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 3:52:33 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.

Critical severity issues:	6
High severity issues:	8
Medium severity issues:	24
Informational severity issues:	29
Total security issues included in the report:	75
Total security issues discovered in the scan:	75

General Information

Scan file name:	Untitled
Scan started:	11/17/2023 3:52:33 PM
Test policy:	Default
CVSS version:	3.1
Test optimization level:	Fast

Host	10.163.2.51
Port	80
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
C	Vulnerable Component	35
M	Body Parameters Accepted in Query	2
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
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 33

TOC

	URL	Number of Issues
C	http://10.163.2.51/sscsr_audit/dataentry/login.php	26
🟩	http://10.163.2.51/sscsr_audit/dataentry/js/	12
🟩	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/webfonts/	1
M	http://10.163.2.51/sscsr_audit/dataentry/admit_card_download_datatable.php	1
M	http://10.163.2.51/	7
M	http://10.163.2.51/sscsr_audit/dataentry/index.php	1
I	http://10.163.2.51/sscsr_audit/dataentry/js/jquery-ui.min.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/js/jquery.cookie.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/js/pdfmake.min.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/	1

I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/css/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/js/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/js/all.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/js/all.min.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/js/brands.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/js/brands.min.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/metadata/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/metadata/icon-families.json	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/metadata/icons.json	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/sprites/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/svgs/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/svgs/brands/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/svgs/regular/	1
I	http://10.163.2.51/sscsr_audit/dataentry/css/fontawesome/svgs/solid/	1
I	http://10.163.2.51/sscsr_audit/dataentry/images/	1
I	http://10.163.2.51/sscsr_audit/dataentry/images/icons/	1
I	http://10.163.2.51/sscsr_audit/dataentry/images/logo/	1
I	http://10.163.2.51/sscsr_audit/dataentry/images/users/	1
I	http://10.163.2.51/sscsr_audit/dataentry/log/	1
I	http://10.163.2.51/sscsr_audit/dataentry/js/jquery.validate.min.js	1
I	http://10.163.2.51/sscsr_audit/dataentry/upload_admitcard_important_instructions.php	1
I	http://10.163.2.51/sscsr_audit/dataentry/upload_excel_file.php	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	35
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	2
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	
C	Using obsolete or vulnerable versions leaves your application open to potential security breaches	35	🟥🟥🟧
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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	6	🟧⬜
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	🟥
C	A vulnerable component is used in the tested application.	35	🟥🟥🟧
🟩	Insecure web application programming or configuration	30	🟧⬜
M	Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute	2	🟧
M	Directory browsing is enabled	2	🟧
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	⬜

TOC

WASC Threat Classification

Threat	Number of Issues
Abuse of Functionality	37
Directory Indexing	2
Information Leakage	33
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://10.163.2.51/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=tnhevrtl5su93h5ok38ph6mtqr
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.51/sscsr_audit/dataentry/login.php
Host: 10.163.2.51
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=2ef5ad764b7b70d4b99b90cc8831c17916dd50f7c4b866b93d2023e44c12b889&submit=Subm
it

HTTP/1.1 302 Found
Date: Fri, 17 Nov 2023 10:23:08 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: add_exam.php

...
```

C Vulnerable Component 35

TOC

Issue 1 of 35

TOC

Vulnerable Component

Severity:	Critical
CVSS Score:	9.8
CVE:	CVE-2022-22720
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 35

TOC

Vulnerable Component

Severity:	Critical
CVSS Score:	9.8
CVE:	CVE-2021-21708
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 3 of 35

TOC

Vulnerable Component

Severity:	Critical
CVSS Score:	9.1
CVE:	CVE-2022-22721
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 35

TOC

Vulnerable Component

Severity:	Critical
CVSS Score:	9.8
CVE:	CVE-2022-23943
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 5 of 35

TOC

Vulnerable Component

Severity:	Critical
CVSS Score:	9.8
CVE:	CVE-2022-31813
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 35

TOC

Vulnerable Component	
Severity:	Critical
CVSS Score:	9.8
CVE:	CVE-2023-25690
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 35

TOC

Vulnerable Component	
Severity:	
CVSS Score:	9.8
CVE:	CVE-2022-37454
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 35

TOC

Vulnerable Component

Severity:	
CVSS Score:	9.1
CVE:	CVE-2022-28615
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 9 of 35

TOC

Vulnerable Component

Severity:	
CVSS Score:	7.1
CVE:	CVE-2022-31630
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 10 of 35

TOC

Vulnerable Component

Severity:	
CVSS Score:	7.5
CVE:	CVE-2022-30556
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 35

TOC

Vulnerable Component

Severity:	
CVSS Score:	9.1
CVE:	CVE-2022-36760
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 35

TOC

Vulnerable Component

Severity:	
CVSS Score:	6.1
CVE:	CVE-2020-11023
URL:	http://10.163.2.51/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 13 of 35

TOC

Vulnerable Component

Severity:	
CVSS Score:	6.1
CVE:	CVE-2020-11022
URL:	http://10.163.2.51/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 14 of 35

TOC

Vulnerable Component

Severity:	High
CVSS Score:	7.5
CVE:	CVE-2022-22719
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 15 of 35

TOC

Vulnerable Component

Severity:	High
CVSS Score:	7.5
CVE:	CVE-2023-27522
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 10:29:00 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
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=83
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=t0p07db004843bqeq7mesnmr0m; 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">
...
```

Issue 16 of 35

TOC

Vulnerable Component

Severity:	High
CVSS Score:	8.1
CVE:	CVE-2022-31625
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 17 of 35

TOC

Vulnerable Component

Severity:	High
CVSS Score:	8.8
CVE:	CVE-2022-31626
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 18 of 35

TOC

Vulnerable Component

Severity:	High
CVSS Score:	7.5
CVE:	CVE-2022-26377
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 19 of 35

TOC

Vulnerable Component

Severity:	High
CVSS Score:	7.5
CVE:	CVE-2022-29404
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 20 of 35

TOC

Vulnerable Component

Severity:	High
CVSS Score:	7.5
CVE:	CVE-2006-20001
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 21 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	5.3
CVE:	CVE-2007-3205
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 10:29:00 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
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=79
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=ri74ndtft7p6qq0qk4v1i0j25q; 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">
...
```

Issue 22 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	5.5
CVE:	CVE-2022-31628
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 23 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	5.3
CVE:	CVE-2022-28330
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 24 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.5
CVE:	CVE-2022-31629
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	PHP 7.4.27 (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 25 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	5.3
CVE:	CVE-2022-28614
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 26 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	5.3
CVE:	CVE-2022-37436
URL:	http://10.163.2.51/sscsr_audit/dataentry/login.php
Entity:	Apache Web Server 2.4.52 (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 27 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2015-9251
URL:	http://10.163.2.51/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 10:43:33 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
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 28 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2015-9251
URL:	http://10.163.2.51/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 10:43:33 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
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 29 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2019-11358
URL:	http://10.163.2.51/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 10:43:33 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
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 30 of 35

TOC

Vulnerable Component	
Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2019-11358
URL:	http://10.163.2.51/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 31 of 35

TOC

Vulnerable Component	
Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2019-11358
URL:	http://10.163.2.51/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 32 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2020-11023
URL:	http://10.163.2.51/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 33 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2020-11023
URL:	http://10.163.2.51/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 34 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2020-11022
URL:	http://10.163.2.51/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 35 of 35

TOC

Vulnerable Component

Severity:	Medium
CVSS Score:	6.1
CVE:	CVE-2020-11022
URL:	http://10.163.2.51/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:

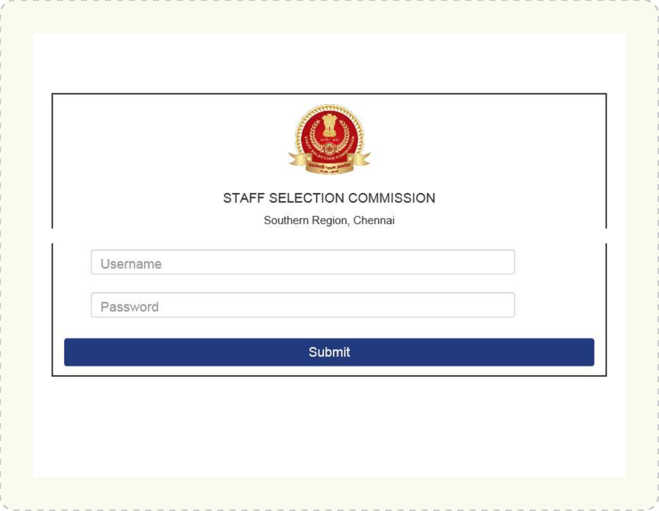
M Body Parameters Accepted in Query 2 TOC

Issue 1 of 2 TOC

Body Parameters Accepted in Query	
Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.51/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

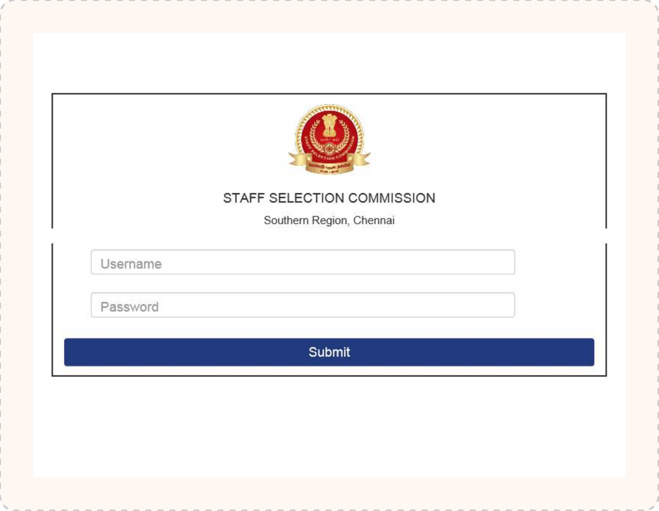
Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Original Response



≈

Test Response



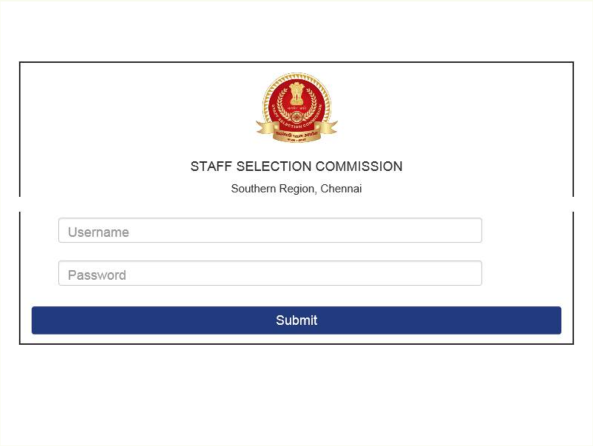
Issue 2 of 2 TOC

Body Parameters Accepted in Query

Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.51/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

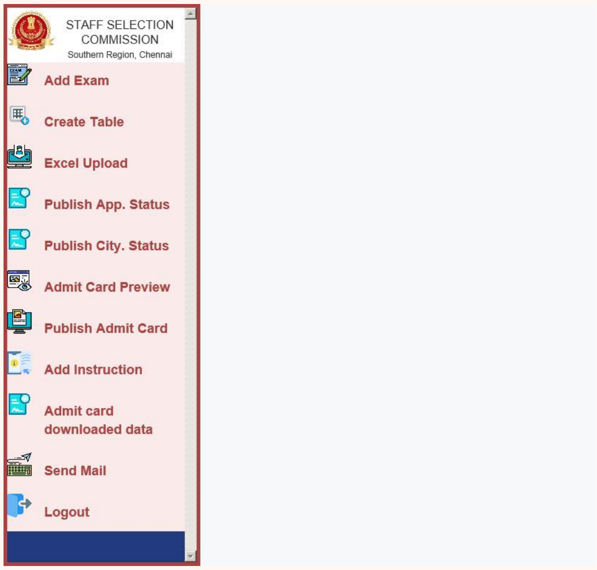
Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Original Response



≈

Test Response



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://10.163.2.51/
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

```
...

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'
location: login.php
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Set-Cookie: name=value; HttpOnly



GET /sscsr_audit/dataentry/login.php HTTP/1.1
Cookie: name=value; PHPSESSID=ktf1j1of2fdnlfiq150c4pu8o5
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.51/sscsr_audit/dataentry/index.php
Host: 10.163.2.51

...
```

Issue 2 of 2

TOC

Cookie with Insecure or Improper or Missing SameSite attribute

Severity:	Medium
CVSS Score:	4.7
URL:	http://10.163.2.51/
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/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
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=87
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=90ti52v4th0033skshl6orfmaa; 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">

...
```

M Directory Listing 1

TOC

Issue 1 of 1

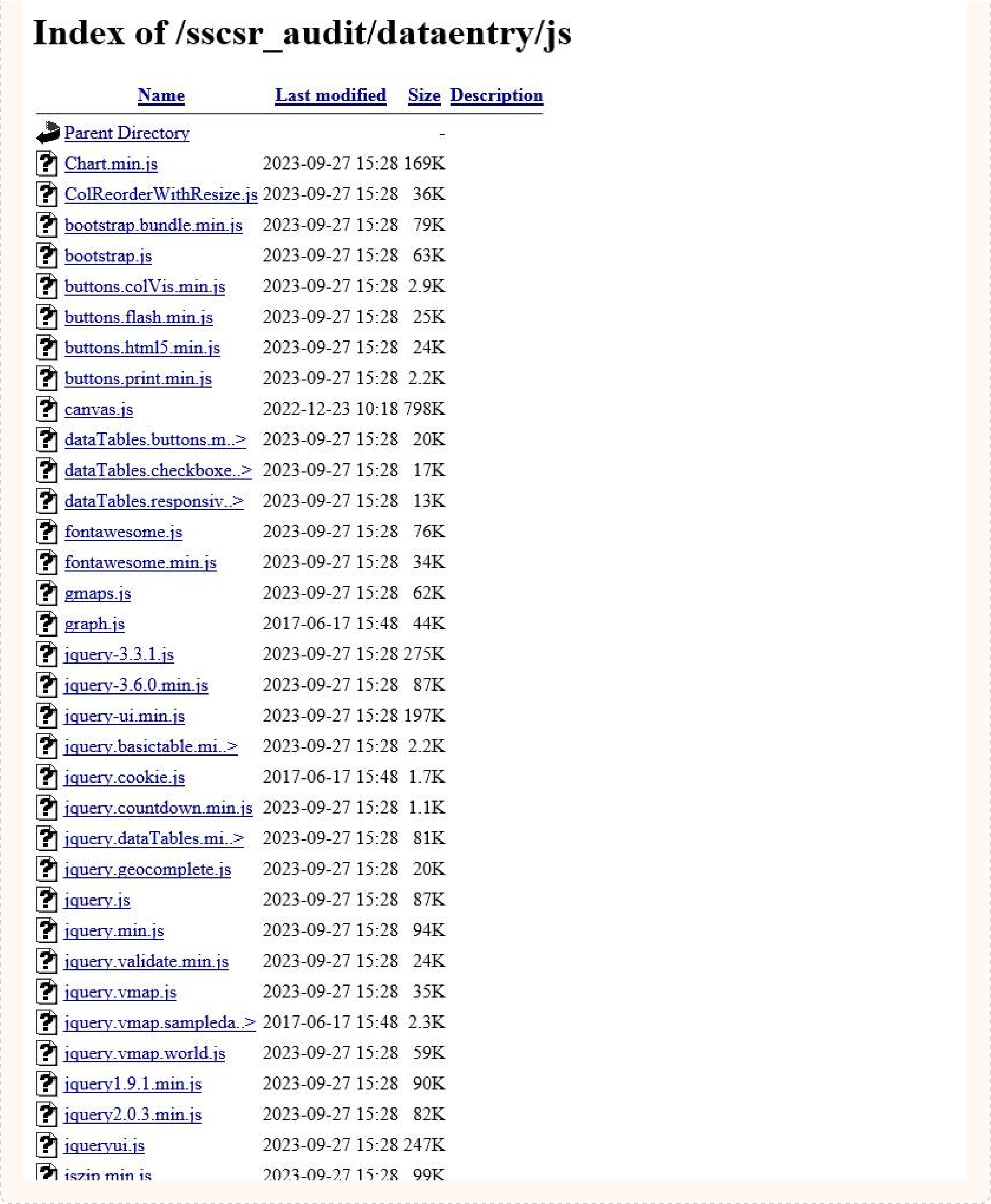
TOC

Directory Listing

Severity:	Medium
CVSS Score:	6.5
URL:	http://10.163.2.51/
Entity:	10.163.2.51 (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		-	
Chart.min.js	2023-09-27 15:28	169K	
ColReorderWithResize.js	2023-09-27 15:28	36K	
bootstrap.bundle.min.js	2023-09-27 15:28	79K	
bootstrap.js	2023-09-27 15:28	63K	
buttons.colVis.min.js	2023-09-27 15:28	2.9K	
buttons.flash.min.js	2023-09-27 15:28	25K	
buttons.html5.min.js	2023-09-27 15:28	24K	
buttons.print.min.js	2023-09-27 15:28	2.2K	
canvas.js	2022-12-23 10:18	798K	
dataTables.buttons.m..>	2023-09-27 15:28	20K	
dataTables.checkboxe..>	2023-09-27 15:28	17K	
dataTables.responsiv..>	2023-09-27 15:28	13K	
fontawesome.js	2023-09-27 15:28	76K	
fontawesome.min.js	2023-09-27 15:28	34K	
gmaps.js	2023-09-27 15:28	62K	
graph.js	2017-06-17 15:48	44K	
jquery-3.3.1.js	2023-09-27 15:28	275K	
jquery-3.6.0.min.js	2023-09-27 15:28	87K	
jquery-ui.min.js	2023-09-27 15:28	197K	
jquery.basictable.mi..>	2023-09-27 15:28	2.2K	
jquery.cookie.js	2017-06-17 15:48	1.7K	
jquery.countdown.min.js	2023-09-27 15:28	1.1K	
jquery.dataTables.mi..>	2023-09-27 15:28	81K	
jquery.geocomplete.js	2023-09-27 15:28	20K	
jquery.js	2023-09-27 15:28	87K	
jquery.min.js	2023-09-27 15:28	94K	
jquery.validate.min.js	2023-09-27 15:28	24K	
jquery.vmap.js	2023-09-27 15:28	35K	
jquery.vmap.sampleda..>	2017-06-17 15:48	2.3K	
jquery.vmap.world.js	2023-09-27 15:28	59K	
jquery1.9.1.min.js	2023-09-27 15:28	90K	
jquery2.0.3.min.js	2023-09-27 15:28	82K	
jqueryui.js	2023-09-27 15:28	247K	
jszip.min.js	2023-09-27 15:28	99K	

M Directory Listing Pattern Found 1

TOC

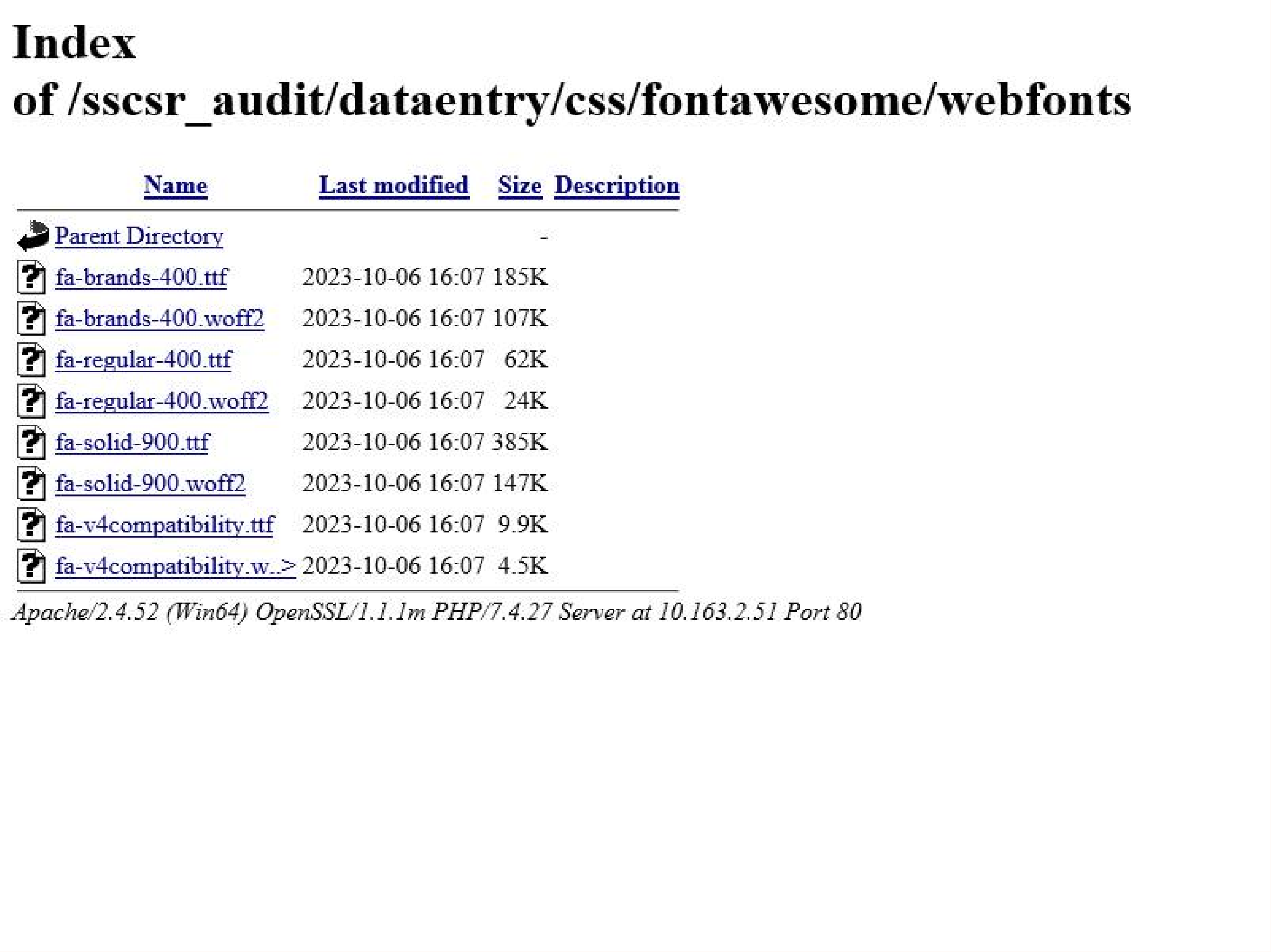
Issue 1 of 1

TOC

Directory Listing Pattern Found	
Severity:	Medium
CVSS Score:	5.3
URL:	http://10.163.2.51/
Entity:	10.163.2.51 (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/css/fontawesome/webfonts

Name	Last modified	Size	Description
Parent Directory		-	
fa-brands-400.ttf	2023-10-06 16:07	185K	
fa-brands-400.woff2	2023-10-06 16:07	107K	
fa-regular-400.ttf	2023-10-06 16:07	62K	
fa-regular-400.woff2	2023-10-06 16:07	24K	
fa-solid-900.ttf	2023-10-06 16:07	385K	
fa-solid-900.woff2	2023-10-06 16:07	147K	
fa-v4compatibility.ttf	2023-10-06 16:07	9.9K	
fa-v4compatibility.w..>	2023-10-06 16:07	4.5K	

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80

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://10.163.2.51/
Entity:	10.163.2.51 (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:

```
...

Upgrade-Insecure-Requests: 1
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:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Connection: keep-alive
Cookie: name=value
Content-Length: 0


HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 10:28:16 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
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=93
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=k9vjpg4m7cevn295p8cf16e1b3; 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">
<!-- Include jQuery -->
<script src="js/jquery-3.6.0.min.js"></script>

...
```

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://10.163.2.51/
Entity:	10.163.2.51 (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:

```
...

Cookie: name=value; PHPSESSID=tnhevrtl5su93h5ok38ph6mtqr
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.51/sscsr_audit/dataentry/add_exam.php
Host: 10.163.2.51
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: 0


HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 10:24:08 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 6835
Content-Type: text/html; charset=UTF-8

<!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">
<!-- Include jQuery -->
<script src="js/jquery-3.6.0.min.js"></script>

...
```

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://10.163.2.51/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 10:29:17 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
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">

...
```

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://10.163.2.51/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://10.163.2.51/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...
...nitizeSelector:function(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...
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://10.163.2.51/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...

...
```

Internal IP Disclosure Pattern Found 23

TOC

Issue 1 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </td><td align="right">4.5K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 2 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-20 11:52  </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">2023-08-01 13:02  </td><td align="right">  0 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 3 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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:

```
...
align="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="sprites/">sprites/</a>          </td><td
align="right">2023-10-06 16:07  </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 16:07  </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 16:07  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="LICENSE.txt">LICENSE.txt</a>          </td>
<td align="right">2023-10-06 16:07  </td><td align="right">7.4K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 4 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-06 16:07  </td><td align="right">479K</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">2023-10-06 16:07  </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">2023-10-06 16:07  </td><td align="right">843K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 5 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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.png">logo.png</a>          </td><td
align="right">2022-09-09 10:30  </td><td align="right">144K</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">2022-09-09 10:30  </td><td align="right">253K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 6 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-06 16:07  </td><td align="right">609K</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">2023-10-06 16:07  </td><td align="right"> 44K</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">2023-10-06 16:07  </td><td align="right"> 11K</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">2023-10-06 16:07  </td><td align="right"> 28K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 7 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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 14:55  </td><td align="right">828K</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 14:55  </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 14:55  </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 14:55  </td><td align="right"> 27K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 8 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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 16:07  </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 16:07  </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 16:07  </td><td align="right">  - </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 9 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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 15:28  </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">2023-09-05 14:09  </td><td align="right">2.9K</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 15:28  </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">2019-06-06 18:25  </td><td align="right">905K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 10 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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:

```
...
d valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="logo/">logo/</a>          </td><td
align="right">2023-09-26 13:00  </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.jpg">logo.jpg</a>          </td><td
align="right">2022-09-09 10:30  </td><td align="right"> 18K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="icons/">icons/</a>          </td><td
align="right">2023-09-26 13:00  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="fpdf_ssc_header.png">fpdf_ssc_header.png</a>    </td><td align="right">2022-09-09 10:30  </td><td
align="right">5.6K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 11 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2022-09-09 10:30  </td><td align="right">3.3K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 12 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-06 16:07  </td><td align="right"> 43K</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">2023-10-06 16:07  </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">2023-10-06 16:07  </td><td align="right">893 </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">2023-10-06 16:07  </td><td align="right">799 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 13 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2022-09-09 10:30  </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">2022-09-09 10:30  </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">2022-09-09 10:30  </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">2022-09-09 10:30  </td><td align="right"> 12K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 14 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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:

```
...
gn="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="bootstrap.css">bootstrap.css</a>          </td><td
align="right">2023-11-15 14:55  </td><td align="right">145K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="basictable.css">basictable.css</a>
</td><td align="right">2023-11-15 14:55  </td><td align="right">927 </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="aaf5c053.proton.css">aaf5c053.proton.css</a>
</td><td align="right">2017-06-17 15:48  </td><td align="right"> 25K</td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="Chart.css">Chart.css</a>          </td><td
align="right">2023-11-15 14:55  </td><td align="right">671 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 15 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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 16 of 23

TOC

Internal IP Disclosure Pattern Found	
Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </td><td align="right">631 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 17 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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 18 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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:

```
...
873 369.01 334.618 374.453 354.747H321.44C316.555 337.262 306.614 321.61 292.865 309.754C279.117 297.899 262.173 290.368
244.16 288.107V354.747H238.373C136.267 354.747 78.0267 284.747 75.6 168.267Z"],
    "untappd": [640, 512, [], "f405", "M401.3 49.9c-79.8 160.1-84.6 152.5-87.9 173.2l-5.2 32.8c-1.9 12-6.6 23.5-13.7
33.4L145.6 497.1c-7.6 10.6-20.4 16.2-33.4 14.6-40.3-5-77.8-32.2-95.3-68.5-5.7-11.8-...
...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, [], "f38b", "M0 32l34.9 395.8L192 480l157.1-52.2L384 32H0zm313.1 80l-4.8 47.3L193 208.6l-
.3.1h111.5l-12.8 146.6-98.2 28.7-98.8-29.2-6.4-73.9h48.9l3.2 38.3 52.6 13.3 54.7-15....
    "square-reddit": [448, 512, ["reddit-square"], "f1a2", "M283.2 345.5c2.7 2.7 2.7 6.8 0 9.2-24.5 24.5-93.8 24.6-118.4 0-
2.7-2.4-2.7-6.5 0-9.2 2.4-2.4 6.5-2.4 8.9 0 18.7 19.2 81 19.6 100.5 0 2.4-2.3...
    "vimeo-v": [448, 512, [], "f27d", "M447.8 153.6c-2 43.6-32.4 103.3-91.4 179.1-60.9 79.2-112.4 118.8-154.6 118.8-26.1 0-
48.2-24.1-66.3-72.3C100.3 250 85.3 174.3 56.2 174.3c-3.4 0-15.1 7.1-35.2 21.1

...

...
-29.2-103.6-55.1 18.8-93.8 56.4-108.1 85.6zm98.8-108.2c-3.4-7.8-7.2-15.5-11.1-23.2C159.6 253 93.4 252.2 87.4 252c0 1.4-.1
2.8-.1 4.2 0 35.1 13.3 67.1 35.1 91.4 22.2-37.9 67.1-77.9 116.5-91.8zm34.9 16....
    "codiepie": [472, 512, [], "f284", "M422.5 202.9c30.7 0 33.5 53.1-.3 53.1h-10.8v44.3h-26.6v-97.4h37.7zM472 352.6C429.9
444.5 350.4 504 248 504 111 504 0 393 0 256S111 8 248 8c97.4 0 172.8 53.7 218...
...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...

...

...

    "instalod": [512, 512, [], "e081",
"M153.384,480H387.113L502.554,275.765,204.229,333.211ZM504.726,240.078,387.113,32H155.669L360.23,267.9ZM124.386,48.809,7.27
4,256,123.236,461.154,225.627,165.561...
    "expeditedssl": [496, 512, [], "f23e", "M248 43.4C130.6 43.4 35.4 138.6 35.4 256S130.6 468.6 248 468.6 460.6 373.4
460.6 256 365.4 43.4 248 43.4zm-97.4 132.9c0-53.7 43.7-97.4 97.4-97.4s97.4 43.7 9...
... 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...
    "square-twitter": [448, 512, ["twitter-square"], "f081", "M64 32C28.7 32 0 60.7 0 96V416c0 35.3 28.7 64 64 64H384c35.3
0 64-28.7 64-64V96c0-35.3-28.7-64-64-64H64zM351.3 199.3v0c0 86.7-66 186.6-186...
    "r-project": [581, 512, [], "f4f7", "M581 226.6C581 119.1 450.9 32 290.5 32S0 119.1 0 226.6C0 322.4 103.3 402 239.4
418.1V480h99.1v-61.5c24.3-2.7 47.6-7.4 69.4-13.9L448 480h112l-67.4-113.7c54.5-35...
    "delicious": [448, 512, [], "f1a5", "M446.5 68c-.4-1.5-.9-3-1.4-4.5-.9-2.5-2-4.8-3.3-7.1-1.4-2.4-3-4.8-4.7-6.9-2.1-2.5-
4.4-4.8-6.9-6.8-1.1-.9-2.2-1.7-3.3-2.5-1.3-.9-2.6-1.7-4-2.4-1.8-1-3.6-1.8-5.5...
```

```
...
```

Issue 19 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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:

```
...
873 369.01 334.618 374.453 354.747H321.44C316.555 337.262 306.614 321.61 292.865 309.754C279.117 297.899 262.173 290.368
244.16 288.107V354.747H238.373C136.267 354.747 78.0267 284.747 75.6 168.267Z"],
    "untappd": [640, 512, [], "f405", "M401.3 49.9c-79.8 160.1-84.6 152.5-87.9 173.2l-5.2 32.8c-1.9 12-6.6 23.5-13.7
33.4L145.6 497.1c-7.6 10.6-20.4 16.2-33.4 14.6-40.3-5-77.8-32.2-95.3-68.5-5.7-11.8-...
...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, [], "f38b", "M0 32l34.9 395.8L192 480l157.1-52.2L384 32H0zm313.1 80l-4.8 47.3L193 208.6l-
.3.1h111.5l-12.8 146.6-98.2 28.7-98.8-29.2-6.4-73.9h48.9l3.2 38.3 52.6 13.3 54.7-15....
    "square-reddit": [448, 512, ["reddit-square"], "f1a2", "M283.2 345.5c2.7 2.7 2.7 6.8 0 9.2-24.5 24.5-93.8 24.6-118.4 0-
2.7-2.4-2.7-6.5 0-9.2 2.4-2.4 6.5-2.4 8.9 0 18.7 19.2 81 19.6 100.5 0 2.4-2.3...
    "vimeo-v": [448, 512, [], "f27d", "M447.8 153.6c-2 43.6-32.4 103.3-91.4 179.1-60.9 79.2-112.4 118.8-154.6 118.8-26.1 0-
48.2-24.1-66.3-72.3C100.3 250 85.3 174.3 56.2 174.3c-3.4 0-15.1 7.1-35.2 21.1

...

...
-29.2-103.6-55.1 18.8-93.8 56.4-108.1 85.6zm98.8-108.2c-3.4-7.8-7.2-15.5-11.1-23.2C159.6 253 93.4 252.2 87.4 252c0 1.4-.1
2.8-.1 4.2 0 35.1 13.3 67.1 35.1 91.4 22.2-37.9 67.1-77.9 116.5-91.8zm34.9 16....
    "codiepie": [472, 512, [], "f284", "M422.5 202.9c30.7 0 33.5 53.1-.3 53.1h-10.8v44.3h-26.6v-97.4h37.7zM472 352.6C429.9
444.5 350.4 504 248 504 111 504 0 393 0 256S111 8 248 8c97.4 0 172.8 53.7 218...
...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...

...

...
    "instalod": [512, 512, [], "e081",
"M153.384,480H387.113L502.554,275.765,204.229,333.211ZM504.726,240.078,387.113,32H155.669L360.23,267.9ZM124.386,48.809,7.27
4,256,123.236,461.154,225.627,165.561...
    "expeditedssl": [496, 512, [], "f23e", "M248 43.4C130.6 43.4 35.4 138.6 35.4 256S130.6 468.6 248 468.6 460.6 373.4
460.6 256 365.4 43.4 248 43.4zm-97.4 132.9c0-53.7 43.7-97.4 97.4-97.4s97.4 43.7 9...
... 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...
    "square-twitter": [448, 512, ["twitter-square"], "f081", "M64 32C28.7 32 0 60.7 0 96V416c0 35.3 28.7 64 64 64H384c35.3
0 64-28.7 64-64V96c0-35.3-28.7-64-64-64H64zM351.3 199.3v0c0 86.7-66 186.6-186...
    "r-project": [581, 512, [], "f4f7", "M581 226.6C581 119.1 450.9 32 290.5 32S0 119.1 0 226.6C0 322.4 103.3 402 239.4
418.1V480h99.1v-61.5c24.3-2.7 47.6-7.4 69.4-13.9L448 480h112l-67.4-113.7c54.5-35...
```

```
    "delicious": [448, 512, [], "f1a5", "M446.5 68c-.4-1.5-.9-3-1.4-4.5-.9-2.5-2-4.8-3.3-7.1-1.4-2.4-3-4.8-4.7-6.9-2.1-2.5-
4.4-4.8-6.9-6.8-1.1-.9-2.2-1.7-3.3-2.5-1.3-.9-2.6-1.7-4-2.4-1.8-1-3.6-1.8-5.5...

...
```

Issue 20 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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 89.9-64.9 138.2-37.2l4.8-8.4c14.3-24.9 52-3.3 37...

...
```

Issue 21 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </td><td align="right">493 </td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

Issue 22 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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 23 of 23

TOC

Internal IP Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </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">2023-10-06 16:07  </td><td align="right">1.7K</td><td>&nbsp;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Server at 10.163.2.51 Port 80</address>
</body></html>

...
```

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://10.163.2.51/
Entity:	10.163.2.51 (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 10:21:03 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
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=98
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=ktf1j1of2fdnlfiq150c4pu8o5; 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">
...
```

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://10.163.2.51/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://10.163.2.51/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=tnhevrtl5su93h5ok38ph6mtqr
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.51/sscsr_audit/dataentry/upload_excel_file.php
Host: 10.163.2.51
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=27ca6276ac9a0570
27922d525897d25ad478aad4ae4db469e4cc67d741042364

HTTP/1.1 302 Found
Date: Fri, 17 Nov 2023 10:23:07 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php

...
```

Issue 2 of 2

TOC

Potential File Upload

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.163.2.51/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=tnhevrtl5su93h5ok38ph6mtqr
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.163.2.51/sscsr_audit/dataentry/upload_admitcard_important_instructions.php
Host: 10.163.2.51
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=fc469f41599d9030508d3fbcda016724c756377658ff4756e44ac114343e3bf4

HTTP/1.1 302 Found
Date: Fri, 17 Nov 2023 10:23:08 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

```
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php

...
```