****

**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 insecure direct object refrences 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**

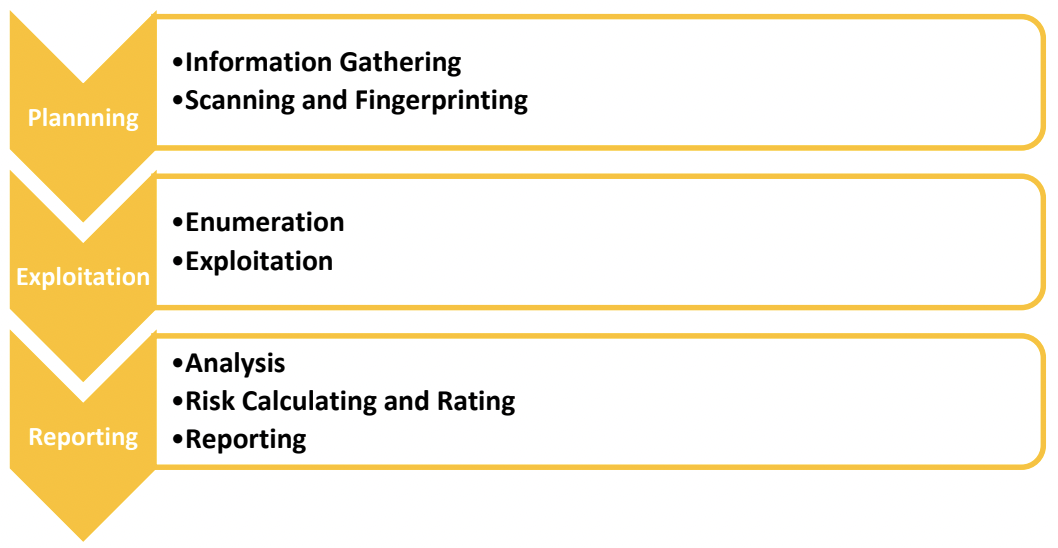
The timeline of this test is as follows:

|  |  |  |
| --- | --- | --- |
| **Scope** | **Start Date/Time** | **End Date/Time** |
| Web Application | 22 November 2022 | 23 November 2022 |

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 22 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. [103.250.10.97/Insecure%20Direct%20Object%20References/2/] IDOR Lab 2

|  |  |
| --- | --- |
| **Bug ID** | SEC-001 |
| **Date Found** | 22 November 2022 |
| **Status** | OPEN |
| **Severity by CVSS 3.1** | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:L  7.5(High) |
| **Endpoint** | http://103.250.10.97/Insecure%20Direct%20Object%20References/2/ |
| **Method** | GET |
| **Description** | The IDOR vulnerability was found when there was a hacker who had 2 accounts or had a friend's account, where the hacker found a loophole that could change the contents of the data by only needing to know the id or certain parameters in the target data or item on another user |
| **Security Risk** | * Steal content * Data Leak |
| **Recommendation** | * An “id” parameter may represent a customer identifier. Using logical validation, it may be checked to ensure authorized access by the user. * An “account” parameter may represent a user’s account. Using logical validation, it may be verified that the information displayed is that of the specific user’s. |
| **Step to**  **Reproduce** | <http://103.250.10.97/Insecure%20Direct%20Object%20References/2/delete-data.php?id=3> to <http://103.250.10.97/Insecure%20Direct%20Object%20References/2/delete-data.php?id=1> |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/Insecure\_Direct\_Object\_Reference\_Prevention\_Cheat\_Sheet.html |
| **Screenshot Before** | Graphical user interface, application  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))