Web Application Security Testing of Training Management Portal

URL:

https://trainingonline.gov.in/demo/

April, 30 2025

AAA Technologies Ltd

278-280, F Wing, Solaris-1,
Saki Vihar Road, Opp. L & T Gate No. 6,
Powai, Andheri (East),
Mumbai 400 072, INDIA
Tel: + 91 22 28573815 / 16
Fax: + 91 22 40152501
info@aaatechnologies.co.in
www.aaatechnologies.co.in

AAA TECHNOLOGIES®
Accurate. Reliable. Innovative.

Web Application Security Test Report for Training Management Portal.

Document Reference

Item	Description
Document Title	Web Application Security Testing of Training Management Portal
Client	NIC
Report Number	1
Version No.	1.0
File Name	Training Management Portal
Type	Pdf Document
Status	Level-1 Report

Document Control Status

Change No.	Date	Prepared by
1.0	30/04/2025	Vikas Sharma

Web Application Security Test Report for Training Management Portal.

Table of Contents

sfsfsfs

Web Application Security Test Report for
Training Management Portal.

HIGH

Web Application Security Test Report for Training Management Portal.

1. Mobile No. And Email Travel In Response

Vulnerability Title: Mobile No. And Email Travel In Response	
Risk	**High**
Abstract	The Mobile No. And Email passed in clear text. It is possible for a malicious user to sniff into the network and access the application and sensitive information.
Impact	An attacker may be able to Sniff the Mobile No. And Email and sensitive information
Recommendations	It is recommended to implement the hashing technique/algorithm used at application. Mobile No. And Email, Password should be encrypted every time while being transmitted over the network. The solution is to implement: a) Salted SHA-512 technique in, authentication or login module b) SHA-512 hash technique in, change password and reset password Modules. The pre-requisite to this is that the backend database stores a SHA-512 hash of the password. (SHA-512hash is a cryptographic technique in which the actual value can never be recovered). Here is how the salted SHA-512technique works: When a client requests for the login page, the server generates a random number, the salt, and sends it to the client along with the page. A JavaScript code on the client computes the SHA-512 hash of the password entered by the user. It then concatenates the salt to the hash and re-computes the SHA-512hash. This result is then sent to the server. The server picks the hash of the password from its database, concatenates the salt and computes the SHA-512hash. If the user entered the correct password these two hashes should match. The server compares the two and if they match, the user is authenticated.
Snapshot	

```
POST /demo/updateManageUserProfileForm.html HTTP/1.1
Host: trainingonline.gov.in
Cookie: JSESSIONID=865A8AFF8DF9D4CDAB862E8B8A5BED84; acopendivids=jason,kelly,michael,cat; acgroupswithpersist=nada
Content-Length: 212
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="125", "Not.A/Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://trainingonline.gov.in
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://trainingonline.gov.in/demo/manageUserProfileForm.html?OWASP_CSRFTOKEN=Z74Q-W8OB-0OLG-JNDW-YUEN-4GWL-NSKC-J8ZY
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: keep-alive

OWASP_CSRFTOKEN=[redacted]&officialNameLocal=Sunita+Jain&gender=36
dob=01%2F01%2F19[redacted]&emailId=jain.sunita%40nic.in&mobileNumber=9891721391&Submit=
```

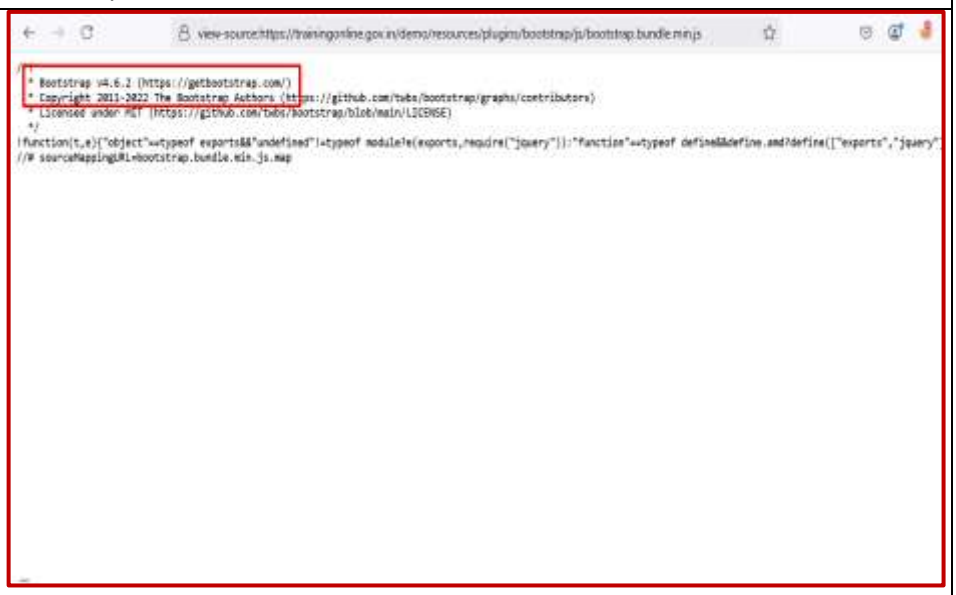
Web Application Security Test Report for Training Management Portal.

	 
Affected URLs	**Throughout The Application**

Web Application Security Test Report for
Training Management Portal.

Medium

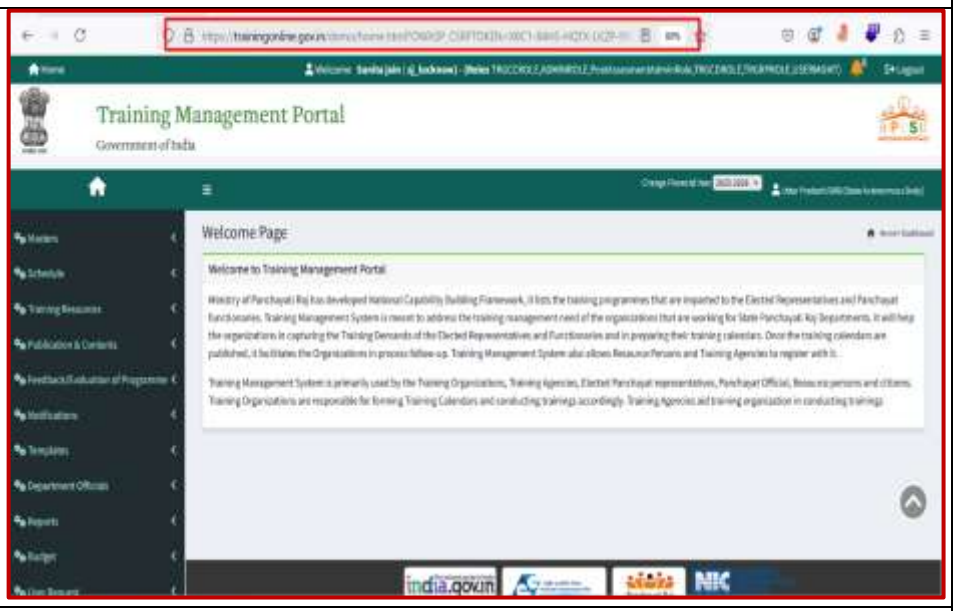
2. Old version of Bootstrap

Vulnerability Title: Old Version Of Bootstrap Is Used In The Application	
Risk	**Medium**
Abstract	Vulnerable version of bootstrap is used in the application.
Ease of Exploitation	Easy
Impact	Vulnerable version of bootstrap used in the application. Affected versions of this package are vulnerable to Cross-site Scripting (XSS) via the tooltip, collapse and scroll spy plugins.
Recommendations	It is recommended that application should use latest/Stable version of bootstrap.
Snapshot	
Affected Site	Throughout The Application

3. Old version of jQuery Migrate

Vulnerability Title: Old Version Of jQuery Migrate	
Risk	**Medium**
Abstract	It was observed that target web site is using jQuery Migrate and detected that it is out of date.
CWE	CWE_209
Ease of Exploitation	Easy
Impact	Since this is an old version of the software, it may be vulnerable to attacks
Recommendations	It is recommended to update to latest version of jQuery Migrate.
Snapshot	
Affected Site	**Throughout The Application**

4. Data travel in URL

Vulnerability Title: Data travel in URL	
Risk	**High**
Abstract	The details between server and client is passed in clear text. It is possible for a malicious user to sniff into the network still the authenticated detail.
Ease of Exploitation	Medium
Impact	An attacker may be able to Sniff the information of the department and may be change the original data.
Recommendations	Sensitive data should be used as per the UIDAI guidelines.
Snapshot	
Affected URLs	**Throughout The Application**

5. Vulnerable version of DataTables

Vulnerability Title: Vulnerable version of DataTables is used in the application	
Risk	**Low**
Abstract	It was observed that this Application is using an older version of DataTables.
Ease of Exploitation	Medium
Impact	DataTables for jQuery Affected versions of this package are vulnerable to Cross-site Scripting (XSS). If an array is passed to the HTML escape entities function it would not have its contents escaped.
Recommendations	It is recommended to update to latest version of DataTables.
Snapshot	
Affected Site	**Throughout The Application**

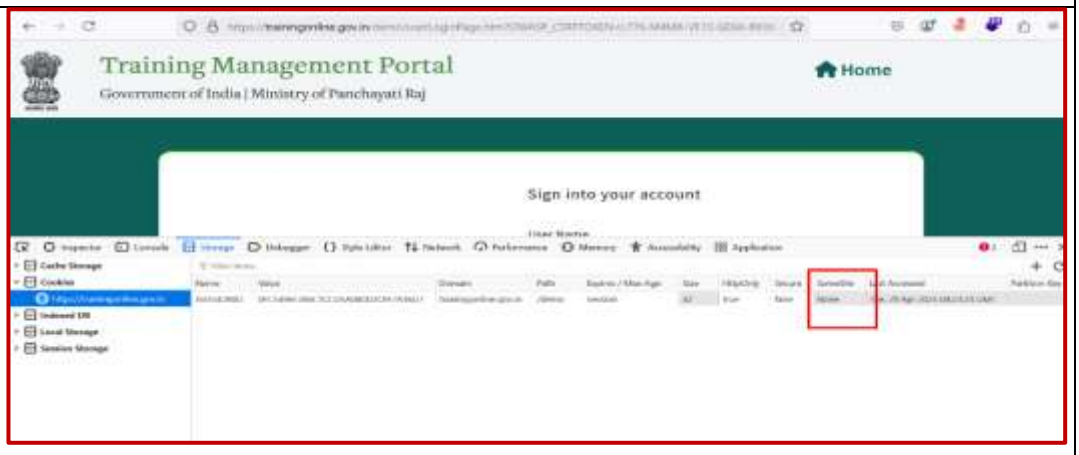
6. Cross-Origin Resource Sharing

Vulnerability Title: Cross-Origin resource sharing misconfiguration	
Vulnerability Title:	Cross Origin Resource Sharing i.e., CORS misconfiguration
Risk	Medium
Abstract	It was observed that the CORS Cross Origin Resource Sharing Misconfiguration | Lead to sensitive information.
Ease of Exploitation	Hard
Impact	Attacker would treat many victims to visit attacker's website, if victim is logged in, then his personal information is recorded in attacker's server.
Recommendations	Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.
Snapshot	
Affected URLs	**Throughout the application**

7. Weak Hash algorithm is used

Vulnerability Title: Weak Hash algorithm is used	
Risk	**Medium**
Abstract	It was observed that weak algorithm is used in the application
Ease of Exploitation	Easy
Impact	An attacker can construct forged data in a variety of forms that will cause software using the MD5 algorithm to incorrectly identify it as trustworthy.MD5 is vulnerable to Collision Attacks in which the Hashing algorithm takes two different inputs and produce the same hash function.
Recommendations	It is recommended to use SHA-256 for more secured application.
Snapshot	
Affected URLs	**Throughout The Application**

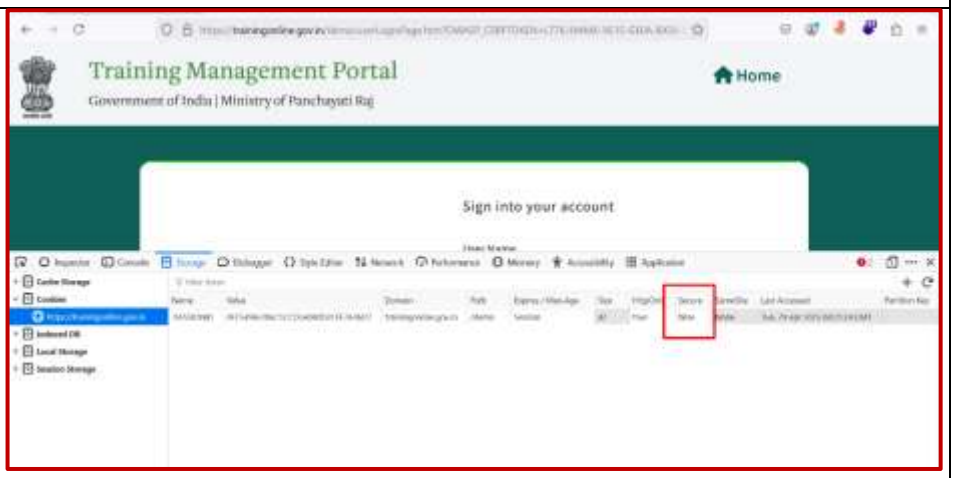
8. Cookie Without Same Site Attribute

Vulnerability Title: Session Cookie without Same Site Attribute	
Risk	**Medium**
Abstract	It is observed that cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request.
Ease of Exploitation	Easy
Impact	Without the **SameSite** flag, the application may be **vulnerable** to cross site request forgery (CSRF) and cross origin information leakage attacks since the browser will send **cookies** across origins. An attacker can use these attacks to trick a user into performing an action or into leaking sensitive data.
Recommendations	The server can set a same-site cookie by adding the SameSite=... attribute tothe Set-Cookie header. There are three possible values for the SameSite attribute: • Lax: In this mode, the cookie will only be sent with a top-level get request. **Set-Cookie: key=value; SameSite=Lax** • Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website. **Set-Cookie: key=value; SameSite=Strict** • None: In this mode, the cookie will be sent with the cross-site requests. Cookies with SameSite=None must also specify the Secureattribute to transfer them via a secure context. Setting a SameSite=None cookie without the Secure attribute will be rejectedby the browsers. **Set-Cookie: key=value; SameSite=None; Secure**
Snapshot	
Affected Site	**Throughout The Application**

Web Application Security Test Report for
Training Management Portal.

Low

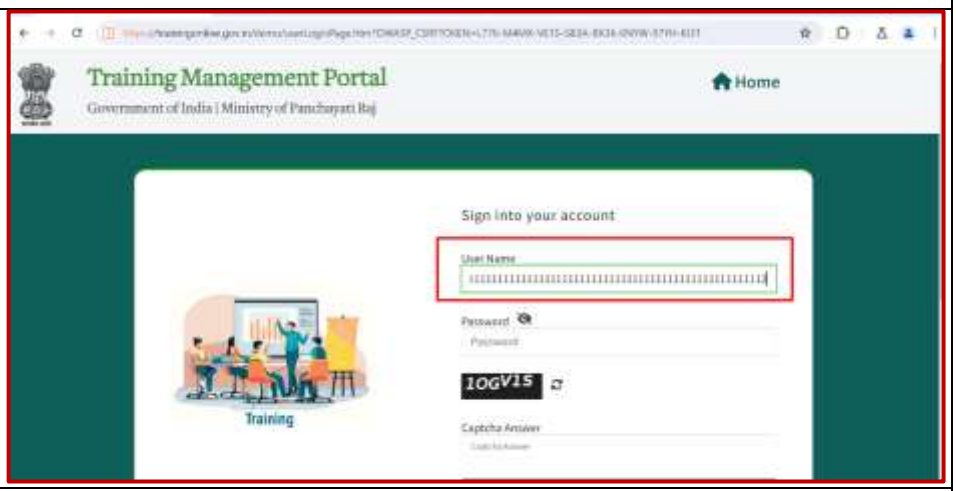
9. Session Cookie without Secure Flag

Vulnerability Title: Session Cookie without Secure Flag	
Risk	**Low**
Abstract	It was observed that Session Cookie did not have Secure Flag Set.
CWE	CWE_614
Ease of Exploitation	Easy
Impact	This session cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.
Recommendations	It is recommended to set the Secure flag for this cookie.
Snapshot	
Affected Site	**Throughout The Application**

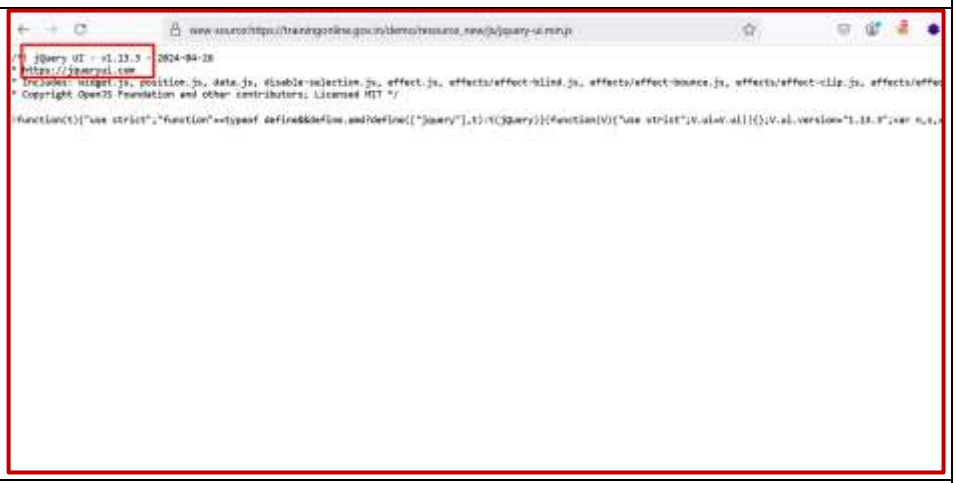
10. HTTP Security Headers Not Implemented

Vulnerability Title: HTTP Security Headers Not Implemented	
Risk	**Low**
Abstract	It was observed that security headers such as Referrer Policy is not implemented in remote application.
CWE	CWE_644
Ease of Exploitation	Medium
Impact	If security headers are not implemented in application, then it may help an attacker to exploit existing vulnerabilities in application logic and results in lack of defense in depth approach to prevent security attacks.
Recommendations	It is recommended to implement security headers to provide additional layer of security in application such as X-XSS protection, Content Security Policy, Strict Transport security policy, X-Content-Type-Options and Referrer Policy.
Snapshot	
Affected Site	Throughout The Application

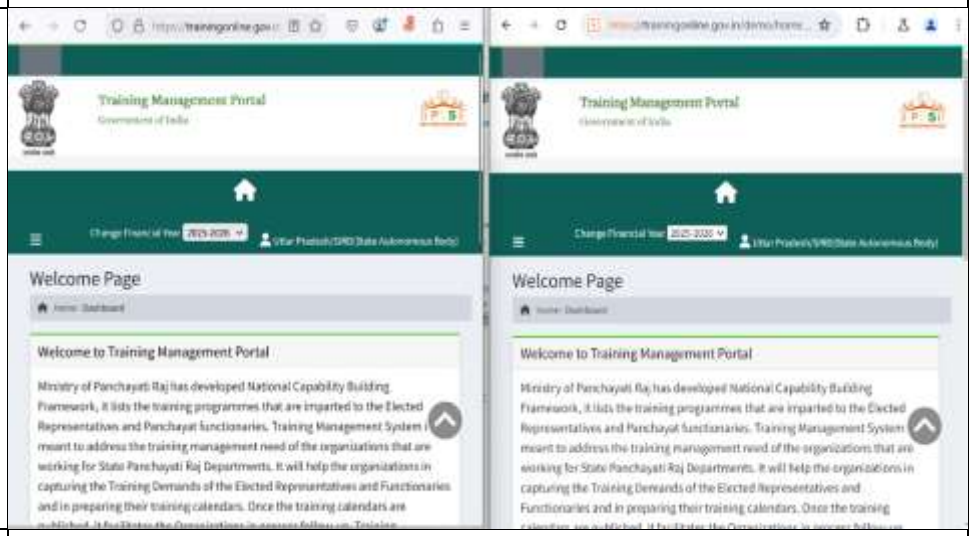
11. Max. Length For Input Fields Is Not Defined Called Buffer Overflow.

Vulnerability Title: Buffer Overflow	
Risk	**Low**
Abstract	It was observed that max. Length for captcha fields is not defined.
Ease of Exploitation	Easy
Impact	This vulnerability can cause a system crash or, worse, create an entry point for a cyberattack.
Recommendations	Length restrictions for every input field should be defined at client as well as at server end.
Snapshot	
Affected Site	**Throught The Application**

12. Vulnerable version of jQuery UI

Vulnerability Title: Vulnerable version of jQuery UI is used in the application	
Risk	**Low**
Abstract	It was observed that this page is using an older version of jQuery UI that is vulnerable to a Cross Site Scripting vulnerability
Ease of Exploitation	Medium
Impact	Affected versions of this package are vulnerable to Cross-site Scripting (XSS) via the initialization of check-box-radio widget on an input tag enclosed within a label, which leads to the parent label contents being considered as the input label
Recommendations	It is recommended to update to latest version of jQuery UI.
Snapshot	
Affected Site	**Throughout The Application**

13. Multiple Browser Login of Admin at the same time

Vulnerability Title: Multiple Browser Login of Admin at the same time	
Risk	**Low**
Abstract	It is observed that the same user can login into via multiple browsers.
CWE	CWE-362
Ease of Exploitation	Medium
Impact	The attacker can use the same login ID for exploitation even if the ID is active.
Recommendations	It is recommended to restrict multiple browser login for admin at the same time.
Snapshot	
Affected Site	Throughout The Application