Vulnerability Assessment Completion Report of C-DAC CTF Platform

APPLICATION URL:

https://ctf.cdac.in

Report Date: 25.07.2024

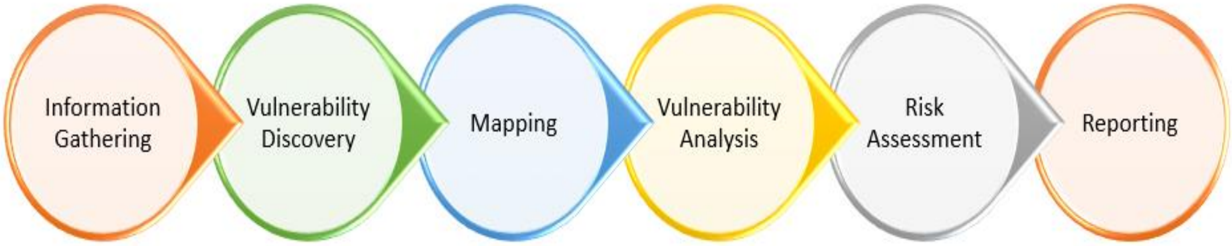
Centre for Development of Advanced Computing (C-DAC)
Kolkata

This report is digitally signed, hence it does not require signature or Company's Stamp to consider valid. The report can be printed by Auditee for further use.

Table of Contents

1. Audit Methodology

The audit methodology followed to the scope involves the following steps:



Different security testing techniques (both manually and using tools) were employed to unearth application security vulnerabilities, weaknesses and concerns in the following aspects

1. Input Validation
2. Authentication and Session Management
3. Access Control
4. Error Handling
5. Data Protection
6. Denial of Service
7. Handling File uploads
8. Web Application Finger Print
9. Logging and Monitoring

Risk Assessment

The risk assessment on the identified vulnerabilities is carried out based on the following risk Matrix.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Informational	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			
Risk Severity Matrix as per OWASP Standards				

2. Overview of Findings

The following table gives of overview of the findings and their status by the end of our security audit process.

S No	Name of Vulnerability	Severity	Stage I	Stage II	Final Stage	Remarks (Mention reason for open issues)
1	HTTP Request Method Validation	High	Open	Closed	Closed	-
2	Arbitrary HTTP method	Medium	Open	Closed	Closed	-
3	Missing Security Headers	Low	Closed	Open	Open	Certain security headers are causing functionality issue on the platform.

Date: 25.07.2024

3. OWASP Compliance Status

The Testing Methodology and Standards followed for performing Security audit was OWASP Methods and Standards and thus this report is generated in compliance with OWASP Vulnerabilities. The following table comments on https://ctf.cdac.in website/web application's compliance status against OWASP top 10 2021 Vulnerability.

#	Vulnerabilities	Status	Remarks
A1	Broken Access Control	Safe	-
A2	Cryptographic Failures	Safe	-
A3	Injection	Safe	-
A4	Insecure Design	Safe	-
A5	Security Misconfiguration	Unsafe	Due to functionality issues caused by certain security headers, the implementation of some important security headers has been deferred.
A6	Vulnerable and Outdated Components	Safe	-
A7	Identification and Authentication Failures	Safe	-
A8	Software and Data Integrity Failures	Safe	-
A9	Security Logging and Monitoring Failures	Safe	-
A10	Server-Side Request Forgery	Safe	-