सत्यमेव जयते

Web Application Security Test Report

Product: NAAC-Online Assessment and Accreditation Process

National Assessment and Accreditation Council (NAAC)

(Report No: ITBg/WAS(TR)-1/14980722)

Dated: 25-07-2022

STQC, IT Services
Ministry of Electronics and Information Technology
ETDC, 100 Feet Road, Peenya Industrial Estate,
Bangalore 560058
(TEL: 080 23893519; FAX: 080 23722314)
E-mail: itbangalore@stqc.gov.in
Web: www.stqc.gov.in

Disclaimer

1. This Report is the record of results of testing/audit pertaining to the particular software/system tested/audited by laboratory and do not apply to any other software/system even though declared to be identical. Also, this should not be considered as approval for the software/system

2. This Report shall not be reproduced, except in full, unless written permission for the publication of an approved abstract has been obtained from the Director, ETDC Bangalore

3. Results reported, in this test report are valid at the time of and under the static condition of testing.

4. STQC IT Services, ETDC Bangalore shall not be liable for any change in the test/ audit observations/ misuse of the report.

5. This Test /audit Report is not to be used for any legal purpose and shall not be produced in court of law.

6. In case of any dispute, the decision of the Director, ETDC Bangalore shall be final and binding.

7. In general, proprietary Information submitted by customer to the laboratory may not be provided to any third party without the consent of customer, unless until the competent authority is satisfied that the larger public interest warrants the disclosure, or it warrants as per the statutory/regulatory requirements.

Table of Contents

1. Client Details		
1.1	**Name of the Client**	M/s National Assessment and Accreditation Council (NAAC)
1.2	**Address of the Client**	National Assessment and Accreditation Council (NAAC), P.B. No. 1075, Nagarbhavi, Bengaluru, Karnataka-560072
2. Description of the Software Product		
2.1	**Software Product Nomenclature**	NAAC- Online Assessment and Accreditation Process
2.2	**Version No.**	27.2
2.3	**Date of Release**	13-May-2022
2.4	**Software Product Description**	NAAC- Online Assessment and Accreditation Process tool
2.5	**Applicable Specification**	OWASP Top 10 Application Security Risks – 2017
2.6	**Name & Address of the Software Product Developing Organization**	Kerala State Electronics Development Corporation, Keltron House, Vellayambalam, Trivandrum, Kerala- 695035
2.7	**Supplied Media**	**Following Test URLs were provided for Testing** http://218.248.45.210/naacfeb7/public/index.php http://218.248.45.210/naacfeb7/public/index.php/hei http://218.248.45.210/naacfeb7/public/index.php/dvv http://218.248.45.210/naacfeb7/public/index.php/assessor http://218.248.45.210/naacfeb7/public/index.php/inflib
2.8	**Documents Submitted**	None
2.9	**Date of Receipt of Product**	06-06-2022
3. Description of Test		
3.1	**Name & Address of the Testing Organization**	STQC IT Services, ETDC, STQC Directorate, Ministry of Electronics and Information Technology, Bangalore, 560058
3.2	**Location of Testing**	STQC IT Services, ETDC, STQC Directorate, Ministry of Electronics and Information Technology, Bangalore, 560058
3.3	**Scope of Testing**	• The security testing is performed as per *OWASP Top 10 Application Security Risks – 2017*. • *Black box testing* method to be used to detect security vulnerabilities in the application. • The scope does not cover security testing of system hardware,

		system software (OS/Utilities), third party software, network components & accessories, deployment environment, captchas or any other human verification systems, OTP generation and verification, digital signature verification, PKI components (encryption and decryption) etc.
3.4	**Test Methodologies**	**Application Security** The Application was scanned as per Test Procedure EP-01-WAS using scanning tool Micro Focus WebInspect (version 21.2.0.117) and Manual testing is performed by Burp Suite (version 2022.1.1).
3.5	**Test Start Date**	**1st Round**- 18-02-2022 **2nd Round**- 06-06-2022
3.6	**Test Completion Date**	**1st Round**- 06-04-2022 **2nd Round**-14-07-2022
3.7	**Standards for Testing**	• *OWASP Top Ten 2017* – The Ten Most Critical Web Application Security Risks. • The Testing activities (test planning, test case designing, testing procedure, defect reporting, test reporting, etc.) are being carried out as per following standard: I. ISO/IEC/IEEE 29119 II. NIST-SP800-53 III. NIST-SP800-115
3.8	**Test Data**	• Static test data to cover all the critical workflows of the application was provided during orientation program by the client. • Dynamic test data was created by the scanning tools which explores/crawls the entire application for security risks.
3.9	**Test Environment**	The following hardware software items used to conduct test:
	Hardware Configurations	**Processor**: Intel® Xeon® CPU E5-2620 V4 @2.10GHz **HDD Capacity**: 353 GB **RAM**: 32 GB
	Software Configurations	**Operating System**: Ubuntu 20.04 **Web Server Name**: Apache **Web Server Version**: 2.4.18 **Database Server Name**: PostgreSQL **Database Server Version**: 9.5.19

4.0 Executive Summary

a. STQC IT Services, Bangalore carried out Application Security testing of NAAC-Online Assessment and Accreditation Process owned by National Assessment and Accreditation Council (NAAC), Bengaluru and developed by Kerala State Electronics Development Corporation. The objective of security testing was to fully examine the application to identify security vulnerabilities and check its compliance with OWASP Top 10 Application Security Risks – 2017.

b. Black Box security testing was carried out on test scenarios & test cases derived from the requirements of the application without any knowledge of the internals. The scope of testing was limited to only Web Application Security testing and did not include system hardware, system software (OS/Utilities), third party software, network components & accessories, deployment environment, captchas or any other human verification systems, OTP generation and verification, digital signature verification, PKI components (encryption and decryption) etc.

c. The security testing was performed for following roles which were hosted at following URLs:
   - **Super Admin**: http://218.248.45.210/naacfeb7/public/index.php
   - **HEI**: http://218.248.45.210/naacfeb7/public/index.php/hei
   - **DVV**: http://218.248.45.210/naacfeb7/public/index.php/dvv
   - **Assessor**: http://218.248.45.210/naacfeb7/public/index.php/assessor
   - **Inflibnet**: http://218.248.45.210/naacfeb7/public/index.php/inflib

   The URLs were provided by the Customer for remote access and to conduct testing

d. The first cycle of Security Testing was conducted from 18-02-2022 to 06-04-2022 and total 28 Anomalies were found, and their details were shared with the client vide *Application Security Anomaly Report: ITBg/WAS(AR)-1/14980522* dated *20.05.2022* for corrective action.

e. Client resubmitted the application after necessary corrective action to STQC IT Services Bangalore on *06.06.2022*. **The second round of security testing was performed from 06.06.2022 to 14.07.2022. It was found that 23 out of 28 reported vulnerabilities are satisfactorily closed. Business Justifications were provided for remaining 5 vulnerabilities (Sr. No. A3.1, A3.3, A3.5, A6.1 and A6.12). No new vulnerability was found in the final test cycle.**

f. Details of security vulnerabilities observed in the first cycle & their closure status after final cycle, Compliance against OWASP Top 10, 2017 and Recommendations for deployment of the Web site in production environment are given in the remaining report.

Following anomalies were detected and categorized as per OWASP 2017 Top 10 Security Risks under different severities.

Sl.no	Security Risk	Severity				Number of Security issues	
		Critical	High	Medium	Low	1st Cycle	2nd Cycle
A1	Injection	1	2	-	1	4	0
A2	Broken authentication	-	1	-	1	2	0
A3	Sensitive Data Exposure	-	2	1	2	5	0
A4	XML External Entities (XXE)	-	-	-	-	Nil	0
A5	Broken Access Control	-	-	-	-	Nil	0
A6	Security Misconfiguration	-	2	2	9	13	0
A7	Cross-Site Scripting (XSS)	1	1	2	-	4	0
A8	Insecure Deserialization	-	-	-	-	Nil	0
A9	Using Components with Known Vulnerabilities	-	-	-	-	Nil	0
A10	Insufficient Logging and Monitoring	-	-	-	-	Nil	0
Severity-wise Total		2	8	5	13	-	
		TOTAL				28	0

Anomaly classification by severity is as follows:

Critical: It can allow attackers to take complete control of the web applications and web servers.

High: Attackers can view information about the system that helps them find or exploit other vulnerabilities that enable them to take control of the website and access sensitive user and administrator information.

Low: These types of issues do not have any significant impact to application or servers.

Medium: By exploiting these security issues, attackers can access to information that helps them exploit other vulnerabilities, or better understand the system so they can refine their attacks.

5. Detailed Observations

S. No	Security Risk	Severity	Description of Security Risk	Resolution Comments by Customer	Closure Comments by STQC
A1- Injection					
A1.1	SQL Injection	Critical	Blind SQL Injection detected at following pages **Assessor:** Please refer Application Security Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report	Fixed	Closed
A1.2	Expression Language Injection	High	Expression Language Injection detected at following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php/admin/param/6/parameters	Fixed	Closed
A1.3	Expression Language Injection (HttpOnly Restriction Bypass)	High	Expression Language Injection (Httponly Restriction Bypass) detected at following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php/admin/param/6/parameters	Fixed	Closed
A1.4	Often Misused: File Upload	Low	File upload capability detected at following pages **Inflibnet**: http://218.248.45.210/naacfeb7/public/index.php/inflib/create-ticket	Fixed	Closed
A2-Broken Authentication					
A2.1	Password Management: Weak Password Policy	High	Weak Password Policy detected for following roles: **Inflibnet:** http://218.248.45.210/naacfeb7/public/index.php/inflib/login	Fixed	Closed
A2.2	Setting	Low	User Controllable Character Set	Fixed	Closed

	Manipulation: Character Set		vulnerability detected at following pages: **Inflibnet:** Please refer Application Security Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor:** Please refer Application Security Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report		
A3-Sensitive Data Exposure					
A3.1	Insecure Transport	High	Logins sent over Unencrypted Connection in following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php/admin/adminhome • http://218.248.45.210/naacfeb7/public/index.php **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/inflib **Assessor**: • http://218.248.45.210/naacfeb7/public/index.php/assessor **HEI:** http://218.248.45.210/naacfeb7/public/index.php/hei	**Business Justification**: SSL is enabled in production	Closed (Based on Justification)
A3.2	Credential Management: Sensitive Information Disclosure	High	Username or password detected at following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php/admin/adminhome **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv/dvvhome **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/inflib	Fixed	Closed

			• http://218.248.45.210/naacfeb7/public/index.php/inflib/inflibdashboard **Assessor:** • http://218.248.45.210/naacfeb7/public/index.php/assessor/assessorhome **HEI:** • http://218.248.45.210/naacfeb7/public/index.php/hei'		
A3.3	Cookie Security: Persistent Cookies	Medium	Persistent cookies detected at following pages **Superadmin:** Please refer Application Security Tool Report for Superadmin role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **DVV:** Please refer Application Security Tool Report for DVV role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Inflibnet:** Please refer Application Security Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor**: Please refer Application Security Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **HEI:** Please refer Application Security Tool Report for HEI role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report	**Business Justification:** This issue is addressed in Production	Closed (Based on Justification)
A3.4	System Information Leak: Internal IP	Low	Internal IP Disclosure in following pages **Superadmin:** Please refer Application Security Tool Report for Superadmin role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv/dvvhome • http://218.248.45.210/naacfeb7/public	Fixed	Closed

			/index.php/dvv • http://218.248.45.210/naacfeb7/public/index.php/hei/ssr_reports/eyJpdiI6InNkaUNUNGl0a3JsK3ZIbndJVVwvb1BBPT0iLCJ2YWx1ZSI6InUweFlVQ0hjMlEzZU8rSkZ0bU4yUXc9PSIsIm1hYyI6IjI0ZWZhYWI1YzIwNTQ4MGIwZGU5OGUyYjAwMmUzYThiMzU3NzVkMTk0ZmE4NGY3YzEzMGMyNzRkZjY1NmQxNmEifQ==/edit **Inflibnet:** Please refer Application Security Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor:** • http://218.248.45.210/naacfeb7/public/index.php/assessor/training/javascript(0) • http://218.248.45.210/naacfeb7/public/index.php/assessor • http://218.248.45.210/naacfeb7/public/index.php/assessor/assessorhome **HEI:** • http://218.248.45.210/naacfeb7/public/index.php/hei/heihome		
A3.5	Cookie Security: HTTPOnly not set	Low	HTTPOnly attribute not set for cookies in following pages **Superadmin**: Please refer Application Security Tool Report for Superadmin role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **DVV:** Please refer Application Security Tool Report for DVV role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Inflibnet:** Please refer Application Security Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor:** Please refer Application Security	**Business Justification:** This issue is addressed in Production	Closed (Based on Justification)

			Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **HEI:** Please refer Application Security Tool Report for HEI role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report		
A4-XML External Entities (XXE)					
A5-Broken Access Control					
--	--	--	--		
A6-Security Misconfiguration					
A6.1	Often Misused: Login	High	Unencrypted login forms in following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php/admin/adminhome • http://218.248.45.210/naacfeb7/public/index.php **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/inflib **Assessor**: • http://218.248.45.210/naacfeb7/public/index.php/assessor **HEI:** http://218.248.45.210/naacfeb7/public/index.php/hei	**Business Justification**: SSL is enabled in production	Closed (Based on Justification)
A6.2	Web Server Misconfiguration: Unprotected File	High	PHP source code disclosure detected at following pages **DVV:** http://218.248.45.210/naacfeb7/public/index.php/dvv/assign_job	Fixed	Closed
A6.3	JavaScript Hijacking:	Medium	JavaScirpt Hijacking detected at following pages:	Fixed	Closed

	JSONP		**Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php/_debugbar/open?op=get&id=9a58da3bf76f6db92b423267c0510194 **Assessor**: http://218.248.45.210/naacfeb7/public/index.php/assessor/training/displayTrainings		
A6.4	HTML5: Overly Permissive Message Posting Policy	Medium	PostMessage Broadcast Vulnerability detected in following function **Superadmin**: function: Window.postMessage • http://218.248.45.210/naacfeb7/public/index.php/logistics/Viewvisit/eyJpdiI6InY1cGpHZUZLbHdKSGdzd1wvRlRBejdRPT0iLCJ2YWx1ZSI6IllFdVVqdGpBbnlVcjJheFUrNldtNkE9PSIsIm1hYyI6IjgxZGM0ZDk5MzY3YjBhYTFkZmQ4YmYzOTE1YjJmZTM1MGUxNTg2MmFlZWRhOGI4Y2IwNTFmNzQzNGRhNmFhODM • http://218.248.45.210/naacfeb7/public/index.php/hei/ssr_reports/eyJpdiI6IkxGZmxKM3ZBcEFDcU9jNXczYUtsR2c9PSIsInZhbHVlIjoidGErSFwvam1pT1RSeGZ4aXhWYUtwK1E9PSIsIm1hYyI6IjIyNjFhZGI3MjE0MzYzMGYyZDQzYmZlMTgxYTM3NWI0YzFmMmM5YjY1ZmEyOWYxZDM5M2E0MWNjZTg3ZDgwNGMifQ= • http://218.248.45.210/naacfeb7/public/index.php/hei/ssr_reports/eyJpdiI6IkxGZmxKM3ZBcEFDcU9jNXczYUtsR2c9PSIsInZhbHVlIjoidGErSFwvam1pT1RSeGZ4aXhWYUtwK1E9PSIsIm1hYyI6IjIyNjFhZGI3MjE0MzYzMGYyZDQzYmZlMTgxYTM3NWI0YzFmMmM5YjY1ZmEyOWYxZDM5M2E0MWNjZTg3ZDgwNGMifQ= **DVV: function:Window.postMessage** • http://218.248.45.210/naacfeb7/public/index.php/dvv/create-ticket **Assessor: function:Window.postMessage** • http://218.248.45.210/naacfeb7/public/index.php/assessor/returnheiname	Fixed	Closed

			• http://218.248.45.210/naacfeb7/public/index.php/assessor/returnheiname • http://218.248.45.210/naacfeb7/public/index.php/assessor/training **HEI: function:Window.postMessage** Please refer Application Security Tool Report for HEI role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report		
A6.5	HTML5: Cross-Site Scripting Protection	Low	Missing Cross-Site scripting protection for all the roles **Superadmin:** • http://218.248.45.210/naacfeb7/public/index.php **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/inflib **Assessor**: • http://218.248.45.210/naacfeb7/public/index.php/assessor **HEI:** http://218.248.45.210/naacfeb7/public/index.php/hei	Fixed	Closed
A6.6	Poor Error Handling: Unhandled Exception	Low	Unhandled Exceptions detected at following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php/hei/preview_university/eyJpdiI6ImJGazFLbXk3VUt0QmNqU0ZScVBqS1E9PSIsInZhbHVlIjoibjBBOWxzWmxvemFZMEJ6eHN1ZVNRdz09IiwibWFjIjoiNzY4NjQzMTI0MGJkOWJkMDU4ZjQ3YTE0ZDBmNzQyYjY5NTM1MWU5YjUxMDc4MDZkYTM1M2IyZWFmNGJlZGM2ZCJ9 • http://218.248.45.210/naacfeb7/public/index.php/_debugbar/open?op=get&id=eaa3f73decc07fb30842d0fe4a1a576e • http://218.248.45.210/naacfeb7/public/index.php/hei/preview_university/eyJ	Fixed	Closed

			pdiI6IkNjSm1UUm14MFFiK3liK2RNdndHUnc9PSIsInZhbHVlIjoiV3NmMzJYOGxockRuK3oyNWlBMVFrQT09IiwibWFjIjoiOTI3NDU1MzYyNDVmYjQyNjlmZjY0MmE0ZjM1NzYyMTVmZjVkNDQ4ZmQ1OGU1NWNjM2VhZTExNjUwNjQ1ZWFhYiJ9 **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/_debugbar/open?op=get&id=ccf9bed810c8e69332dc4514c7a8facc • http://218.248.45.210/naacfeb7/public/index.php/_debugbar/open?op=get&id=afaf05de36a9b1db6b8e76db94d707ab **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/_debugbar/open?op=get&id=d0179ad5daab15203f3e83203e294251 **Assessor:** • http://218.248.45.210/naacfeb7/public/index.php/assessor/training/javascript(0) http://218.248.45.210/naacfeb7/public/index.php/_debugbar/open?op=get&id=c92d720c74386371637a46179e7efcdd		
A6.7	Cookie Security: Missing SameSite Attribute	Low	Missing SameSite attribute in cookies set in following pages: **Superadmin**: Please refer Application Security Tool Report for Superadmin role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **DVV:** Please refer Application Security Tool Report for DVV role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Inflibnet:** Please refer Application Security Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor:** Please refer Application Security	Fixed	Closed

			Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **HEI:** Please refer Application Security Tool Report for HEI role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report		
A6.8	Cache Management: Web Cache Poisoning	Low	Web Cache Poisoning vulnerability detected in following URLs **Superadmin**: Please refer Application Security Tool Report for Superadmin role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv/dvv_validation/593?criteria_id=19&assessment_id=7457&job_id=4931&cacheBuster=WEBINSPECT1824514838 • http://218.248.45.210/naacfeb7/public/index.php/dvv/view_clarification/create?metrics_id=18679&jobid=4861&cacheBuster=WEBINSPECT2005796355 **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/inflib/inflibdashboard/2/edit **Assessor:** Please refer Application Security Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **HEI:** Please refer Application Security Tool Report for HEI role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report	Fixed	Closed
A6.9	Web Server Misconfiguration:	Low	Environmental variables were disclosed in many pages **Superadmin**: Please refer Application Security Tool Report for Superadmin role for complete list of pages with the	Fixed	Closed

	Unprotected File		vulnerability as the list is very long to be accommodated in the report **DVV:** Please refer Application Security Tool Report for DVV role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Inflibnet:** Please refer Application Security Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor**: Please refer Application Security Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report		
A6.10	Web Server Misconfiguration: Unprotected File	Low	Common documentation text files at following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/bower_components/admin-lte/plugins/jQueryUI/jquery-ui/LICENSE.txt **Assessor:** • http://218.248.45.210/naacfeb7/public/bower_components/admin-lte/plugins/jQueryUI/jquery-ui/LICENSE.txt **HEI:** http://218.248.45.210/naacfeb7/public/bower_components/admin-lte/plugins/jQueryUI/jquery-ui/LICENSE.txt	Fixed	Closed
A6.11	System Information Leak: External	Low	System Information are being leaked in following pages **Superadmin**: http://218.248.45.210/naacfeb7/public/js/jquery.treeview.js	Fixed	Closed
A6.12	Web Server Misconfiguration:	Low	Internal Server Error is displayed for following pages **Superadmin**: Please refer Application Security Tool Report for Superadmin role for complete list of pages with the	**Business Justification**: it is due to the laravel version and php	Closed (Based on Justification)

	Server Error Message		vulnerability as the list is very long to be accommodated in the report **DVV:** Please refer Application Security Tool Report for DVV role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Inflibnet:** Please refer Application Security Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor**: Please refer Application Security Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **HEI:** Please refer Application Security Tool Report for HEI role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report	version specific. The production server system is already installed with a newer version, so this issue is already solved in production.	
A6.13	Web Server Misconfiguration: Insecure Content-Type Setting	Low	Browser Mime Sniffing is not disabled in following pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/inflib **Assessor:** • http://218.248.45.210/naacfeb7/public/index.php/assessor **HEI:** • http://218.248.45.210/naacfeb7/public/index.php/hei	Fixed	Closed
A7-Cross-site Scripting (XSS)					
A7.1	Cross-Site Scripting: Reflected	Critical	Reflected Cross-Site Scripting detected at following pages **Inflibnet:** • http://218.248.45.210/naacfeb7/public	Fixed	Closed

			/index.php/inflib/inflibnethome/eyJpdiI6Ik9NQlBFelpEVm1JdlVWZkNIanNSYUE9PSIsInZhbHVlIjoiVkxjNTcxYVNTM2xSYUpvcFVDWlwvc2c9PSIsIm1hYyI6IjMwMzA0Y2NiMTQ5ZGJhYTYwN2EzMDdjZGMzMDRmNmExMzliNzIyYWU2YzVhNTRjNmYyZTI5ZTJkMzgwYjIzMGIifQ==/eyJpdiI6ImlNZURjRVJuSTJ2ckNjcmorbG5kU1E9PSIsInZhbHVlIjoibWlVVVJYRGkzSXgxNnMxaFVKTW1KUT09IiwibWFjIjoiOWI5ZmRkYjEyODIxYzA3NWYxMDAxNDBkNmQxMTk1ZDViOTNjNDIwZTI2ZWYxZGQ2MGY1ODQ0ZGUzYzVmNGM0NSJ9/53738		
A7.2	Cross-Frame Scripting	High	Following pages can be loaded in frames in external pages **Superadmin**: • http://218.248.45.210/naacfeb7/public/index.php **DVV:** • http://218.248.45.210/naacfeb7/public/index.php/dvv **Inflibnet:** • http://218.248.45.210/naacfeb7/public/index.php/inflib **Assessor:** • http://218.248.45.210/naacfeb7/public/index.php/assessor **HEI:** http://218.248.45.210/naacfeb7/public/index.php/hei	Fixed	Closed
A7.3	Cross-Site Scripting: Reflected	Medium	Reflected Cross-Site Scripting detected at following pages **Superadmin**: Please refer Application Security Tool Report for Superadmin role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **DVV**: Please refer Application Security Tool Report for DVV role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Inflibnet:** Please refer Application Security	Fixed	Closed

			Tool Report for Inflibnet role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report **Assessor**: Please refer Application Security Tool Report for Assessor role for complete list of pages with the vulnerability as the list is very long to be accommodated in the report		
A7.4	Cross-Frame Scripting	Medium	Cross-Frame Scripting detected at following pages **Assessor**: http://218.248.45.210/naacfeb7/public/index.php/assessor/training	Fixed	Closed
A8-Insecure Deserialization					
--	--	--	--	--	--
A9- Using Components with Known Vulnerabilities					
--	--	--	--	--	--
A10-Insufficient Logging and Monitoring					
--	--	--	--	--	--

6. Recommendation

1. All the sensitive data must be suitably protected using *TLS ver1.2* or higher for the application to be hosted in the production environment.
2. User access log & transaction log of the Web application should be enabled and stored on a separate secure server.
3. Before deploying the Website in the production environment, the hardening of IT infrastructure (Network, Hosts and OS) must be ensured.