Report for CyberSmithSecure

**{{Application Name/IP}} Report**

|  |  |
| --- | --- |
| **Report Release Date** | 1952-05-20 00:00:00 |
| **Type of Audit** | XSS |
| **Type of Audit Report** | Server |
| **Period** | 9 |

Document Control

|  |  |
| --- | --- |
| **Document Preparation** | |
| **Document Title** |  |
| **Document ID** |  |
| **Document Version** |  |
| **Prepared by** |  |
| **Reviewed by** |  |
| **Approved by** |  |
| **Released by** |  |
| **Release date** |  |

|  |  |  |
| --- | --- | --- |
| **Document Change History** | | |
| **Version** | **Date** | **Remarks / Reason of change** |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Distribution List** | | | |
| **Name** | **Organization** | **Designation** | **Email Id** |
|  |  |  |  |
|  |  |  |  |

Contents

[**Introduction** 4](#_Toc193797020)

[**Engagement Scope** 5](#_Toc193797021)

[**Details of the Auditing team** 6](#_Toc193797022)

[**Audit Activities and Timelines** 7](#_Toc193797023)

[**Audit Methodology and Criteria / Standard referred for audit** 8](#_Toc193797024)

[**Tools/ Software used** 9](#_Toc193797025)

[**Executive Summary** 10](#_Toc193797026)

[**Detailed Observations** 11](#_Toc193797027)

[**Appendices** 13](#_Toc193797028)

# **Introduction**

|  |  |
| --- | --- |
| Objectives | Status |
| Detection of Vulnerabilities causing Data-Theft or Intrusion on Public Infrastructure | A picture containing drawing  Description automatically generatedCompleted |
| Identification of Critical Vulnerabilities in the CyberSmithSecure Infrastructure | A picture containing drawing  Description automatically generatedCompleted |
| Reporting the Vulnerabilities with Detailed Recommendation & Sharing Proof of Concept | A picture containing drawing  Description automatically generatedCompleted |
| Prioritization of Vulnerabilities for Undergoing Patch Management and Re-Validation | A picture containing drawing  Description automatically generatedCompleted |

The Information security assessment was carried from {{Dec 1st, 2021}}, till {{28th of February 2022}} out to identify the critical threats inside the application, causing the application system to malfunction and/or leak out critical data. The objective of this assessment was to find out critical gaps in different areas, through which malicious intervention could take place resulting in a major impact to Ather Energy.

In this assessment team CyberSmithSECURE went aggressively in terms of identifying critical vulnerabilities as per the guidelines of OWASP Top 10, SANS Top 25 & CWE for the application security side It was emphasized on Business Logic Vulnerabilities to Account Takeover Vulnerabilities and Code Execution Level Vulnerabilities were prioritized ensuring that the application underwent an entirely extensive analysis to counter various critical loopholes through which any sort of logical intrusion can take place externally. Our entire analysis was based on analyzing a series of test cases from Gray box methodology that we analysed on the application for identification of security vulnerabilities on the application side after getting credentials of the application and environment. The overall IT asset analysis for the quarter was decided based on the inventory sheet which was shared with team CyberSmithSECURE during the initial starting of the project.

The Reporting and Triggering of vulnerabilities were provided into excel and pdf. Our approach was not only specifically limited to vulnerability detection but also provided the linkages and strategies to have patch management, remediation explanation by our secure code developer and technical expert was part of the activity, along with project coordinator.

In the Current ongoing Assessment, CyberSmithSECURE had kept the entire higher management of CyberSmithSecure in complete confidence about the schedule and complexity of the range of the attack that was to be exercised and targeted on the public infrastructure. However, denial-based attacks and stress testing were avoided. Participation in security-related meetings for the bug fixations and regular attending bi-weekly meetings were some steps taken forward for achieving the various objectives for the current quarter.

The Applications and Systems underwent different series of testing considering its Current and Future deployment and requirements that the application might be undergoing from the regulatory barriers to industry best practices, all of these were a part of security testing that team CyberSmithSECURE conducted. As a result of our test, the researchers identified a total of 1168 vulnerabilities (8 Critical, 76 High, 519 Medium, 401 Low, and 164 Informational vulnerabilities) in 44 Web Applications, 2 Mobile Application, 236 IPs, 453 Cloud Buckets. The components for the assessment included S3 Buckets, Google Cloud Storage, IP Address, Web Applications, Mobile Application iOS, Android.

The overall vulnerabilities that were identified in the current quarter have been prioritized jointly by the Infrastructure Security Beta team along with the VCISO team for undergoing the patch management process and based on the competition of patch management process from the development team the Re-validation of those vulnerabilities shall be initiated.

In the assessment, it was identified that relevant security strategies and approaches have been taken forward to secure the public-facing IP address and storage components belonging to CyberSmithSecure.

# **Engagement Scope**

*<Below details of assets (whichever is / are applicable based on the type of audit) covered in the scope be included in this section along with other relevant details:>*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S. No. | Asset Description | Criticality of Asset | Internal IP Address | URL | Public IP Address | Location | Hash Value (in case of applications) | Version (in case of applications) | Other details such as make and model in case of network devices or security devices. |

Date up to which the list has been updated: 1952-05-20 00:00:00 (to be shared by Auditee organization with the Auditing organization before commencing the audit assignment)

# **Details of the Auditing team**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S. No | Name | Designation | Email Id | Professional Qualifications/ Certifications | Whether the resource has been listed in the Snapshot information published on CERT-In’s website(Yes/No) |

# **Audit Activities and Timelines**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initial Date | | Revalidation Date | | Report Submission Date |
| Start Date | End Date | Start Date | End Date |
| 2025-02-05 00:00:00 | 2025-02-09 00:00:00 | 2025-07-06 00:00:00 | {{Revalidation End Date}} | {{Report Submission Date}} |

# **Audit Methodology and Criteria / Standard referred for audit**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **Standard / Framework used** | **Severity Score System** | **Other References** |
| 1 | OWASP Top Ten | CVSS 3.1 | [https://owasp.org](https://owasp.org/) |
| 2 | SANS Top 25 Software Errors | CVSS 3.1 | [https://www.sans.org](https://www.sans.org/) |
| 3 | NIST | CVSS 3.1 | <https://www.nist.gov/> |

# **Tools/ Software used**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **Name of Tool / Software used** | **Version of the tool**  **/ Software used** | **Open Source/Licensed** |
| 1. | Nmap | 7.95 | Open Source |
| 2. | Nessus Pro | 10.7.1 | Licensed |
| 3. | Metasploit | 4.22.2-2024061001 | Open Source |
| 4. | Sqlmap | 1.8.5 | Open Source |
| 5. | Dirb | 2.22 | Open Source |
| 6. | BurpSuite Pro | 2024.5.3 | Licensed |

# **Executive Summary**

*<A high-level overview of the key audit findings and vulnerabilities. This section is for senior management to understand business risks. This section should include charts to represent the count of observations severity wise along with list of observations in tabular format as mentioned below >*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S.No | Affected Asset i.e. IP/URL/Application etc | Observation/ Vulnerability title | CVE/CWE | Control Objective | Control Name | Audit Requirement | Severity | Recommendation | Reference | New or  Repeat observation |

# **Detailed Observations**

|  |
| --- |
| **1.** |
| **Affected Asset: {{IP/URL/Application etc.}}** |
| **Vulnerability Name: k12** |
| **Detailed observation: iii** |
| **CVE/CWE: {{ CVE/CWE}}** |
| **Severity: huiii** |
| **Recommendations: ,mnbvftyujk** |
| **Reference: gggy** |
| **New or Repeat observation: ..,>** |
| **Proof of concept and steps of verification with clearly visible screenshots:**  **Step 1: image**  **C:\Users\lopes\Downloads\FB_Final\12\1.png**  **Step 2:image**  **C:\Users\lopes\Downloads\FB_Final\12\2.png** |

|  |
| --- |
| **2.** |
| **Affected Asset: {{IP/URL/Application etc.}}** |
| **Vulnerability Name: k12** |
| **Detailed observation: iii** |
| **CVE/CWE: 555** |
| **Severity: huiii** |
| **Recommendations: ,mnbvftyujk** |
| **Reference: gggy** |
| **New or Repeat observation: ..,>** |
| **Proof of concept and steps of verification with clearly visible screenshots:**  **Step 1: image**  **C:\Users\lopes\Downloads\FB_Final\12\1.png**  **Step 2: {{step2}}**  **C:\Users\lopes\Downloads\FB_Final\12\2.png** |

# **Appendices**

1. **SANS Top 25 Software Errors:** The SANS Top 25 is a list of the most dangerous software errors that can lead to serious vulnerabilities. These errors are frequently exploited by attackers. The list is developed by the SANS Institute in collaboration with other cybersecurity experts and is regularly updated to reflect the evolving threat landscape.  
   Reference - [Top 25 Software Errors | SANS Institute](https://www.sans.org/top25-software-errors/)
2. **OWASP Top Ten**: The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. The list is regularly updated and is globally recognized as the first step towards more secure coding practices.  
   Reference - [OWASP Top Ten | OWASP Foundation](https://owasp.org/www-project-top-ten/)
3. **NIST Cybersecurity Framework:** The National Institute of Standards and Technology (NIST) plays a crucial role in cybersecurity by developing standards, guidelines, and best practices to help organizations manage and reduce cybersecurity risks. NIST's Cybersecurity Framework, provides a policy framework of computer security guidance for how private sector organizations in the U.S. can assess and improve their ability to prevent, detect, and respond to cyberattacks. This framework is widely adopted and helps organizations of all sizes to enhance their cybersecurity posture.

Reference - [National Institute of Standards and Technology](https://www.nist.gov/)

1. **CVE (Common Vulnerabilities and Exposures):** CVE is a list of publicly disclosed computer security flaws. Each flaw is assigned a unique identifier known as a CVE ID, which helps IT professionals coordinate their efforts to prioritize and address these vulnerabilities. The CVE system, maintained by The MITRE Corporation, provides a reference method for publicly known information-security vulnerabilities and exposure.

Reference - [CVE: Common Vulnerabilities and Exposures](https://www.cve.org/)

1. **CWE (Common Weakness Enumeration)**: CWE is a community-developed list of common software and hardware weaknesses that can lead to vulnerabilities. Each CWE entry describes a specific type of weakness that can be exploited to compromise a system. The list helps developers and security professionals understand and mitigate these weaknesses before they can be exploited.

Reference - [CWE - Common Weakness Enumeration](https://cwe.mitre.org/)