Web Application Security Report of FACT CHECK

Name of Software/Project: FACT CHECK

Name of Module: Home Page

Document Name: FACTCHECK_1.0.2_C-DIT

Classification: Confidential

Version: 1.2

Date: 20/02/2021

Prepared by

Application Testing & Integration Division@Informatics Division

Centre for Development of Imaging Technology (C-DIT)

Thiruvallom

The information contained within this report is considered proprietary and confidential to I&PRD. Inappropriate and unauthorized disclosure of this report or portions of it could result in considerable damage or loss to the I&PRD. This report should be distributed to individuals on a Need-to-Know basis only. Paper copies should be locked up when not in use. Electronic copies should be stored offline and protected appropriately.

	Client Details	
1	Name of client	I&PRD, Govt. of Kerala
2	Address of client	Information & Public Relations Department South Block, Government Secretariat, Thiruvananthapuram
	Details of Application	
3	Product nomenclature	**FACT CHECK**
4	Version No:	1.0.2
5	Date of release	NA
6	Document Name	FACTCHECK _1.0.2_C-DIT
7	Test environment URL	**https://factcheck.kerala.gov.in//**
8	Date of receipt for audit	20th February 2021
	Audit Description	
9	Name and Address of auditing agency	Application Testing & Integration Department Informatics Division, C-DIT
10	Scope of work	The security audit is carried out on **FACTCHECK** web application to gauge the security posture of the application. The result of the assessment is evaluated for vulnerabilities, its likelihood, impact and severity of risk.
11	Audit standard	The security audit of the application is done based on OWASP Top 10 vulnerabilities.
12	Audit report version	1.0
13	Audit start date	20h February 2021
14	Audit completion date	20th February 2021
15	Software Configurations (Test Server -Client)	PHP 5.6, MySQL 5.6
16	Tools used	Burp Suit, Zap

Quality Assurance				
	Date	Name	Role	Completed
Issue	20/02/2021	Anu Sivaraj	Programmer-Test Engineer	☑
Review	20/02/2021	Rajitha KS	HoD-Testing	☑
Approval	20/02/2021	Biju SB	Head-Informatics	☑

Schedule		
Activity	**Start Date**	**End Date**
Web Application Security Assessment	20th –February 2021	20th-February 2021

Task Professionals	
Assessment done by	Anu Sivaraj
Report Prepared by	Anu Sivaraj

Table of Content

1. Summary

The likelihood estimate and the impact estimate are put together to calculate an overall severity for this risk. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. This reflects the inherent reliability of the OWASP technique that was used to identify the issue. The 0 to 9 scale is split into three parts

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

2. Approach

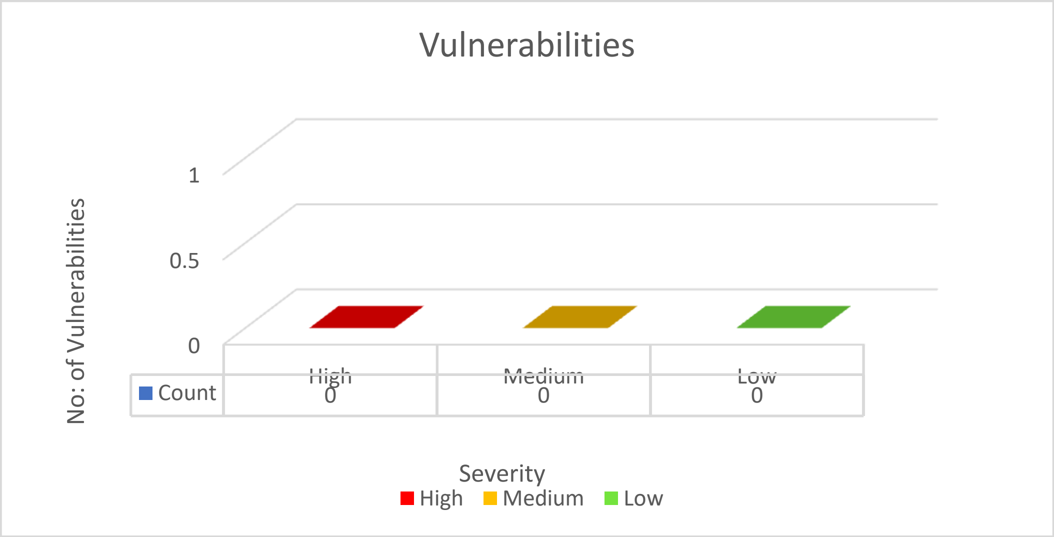
- Perform broad VAPT to identify potential areas of exposure and services that may act as entry points.
- Perform targeted scans and manual investigation to validate vulnerabilities.
- Identify and validate vulnerabilities.
- Rank vulnerabilities based on threat level, loss potential, and likelihood of exploitation
- Perform supplemental research and development activities to support analysis.
- Identify issues of immediate consequence and recommend solutions.
- Develop long-term recommendations to enhance security.

3. Key Findings

Sl No	Vulnerability Name	Rating	Status
1.	Cross-site scripting (reflected)	H	Closed

4. Chart

- The chart below shows the number of vulnerabilities found against each severity level from Security Assessment which was done on website of **http://192.168.3.190/factcheck//**



5. Scope

Vulnerability and Penetration Test of Fact Check Department of I&PRD web application https://factcheck.kerala.gov.in//

6. Application Security Assessment

Below are the detailed findings of the assessment performed. The findings are sorted based on the criticality that has been derived from the risk rating matrix, with CVSS (Common Vulnerabilities Scoring System) as the primary reference.

7. Conclusion

It is observed that the application has vulnerabilities (0-high, 0- medium and 0- low). The vulnerabilities may be fixed or reproduced for the next version of application testing.

1. Sensitive data should always be transferred to the server over an encrypted connection. Hence it is recommended to implement SSL to the application within one month of production server hosting.
2. Update the application/server software when patches are available.
3. Limit Dashboard access to administrator only or limit by specific capability. Change the default name of the login page to a customized one.
4. Implement some type of account lockout after a defined number of incorrect password attempts and Captcha Settings.
5. Use strong credentials: Always use various combinations of characters with minimum 8 characters which should be difficult to guess. An example of strong password is E@^M!$<9@k.
6. Disable directory listing in the web or application - server configuration by default. Restrict access to unnecessary directories and files. Create an index (default) file for each directory.
7. Make sure that sensitive information is not disclosing through error message page.
8. Make sure that all the junk data/files uploaded during the scan are cleared from the server.
9. Make sure that the upload directory has no write & execute permission.

10. Make sure that a dedicated User account with limited privileges should be used for the Web Server Processes.
11. The application should be audited periodically at least once in 2 years or whenever there are major changes.
12. It is recommended to use TLS 1.2 or higher. Disable older protocols (like TLS 1.1, 1.0, SSLV3 etc) in the server.