****

**SiberTren ID**

**BLACKBOX PENTEST REPORT INTERNAL**

**I. Introduction**

This report contains the results of penetration testing documentation. The objective of the project contract is to identify and validate the findings of unrestricted file upload and misconfiguration vulnerabilities within the web scope as per a nondisclosure agreement.

**II. Security Information**

**Team**

|  |  |
| --- | --- |
| **Role** | **Name** |
| Pentester | Taukhid Aji Nurwijayadi |

**Scope of Work**

Scope of this Penetration testing project

* Web Application

**Time Line**

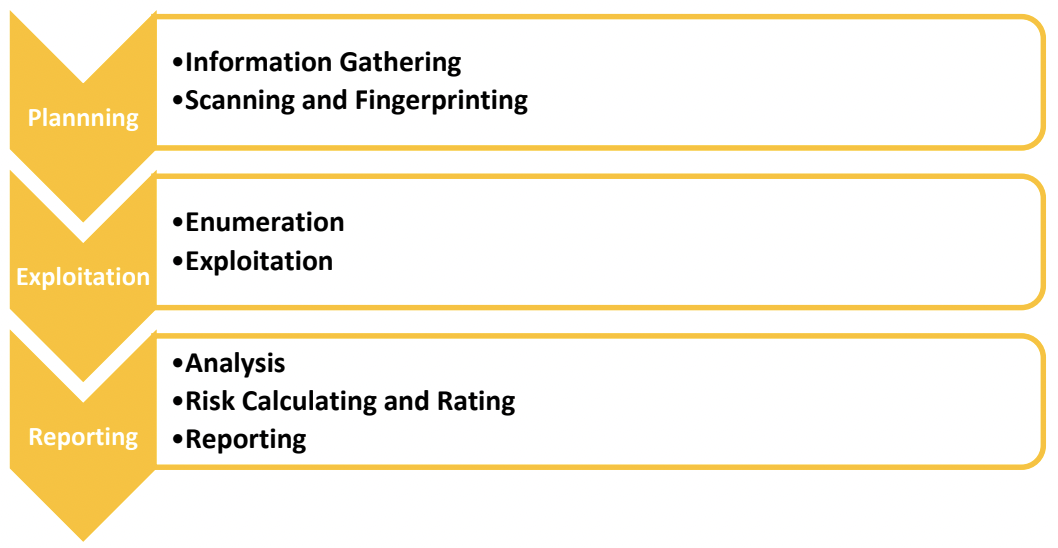
The timeline of this test is as follows:

|  |  |  |
| --- | --- | --- |
| **Scope** | **Start Date/Time** | **End Date/Time** |
| Web Application | 26 November 2022 | 27 November 2022 |

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 26 November 2022 | Initial Reporting lab 1 |

**III. Methodology**



**Security Reference**

Application testing uses references based on OWASP 2017.



**IV. Vulnerability Findings**

|  |  |
| --- | --- |
| **Total Findings** | **Severity** |
| 1 | Low |
| 1 | Critical |

1. [103.250.10.97/Unrestricted%20File%20Upload/] Unrestricted File Upload labs 3

|  |  |
| --- | --- |
| **Bug ID** | SEC-001 |
| **Date Found** | 26 November 2022 |
| **Status** | OPEN |
| **Severity by CVSS 3.1** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N  0.0(None) |
| **Endpoint** | http://103.250.10.97/Unrestricted%20File%20Upload/2 |
| **Method** | GET |
| **Description** | A misconfiguration vulnerability here was found due to an error in the url to load a page that shouldn't be loaded |
| **Security Risk** | None |
| **Recommendation** | Repair from  <http://103.250.10.97/Unrestricted%20File%20Upload/2>  Becomes  [http://103.250.10.97/Unrestricted%20File%20Upload/](http://103.250.10.97/Unrestricted%20File%20Upload/2)3 |
| **Step to**  **Reproduce** | By simply clicking the link button, you can enter pages that are not supposed to be displayed |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated\_Redirects\_and\_Forwards\_Cheat\_Sheet.html |
| **Screenshot Before** |  |
| **Video Proof of Concept** |  |
| **Close Date** |  |

2. [103.250.10.97/Unrestricted%20File%20Upload/3] Unrestricted File Upload labs 3

|  |  |
| --- | --- |
| **Bug ID** | SEC-002 |
| **Date Found** | 26 November 2022 |
| **Status** | OPEN |
| **Severity by CVSS 3.1** | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H  9.0(Critical) |
| **Endpoint** | http://103.250.10.97/Unrestricted%20File%20Upload/3/uploads/wkwk.php?cmd=ls%20-la |
| **Method** | GET |
| **Description** | An Unrestricted File Upload vulnerability that threatens the web has been discovered, which poses a risk to the security of a website and from the server side as well |
| **Security Risk** | * Client side attacks * Uploading malicious files * DDOS attack |
| **Recommendation** | Add extension validation features such as double, null bytes, or extension block validation |
| **Step to**  **Reproduce** | Upload the .jpeg file, and after that do the replacement of the intercept feature on burpsuite, and change the file extension to .php, then do the remote code by calling the file .php according to the file location on the web. Then add the parameter **?cmd=ls -la** |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/File\_Upload\_Cheat\_Sheet.html |
| **Screenshot Before** | Graphical user interface, text  Description automatically generated |
| **Video Proof of Concept** |  |
| **Close Date** |  |

**V. Closing**

I am so grateful for the opportunity to penetrate

testing, I hope the information in this document will be useful to your company. If you have any questions or need further information, please get in touch

one of the following:

* Taukhid Aji Nurwijayadi ([taukhidajin@gmail.com](mailto:taukhidajin@gmail.com))