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: 8/22/2023 4:34:09 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.

Medium severity issues:	42
Informational severity issues:	1
Total security issues included in the report:	43
Total security issues discovered in the scan:	43

General Information

Scan file name:	Untitled
Scan started:	8/22/2023 4:34:09 PM
Test policy:	Default
CVSS version:	3.1
Test optimization level:	Fast

Host	hwcs.tn.gov.in
Port	443
Operating system:	Unknown
Web server:	Apache
Application server:	PHP

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
In-session detection:	Disabled
In-session pattern:	
Tracked or session ID cookies:	`PHPSESSID`
Tracked or session ID parameters:	`token_new` `token_new`

Login sequence:	`https://hwcs.tn.gov.in/`
	`https://hwcs.tn.gov.in/`
	`https://hwcs.tn.gov.in/login.php`
	`https://hwcs.tn.gov.in/login.php`
	`https://hwcs.tn.gov.in/login.php`

Summary

Issue Types 15

TOC

	Issue Type	Number of Issues
M	Apache Multiviews Attack	2
M	Autocomplete HTML Attribute Not Disabled for Password Field	1
M	Body Parameters Accepted in Query	2
M	Cookie with Insecure or Improper or Missing SameSite attribute	1
M	Cross-Site Request Forgery	1
M	Directory Listing	1
M	Directory Listing Pattern Found	1
M	Encryption Not Enforced	1
M	Hidden Directory Detected	20
M	Missing "Content-Security-Policy" header	1
M	Missing or insecure "X-Content-Type-Options" header	1
M	Missing or insecure HTTP Strict-Transport-Security Header	1
M	Overly Permissive CORS Access Policy	8
M	Unnecessary Http Response Headers found in the Application	1
I	Email Address Pattern Found	1

Vulnerable URLs 8

TOC

	URL	Number of Issues
M	https://hwcs.tn.gov.in/icons/	3
M	https://hwcs.tn.gov.in/icons/small/	2
M	https://hwcs.tn.gov.in/forgotpassword.php	3
M	https://hwcs.tn.gov.in/	30
M	https://hwcs.tn.gov.in/assets/css/bootstrap.min.js	1
M	https://hwcs.tn.gov.in/assets/js/redirect.js	1
M	https://hwcs.tn.gov.in/js/bootstrap.bundle.min.js	1
M	https://hwcs.tn.gov.in/js/fontawesome.js	2

Fix Recommendations 14

TOC

	Remediation Task	Number of Issues
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	Correctly set the "autocomplete" attribute to "off"	1
M	Do not accept body parameters that are sent in the query string	2
M	Do not allow sensitive information to leak.	1
M	Enforce the use of HTTPS when sending sensitive information	1
M	Implement the HTTP Strict-Transport-Security policy with a long "max-age"	1
M	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely	20
M	Modify the "Access-Control-Allow-Origin" header to contain only allowed sites	8
M	Modify the server configuration to deny directory listing, and install the latest security patches available	2
M	Modify the server configuration to disable the Multiviews feature	2
M	Review possible solutions for configuring SameSite Cookie attribute to recommended values	1
M	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form	1
L	Remove e-mail addresses from the website	1

Security Risks 9

TOC

	Risk	Number of Issues
M	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	2
M	It may be possible to bypass the web application's authentication mechanism	1
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	15
M	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	13
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).	1
M	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.	1
M	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files	2
M	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted	1
M	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site	20

Causes 10

TOC

	Cause	Number of Issues
M	The web server or application server are configured in an insecure way	22
M	Insecure web application programming or configuration	16
M	Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute	1
M	This vulnerability arises because the application allows the user to perform some sensitive action without verifying that the request was sent intentionally.	1
M	An attacker can cause a victim's browser to emit an HTTP request to an arbitrary URL in the application. When this request is sent from an authenticated victim's browser, it will include the victim's session cookie or authentication header. The application will accept this as a valid request from an authenticated user.	1
M	When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, an attacker may be able to trick a client into making an unintentional request from a different site, which will be treated as an authentic request by the application. This can be done by submitting a form, loading an image, sending an XMLHttpRequest in JavaScript, and more.	1
M	For example, this IMG tag can be embedded in an attacker's webpage, and the victim's browser will submit a request to retrieve the image. This valid request will be processed by the application, and the browser will not display a broken image. `<img src="https://myapp.com/transfer?acct=VICTIM&amount=10000" width=0 height=0 border=0>`. As a result, money is transferred from the victim's account to the attacker, using the victim's session.	1
M	Directory browsing is enabled	2
M	The application does not use a secure channel, such as TLS/SSL, to exchange sensitive information.	1
M	An attacker with access to the network traffic can eavesdrop on packets over the connection. This attack is not technically difficult, but does require physical access to some portion of the network over which the sensitive data travels.	1

WASC Threat Classification

TOC

Threat	Number of Issues
Cross-site Request Forgery	1
Directory Indexing	2
Information Leakage	39
Server Misconfiguration	1

Issues Sorted by Issue Type

M Apache Multiviews Attack 2 TOC

Issue 1 of 2 TOC

Apache Multiviews Attack

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/icons/
Entity:	index (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:	The web server or application server are configured in an insecure way
Fix:	Modify the server configuration to disable the Multiviews feature

Reasoning: The test response indicates that the server reveals some of its pages names in the response

Raw Test Response:

```
...

Content-Length: 0


HTTP/1.1 406 Not Acceptable
Date: Tue, 22 Aug 2023 11:11:14 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Alternates: {"index.gif" 1 {type image/gif} {length 268}}, {"index.png" 1 {type image/png} {length 332}}
Vary: negotiate,accept
TCN: list
Content-Length: 400
Keep-Alive: timeout=600, max=181
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
...
```

Issue 2 of 2

TOC

Apache Multiviews Attack

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/icons/small/
Entity:	index (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:	The web server or application server are configured in an insecure way
Fix:	Modify the server configuration to disable the Multiviews feature

Reasoning: The test response indicates that the server reveals some of its pages names in the response

Raw Test Response:

```
...

Content-Length: 0


HTTP/1.1 406 Not Acceptable
Date: Tue, 22 Aug 2023 11:11:14 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Alternates: {"index.gif" 1 {type image/gif} {length 268}}, {"index.png" 1 {type image/png} {length 332}}
Vary: negotiate,accept
TCN: list
Content-Length: 400
Keep-Alive: timeout=600, max=181
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
...
```

M Autocomplete HTML Attribute Not Disabled for Password Field 1

TOC

Issue 1 of 1

TOC

Autocomplete HTML Attribute Not Disabled for Password Field

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/forgotpassword.php
Entity:	forgotpassword.php (Page)
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.
Raw Test Response:

```
...

        </div>
        <form class="p-3 mt-3" actiom=""  id="myform" name="myform" method="POST" >

          <div class="form-field d-flex align-items-center">
          <span class="fa fa-user"></span>
          <input type="text" name="usermail" id="usermail"  maxlength="50" value="" placeholder="Email">
          </div>
          <div class="form-field d-flex align-items-center">
          <span class="fa fa-key"></span>
          <input type="password" name="newpassword" onchange="chkPassword();" id="newpassword" maxlength="50" value=""
placeholder="Newpassword">
          </div>
          <div class="form-group">
          <label for="Society_type">Role Type:</label>
          <select id="role_type" name="role_type" class="form-control"  value="" data-error="">
          <option value="">--Select--</option>
      <option value="1"  >SUPER ADMIN</option><option value="2"  >HEAD OFFICE</option><option value="3"  >CIRCLE
OFFICE</option><option value="4"  >SOCIETY OFFICE</option>        </select>
        </div>
          <div class="form-group">
  <input type="hidden" name="token" value="88c26d328d5f9895d8e25137185c468c">

...
```

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:	https://hwcs.tn.gov.in/forgotpassword.php
Entity:	forgotpassword.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

Issue 2 of 2

TOC

Body Parameters Accepted in Query

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
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

M Cookie with Insecure or Improper or Missing SameSite attribute 1

TOC

Issue 1 of 1

TOC

Cookie with Insecure or Improper or Missing SameSite attribute

Severity:	Medium
CVSS Score:	4.7
URL:	https://hwcs.tn.gov.in/
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

```
...

X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Length: 12662
Keep-Alive: timeout=600, max=200
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=bjfvjkf4adi1lcjsb4uafcf1go; path=/;HttpOnly;Secure;SameSite=None


<!-- <link href="assets/js/redirect.js" rel="stylesheet" media="all"> -->

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">

...
```

M Cross-Site Request Forgery 1 TOC

Issue 1 of 1 TOC

Cross-Site Request Forgery

Severity:	Medium
CVSS Score:	6.5
URL:	https://hwcs.tn.gov.in/
Entity:	token_new (Parameter)
Risk:	It may be possible to force an end-user to execute unwanted actions on a web application in which they're currently authenticated.
Cause:	This vulnerability arises because the application allows the user to perform some sensitive action without verifying that the request was sent intentionally. An attacker can cause a victim's browser to emit an HTTP request to an arbitrary URL in the application. When this request is sent from an authenticated victim's browser, it will include the victim's session cookie or authentication header. The application will accept this as a valid request from an authenticated user. When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, an attacker may be able to trick a client into making an unintentional request from a different site, which will be treated as an authentic request by the application. This can be done by submitting a form, loading an image, sending an XMLHttpRequest in JavaScript, and more. For example, this IMG tag can be embedded in an attacker's webpage, and the victim's browser will submit a request to retrieve the image. This valid request will be processed by the application, and the browser will not display a broken image. `<img src="https://myapp.com/transfer?acct=VICTIM&amount=10000" width=0 height=0 border=0>`. As a result, money is transferred from the victim's account to the attacker, using the victim's session.
Fix:	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

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

M Directory Listing 1

TOC

Issue 1 of 1

TOC

Directory Listing

Severity:	Medium
CVSS Score:	6.5
URL:	https://hwcs.tn.gov.in/
Entity:	hwcs.tn.gov.in (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.

M Directory Listing Pattern Found 1 TOC

Issue 1 of 1 TOC

Directory Listing Pattern Found	
Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	hwcs.tn.gov.in (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.

M Encryption Not Enforced 1 TOC

Issue 1 of 1 TOC

Encryption Not Enforced	
Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	hwcs.tn.gov.in (Page)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Cause:	The application does not use a secure channel, such as TLS/SSL, to exchange sensitive information. An attacker with access to the network traffic can eavesdrop on packets over the connection. This attack is not technically difficult, but does require physical access to some portion of the network over which the sensitive data travels.
Fix:	Enforce the use of HTTPS when sending sensitive information

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Issue 1 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	head/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:06:31 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=192
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 2 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	small/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 200 OK
Date: Tue, 22 Aug 2023 11:06:35 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Length: 14299
Keep-Alive: timeout=600, max=146
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons/small</title>
 </head>
 <body>
<h1>Index of /icons/small</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>
...
```

Issue 3 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	icons/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 200 OK
Date: Tue, 22 Aug 2023 11:06:35 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Length: 74642
Keep-Alive: timeout=600, max=153
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons</title>
 </head>
 <body>
<h1>Index of /icons</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>
...
```

Issue 4 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	cgi-bin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 5 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	assets/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 6 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	member/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
...
```

Issue 7 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	new/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 8 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	scripts/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 9 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	purchase/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 10 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	sales/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
...
```

Issue 11 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	report/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 12 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	image/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 13 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	files/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 14 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	images/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
...
```

Issue 15 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	js/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 16 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	include/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 17 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	accounts/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 18 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	uploads/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

```
...
```

Issue 19 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	password/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

Issue 20 of 20

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	css/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Raw Test Response:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 403 Forbidden
Date: Tue, 22 Aug 2023 11:07:03 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Content-Length: 199
Keep-Alive: timeout=600, max=175
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

...
```

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:	https://hwcs.tn.gov.in/
Entity:	hwcs.tn.gov.in (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:

```
...

Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 200 OK
Date: Tue, 22 Aug 2023 11:06:34 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:13 GMT
Accept-Ranges: bytes
Content-Length: 11023
Access-Control-Allow-Origin: *
Keep-Alive: timeout=600, max=163
Connection: Keep-Alive
Content-Type: application/javascript

window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":false},"autoA11y":{"enabled":true},"baseUrl...
!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e)
{return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){r...

...
```

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:	https://hwcs.tn.gov.in/
Entity:	hwcs.tn.gov.in (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Raw Test Response:

```
...

Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://hwcs.tn.gov.in/
Host: hwcs.tn.gov.in
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 200 OK
Date: Tue, 22 Aug 2023 11:04:28 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:13 GMT
Accept-Ranges: bytes
Content-Length: 11023
Access-Control-Allow-Origin: *
Content-Type: application/javascript

window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":false},"autoA11y":{"enabled":true},"baseUrl...
!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e)
{return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){r...

...
```

M Missing or insecure HTTP Strict-Transport-Security Header 1

TOC

Issue 1 of 1

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	hwcs.tn.gov.in (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:	Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Raw Test Response:

```
HTTP/1.1 200 OK
Date: Tue, 22 Aug 2023 11:04:28 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:13 GMT
Accept-Ranges: bytes
Content-Length: 11023
Access-Control-Allow-Origin: *
Content-Type: application/javascript

window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":false},"autoA11y":{"enabled":true},"baseUrl":"https://ka-
f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":
{},"id":68486381,"license":"free","method":"css","minify":{"enabled":true},"token":"c7c269fc9c","v4FontFaceShim":
{"enabled":true},"v4shim":{"enabled":true},"v5FontFaceShim":{"enabled":true},"version":"6.2.0"};
!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e)
{return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return
t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return
e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var
n=Object.keys(t);if(Object.getOwnPropertySymbols){var o=Object.getOwnPropertySymbols(t);e&&(o=o.filter((function(e){return
Object.getOwnPropertyDescriptor(t,e).enumerable}))),n.push.apply(n,o)}return n}function o(t){for(var
o=1;o<arguments.length;o++){var r=null!=arguments[o]?arguments[o]:{};o%2?n(Object(r),!0).forEach((function(...
```

M Overly Permissive CORS Access Policy 8

TOC

Issue 1 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/js/fontawesome.js
Entity:	fontawesome.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 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:

```
...

Date: Tue, 22 Aug 2023 11:04:28 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:13 GMT
Accept-Ranges: bytes
Content-Length: 11023
Access-Control-Allow-Origin: *
Content-Type: application/javascript

window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":false},"autoA11y":{"enabled":true},"baseUrl":"https://ka-
f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":
{},"id":68486381,"license":"free","method":"css","minify":{"enabled":true},"token":"c7c269fc9c","v4FontFaceShim":
{"enabled":true},"v4shim":{"enabled":true},"v5FontFaceShim":{"enabled":true},"version":"6.2.0"};
!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(e)
{return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return
t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return
e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var
n=Object.keys(t);if(Object.getOwnPropertySymbols){var o=Object.getOwnPropertySymbols(t);e&&(o=o.filter((function(e){return
Object.getOwnPropertyDescriptor(t,e).enumerable}))),n.push.apply(n,o)}return n}function o(t){for(var
o=1;o<arguments.length;o++){var r=null!=arguments[o]?arguments[o]:{};o%2?n(Object(r),!0).forEach((function
...
```

Issue 2 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/forgotpassword.php
Entity:	forgotpassword.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:

```
...

Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">

<link href="css/style.css"  rel="stylesheet" >
 <link href="css/style.css">
<!--

...
```

Issue 3 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
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:

```
...

Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Length: 12662
Keep-Alive: timeout=600, max=182
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=trbjdddmm7c9839bodhktco8om; path=/;HttpOnly;Secure;SameSite=None


<!-- <link href="assets/js/redirect.js" rel="stylesheet" media="all"> -->

...
```

Issue 4 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/assets/js/redirect.js
Entity:	redirect.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 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:

```
...

Date: Tue, 22 Aug 2023 11:04:30 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:20 GMT
Accept-Ranges: bytes
Content-Length: 91192
Access-Control-Allow-Origin: *
Content-Type: application/javascript
```

```
(function(a,b){function cv(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}function cs(a)
{if(!cg[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e===""){ch||
(ch=c.createElement("iframe"),ch.frameBorder=ch.width=ch.height=0),b.appendChild(ch);if(!ci||!ch.createElement)ci=
(ch.contentWindow||ch.contentDocument).document,ci.write((c.compatMode==="CSS1Compat"?"<!doctype html>":"")+"<html>
<body>"),ci.close();d=ci.createElement(a),ci.body.appendChild(d),e=f.css(d,"display"),b.removeChild(ch)}cg[a]=e}return
cg[a]}function cr(a,b){var c={};f.each(cm.concat.apply([],cm.slice(0,b)),function(){c[this]=a});return c}function cq()
{cn=b}function cp(){setTimeout(cq,0);return cn=f.now()}function cf(){try{return new
a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ce(){try{return new a.XMLHttpRequest}catch(b){}}function b$(a,c)
{a.dataFilter&&(c=a.dataFilter(c,a.dataType));var d=a.dataTypes,e={},g,h,i=d.length,j,k=d[0],l,m,n,o,p;for(g=1;g<i;g++)
{if(g===1)for(h in a.converters)typeof h=="string"&&(e[h.toLowerCase()]=a.converters[h]);l=k,k=d[g];if(k==="*")k=l;else
if(l!=="*"&&l!==k){m=l+" "+k,n=e[m]||e["* "+k];if(!n){p=b;for(o in e){j
...
```

Issue 5 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/assets/css/bootstrap.min.js
Entity:	bootstrap.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 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:

```
...

Date: Tue, 22 Aug 2023 11:04:30 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:15 GMT
Accept-Ranges: bytes
Content-Length: 59855
Access-Control-Allow-Origin: *
Content-Type: application/javascript


!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?
module.exports=e(require("@popperjs/core")):"function"==typeof define&&define.amd?define(["@popperjs/core"],e):
(t="undefined"!=typeof globalThis?globalThis:t||self).bootstrap=e(t.Popper)}(this,(function(t){"use strict";function e(t)
{if(t&&t.__esModule)return t;var e=Object.create(null);return t&&Object.keys(t).forEach((function(s){if("default"!==s){var
i=Object.getOwnPropertyDescriptor(t,s);Object.defineProperty(e,s,i.get?i:{enumerable:!0,get:function(){return
t[s]}})}})),e.default=t,Object.freeze(e)}var s=e(t);const i={find:(t,e=document.documentElement)=>
[].concat(...Element.prototype.querySelectorAll.call(e,t)),findOne:
(t,e=document.documentElement)=>Element.prototype.querySelector.call(e,t),children:(t,e)=>
[].concat(...t.children).filter(t=>t.matches(e)),parents(t,e){const s=[];let
i=t.parentNode;for(;i&&i.nodeType===Node.ELEMENT_NODE&&3!==i.nodeType;)i.matches(e)&&s.push(i),i=i.parentNode;return
s},prev(t,e){let s=t.previousElementSibling;for(;s;)
{if(s.matches(e))return[s];s=s.previousElementSibling}return[]},next(t,e){let s=t.nextElementSibling;for(;s;)
{if(s.matches(e))return[s];s=s.nextElementSibling}return[]}},n
...
```

Issue 6 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/js/bootstrap.bundle.min.js
Entity:	bootstrap.bundle.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 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:

```
...

Date: Tue, 22 Aug 2023 11:04:30 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:13 GMT
Accept-Ranges: bytes
Content-Length: 80138
Access-Control-Allow-Origin: *
Content-Type: application/javascript


!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof
define&&define.amd?define(e):(t="undefined"!=typeof globalThis?globalThis:t||self).bootstrap=e()}(this,(function(){"use
strict";const t="transitionend",e=t=>{let e=t.getAttribute("data-bs-target");if(!e||"#"===e){let
i=t.getAttribute("href");if(!i||!i.includes("#")&&!i.startsWith("."))return null;i.includes("#")&&!i.startsWith("#")&&
(i=`#${i.split("#")[1]}`),e=i&&"#"!==i?i.trim():null}return e},i=t=>{const i=e(t);return i&&document.querySelector(i)?
i:null},n=t=>{const i=e(t);return i?document.querySelector(i):null},s=e=>{e.dispatchEvent(new Event(t))},o=t=>!
(!t||"object"!=typeof t)&&(void 0!==t.jquery&&(t=t[0]),void 0!==t.nodeType),r=t=>o(t)?t.jquery?t[0]:t:"string"==typeof
t&&t.length>0?document.querySelector(t):null,a=t=>{if(!o(t)||0===t.getClientRects().length)return!1;const
e="visible"===getComputedStyle(t).getPropertyValue("visibility"),i=t.closest("details:not([open])");if(!i)return
e;if(i!==t){const e=t.closest("summary");if(e&&e.parentNode!==i)return!1;if(null===e)return!1}return
e},l=t=>!t||t.nodeType!==Node.ELEMENT_NODE||!!t.classList.contains("disabled")||(void 0!==t.disa
...
```

Issue 7 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/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 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: Tue, 22 Aug 2023 11:11:01 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Transfer-Encoding: chunked
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons</title>
 </head>
 <body>
...
```

Issue 8 of 8

TOC

Overly Permissive CORS Access Policy

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/icons/small/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
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: Tue, 22 Aug 2023 11:11:08 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Length: 14299
Keep-Alive: timeout=600, max=162
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons/small</title>
...
```

M Unnecessary Http Response Headers found in the Application 1 TOC

Issue 1 of 1 TOC

Unnecessary Http Response Headers found in the Application

Severity:	Medium
CVSS Score:	5.3
URL:	https://hwcs.tn.gov.in/js/fontawesome.js
Entity:	hwcs.tn.gov.in (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:	Do not allow sensitive information to leak.

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.
Raw Test Response:

```
...

Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip
Cookie: PHPSESSID=srmfm8pc7mt2n1gb2p6eadfpa0
Content-Length: 0


HTTP/1.1 200 OK
```

```
Date: Tue, 22 Aug 2023 11:04:28 GMT
Server: Apache
X-XSS-Protection: 1;  mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin
Referrer-Policy: no-referrer
Last-Modified: Mon, 21 Aug 2023 08:29:13 GMT
Accept-Ranges: bytes
Content-Length: 11023
Access-Control-Allow-Origin: *
Content-Type: application/javascript

...
```

I Email Address Pattern Found 1 TOC

Issue 1 of 1 TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://hwcs.tn.gov.in/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 e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Raw Test Response:

```
...

<p>These icons were originally made for Mosaic for X and have been
included in the NCSA httpd and Apache server distributions in the
past. They are in the public domain and may be freely included in any
application. The originals were done by Kevin Hughes (kevinh@kevcom.com).
Andy Polyakov tuned the icon colors and added few new images.</p>

<p>If you'd like to contribute additions to this set, contact the httpd
documentation project <a href="http://httpd.apache.org/docs-project/"
>http://httpd.apache.org/docs-project/</a>.</p>

<p>Almost all of these icons are 20x22 pixels in size.  There are
alternative icons in the "small" directory that are 16x16 in size,
provided by Mike Brown (mike@hyperreal.org).</p>
...
```