****

**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 file inclusion 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**

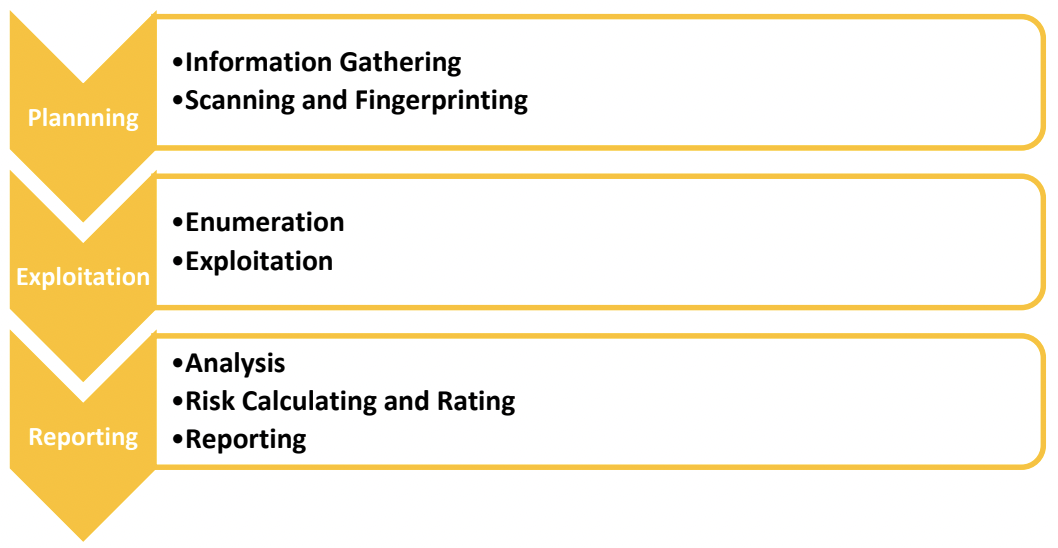
The timeline of this test is as follows:

|  |  |  |
| --- | --- | --- |
| **Scope** | **Start Date/Time** | **End Date/Time** |
| Web Application | 25 November 2022 | 26 November 2022 |

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 25 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 | Medium |

1. [http://103.250.10.97/File%20Inclusion/1/index.php?lang=en.php] File Inclusion Lab 1

|  |  |
| --- | --- |
| **Bug ID** | SEC-001 |
| **Date Found** | 25 November 2022 |
| **Status** | OPEN |
| **Severity by CVSS 3.1** | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L  5.6(Medium) |
| **Endpoint** | http://103.250.10.97/File%20Inclusion/1/index.php?lang=../../../../../etc/passwd |
| **Method** | GET |
| **Description** | The file inclusion vulnerability was discovered when hackers tried to type commands to access a local directory on a website, to be able to view the contents of that web directory. |
| **Security Risk** |  |
| **Recommendation** | By leaving configurations such as allow\_url\_fopen and allow\_url\_include set to On, make sure to change the allow\_url\_fopen and allow\_url\_include settings to Off and disable some PHP functions such as exec, passthru, shell\_exec, system in php.ini and added to disable\_functions. |
| **Step to**  **Reproduce** | By typing **../etc/passwd** in a parameter that appears in the website url, if it's still not visible you can add it again to **../** |
| **More Info** | https://highon.coffee/blog/lfi-cheat-sheet/ |
| **Screenshot Before** |  |
| **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))