****

**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 sql injection 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**

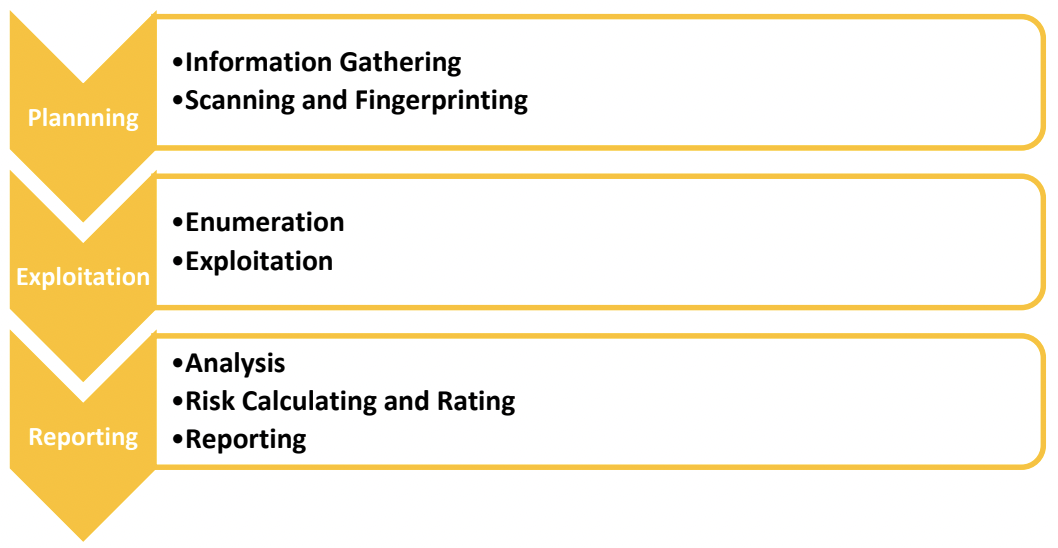
The timeline of this test is as follows:

|  |  |  |
| --- | --- | --- |
| **Scope** | **Start Date/Time** | **End Date/Time** |
| Web Application | 19 November 2022 | 21 November 2022 |

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 19 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 | Critical |
| 1 | Medium |

1. [http://103.250.10.97/SQL%20Injection/3/read.php?id=1] SQL Injection labs 3

|  |  |
| --- | --- |
| **Bug ID** | SEC-001 |
| **Date Found** | 19 Oktober 2022 |
| **Status** | OPEN |
| **Severity by CVSS 3.1** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H  10.0(Critical) |
| **Endpoint** | http://103.250.10.97/SQL%20Injection/3/read.php?id=1 |
| **Method** | GET |
| **Description** | A sql injection vulnerability has been found a parameter in the read.php pageview, where one can risk the sql injection being misused, to get data or something of value |
| **Security Risk** | * Data leak * Administrator account abuse |
| **Recommendation** | Add a validation to the sql command, and add a sql statement to protect tracked data from sql injection cases |
| **Step to**  **Reproduce** | Try to add quotes ' in the parameter ?id=1 to ?id=1' |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/SQL\_Injection\_Prevention\_Cheat\_Sheet.html |
| **Screenshot Before** |  |
| **Video Proof of Concept** |  |
| **Close Date** |  |

2. [http://103.250.10.97:5001/contact] Misconfiguration Lab 3

|  |  |
| --- | --- |
| **Bug ID** | SEC-002 |
| **Date Found** | 20 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://103.250.10.97:5001/contact |
| **Method** |  |
| **Description** | Misunderstanding of the appearance of the web that results in visitors not visiting the site again |
| **Security Risk** | None |
| **Recommendation** | Fix the url so that the web can run normally |
| **Step to**  **Reproduce** | Fix the url to http://103.250.10.97/Misconfiguration/3/ |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated\_Redirects\_and\_Forwards\_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))