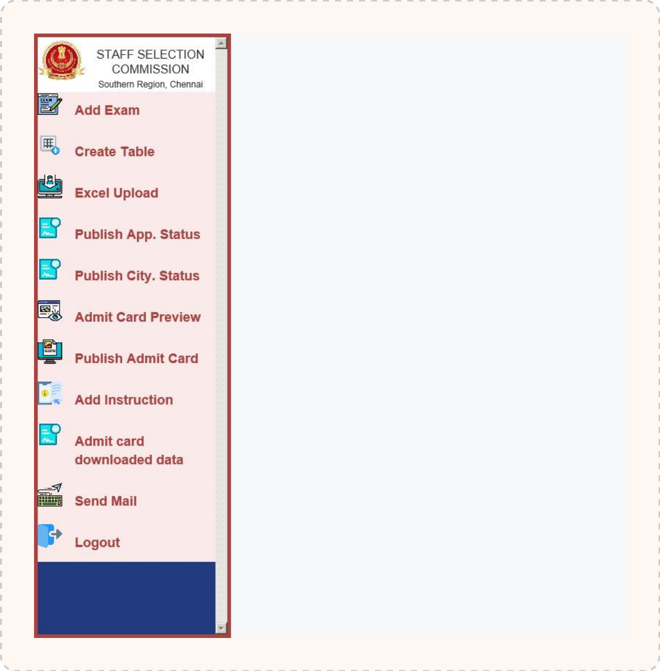
Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Original Response

Test Response



≈



Issue 5 of 5

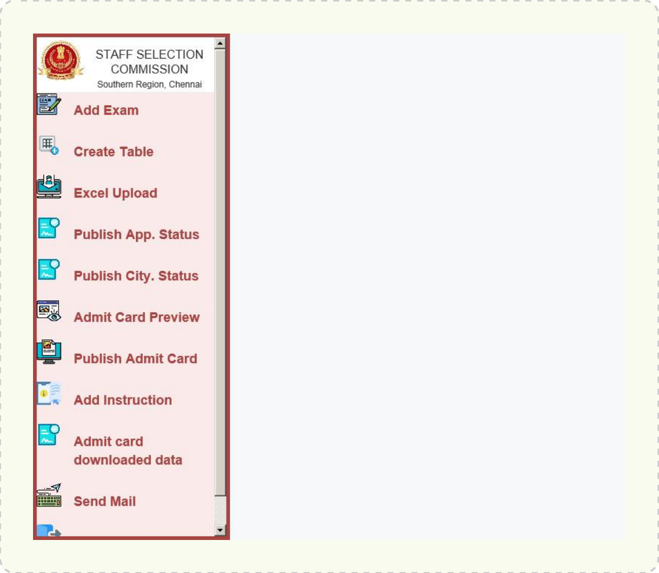
TOC

Body Parameters Accepted in Query

Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/upload_admitcard_important_instructions.php
Entity:	upload_admitcard_important_instructions.php (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.
Cause:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

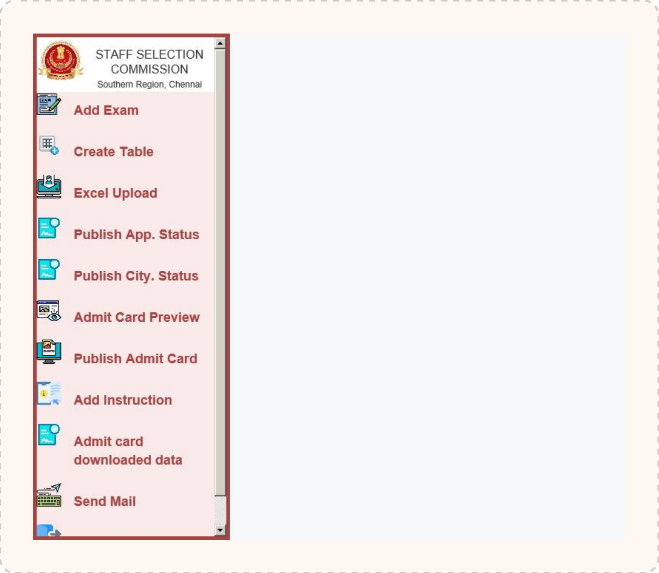
Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Original Response **Test Response**



STAFF SELECTION COMMISSION
Southern Region, Chennai

≈



STAFF SELECTION COMMISSION
Southern Region, Chennai

M Cookie with Insecure or Improper or Missing SameSite attribute 2

TOC

Issue 1 of 2

TOC

Cookie with Insecure or Improper or Missing SameSite attribute

Severity:	Medium
CVSS Score:	4.7
URL:	http://10.163.2.181:8080/
Entity:	PHPSESSID (Cookie)
Risk:	Prevent cookie information leakage by restricting cookies to first-party or same-site context, Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).
Cause:	Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute
Fix:	Review possible solutions for configuring SameSite Cookie attribute to recommended values

Reasoning: The response contains Sensitive Cookie with Insecure or Improper or Missing SameSite attribute, which may lead to Cookie information leakage, which may extend to Cross-Site-Request-Forgery(CSRF) attacks if there are no additional protections in place.

Original Response

```
...

Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 6835
Keep-Alive: timeout=5, max=22
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
Set-Cookie: PHPSESSID=me5jvpdronnpbdt01d5m19daio; path=/

<!doctype html>
<html>
<title>SSCSR</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="stylesheet" href="css/bootstrap.css">
<link rel="icon" type="image/png" sizes="16x16" href="images/logo/logo.png">
<link rel="stylesheet" href="css\sweetalert2.min.css">

...
```

Issue 2 of 2

TOC

Cookie with Insecure or Improper or Missing SameSite attribute

Severity:	Medium
CVSS Score:	4.7
URL:	http://10.163.2.181:8080/
Entity:	name (Cookie)
Risk:	Prevent cookie information leakage by restricting cookies to first-party or same-site context, Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).
Cause:	Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute
Fix:	Review possible solutions for configuring SameSite Cookie attribute to recommended values

Reasoning: The response contains Sensitive Cookie with Insecure or Improper or Missing SameSite attribute, which may lead to Cookie information leakage, which may extend to Cross-Site-Request-Forgery(CSRF) attacks if there are no additional protections in place.

Original Response

```
...

Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 0; mode=block
Access-Control-Allow-Origin: *
content-secuity-policy: default-src 'self'
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Set-Cookie: name=value; HttpOnly

 <!DOCTYPE html>
<head>
 <title>SSCSR</title>
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
 <link rel="icon" type="image/png" sizes="16x16" href="images/logo/logo.png">
 <script type="application/x-javascript">
  addEventListener("load", function() {

...
```

M Directory Listing 1

TOC

Issue 1 of 1

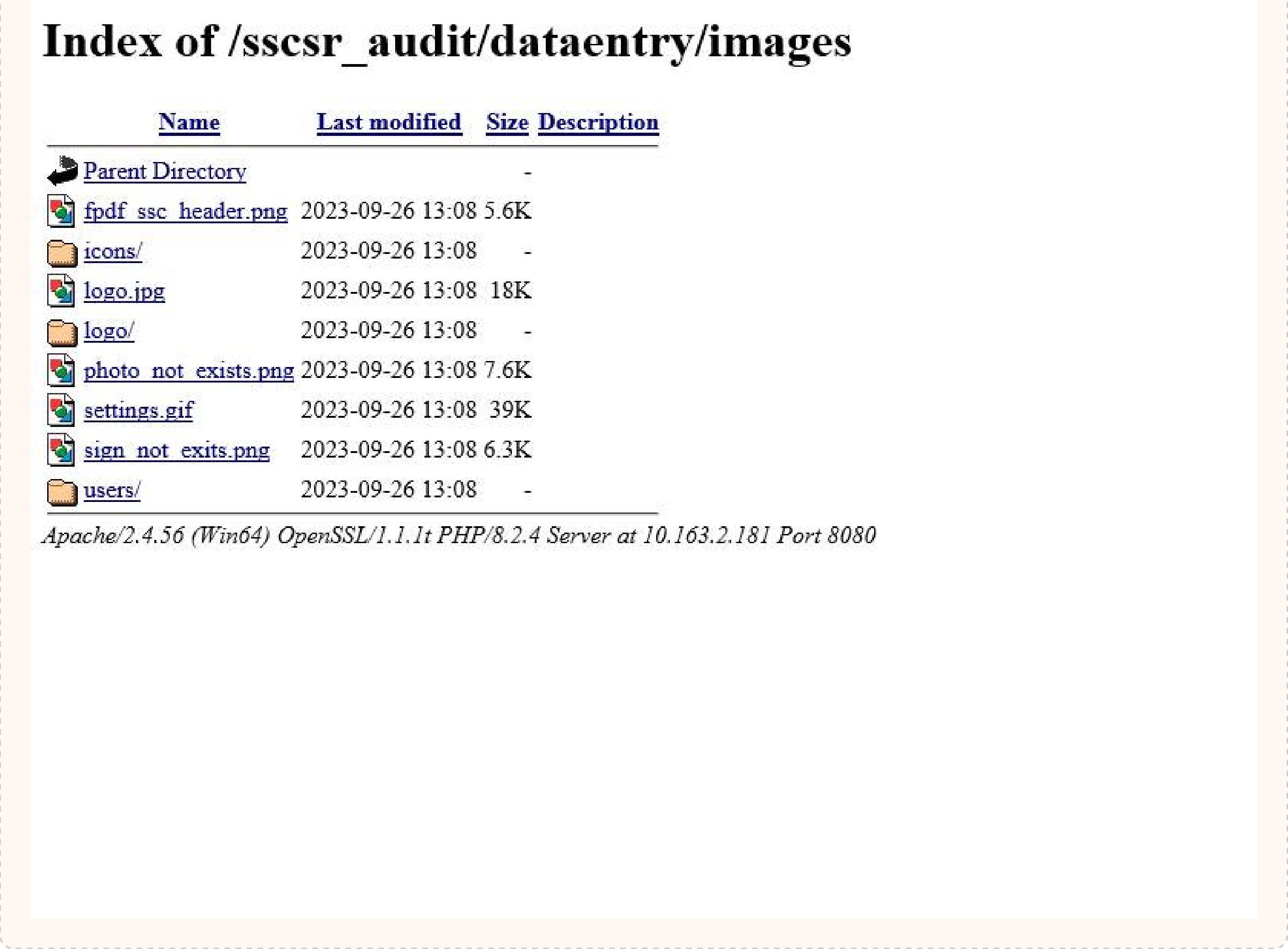
TOC

Directory Listing

Severity:	**Medium**
CVSS Score:	6.5
URL:	http://10.163.2.181:8080/
Entity:	10.163.2.181 (Page)
Risk:	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Cause:	Directory browsing is enabled
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Reasoning: The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Test Response



Index of /sscsr_audit/dataentry/images

Name	Last modified	Size	Description
Parent Directory		-	
fpdf_ssc_header.png	2023-09-26 13:08	5.6K	
icons/	2023-09-26 13:08	-	
logo.jpg	2023-09-26 13:08	18K	
logo/	2023-09-26 13:08	-	
photo_not_exists.png	2023-09-26 13:08	7.6K	
settings.gif	2023-09-26 13:08	39K	
sign_not_exits.png	2023-09-26 13:08	6.3K	
users/	2023-09-26 13:08	-	

Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080

M Directory Listing Pattern Found 1

TOC

Issue 1 of 1

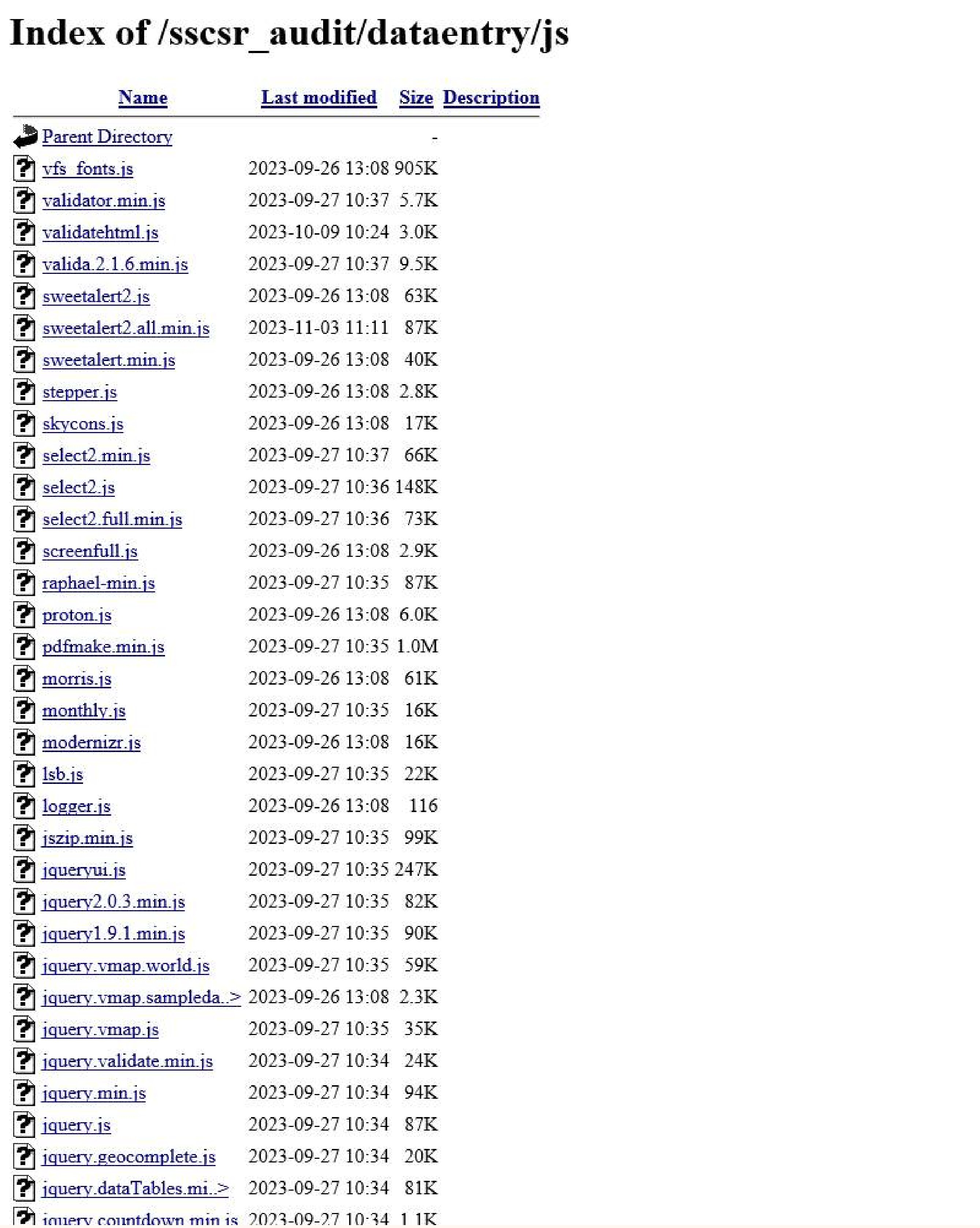
TOC

Directory Listing Pattern Found

Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/
Entity:	10.163.2.181 (Page)
Risk:	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Cause:	Directory browsing is enabled
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Reasoning: The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Test Response



Index of /sscsr_audit/dataentry/js

Name	Last modified	Size	Description
Parent Directory		-	
vfs_fonts.js	2023-09-26 13:08	905K	
validator.min.js	2023-09-27 10:37	5.7K	
validatehtml.js	2023-10-09 10:24	3.0K	
valida.2.1.6.min.js	2023-09-27 10:37	9.5K	
sweetalert2.js	2023-09-26 13:08	63K	
sweetalert2.all.min.js	2023-11-03 11:11	87K	
sweetalert.min.js	2023-09-26 13:08	40K	
stepper.js	2023-09-26 13:08	2.8K	
skycons.js	2023-09-26 13:08	17K	
select2.min.js	2023-09-27 10:37	66K	
select2.js	2023-09-27 10:36	148K	
select2.full.min.js	2023-09-27 10:36	73K	
screenfull.js	2023-09-26 13:08	2.9K	
raphael-min.js	2023-09-27 10:35	87K	
proton.js	2023-09-26 13:08	6.0K	
pdfmake.min.js	2023-09-27 10:35	1.0M	
morris.js	2023-09-26 13:08	61K	
monthly.js	2023-09-27 10:35	16K	
modernizr.js	2023-09-26 13:08	16K	
lsb.js	2023-09-27 10:35	22K	
logger.js	2023-09-26 13:08	116	
jszip.min.js	2023-09-27 10:35	99K	
jqueryui.js	2023-09-27 10:35	247K	
jquery2.0.3.min.js	2023-09-27 10:35	82K	
jquery1.9.1.min.js	2023-09-27 10:35	90K	
jquery.vmap.world.js	2023-09-27 10:35	59K	
jquery.vmap.sampleda..>	2023-09-26 13:08	2.3K	
jquery.vmap.js	2023-09-27 10:35	35K	
jquery.validate.min.js	2023-09-27 10:34	24K	
jquery.min.js	2023-09-27 10:34	94K	
jquery.js	2023-09-27 10:34	87K	
jquery.geocomplete.js	2023-09-27 10:34	20K	
jquery.dataTables.mi..>	2023-09-27 10:34	81K	
jquery.countdown.min.js	2023-09-27 10:34	1.1K	

M Missing "Content-Security-Policy" header 1

TOC

Issue 1 of 1

TOC

Missing "Content-Security-Policy" header

Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/
Entity:	10.163.2.181 (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.
Cause:	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:

```
...

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: */*
Accept-Language: en-US
Referer: http://10.163.2.181:8080/sscsr_audit/dataentry/login.php
Connection: keep-alive
Cookie: name=value; PHPSESSID=5k44cos7uiiungervnu7rql1nb
Content-Length: 0


HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 13:00:45 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Last-Modified: Wed, 27 Sep 2023 05:04:56 GMT
ETag: "5f8f-6065021e72a74"
Accept-Ranges: bytes
Content-Length: 24463
Keep-Alive: timeout=5, max=86
Connection: Keep-Alive
Content-Type: application/javascript

!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof module&&mod...

...
```

M Missing or insecure "X-Content-Type-Options" header 1 TOC

Issue 1 of 1 TOC

Missing or insecure "X-Content-Type-Options" header	
Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/
Entity:	10.163.2.181 (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.
Cause:	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:

```
...

Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.181:8080/sscsr_audit/dataentry/index.php
Host: 10.163.2.181:8080
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: name=value; PHPSESSID=5k44cos7uiiungervnu7rql1nb
Content-Length: 0


HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 12:56:23 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<!-- session -->
 <!-- header -->
 <!DOCTYPE html>
<head>
 <title>SSCSR</title>
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
 <link rel="icon" type="image/png" sizes="16x16" href="images/logo/logo.png">
 <script type="application/x-javascript">
  addEventListener("load", function() {

...
```

M Overly Permissive CORS Access Policy 1 TOC

Issue 1 of 1 TOC

Overly Permissive CORS Access Policy	
Severity:	**Medium**
CVSS Score:	5.3
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/index.php
Entity:	index.php (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.
Cause:	Insecure web application programming or configuration
Fix:	Modify the "Access-Control-Allow-Origin" header to contain only allowed sites

Reasoning: AppScan detected that the "Access-Control-Allow-Origin" header is too permissive

Raw Test Response:

```
...

HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 12:56:27 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 0; mode=block
Access-Control-Allow-Origin: *
content-secuity-policy: default-src 'self'
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Set-Cookie: name=value; HttpOnly

 <!DOCTYPE html>
<head>
 <title>SSCSR</title>
 <meta name="viewport" content="width=device-width, initial-scale=1">

...
```

Vulnerable Component 12

TOC

Issue 1 of 12

TOC

Vulnerable Component

Severity:	
CVSS Score:	6.1
CVE:	CVE-2020-11022
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 3.3.1 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Issue 2 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	5.3
CVE:	CVE-2007-3205
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/jquery.validate.min.js
Entity:	PHP 8.2.4 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Raw Test Response:

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 13:02:35 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Last-Modified: Wed, 27 Sep 2023 05:04:56 GMT
ETag: "5f8f-6065021e72a74"
Accept-Ranges: bytes
```

```
Content-Length: 24463
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/javascript

!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof module&&module.exports?
module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,{validate:function(b){if(!this.length)return
void(b&&b.debug&&window.console&&console.warn("Nothing selected, can't validate, returning nothing."));var
c=a.data(this[0],"validator");return c?c:(this.attr("novalidate","novalidate"),c=new
a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&&(this.on("click.validate",":submit",function(b)
{c.submitButton=b.currentTarget,a(this).hasClass("cancel")&&(c.cancelSubmit=!0),void 0!==a(this).attr("formnovalidate")&&
(c.cancelSubmit=!0)}),this.on("submit.validate",function(b){function d(){var d,e;return c.submitButton&&
(c.settings.submitHandler||c.formSubmitted)&&(d=a("<input
type='hidden'/>").attr("name",c.submitButton.name).val(a(c.submitButton).val()).appendTo(c.currentForm)),!
(c.settings.submitHandler&&!c.settings.debug)||(e=c.settings.submitHandler.call(c,c.currentForm,b),d&&d.remove(),void
0!==e&&e)}return c.settings.debug&&b.preventDefault(),c.cancelSubmit?(c.cancelSubmit=!1,d()):c.form()?c.pendingRequest?
(c.formSubmitted=!0,!1):d():(c.focusInvalid(),!1)})),c)},valid:function(){var b,c,d;return a(this[0]).is("form")?
b=this.validate().form():(d=[],b=!0,c=a(this[0].form).validate(),this.each(function(){b=c.element(this)&&b,b||
(d=d.concat(c.errorList))}),c.errorList=d),b},rules:function(b,c){var d,e,f,g,h,i,j=this[0],k="undefined"!=typeof
this.attr("contenteditable")&&"false"!==this.attr("contenteditable");if(null!=j&&(!j.form&&k&&(j.form=this.closest("form")
[0],j.name=this.attr("name")),null!=j.form))
{if(b)switch(d=a.data(j.form,"validator").settings,e=d.rules,f=a.validator.staticRules(j),b)
{case"add":a.extend(f,a.validator.normalizeRu...
```

Issue 3 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2019-11358
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 1.9.1 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Issue 4 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2015-9251
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 1.9.1 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Raw Test Response:

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 13:15:31 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /sscsr_audit/dataentry/js</title>
 </head>
 <body>
<h1>Index of /sscsr_audit/dataentry/js</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?
C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></t...
```

Issue 5 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2020-11023
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 2.0.3 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Issue 6 of 12

TOC

Vulnerable Component

Severity:	**Medium**
CVSS Score:	6.1
CVE:	CVE-2020-11023
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 1.9.1 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Issue 7 of 12

TOC

Vulnerable Component

Severity:	**Medium**
CVSS Score:	6.1
CVE:	CVE-2020-11022
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 1.9.1 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Issue 8 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2019-11358
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 3.3.1 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Raw Test Response:

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 13:15:31 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /sscsr_audit/dataentry/js</title>
 </head>
 <body>
<h1>Index of /sscsr_audit/dataentry/js</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?
C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></t...
```

Issue 9 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2015-9251
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 2.0.3 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Raw Test Response:

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 13:15:31 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /sscsr_audit/dataentry/js</title>
 </head>
 <body>
<h1>Index of /sscsr_audit/dataentry/js</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?
C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></t...
```

Issue 10 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2020-11023
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 3.3.1 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Issue 11 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2020-11022
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 2.0.3 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

Issue 12 of 12

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2019-11358
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
Entity:	jQuery 2.0.3 (Component)
Risk:	Using obsolete or vulnerable versions leaves your application open to potential security breaches
Cause:	A vulnerable component is used in the tested application.
Fix:	Upgrade the component to the latest stable version

Reasoning:

I Client-Side (JavaScript) Cookie References 2 TOC

Issue 1 of 2 TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/jquery.cookie.js
Entity:	(function(factory){if(typeof define==='function'&&define.amd){define(['jquery'],factory);}else{facto... (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
Cause:	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

```
...

Content-Type: application/javascript

(function(factory){if(typeof define==='function'&&define.amd){define(['jquery'],factory);}else{factory(jQuery);}}
(function($){var pluses=/\+/g;function encode(s){return config.raw?s:encodeURIComponent(s);}
function decode(s){return config.raw?s:decodeURIComponent(s);}
function stringifyCookieValue(value){return encode(config.json?JSON.stringify(value):String(value));}
function parseCookieValue(s){if(s.indexOf('"')===0){s=s.slice(1,-1).replace(/\\"/g,'"').replace(/\\\\/g,'\\');}
try{s=decodeURIComponent(s.replace(pluses,' '));return config.json?JSON.parse(s):s;}catch(e){}}
function read(s,converter){var value=config.raw?s:parseCookieValue(s);return $.isFunction(converter)?
converter(value):value;}
var config=$.cookie=function(key,value,options){if(value!==undefined&&!$.isFunction(value))
{options=$.extend({},config.defaults,options);if(typeof options.expires==='number'){var
days=options.expires,t=options.expires=new Date();t.setDate(t.getDate()+ days);}
return(document.cookie=[encode(key),'=',stringifyCookieValue(value),options.expires?'; expires='+
options.expires.toUTCString():'',options.path?'; path='+ options.path:'',options.domain?'; domain='+
options.domain:'',options.secure?'; secure':''].join(''));}
var result=key?undefined:{};var cookies=document.cookie?document.cookie.split('; '):[];for(var
i=0,l=cookies.length;i<l;i++){var parts=cookies[i].split('=');var name=decode(parts.shift());var
cookie=parts.join('=');if(key&&key===name){result=read(cookie,value);break;}
if(!key&&(cookie=read(cookie))!==undefined){result[name]=cookie;}}
return result;};config.defaults={};$.removeCookie=function(key,options){if($.cookie(key)===undefined){return false;}
$.cookie(key,'',$.extend({},options,{expires:-1}));return!$.cookie(key);};}));
...
```

Issue 2 of 2 TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/jquery-ui.min.js
Entity:	(function(a,c){function d(h,g){var i=h.nodeName.toLowerCase();if("area"===i){g=h.parentNode;i=g.name... (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
Cause:	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

```
...
"%"},d.animate);if(o===1)e.range[h?"animate":"css"]({height:g-b+"%"},
{queue:false,duration:d.animate})}b=g});else{f=this.value();j=this._valueMin();l=this._valueMax();g=l!==j?(f-j)/(l-
j)*100:0;i[e.ori...
d.animate);if(c==="max"&&this.orientation==="horizontal")this.range[h?"animate":"css"]({width:100-g+"%"},
{queue:false,duration:d.animate});if(c==="min"&&this.orientation==="vertical")this.range.stop(1...
(function(a,c){function d(){return++h}function e(){return++g}var h=0,g=0;a.widget("ui.tabs",{options:
{add:null,ajaxOptions:null,cache:false,cookie:null,collapsible:false,disable:null,disabled:[],enabl...
...tion(i){return i.replace(/:/g,"\\:")},_cookie:function(){var i=this.cookie||(this.cookie=this.options.cookie.name||"ui-
tabs-"+e());return a.cookie.apply(null,[i].concat(a.makeArray(arguments)))},_ui:function(i...
a(this);i.html(i.data("label.tabs")).removeData("label.tabs")})},_tabify:function(i){function b(r,u)
{r.css("display","");!a.support.opacity&&u.opacity&&r[0].style.removeAttribute("filter")}var f=this,...
(x=a("base")[0])&&w===x.href))
{v=u.hash;u.href=v}if(l.test(v))f.panels=f.panels.add(f.element.find(f._sanitizeSelector(v)));else if(v&&v!=="#")
{a.data(u,"href.tabs",v);a.data(u,"load.tabs",v.replace(/...
this.list.addClass("ui-tabs-nav ui-helper-reset ui-helper-clearfix ui-widget-header ui-corner-all");this.lis.addClass("ui-
state-default ui-corner-top");this.panels.addClass("ui-tabs-panel ui-widget-co...

...
```

I Email Address Pattern Found 1

TOC

Issue 1 of 1

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/pdfmake.min.js
Entity:	pdfmake.min.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
Cause:	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:

```
...
(t,e,n,r,23,4),n+4}function W(t,e,n,r,i){return i||z(t,e,n,8,1.7976931348623157e308,-
1.7976931348623157e308),J.write(t,e,n,r,52,8),n+8}function U(t){if(t=j(t).replace(tt,""),t.length<2)return"";for(;t...
 * The buffer module from node.js, for the browser.
 *
 * @author   Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
 * @license  MIT
 */
var K=n(207),J=n(208),Q=n(136);e.Buffer=o,e.SlowBuffer=g,e.INSPECT_MAX_BYTES=50,o.TYPED_ARRAY_SUPPORT=void
0!==t.TYPED_ARRAY_SUPPORT?t.TYPED_ARRAY_SUPPORT:function(){try{var t=new Uint8Array(1);return...

...

...
1,t&&("function"==typeof t.transform&&(this._transform=t.transform),"function"==typeof t.flush&&
(this._flush=t.flush)),this.on("prefinish",o)}function o(){var t=this;"function"==typeof this._flush?thi...
 * The buffer module from node.js, for the browser.
 *
 * @author   Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
 * @license  MIT
 */
function r(t,e){if(t===e)return 0;for(var n=t.length,r=e.length,i=0,o=Math.min(n,r);i<o;++i)if(t[i]!==e[i])
{n=t[i],r=e[i];break}return n<r?-1:r<n?1:0}function i(t){return e.Buffer&&"function"==typeof ...

...

...
erations;u.length<c;){var h=r.update(e).finalize(a);r.reset();for(var d=h.words,p=d.length,g=h,v=1;v<f;v++)
{g=r.finalize(g),r.reset();for(var y=g.words,b=0;b<p;b++)d[b]^=y[b]}o.concat(h),l[0]++}return...
  * Counter block mode compatible with  Dr Brian Gladman fileenc.c
  * derived from CryptoJS.mode.CTR
  * Jan Hruby jhruby.web@gmail.com
  */
return t.mode.CTRGladman=function(){function e(t){if(255==(t>>24&255)){var e=t>>16&255,n=t>>8&255,r=255&t;255===e?
(e=0,255===n?(n=0,255===r?r=0:++r):++n):++e,t=0,t+=e<<16,t+=n<<8,t+=r}else t+=1<<24;re...

...
```

I Internal IP Disclosure Pattern Found 23

TOC

Issue 1 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/
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
Cause:	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:

```
...
p"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="sweetalert2.min.css">sweetalert2.min.css</a>    </td><td
align="right">2023-11-03 11:13  </td><td align="right"> 31K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="table-style.css">table-style.css</a>
</td><td align="right">2023-11-15 11:10  </td><td align="right">5.1K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a
href="transparentlogin.css">transparentlogin.css</a>   </td><td align="right">2023-09-26 13:08  </td><td
align="right">1.1K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="typo.css">typo.css</a>          </td><td
align="right">2023-11-15 11:10  </td><td align="right">5.0K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 2 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/images/logo/
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
Cause:	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:

```
...

   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/images/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="logo.ico">logo.ico</a>          </td><td
align="right">2023-09-26 13:08  </td><td align="right">253K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="logo.png">logo.png</a>          </td><td
align="right">2023-09-26 13:08  </td><td align="right">144K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 3 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/metadata/
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
Cause:	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:

```
...
ign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="icons.yml">icons.yml</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right">568K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="shims.json">shims.json</a>          </td>
<td align="right">2023-10-04 17:48  </td><td align="right"> 40K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="shims.yml">shims.yml</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right">9.9K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="sponsors.yml">sponsors.yml</a>
</td><td align="right">2023-10-04 17:48  </td><td align="right"> 26K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 4 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/log/
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
Cause:	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:

```
...

   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>
```

```
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="sscsr_log.log">sscsr_log.log</a>
</td><td align="right">2023-11-15 18:57  </td><td align="right">764 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="sscsr_log.log.txt">sscsr_log.log.txt</a>
</td><td align="right">2023-09-26 13:08  </td><td align="right">  0 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 5 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/images/
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
Cause:	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:

```
...
<img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="photo_not_exists.png">photo_not_exists.png</a>   </td><td
align="right">2023-09-26 13:08  </td><td align="right">7.6K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="settings.gif">settings.gif</a>
</td><td align="right">2023-09-26 13:08  </td><td align="right"> 39K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="sign_not_exits.png">sign_not_exits.png</a>
</td><td align="right">2023-09-26 13:08  </td><td align="right">6.3K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="users/">users/</a>          </td><td
align="right">2023-09-26 13:08  </td><td align="right">  - </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 6 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/css/
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
Cause:	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:

```
...
ign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="v4-shims.css">v4-shims.css</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right"> 41K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="v4-shims.min.css">v4-shims.min.css</a>
</td><td align="right">2023-10-04 17:48  </td><td align="right"> 27K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="v5-font-face.css">v5-font-face.css</a>
</td><td align="right">2023-10-04 17:48  </td><td align="right">871 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="v5-font-face.min.css">v5-font-
face.min.css</a>   </td><td align="right">2023-10-04 17:48  </td><td align="right">794 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 7 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/
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
Cause:	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:

```
...
d valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="scss/">scss/</a>          </td><td
align="right">2023-10-06 13:05  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sprites/">sprites/</a>          </td><td
align="right">2023-10-06 13:05  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="svgs/">svgs/</a>          </td><td
```

```
align="right">2023-10-06 13:05  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="webfonts/">webfonts/</a>          </td><td
align="right">2023-10-06 13:06  </td><td align="right">  - </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 8 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/
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
Cause:	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:

```
...
p"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/css/fontawesome/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="brands/">brands/</a>          </td><td
align="right">2023-10-06 13:05  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="regular/">regular/</a>          </td><td
align="right">2023-10-06 13:05  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="solid/">solid/</a>          </td><td
align="right">2023-10-06 13:06  </td><td align="right">  - </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 9 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/images/icons/
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
Cause:	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:

```
...
ign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="logout.png">logout.png</a>          </td><td
align="right">2023-09-26 13:08  </td><td align="right"> 10K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="mul-chk.png">mul-chk.png</a>          </td>
<td align="right">2023-09-26 13:08  </td><td align="right">1.6K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="publish_admitcard.png">publish_admitcard.png</a>  </td><td align="right">2023-09-26 13:08  </td><td align="right">
15K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="send_mail.png">send_mail.png</a>
</td><td align="right">2023-09-26 13:08  </td><td align="right"> 12K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 10 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/
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
Cause:	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:

```
...
<img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="valida.2.1.6.min.js">valida.2.1.6.min.js</a>    </td><td
align="right">2023-09-27 10:37  </td><td align="right">9.5K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="validatehtml.js">validatehtml.js</a>
</td><td align="right">2023-10-09 10:24  </td><td align="right">3.0K</td><td>&nbsp;</td></tr>
```

```
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="validator.min.js">validator.min.js</a>
</td><td align="right">2023-09-27 10:37  </td><td align="right">5.7K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="vfs_fonts.js">vfs_fonts.js</a>
</td><td align="right">2023-09-26 13:08  </td><td align="right">905K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 11 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/images/users/
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
Cause:	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:

```
...

   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?
C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/images/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="admin.png">admin.png</a>          </td><td
align="right">2023-09-26 13:08  </td><td align="right">3.3K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 12 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/brands.js
Entity:	brands.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
Cause:	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:

```
...
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z"],
    "css3-alt": [384,...

...

...
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...
... 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-10.7-
27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6 24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-18.5-
10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.2l4.8-8.4c14.3-24.9 52-3.3 37...

...
```

Issue 13 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/all.min.js
Entity:	all.min.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
Cause:	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:

```
...
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z"],"css3-alt":[384,512,[]...

...

...
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...
... 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-10.7-
27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6 24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-18.5-
10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.214.8-8.4c14.3-24.9 52-3.3 37...

...
```

Issue 14 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/
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
Cause:	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:

```
...
lign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="solid.js">solid.js</a>          </td><td
align="right">2023-11-15 10:58  </td><td align="right">826K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="solid.min.js">solid.min.js</a>
</td><td align="right">2023-11-15 10:59  </td><td align="right">807K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="v4-shims.js">v4-shims.js</a>
</td><td align="right">2023-11-15 10:59  </td><td align="right"> 33K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="v4-shims.min.js">v4-shims.min.js</a>
</td><td align="right">2023-11-15 10:59  </td><td align="right"> 27K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 15 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/sprites/
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
Cause:	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:

```
...
p"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/sscsr_audit/dataentry/css/fontawesome/">Parent
Directory</a>       </td><td>&nbsp;</td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="brands.svg">brands.svg</a>          </td>
<td align="right">2023-10-04 17:48  </td><td align="right">477K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="regular.svg">regular.svg</a>          </td>
<td align="right">2023-10-04 17:48  </td><td align="right">111K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="solid.svg">solid.svg</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right">839K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 16 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/webfonts/
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
Cause:	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:

```
...
p"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="fa-solid-900.ttf">fa-solid-900.ttf</a>       </td><td
align="right">2023-10-04 17:49  </td><td align="right">385K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="fa-solid-900.woff2">fa-solid-900.woff2</a>
</td><td align="right">2023-10-04 17:49  </td><td align="right">147K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="fa-v4compatibility.ttf">fa-
v4compatibility.ttf</a> </td><td align="right">2023-10-04 17:49  </td><td align="right">9.9K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="fa-v4compatibility.woff2">fa-
v4compatibility.w..&gt;</a></td><td align="right">2023-10-04 17:49  </td><td align="right">4.5K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 17 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/metadata/icons.json
Entity:	icons.json (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	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:

```
...


"svg": {

"brands": {

"last_modified": 1660014481,
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z\"/></svg>",

"viewBox": [

0,

0,

448,


...

...
```

```
512

    ],

"width": 448,

"height": 512,
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z"

   }

  },

"free": [

"brands"



...

...

"svg": {

"brands": {

"last_modified": 1660014477,
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...

    ],

"width": 640,

"height": 512,
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...


"svg": {

"brands": {

"last_modified": 1660014477,

"raw": "<svg xmlns=\"http://www.w3.org/2000/svg\" viewBox=\"0 0 448 512\"><path d=\"M353.4 32H94.7C42.6 32 0 74.6 0
126.6v258.7C0 437.4 42.6 480 94.7 480h258.7c52.1 0 94.7-42.6 94.7-94.6V126.6c0-52-42.6-94.6-94.7-94.6zm-50 316.4c-27.9
48.2-89.9 64.9-138.2 37.2-22.9 39.8-54.9 8.6-42.3-13.2l15.7-27.2c5.9-10.3 19.2-13.9 29.5-7.9 18.6 10.8-.1-.1 18.5 10.7 27.6
15.9 63.4 6.3 79.4-21.3 15.9-27.6 6.3-63.4-21.3-79.4-17.8-10.2-.6-.4-18.6-10.6-24.6-14.2-3.4-51.9 21.6-37.5 18.6 10.8-.1-.1
18.5 10.7 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-
10.7-27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6 24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-
18.5-10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.2l4.8-8.4c14.3-24.9 52-3.3 37.7 21.5z\"/></svg>",

"viewBox": [

0,

0,

448,

...

...


    ],
"width": 448,

"height": 512,

"path": "M353.4 32H94.7C42.6 32 0 74.6 0 126.6v258.7C0 437.4 42.6 480 94.7 480h258.7c52.1 0 94.7-42.6 94.7-94.6V126.6c0-52-
42.6-94.6-94.7-94.6zm-50 316.4c-27.9 48.2-89.9 64.9-138.2 37.2-22.9 39.8-54.9 8.6-42.3-13.2l15.7-27.2c5.9-10.3 19.2-13.9
29.5-7.9 18.6 10.8-.1-.1 18.5 10.7 27.6 15.9 63.4 6.3 79.4-21.3 15.9-27.6 6.3-63.4-21.3-79.4-17.8-10.2-.6-.4-18.6-10.6-
24.6-14.2-3.4-51.9 21.6-37.5 18.6 10.8-.1-.1 18.5 10.7 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-
6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-10.7-27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6
24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-18.5-10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.2l4.8-
8.4c14.3-24.9 52-3.3 37.7 21.5z"

    }

   },

"free": [

"brands"


...
```

Issue 18 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/metadata/icon-families.json
Entity:	icon-families.json (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	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:

```
...


"classic": {

"brands": {

"lastModified": 1660014481,
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z\"/></svg>",

"viewBox": [

0,

0,

448,
...

...

512

     ],

"width": 448,

"height": 512,
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z"

    }

   }

  },

"familyStylesByLicense": {


...

...

"classic": {

"brands": {

"lastModified": 1660014477,
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...

     ],

"width": 640,

"height": 512,
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...


"classic": {

"brands": {

"lastModified": 1660014477,

"raw": "<svg xmlns=\"http://www.w3.org/2000/svg\" viewBox=\"0 0 448 512\"><path d=\"M353.4 32H94.7C42.6 32 0 74.6 0
126.6v258.7C0 437.4 42.6 480 94.7 480h258.7c52.1 0 94.7-42.6 94.7-94.6V126.6c0-52-42.6-94.6-94.7-94.6zm-50 316.4c-27.9
48.2-89.9 64.9-138.2 37.2-22.9 39.8-54.9 8.6-42.3-13.2l15.7-27.2c5.9-10.3 19.2-13.9 29.5-7.9 18.6 10.8-.1-.1 18.5 10.7 27.6
15.9 63.4 6.3 79.4-21.3 15.9-27.6 6.3-63.4-21.3-79.4-17.8-10.2-.6-.4-18.6-10.6-24.6-14.2-3.4-51.9 21.6-37.5 18.6 10.8-.1-.1
18.5 10.7 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-
10.7-27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6 24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-
18.5-10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.2l4.8-8.4c14.3-24.9 52-3.3 37.7 21.5z\"/></svg>",

"viewBox": [

0,

0,

448,

...

...
```

```
     ],

"width": 448,

"height": 512,

"path": "M353.4 32H94.7C42.6 32 0 74.6 0 126.6v258.7C0 437.4 42.6 480 94.7 480h258.7c52.1 0 94.7-42.6 94.7-94.6V126.6c0-52-
42.6-94.6-94.7-94.6zm-50 316.4c-27.9 48.2-89.9 64.9-138.2 37.2-22.9 39.8-54.9 8.6-42.3-13.2l15.7-27.2c5.9-10.3 19.2-13.9
29.5-7.9 18.6 10.8-.1-.1 18.5 10.7 27.6 15.9 63.4 6.3 79.4-21.3 15.9-27.6 6.3-63.4-21.3-79.4-17.8-10.2-.6-.4-18.6-10.6-
24.6-14.2-3.4-51.9 21.6-37.5 18.6 10.8-.1-.1 18.5 10.7 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-
6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-10.7-27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6
24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-18.5-10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.2l4.8-
8.4c14.3-24.9 52-3.3 37.7 21.5z"

    }

   }

  },

"familyStylesByLicense": {

...
```

Issue 19 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/regular/
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
Cause:	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:

```
...
align="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="user.svg">user.svg</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right">590 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="window-maximize.svg">window-
maximize.svg</a>    </td><td align="right">2023-10-04 17:48  </td><td align="right">578 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="window-minimize.svg">window-
minimize.svg</a>    </td><td align="right">2023-10-04 17:48  </td><td align="right">378 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="window-restore.svg">window-restore.svg</a>
</td><td align="right">2023-10-04 17:48  </td><td align="right">631 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 20 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/brands/
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
Cause:	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:

```
...
align="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="yelp.svg">yelp.svg</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right">1.0K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="yoast.svg">yoast.svg</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right">731 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="youtube.svg">youtube.svg</a>          </td>
<td align="right">2023-10-04 17:48  </td><td align="right">761 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="zhihu.svg">zhihu.svg</a>          </td><td
align="right">2023-10-04 17:48  </td><td align="right">1.7K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 21 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/svgs/solid/
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
Cause:	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:

```
...
```

```
d valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="y.svg">y.svg</a>          </td><td
align="right">2023-10-04 17:49  </td><td align="right">471 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="yen-sign.svg">yen-sign.svg</a>
</td><td align="right">2023-10-04 17:49  </td><td align="right">655 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="yin-yang.svg">yin-yang.svg</a>
</td><td align="right">2023-10-04 17:49  </td><td align="right">524 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="z.svg">z.svg</a>          </td><td
align="right">2023-10-04 17:49  </td><td align="right">493 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Server at 10.163.2.181 Port 8080</address>
</body></html>

...
```

Issue 22 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/all.js
Entity:	all.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
Cause:	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:

```
...
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z"],
    "css3-alt": [384,...

...

...
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...
... 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-10.7-
27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6 24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-18.5-
10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.214.8-8.4c14.3-24.9 52-3.3 37...

...
```

Issue 23 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/css/fontawesome/js/brands.min.js
Entity:	brands.min.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
Cause:	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:

```
...
...22-5.41 7.06.85 3.74 10-2.71 22.6-3.48 7-.44 12.8 1.75 17.26 3.71zm-9 5.13c-9.07 1.42-15 6.53-13.47 10.1.9.34 1.17.81
5.21-.81a37 37 0 0 1 18.72-1.95c2.92.34 4.31.52 4.94-.49 1.46-2.22-5.71-8-15.39-6.85zm54.17...

...

...
...9-17.3a.77.77 0 0 1 .52 1.38 41.86 41.86 0 0 0-7.71 7.74.75.75 0 0 0 .59 1.19c12.31.09 29.66 4.4 41 10.74.76.43.22 1.91-
.64 1.72-69.55-15.94-123.08 18.53-134.5 26.83a.76.76 0 0 1-1-1.12z"],"css3-alt":[384,512,[]...

...

...
...65.8c0-12.5-8.4-15.8-26.2-18.2-18-2.4-19.8-3.6-19.8-7.8 0-3.5 1.5-8.1 14.8-8.1 11.9 0 16.3 2.6 18.1 10.6.2.8.8 1.3 1.6
1.3h7.5c.5 0 .9-.2 1.2-.5.3-.4.5-.8.4-1.3-1.2-13.8-10.3-20.2-28.8-20.2-16.5 0-26.3 7-26.3...

...

...
... 48.4 28 65.1 90.3 37.2 138.5zm21.8-208.8c-17 29.5-16.3 28.8-19 31.5-6.5 6.5-16.3 8.7-26.5 3.6-18.6-10.8.1.1-18.5-10.7-
27.6-15.9-63.4-6.3-79.4 21.3s-6.3 63.4 21.3 79.4c0 0 18.5 10.6 18.6 10.6 24.6 14.2 3.4 51.9-21.6 37.5-18.6-10.8.1.1-18.5-
10.7-48.2-27.8-64.9-90.1-37.1-138.4 27.9-48.2 89.9-64.9 138.2-37.214.8-8.4c14.3-24.9 52-3.3 37...

...
```

I Missing "Referrer policy" Security Header 1

TOC

Issue 1 of 1

TOC

Missing "Referrer policy" Security Header

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/
Entity:	10.163.2.181 (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.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Referrer Policy" header with secure policies

Reasoning: AppScan detected that the Referrer Policy Response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Raw Test Response:

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 12:55:28 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
Last-Modified: Wed, 27 Sep 2023 05:04:56 GMT
ETag: "5f8f-6065021e72a74"
Accept-Ranges: bytes
Content-Length: 24463
Content-Type: application/javascript

!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof module&&module.exports?
module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,{validate:function(b){if(!this.length)return
void(b&&b.debug&&window.console&&console.warn("Nothing selected, can't validate, returning nothing."));var
c=a.data(this[0],"validator");return c?c:(this.attr("novalidate","novalidate"),c=new
a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&&(this.on("click.validate",":submit",function(b)
{c.submitButton=b.currentTarget,a(this).hasClass("cancel")&&(c.cancelSubmit=!0),void 0!==a(this).attr("formnovalidate")&&
(c.cancelSubmit=!0)}),this.on("submit.validate",function(b){function d(){var d,e;return c.submitButton&&
(c.settings.submitHandler||c.formSubmitted)&&(d=a("<input
type='hidden'/>").attr("name",c.submitButton.name).val(a(c.submitButton).val()).appendTo(c.currentForm)),!
(c.settings.submitHandler&&!c.settings.debug)||(e=c.settings.submitHandler.call(c,c.currentForm,b),d&&d.remove(),void
0!==e&&e)}return c.settings.debug&&b.preventDefault(),c.cancelSubmit?(c.cancelSubmit=!1,d()):c.form()?c.pendingRequest?
(c.formSubmitted=!0,!1):d():(c.focusInvalid(),!1)})),c)},valid:function(){var b,c,d;return a(this[0]).is("form")?
b=this.validate().form():(d=[],b=!0,c=a(this[0].form).validate(),this.each(function(){b=c.element(this)&&b,b||
(d=d.concat(c.errorList))}),c.errorList=d),b},rules:function(b,c){var d,e,f,g,h,i,j=this[0],k="undefined"!=typeof
this.attr("contenteditable")&&"false"!==this.attr("contenteditable");if(null!=j&&(!j.form&&k&&(j.form=this.closest("form")
[0],j.name=this.attr("name")),null!=j.form))
{if(b)switch(d=a.data(j.form,"validator").settings,e=d.rules,f=a.validator.staticRules(j),b)
{case"add":a.extend(f,a.validator.normalizeRule(c)),delete f.messages,e[j.name]=f,c.messages&&
(d.messages[j.name]=a.extend(d.messages[j.name],c.messages));break;case"remove":return c?(i=
{},a.each(c.split(/\s/),function(a,b){i[b]=f[b],delete f[b]}),i):(delete e[j.name],f)}return
g=a.validator.normalizeRules(a.extend({},a.validator.classRules(j),a.validator.attributeRules(j),a.validator.dataRules(j),a
.validator.staticRules(j)),j),g.required&&(h=...
```

I Possible Server Path Disclosure Pattern Found 1

TOC

Issue 1 of 1

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/js/jquery.validate.min.js
Entity:	jquery.validate.min.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
Cause:	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:

```
...
...&&"undefined"!=typeof b.validity?b.validity.badInput?"NaN":e.val():(c=g?
e.text():e.val(),"file"===f?"C:\\fakepath\\"===c.substr(0,12)?c.substr(12):(d=c.lastIndexOf("/"),d>=0?c.substr(d+1):
(d=c.lastIndexOf...

...
```

I Potential File Upload 2

TOC

Issue 1 of 2

TOC

Potential File Upload

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/upload_excel_file.php
Entity:	excel_file_attachment (Parameter)
Risk:	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The software allows the attacker to upload or transfer files of dangerous types (for example, containing malicious code) and unlimited size that could be automatically processed within the product's environment.
Fix:	Restrict user capabilities and permissions during the file upload process

Reasoning: AppScan found a parameter of type FILENAME, which indicates that it is used to upload files to the server.

Original Request

```
...

Content-Type: application/x-www-form-urlencoded
```

```
Cookie: name=value; PHPSESSID=5k44cos7uiiungervnu7rql1nb
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.181:8080/sscsr_audit/dataentry/upload_excel_file.php
Host: 10.163.2.181:8080
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 171

exam_year=09&selectedTableFormat=is_pet&selectedtier=0&no_of_days=01&excel_file_attachment=1234&csrf_token=0c9985e97fc84400
9502acdb81577619f852efa393d694b48708934c5d2358e5

HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 12:55:26 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Transfer-Encoding: chunked

...
```

Issue 2 of 2

TOC

Potential File Upload

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.181:8080/sscsr_audit/dataentry/upload_admitcard_important_instructions.php
Entity:	image_file_attachment (Parameter)
Risk:	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents It is possible to upload, modify or delete web pages, scripts and files on the web server
Cause:	The software allows the attacker to upload or transfer files of dangerous types (for example, containing malicious code) and unlimited size that could be automatically processed within the product's environment.
Fix:	Restrict user capabilities and permissions during the file upload process

Reasoning: AppScan found a parameter of type FILENAME, which indicates that it is used to upload files to the server.

Original Request

```
...

Content-Type: application/x-www-form-urlencoded
Cookie: name=value; PHPSESSID=5k44cos7uiiungervnu7rql1nb
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.181:8080/sscsr_audit/dataentry/upload_admitcard_important_instructions.php
Host: 10.163.2.181:8080
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 113

exam_year=09&image_file_attachment=25&csrf_token=8b63eddb73c9f67cba57df9110188a90b32b60c55657aec9b41dcfd3c95928fe

HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 12:55:31 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Transfer-Encoding: chunked

...
```