****

**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 brocken authentication 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**

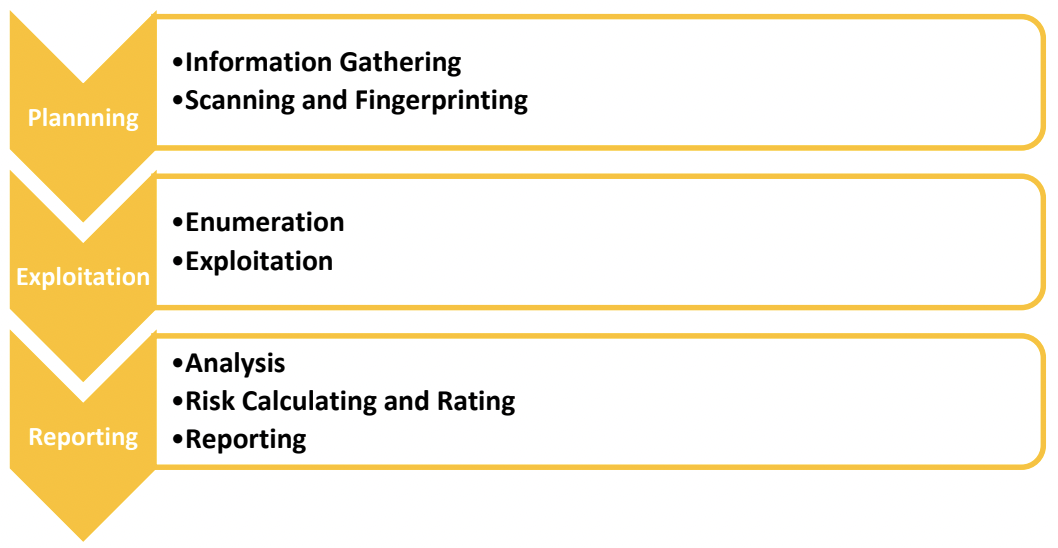
The timeline of this test is as follows:

|  |  |  |
| --- | --- | --- |
| **Scope** | **Start Date/Time** | **End Date/Time** |
| Web Application | 28 November 2022 | 29 November 2022 |

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 28 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 | High |

1. [http://103.250.10.97/Broken%20Authentication/2/] Broken Authentication labs 2

|  |  |
| --- | --- |
| **Bug ID** | SEC-001 |
| **Date Found** | 28 November 2022 |
| **Status** | OPEN |
| **Severity by CVSS 3.1** | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H  8.0(High) |
| **Endpoint** | <http://103.250.10.97/Broken%20Authentication/2/dashboard.php> |
| **Method** | GET |
| **Description** | Broken authentication caused by cookies that can be modified from the client side, risks misuse of data or unwanted things |
| **Security Risk** | * Misuse of confidential data |
| **Recommendation** | Securing cookie data so that it cannot be changed from the client side, you can use a signature in the form of hasing from the session value |
| **Step to**  **Reproduce** | User-Id : attacker Admin : false Signature : Hash(User-Id + Admin) |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/Session\_Management\_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))