Global IT – Department of Defense Product

Web VAPT Report

Aug 2019

A comprehensive VAPT report of web application by using an Attacker oriented approach, to uncover potential Security threats

Risk Advisory

Audit Conducted for: Department of Defense Product

Audit Conducted by: Ankur Verma (v.ank@crrisk.com), Bhaskar Dev Mayank (m.bha@crrisk.com)

Location of Audit: 023, 5th Floor, Tower A, Emaar Digital Greens, Sector 61, Gurugram - 122102, Haryana

Report Submitted On: 07th Aug 2019

Test Duration: 01st Aug to 07th Aug 2019

URL of the Web-Application: http://103.73.189.114:803/

Report Reviewed by: Mr. Vibhor Sharma (s.vib@crriskadvisory.com)

Report Handed over to: Mr. Uttam (uttam@globalitpoint.com)

Table of Contents

Part 1: Executive Summary

We thank you for choosing CyberRoot Risk Advisory Pvt. Ltd. as your Information Security partner. We appreciate your business and look forward to provide you services in the near future as well. The following report presents the results of the audit of web application as per your request. In case you have any questions, please contact your CR Risk Advisory representative or email cert@crriskadvisory.com

Section 1. Overview

SCOPE

In depth Security Assessment of the following Web Application:

Web Application	http://103.73.189.114:803/	
Audit Dates	01st Aug to 07th Aug 2019	
Nature Of Site	Dynamic	
Server	Staging	
User Group	Open Group	
User Role	rgera@nic.in	Admin

EXCLUSIONS

- NA

TOOLS USED

- Burp Suite
- Advance cookie manager
- sqlmap
- nmap
- Wappalyzer Extension

STANDARDS FOLLOWED

Comprehensive vulnerability assessment has been carried out as per recommendations by CERT-In and not limited to OWASP Top 10 only.

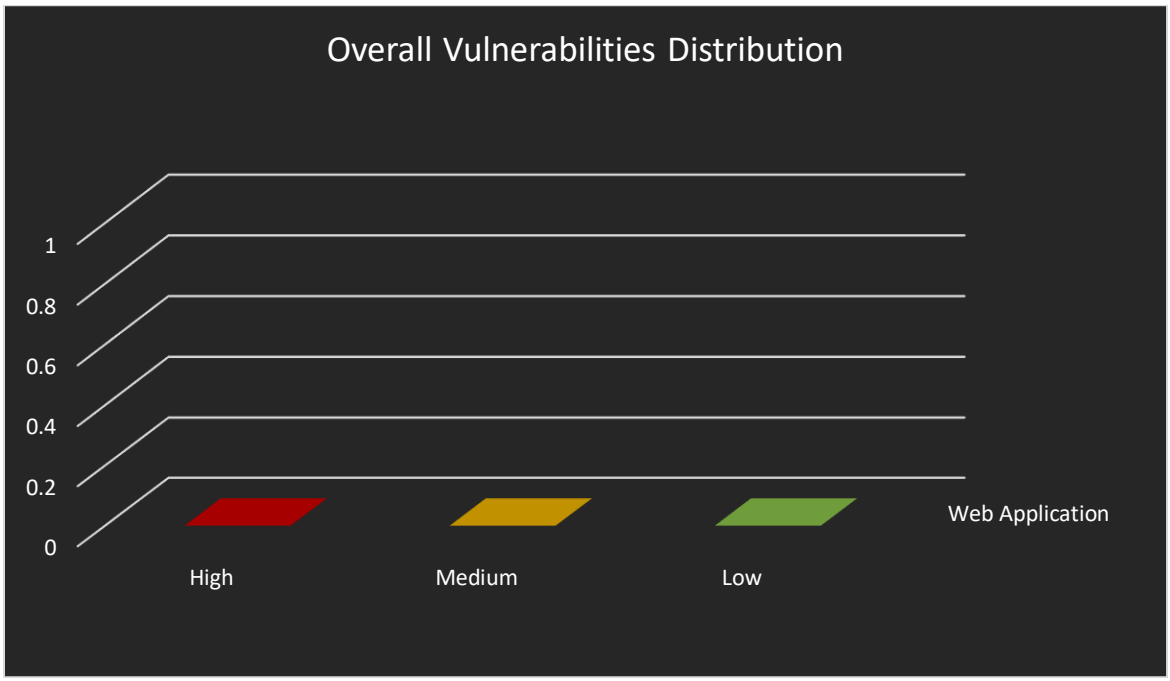
http://103.73.189.114:803/	
Based on OWASP Top 10 - 2017	Based on OWASP Top 10 - 2013
Injection	Injection
Broken Authentication & Session Management	Broken Authentication & Session Management
Sensitive Data Exposure	Cross-Site Scripting
XML External Entities	Insecure Direct Object References
Broken Access Control	Security Misconfiguration
Security Misconfiguration	Sensitive Data Exposure
Cross Site Scripting	Missing Function Level Access Control
Insecure Deserialization	Cross-Site Request Forgery
Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities
Insufficient Logging & Monitoring	Unvalidated Redirects and forwards

OBSERVATIONS SUMMARY

Based on tests carried out on the Web Application it was found that Web Application did not contain any vulnerability as per OWASP Top 10 standards.

The total vulnerabilities found were:

Web Application Vulnerabilities: High=0, Medium=0, Low=0 (Total 0 Vulnerabilities)



Summary of Previous Findings

High | Medium | Low

S. No.	Vulnerability	Current Status
1.	Cross-Site Request Forgery	Fixed
2.	Broken Authentication	Fixed
3.	Arbitrary File Upload / Remote Code Execution	Fixed
4.	Clear Text Password Submission	Fixed
5.	Missing Security Headers	Fixed
6.	Weak Password Policy	Fixed
7.	TRACE Method	Fixed
8.	Version Disclosure	Fixed
9.	Outdated JQuery library	Fixed
10.	Outdated JQuery UI library	Fixed
11.	Error Handling	Fixed

General Recommendations As Per Audit Activity

- Hide sensitive resources from unauthorized users
- Implement custom 404 Not Found and error handling pages
- Remove broken links throughout the application
- Third party libraries and frameworks should be updated to their latest versions
- Use TLS 1.3 to transmit sensitive information between the browser and the server
- Use the strong encryption algorithms/cipher suites (3DES, RSA, Blowfish, AES)
- Set expiration dates on cookies to the shortest practical time
- Proper permissions should be set on Search Engine Optimization related files
- Implement best security practices for OS and Server hardening on production server

Mandatory Recommendations For Hosting The Website On Production Server

- Captcha should to be implemented on login pages
- Implement CSRF token on every form throughout the application
- Input validation should be implemented on all parameters on client side as well as server side
- Use TLS 1.2 or above to transmits sensitive information between the browser and the server
- Set the Secure and HttpOnly flags on the cookies to true
- TRACE method should be disabled
- Version Disclosure should be barred from the server side
- Create custom error handling pages for situations that are prone to error
- Remove unwanted commented code throughout the application
- Password should be saved as salted hash (SHA-256 or higher) in the database
- Implement HTTP Security Headers
- Implement CORS (Cross-Origin Resource Sharing) policy and whitelist domains needed for resource sharing if cross domain sharing is required

CONCLUSION

On the basis of tests carried out in the 2nd phase of Web Application Audit it can be concluded that all the vulnerabilities found in the 1st phase Web Audit are patched and Web Application does not contain any vulnerabilities as per OWASP Top 10 2013 & OWASP Top 10 2017.

Website with staging http://103.73.189.114:803/ or permanent URL http://srijandefence.gov.in/ is safe to host.

Certificate issued will be valid until code changes are made to the Web Application or 2 years from date of issue whichever is earlier.

Details of Team Engaged for Audit

S.No.	Name	Email-id	Phone	Qualification and Certification
1	Ankur Verma	v.ank@crrisk.com	+91- 8447771158	B. Tech
2	Bhaskar Dev Mayank	m.bha@crrisk.com	+91-8447771158	B.Tech, CEH
3	Vibhor Sharma	s.vib@crriskadvisory.com	+91-8750900111	B.Tech, ISO 27001 LA