# 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







#### **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
Туре	Pdf Document
Status	Level-1 Report

#### **Document Control Status**

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



#### **Table of Contents**

1. Mobile No. And Email Travel In Response	5
2. Old version of Bootstrap	8
3. Old version of jQuery Migrate	9
4. Data travel in URL	10
5. Vulnerable version of DataTables	11
6. Cross-Origin Resource Sharing	12
7. Weak Hash algorithm is used	13
8. Cookie Without Same Site Attribute	14
9. Session Cookie without Secure Flag	16
10. HTTP Security Headers Not Implemented	17
11. Max. Length For Input Fields Is Not Defined Called Buffer Overflow.	
12. Vulnerable version of jQuery UIsfsfsfs	19
13. Multiple Browser Login of Admin at the same time	20



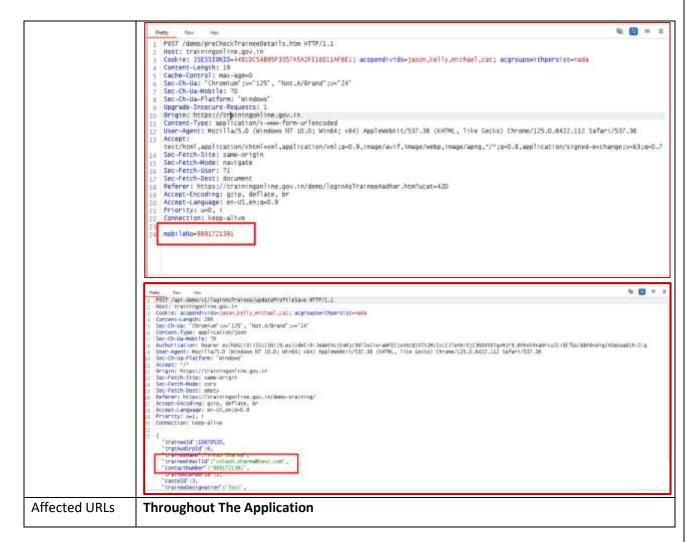
## HIGH



#### 1. Mobile No. And Email Travel In Response

Vulnerability Ti	tle: 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
Recommendat	It is recommended to implement the hashing technique/algorithm used at
ions	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	Posty Nor No. No. No. 1 POST /demo/updateManageUserProfileForm.html HTTP/1/1
	2 Most: trainingonline.gov.in Cookie: JSESSIGNID-865AZAFFRDF904CDAB96SEB8EASBED84; acopendivids=jason,kelly,michael,cat; acgroupswithpersist=nada & Content-Length; 212
	<pre>5 Cache-Control: max-age=0 6 Sec-Ch-Us-Mobile: 70 5 Sec-Ch-Us-Mobile: 70</pre>
	<pre>Sec_Ch_Ua-Flatform: "Windows" Usgrade_Insecurs-Requests: 1 0 0 right https://raniningonline.gov.in</pre>
	11 Content-Type: application/x-www-form-unlencoded 1) User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) ApploWebKit/537.36 (WMTML, like Gatko) Chromw/125.0.6422.112 Safari/537.36
	13 Accept:  text/html.application/whosi+wml.application/wml;q=0.8,image/avif.image/eabp.image/apng."/";q=0.8,application/signed-exchange;v=b3;q=0.7 14 Sec-Fetch-Site: name-origin
	13 Sec-Fatch-Mode: mavigate 16 Sec-Fatch-Dest: document 17 Sec-Fatch-Dest: document
	16 Referer: https://crainingonline.gov.in/demo/manageUserFrofileForm.html?OWASF_CSRFTOKEN=Z74Q-W608-00LC-JROW-VEH-4CWL-NSKC-J820 16 Accept-Emoding: grip, defiate, br 26 Accept-Language: en-US.gn:g=-0.9
	21 Priority: u=0, t 22 Connection: keep-alive
	23 GWASF_CSRFTGKU: 144-W00 40L6 W0W WD1-40a NSW 302-Modele SEVELANGE CONTRACT CONTRA







# 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	**Bootstrap va.6.2 (https://getbootstrap.com/) **Bootstrap va.6.2 (https://getbootstrap.com/) **Easyright 2011-2022 The Bootstrap Eachers (time://github.com/twbs/bootstrap/graphs/coetributors) **ISome wide "If https://github.com/twbs/bootstrap/graphs/coetributors) **ISome wide "If https://github.com/twbs/bootstrap/graphs/coetributors) **Joint Coeffect varypeof exports&fundefined*/utypeof modulate(exports, "equire("jouery")): "function" utypeof define@define.and?define(("exports", "jouery")/# sourceMappingEM.nbootstrap.bundle.wis.js.map	
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	Training Management Portal  Government of tatu  Training Management Portal  Government of tatu	
	Welcome Page  Welcome (Page)  Welcome to Training Management Portal  Welcome (Page)  Welcome (	
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	## C B view-southintspecificaling gov in termination of the content of the conten	
Affected Site	Throughout The Application	



#### **6. Cross-Origin Resource Sharing**

Vulnerability Title: 0	Cross-Origin resource sharing miscon	figuration
Vulnerability Title:	Cross Origin Resource Sharing i.e., C	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 is logged in, then his personal information server.	,
Recommendations	Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.	
Snapshot	Request	Arquise
	Amount of the Teach of the William STEP/1.1  Past Transmapoline.gov.in  Coder: ISSISTAND-60040000000000000000000000000000000000	i MTTP/1.1 DOS  Set-Cockie: J05531MNP-10013160958710048385460317 AP; #trp8mly Cache-Control: J05531MNP-10013160958710048385460317 AP; #trp8mly Cache-Control: J0-50078, #u-cathe, #unt-reval/date, #un-uge-O, pott-check-O, pre-t-deck-O Espires: Thu, OI law 1870 CO:00100 OH  #cock-Control Allow-Pright: J1871 #CC013-CONTrol Allow-Pright: J1871 #CC013-CONTrol Allow-Pright: J1871 #Accest-Control Allow-Pright: J1871 #Accest-Control Allow-Pright: BMD #A
Affected URLs	Throughout the application	



#### 7. Weak Hash algorithm is used

Medium
It was observed that weak algorithm is used in the application
Easy
An attacker can construct forged data in a variety of forms that will cause software usin the MD5 algorithm to incorrectly identify it as trustworthy.MD5 is vulnerable to Collisio Attacks in which the Hashing algorithm takes two different inputs and produce the same hash function.
It is recommended to use SHA-256 for more secured application.
Post /demo/userLoginPage.htm HTTP/I.1  Wost: crainingonline.gov.in Cookie: JSESSIGNID=&CD0480D70072C28062835A62A3EF18 acopendivide=jason,kelly,michael.cat; acgroupswithpersist=nada Content-Length: 183 Cache-Control: max-age-0 Sec-Ch-Uar-Neronium*; v="105", "Not.A/Brans"; v="24" Sec-Ch-Uar-Neronium*; v="25", "Not.A/Brans"; v="25",



#### 8. Cookie Without Same Site Attribute

Vulnerability 1	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	Easy
Exploitation Impact	Without the <b>SameSite</b> flag, the application may be <b>vulnerable</b> to cross site request forgery (CSRF) and cross origin information leakage attacks since the browser will send <b>cookies</b> across origins. An attacker can use these attacks to trick a user into performing an action or into leaking sensitive data.
Recommendat	The server can set a same-site cookie by adding the SameSite= attribute to the 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 rejected by the browsers.  Set-Cookie: key=value; SameSite=None; Secure
Snapshot	Training Management Portal  Groverrunters of India   Ministry of Panchayati Raj  Sign into your account    Sign into your account
Affected Site	Throughout The Application



# 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	Training Management Portal  Government of India   Ministry of Panchayati Raj	
	Sign into your account    Companies   Commander   Comm	
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	Section of Teaching and Teach	N. CO. Ser 1970-00300-0007  Cable  Tyll-41 (no-dright: "  Tyll-41 (n	
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	Training Management Portal  Greenment of India i Ministry of Panchoyatt Raj  Sign Into your account  User Name  Financial  Financial  Financial  Financial  Financial  Capture Answer  Capture Answer  Capture Answer  Capture Answer  Capture Answer  Capture Answer		
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	### C A new autocitiqui/transpoints gounderects autoc new[a]guary-armsup    joury UT = v1.3.5     interpolity committee   variable   variable	
Affected Site	Throughout The Application	



#### 13. Multiple Browser Login of Admin at the same time

vullerability fitte: wi	ultiple 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	Training Management Portal Communicated Table	Training Management Portal  Charge and Charles  Training Management Portal  Charles and Charles and Charles  Training Management Portal  Charles and Cha	
	Welcome Page  Welcome to Training Management Portal  Minorty of Ponchayati Ital itas developed National Capability Building, Pransversi, it lists the training programmes that are imparted to the Elected Representatives and Penchayati functionaries. Training Management System is ment to address the training management need of the regenizations that are sensing for Stan Panchayati Rip Departments. It will help the organizations in Capituring the Training Demands of the Elected Representatives and Functionaries.	Welcome Page    Interference   Inter	
Affected Site	and in preparing their training calendars. Once the training calendars are  Functionaries and in preparing their training calendars. Once the training Throughout The Application		