Report No: STQC-IT(Kol)/ES/ NIOT/181901/1085

Web Application Security Evaluation Report

National Institute of Technology, Srinagar

Computer Services Centre, Hazratbal
Srinagar - 190006
Jammu & Kashmir

Developed by
MasterSoft ERP Solutions Pvt. Ltd.

STQC IT SERVICES, Kolkata
ERTL (EAST), STQC DIRECTORATE
Ministry of Electronics & Information Technology
Govt. of India
DN - 63, Sector - V, Salt Lake
Kolkata –700091, India

(This report consists of 10 pages and it shall always be reproduced in full.)

Application Security Audit Report

Contents

Application Security Audit Report

Table 1: Evaluation Summary

Application Name	Website of National Institute of Technology, Srinagar Version & Build: Release Date:
Customer Name and Address	National Institute of Technology Computer Services Centre, Hazratbal Srinagar Jammu and Kashmir PIN-190006
Production URL	https://www.nitsri.ac.in
Test / Temporary URL	http://new.nitsri.ac.in https://www.nitsri.ac.in
Infrastructure Details	Operating System : Windows Server 2016 Web Server : Microsoft-IIS/10.0 Server-side Script : ASP.NET Database Server : MS SQL Server/2016
User Roles	Centre-wise users, Department-wise users and Alumni users CPanel user
Hash of Final Build	Not available
Audited on	14th December 2018 to 20th December 2018 (Cycle-1) 3rd March 2020 to 11th March 2020 and 18th June 2020 to 26th June 2020 (Cycle-2)
Audit Location	STQC IT Services, Kolkata
Evaluation Method	Different software testing techniques (both manually and using tools) has been used to unearth application security vulnerabilities, weaknesses in the following broad application aspects. a) Data and Input Validation b) Authentication c) Authorization and Access Control d) Session Management e) Error Handling f) Use of Cryptography / Data Protection g) Others (Reference Operating Procedure of the laboratory: OP09)
Evaluated By	Subrata Giri, Scientist 'C'
Report Prepared By	Arpita Datta, Scientist 'E'
Report Reviewed By	Subhendu Das, Scientist 'G' and Head, e-Security
Other Remarks	The report presents the findings of the audit during the audit period only.

Application Security Audit Report

1.0 Introduction

STQC IT Services, Kolkata has carried out security evaluation of the application as detailed in the Table-1. The vulnerabilities/weaknesses observed during the testing along with the recommendations to plug the vulnerabilities are given below. The observations indicate the status of the application during the evaluation period (Ref. Table-1) only.

2.0 Summary Observations

The audit was conducted on the Website of National Institute of Technology, Srinagar, hosted in the test server, by using automated tools followed by manual verification of discovered security vulnerabilities.

The application has been audited, following Open Web Application Security Project (OWASP) Application Security Verification Standard 4.0 [ASVS v4.0], to discover Security vulnerabilities / weaknesses. The assessment focused to discover the listed security vulnerabilities as per the OWASP Top 10 - 2017 list. Discovery of typical security issues of an web application, related to, improper input validation, insecure direct object reference, unvalidated directs and forwards, Cross-Site Scripting(XSS),Cross-Site Request Forgery(CSRF), Broken Authentication and Session Management (e.g. weak passwords, weak session management), various injection flaws (like SQL injection, command injection etc.), security mis-configurations, sensitive data exposure, missing or improper access control etc. and also related to well-known platform and components, are attempted in this exercise. This Assessment result presents the state of Security of the Web Application as it appears through its web interface and does not include the assessment result of Application code review, hosting infrastructure and associated security processes.

The initial assessment observation has been shared as Cycle-1and Cycle-2 reports (as referred below). On receipt of the confirmation of the closure of the Cycle-2 issues, the Assessment team has verified and made this final comment.

[Ref 1]: Cycle-1 Observation report: Report No. ES/NIOT/181901/OR/C1/043609
[Ref 2]: Cycle-2 Observation report: Report No. ES/NIOT/181901/OR/C2/020113

Disclaimer: *This report is valid for the web application code in its present state only. Reassessment is recommended for any change in the application code.*

3.0 Detailed Observations

SN	Test / Parameter	Observation	Remarks
3.1 Data & Input Validation			
3.1.1	Input Validation	Vulnerabilities, observed in cycle-1 audit [Ref 1], are closed by the developer and verified by us in cycle-2 audit [Ref 2].	Complied.
3.1.2	Sanitization and sandboxing	Vulnerabilities, observed in cycle-1 audit [Ref 1], are closed by the developer and verified by us in cycle-2 audit [Ref 2].	Complied.
3.1.3	Output encoding and Injection Prevention	Vulnerabilities, observed in cycle-1 audit [Ref 1], are closed by the developer and verified by us in cycle-2 audit [Ref 2].	Complied.
3.1.4	Deserialization Prevention	No issues are found during audit.	Complied.
3.1.5	File Upload	No issues are found during audit.	Complied.
3.1.6	File execution	Not Applicable. Such options are not available in the application.	N/A
3.1.7	File Storage	Not Applicable. Such options are not available in the application.	N/A
3.1.8	File Download	No issues are found during audit.	Complied.
3.2 Authentication			
3.2.1	Password Security	No issues are found during audit.	Complied.
3.2.2	General Authenticator	No issues are found during audit.	Complied.
3.2.3	Authenticator Lifecycle	No issues are found during audit.	Complied.
3.2.4	Credential Recovery	No issues are found during audit.	Complied.
3.2.5	Out of Band Verifier	No issues are found during audit.	Complied.
3.2.6	Single or Multi Factor One Time Verifier	Two-factor authentication is missing for cPanel, centre-wise login, department-wise login and alumni login forms.	Two-factor authentication may be implemented in production environment.
3.3 Authorization & Access Control			
3.3.1	General Access Control Design	No issues are found during audit.	Complied.
3.3.2	Operation Level Access Control	No issues are found during audit.	Complied.
3.3.3	Other Access Control Considerations	No issues are found during audit.	Complied.
3.4 Session Management			
3.4.1	Fundamental Session Management	Vulnerabilities, observed in cycle-1 audit [Ref 1], are closed by the developer and verified by us in cycle-2 audit [Ref 2].	Complied.

Application Security Audit Report

3.4.2	Session Binding	No issues are found during audit.	Complied.
3.4.3	Session Logout and Timeout	No issues are found during audit.	Complied.
3.4.4	Cookie-based Session Management	Vulnerabilities, observed in cycle-1 audit [Ref 1], are closed by the developer and verified by us in cycle-2 audit [Ref 2].	Complied.
3.4.5	Defenses against Session Management Exploits	Issue is not applicable for the application.	N/A
3.5 Error Handling			
3.5.1	Log Content Requirements	Not Applicable. No logs are captured by the web application	N/A
3.5.2	Error Handling	No issues are found during audit.	Complied.
3.6 Use of Cryptography / Data Protection			
3.6.1	Algorithm	Not Applicable. Because no cryptography is used.	N/A
3.6.2	Client-side Data Protection	No issues are found during audit.	Complied.
3.6.3	Sensitive Private Data	No issues are found during audit.	Complied.
3.6.4	Communications Security	No issues are found during audit.	Complied.
3.6.5	Deployed Application Integrity Controls	Issue is not applicable for the application	N/A
3.7 Configuration Management			
3.7.1	Dependency	No issues are found during audit.	Complied.
3.7.2	Unintended Security Disclosure	No issues are found during audit.	Complied.
3.7.3	HTTP Security Headers	Vulnerabilities, observed in cycle-1 audit [Ref 1], are closed by the developer and verified by us in cycle-2 audit [Ref 2].	Complied.
3.7.4	Validate HTTP Request Header	No issues are found during audit.	Complied.
3.8 Others			
3.8.1	Business Logic Security	No issues are found during audit.	N/A
3.8.2	SSRF Protection	No issues are found during audit.	Complied.