



**Level 1 Web Application Security Audit Report of {{ project.name }}**

**For**

**{{ project.companyname.name }}**

**Audited By:**

**DR CBS CYBER SECURITY SERVICES LLP**

***CERT-In Empanelled Information Security Auditing Organization (2024-2027)***

**{{ project.startdate.strftime("%d/%m/%Y") }}**



**Level 1 Security Audit Report**

|  |  |
| --- | --- |
| **Report Release Date** |  |
| **Type of Audit** | Web Application Audit |
| **Type of Audit Report** | {{ Report\_type }} Audit Report |
| **Period** |  |

**Document Control**

|  |  |
| --- | --- |
| **Document Title** |  |
| **Document ID** |  |
| **Document Version** |  |
| **Prepared by** | **{% for owner in owners -%}**  **{{ owner.full\_name + '\n' }}**  **{% endfor %}** |
| **Reviewed by** |  |
| **Verified by** |  |
| **s** | DRCBS-17-001 |
| **Released by** |  |
| **Release date** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Distribution List** | | | |
| **Name** | **Organization** | **Designation** | **Email ID** |
| {{ user.full\_name }} | {{project.companyname.name}} | {{ user.position }} | {{ user.email }} |

**{% endfor %}**

# [Content](#_top)

[**Introduction**](#_Introduction) **5**

[**Engagement Scope**](#_Engagement Scope) **5**

[**Details of the Auditing team**](#_Details of the Auditing team) **6**

[**Audit Activities and Timelines**](#_Audit Activities and Timelines) **7**

[**Audit Methodology and Criteria / Standard referred for audit**](#_Audit Methodology and Criteria/Standard referred for audit) **7**

[**Tools/ Software Used**](#_Tools/ Software Used) **8**

[**Software Components & Dependencie**](#_Software Components & Dependencies)**s 8**

[**Limitations/Exceptions**](#_Limitations/Exceptions) **8**

[**Risk/**](#_Limitations/Exceptions)**Vulnerability Rating Criteria 9**

[**Executive Summar**](#_Executive Summary)**y 10**

[**Detailed Observations**](#_Detailed Observations) **12**

[**Conclusion**](#_Conclusion) **14**

[**Recommendation**](#_Recommendations) **15**

[**Appendix 1: POC**](#_Appendix 1: Proof of Concept of the Software Components & Dependencies) **16**

**Glossary 19**

# [Introduction](#_Content)

The Audit Team conducted a comprehensive web-based vulnerability assessment and penetration testing (VAPT) of **<Web App Name>** hosted at<staging URL>.

The reference of the work order given to us is **<work order reference dated 10/10/2024>**

The objective of this testing was to conduct Vulnerability assessment and penetration testing as per various security standards and Guidelines, Vulnerability Notes, Advisories and White Papers issued by Computer Emergency Response Team (CERT-In).

**Following are the details of the application given by the auditee.**

|  |  |  |
| --- | --- | --- |
| **S.No** | **Website/ Portal Name** | **Test URL** |
| 1. | **Web app name** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No** | **Website/ Portal Name** | **Test URL** | **Location** | **Hash Value** | **Version** |
| 1. |  |  |  |  |  |

# Details of the Auditing team {% for user in projectmanagers %}. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.No.** | **Name/Employee Code** | **Designation** | **Email Id** | **Professional Qualifications/ Certifications** | **Whether the resource has been listed in the Snapshot information published on CERT-In’s website(Yes/No)** |
| {{ loop.index }} | {{ user.full\_name }} | {{ user.position }} | {{ user.email }} | * {{ user.certifications }} |  |

{% endfor %}

# [Audit Activities and Timelines](#_Content)

|  |  |
| --- | --- |
| **Audit Activities** | **Time Period** |
| **Work Order Received** |  |
| **URL Working** |  |
| **Audit conducted (From-To)** |  |
| **L1 Report Submitted** |  |

# [Audit Methodology and Criteria/Standard referred for audit](#_Content)

The audit team conducted manual as well as tool based audit to identify maximum of vulnerabilities. In tool based method, we were used industry standard tools as mentioned in the tool list supplemented by In house scripts and payloads to achieve optimum results. Sometimes, tools provide false positive results. For it, the auditor team verified the locations of the vulnerabilities through manual methods. Software arithmetic errors and validations related issues are also verified through Manual method.

A comprehensive IT security audit of the web application was performed as per legal mandate and based on web application security Standards of Open Web Application Security Project (OWASP) Comprehensive Framework, Directions by CERT-In under Section 70B, Information Technology Act 2000, Guidelines for Secure Application Design, Development, Implementation & Operations, SANS Top 25 Software Errors, Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE) Guidelines for Secure Application, Design, Development, Implementation & Operations and The Open Source Security Testing Methodology Manual (OSSTMM) etc.

Add Methodology as required as per the scope of work

# [Tools/ Software Used](#_Content)

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No.** | **Name of Tool/Software used** | **Version of the tool /Software used** | **Open Source/Licensed** |
|  | **BurpSuite** | **2024.3.1** | **Licensed** |
|  | **OWASP ZAP** | **2.14.0** | **Open Source** |
|  | **Kali Linux** | **2024.1** | **Open Source** |
|  |  |  |  |

# [Software Components & Dependencies](#_Content)

The following software components and dependencies were identified during the audit:

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Name of Software Components & Dependencies used** | **Version of the Software Components & Dependencies used** |
|  | **jQuery** | **1.11.3** |
|  |  |  |
|  |  |  |
|  |  |  |

# [Limitations/Exceptions](#_Content)

Penetration testing on the web application was avoided to mitigate potential risks associated with destructive payloads, scripts, or attacks. Instead, a thorough vulnerability assessment was conducted within the defined scope of work. This ensured that no harmful or intrusive techniques were employed during the process. This approach was adopted to minimize disruption to the application's functionality, safeguard sensitive data, and maintain the integrity and security of the system without causing any operational impact.

The Auditee is accountable for its assertions, while our role is to express an opinion on the validity of management's assertions based on our audit findings.

Add limitations as required as per the scope of work

# [Risk/Vulnerability Rating Criteria](file://C:\Users\Vivek%20Dadhich\Desktop\Template\level%201%20template%20of%20mobile%20application.docx#_Content)

The risk/ vulnerability of an audit finding is determined by assessing the potential negative impact and the probability that it materializes. Audit findings are classified into three risk/ vulnerability classifications. These risk/ vulnerability categories assist the Management in identification, prioritization and implementation of Audit recommendations.

The three risk/ vulnerability ratings are as under:-

|  |  |
| --- | --- |
| **High** | These risks/ vulnerabilities are so significant that the Management should determine any exposure to date and effect an agreed program for their immediate and permanent resolution in order to provide assurance that they will not recur in the future. These are weaknesses that have compromised control or security, and should therefore be addressed immediately. |
| **Medium** | These risks/ vulnerabilities are important and the Management should quickly develop action plans that will ensure timely and permanent resolution of the weaknesses noted. Typically, these are weaknesses in control or security, which could develop into a potential exposure. This should be addressed at the earliest opportunity. |
| **Low** | These risks/ vulnerabilities are not material in the context of current levels of activity but the Management should be aware of them and ensure that they are resolved as soon as possible as they may become material if activities increase. These risks, even though not a direct threat to control or security, should be addressed in the interest of efficiency. |

# [Executive Summary](#_Content)

The summary of Vulnerabilities/Non-conformities identified during the audit is mentioned below:

{% for vulnerability in vulnerabilities %}

|  |  |  |
| --- | --- | --- |
| **S. No** | **Severity of Vulnerabilities/Non-Conformities** | **Status** |
| {{loop.index}} | {% if vulnerability.vulnerabilityseverity == 'Critical' %}  {{ vulnerability.vulnerabilityseverity }}  {% elif vulnerability.vulnerabilityseverity == 'High' %}  {{ vulnerability.vulnerabilityseverity }}  {% elif vulnerability.vulnerabilityseverity == 'Medium' %}  {{ vulnerability.vulnerabilityseverity }}  {% elif vulnerability.vulnerabilityseverity == 'Low' %}  {{ vulnerability.vulnerabilityseverity }}  {% else %}  Informational  {% endif %} | {% if vulnerability.status == 'Vulnerable' %}  {{ vulnerability.status }}  {% elif vulnerability.status == 'Confirm Fixed' %}  {{ vulnerability.status }}  {% elif vulnerability.status == 'Accepted Risk' %}  {{ vulnerability.status }}  {% endif %} |

{%tr endfor %}

Figure 1. Vulnerabilities Chart{% for vulnerability in vulnerabilities %}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **List of Vulnerable Points** | | | | | |
| **S.No.** | **Vulnerable Point / Location** | **Vulnerability** | | **Means of identification Manually/ Tool based** | **Comments/ Review of flaw / Reference** |
| **(1)** | **(2)** | **(3)** | | **(4)** | **(5)** |
|  | | | | | |
| **1.1** | {{ vulnerability.instances\_data[0].URL }} | **{{ vulnerability.vulnerabilityname }}** |  | |  |
|  | | | | | |
| **2.1** |  |  |  | |  |

{% endfor %}

{% for vulnerability in vulnerabilities %}

|  |  |
| --- | --- |
| 1. **Vulnerability title** | **{{ vulnerability.vulnerabilityname }}** |
| * **Affected IP/URL** | {{vulnerability.instances\_data[0].URL }} |
| * **CVE/ CWE** |  |
| * **Severity** | **{{ vulnerability.vulnerabilityseverity }}** |
| * **Vulnerability Description:**   {{p vulnerability.vulnerabilitydescription }} | |
| * **References to evidences / Proof of Concept** | |
| **POC**  **{{p vulnerability.POC }}** | |
| * **Solution & Work around: {{p vulnerability.vulnerabilitysolution }}** | |
| * **References: {{p vulnerability.vulnerabilityreferlnk }}** | |

{% if not loop.last %}{{r page\_break}}{% endif %}

{% endfor %}

# [Conclusion](#_Content)

The developer team of auditee is advised to provide the compliance as per mentioned recommendation in details of the vulnerabilities at the earliest. Ensure that security is properly integrated in all phases of the development process and developers are aware with common web application vulnerabilities. We recommend the Guidelines for Secure Application Design, Development, Implementation & Operations issued by Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology Government of India. Conduct the regular external and internal audit to enhance the security posture of the application.

# [Recommendations](#_Content)

Following are the other recommendations to improve the cyber security posture of the application and associated IT Infrastructure of the auditee organization.

1. Web Server Security and the OS hardening need to be in place for the production Server.
2. It is recommended that deploy and proper configure the SSL.
3. Web Application should comply with Guidelines for Indian Government Websites (GIGW).
4. Employ the latest stable version of the Transport Layer Security (TLS) protocol to ensure secure communication between the application and its users. Additionally, disable outdated and weak SSL cipher suites to enhance security and prevent potential exploits.
5. The developer team should follow the Guidelines for Secure Application Design, Development, Implementation & Operations issued by Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology Government of India. Conduct the regular external and internal audit to enhance the security posture of the application.
6. The Auditee organization must comply with the Directions issued by CERT-In (Notification No. 20(3)/2022-CERT-In) dated 28 April 2022 under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
7. The Developer Team must follow the Technical Guidelines on Software Bill Of Materials (SBOM) issued by CERT-In dated 03.10.2024.

# [Appendix 1: Proof of Concept of the Software Components & Dependencies](#_Content)

1. Bootstrap  
   

# Compliance to Directions issued by CERT-In under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet dated 28 April 2022

The Government of India appointed “Indian Computer Emergency Response Team (CERT-In)” vide notification dated 27th October 2009 published in the official Gazette in terms of the provisions of sub-section (1) of section 70B of the Information Technology Act, 2000 (IT Act, 2000). As per provisions of sub-section (4) of section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:-

1. collection, analysis and dissemination of information on cyber incidents;  
   b) forecast and alerts of cyber security incidents;  
   c) emergency measures for handling cyber security incidents  
   d) coordination of cyber incident response activities;  
   e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;  
   f) such other functions relating to cyber security as may be prescribed.

.   
As per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000.The failure to furnish the information or non-compliance with the ibid. directions, may invite punitive action under sub- section (7) of the section 70B of the IT Act, 2000 and other laws as applicable.

**All Service providers, intermediaries, data centres, body corporate, Virtual Private Server (VPS) providers, Cloud service providers , VPN Service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and Government organisations shall follow these Cyber Security Directions issued by CERT-In dated 28.4.2022.**

Following are the current status requirement as mentioned in the directions issued by CERT-In under sub-section (6) of section 70B of the Information Technology Act, 2000 dated 28 April 2022.

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Direction Requirement** | **Auditee Remark**  **\* NA : For Not Applicable Points.** |
| 1. | All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC. |  |
| 2. | Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). |  |
| 3. | Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration:   1. Validated names of subscribers/customers hiring the services 2. Period of hire including dates 3. IPs allotted to / being used by the members 4. Email address and IP address and time stamp used at 5. the time of registration / on-boarding Purpose for hiring services 6. Validated address and contact numbers 7. Ownership pattern of the subscribers / customers hiring 8. services |  |
| 4. | The virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years. |  |
| 5. | All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In. |  |
|  | Details of Nodal Point of Contact to CERT-In.  Point of Contact (PoC) information by Service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In The Information relating to the Point of Contact shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified below and shall be updated from time to time: |  |

# Glossary

1. **CERT-In:** The Government of India appointed “**Indian Computer Emergency Response   
    Team (CERT-In)**” vide notification dated 27th October 2009 published in the official Gazette   
    In terms of the provisions of sub-section (1) of section 70B of the Information Technology Act,   
    2000 (IT Act, 2000). As per provisions of sub-section (4) of section 70B of the Information   
    Technology Act, 2000, the Indian Computer Emergency Response Team shall serve as the   
    national agency for performing the following functions in the area of Cyber security:-
2. collection, analysis and dissemination of information on Cyber incidents;
3. forecast and alerts of Cyber security incidents;
4. emergency measures for handling Cyber security incidents
5. coordination of Cyber incident response activities;
6. issue guidelines, advisories, vulnerability notes and white-papers relating to information security practices, procedures, prevention, response and reporting of Cyber incidents;
7. such other functions relating to Cyber security as may be prescribed.
8. **Directions issued by CERT-In dated 28 April 2022 :** As per provisions of sub-section (6) of   
    section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information   
    and give directions to the service providers, intermediaries, data centers, body corporate and   
    any other person for carrying out the activities enshrined in sub-section (4) of section 70B of   
    the IT Act, 2000.The failure to furnish the information or non-compliance with the ibid.   
    directions, may invite punitive action under sub- section (7) of the section 70B of the IT Act,   
    2000 and other laws as applicable. All Service providers, intermediaries, data centers, body   
    corporate, Virtual Private Server (VPS) providers, Cloud service providers , VPN Service   
    providers, virtual asset service providers, virtual asset exchange providers, custodian wallet   
    providers and Government organizations shall follow these Cyber Security Directions issued by   
    CERT-In dated 28.4.2022.

<https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf>

1. **Common Vulnerability and Exposure(CVE):** The Common Vulnerabilities and Exposures (CVE) system provides a reference method for publicly known information-security vulnerabilities and exposures.
2. **Common Weakness Enumeration (CWE)**: Common Weakness Enumeration (CWE) is a list of common software and hardware weakness types that have security ramifications. A “weakness” is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities.

**[END OF REPORT]**

# {{r page\_break}}

# {% endif %}

# {% endfor %}