****

**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 command injection 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**

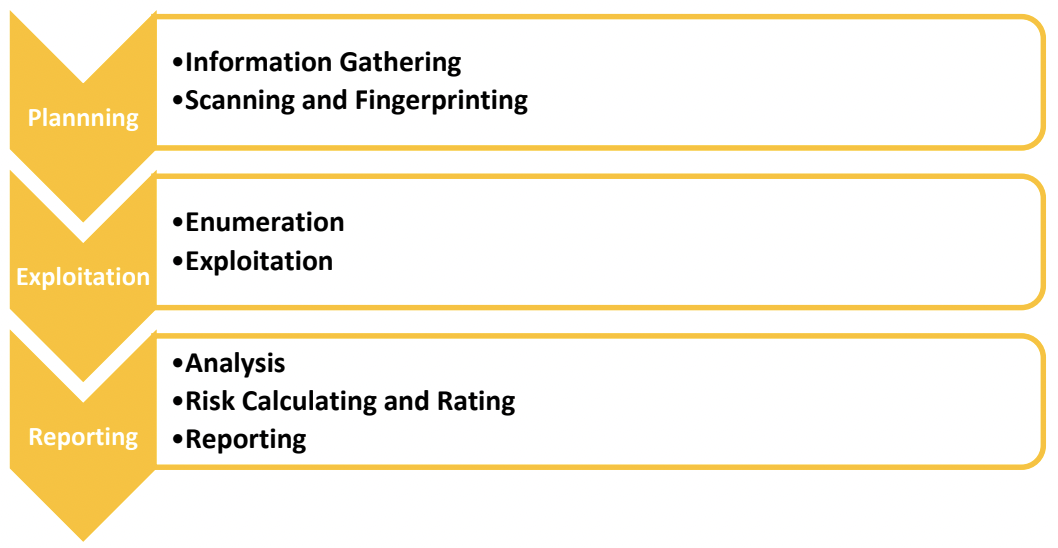
The timeline of this test is as follows:

|  |  |  |
| --- | --- | --- |
| **Scope** | **Start Date/Time** | **End Date/Time** |
| Web Application | 23 November 2022 | 24 November 2022 |

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 23 November 2022 | Initial Reporting lab 1 |

**III. Methodology**



**Security Reference**

Application testing uses references based on OWASP 2017.

Graphical user interface

Description automatically generated

**IV. Vulnerability Findings**

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

1. [103.250.10.97/Command%20Injection/3] Command Injection Lab 3

|  |  |
| --- | --- |
| **Bug ID** | SEC-001 |
| **Date Found** | 23 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/Command%20Injection/3/ |
| **Method** | GET |
| **Description** | The command injection vulnerability was found after the Blind command injection process was carried out through the stages of checking via other labs that were connected to the web, so that a bug was found |
| **Security Risk** | * Data Leak * Someone can insert malicious code easily to be abused |
| **Recommendation** | Just enough to call the file index.php because your web script is the cause of the death of the web |
| **Step to**  **Reproduce** | Please enter this command **;cat index.php**  By running this command you can reactivate your website as before |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/OS\_Command\_Injection\_Defense\_Cheat\_Sheet.html |
| **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))