****

**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 cross site request forgery 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**

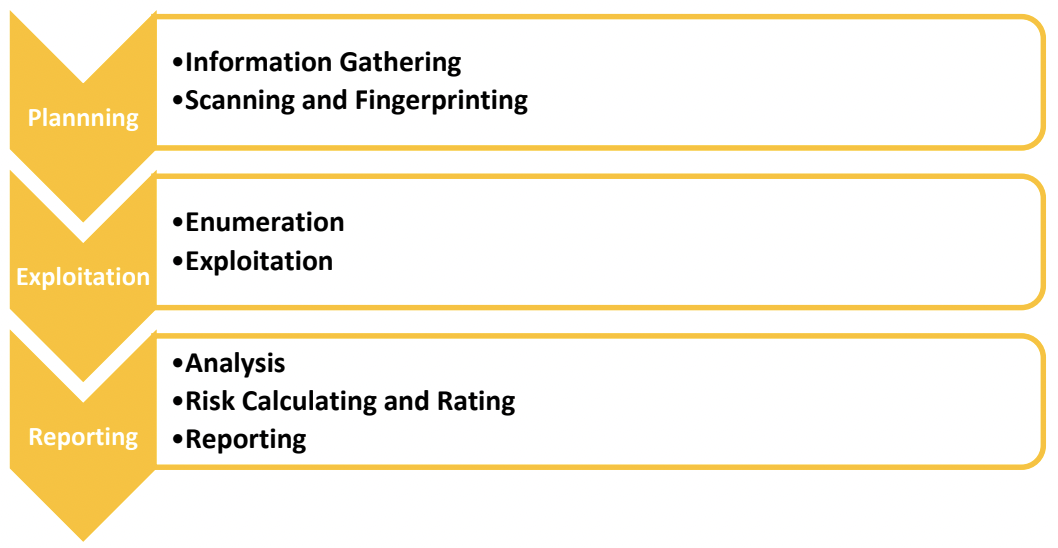
The timeline of this test is as follows:

|  |  |  |
| --- | --- | --- |
| **Scope** | **Start Date/Time** | **End Date/Time** |
| Web Application | 29 November 2022 | 30 November 2022 |

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 29 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/Cross%20Site%20Request%20Forgery/2/] Cross Site Request Forgery 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:H/UI:R/S:C/C:H/I:H/A:H  7.6(High) |
| **Endpoint** | http://103.250.10.97/Cross%20Site%20Request%20Forgery/2/delete-data.php?id=4 |
| **Method** | GET |
| **Description** | The Cross-Site Request Forgery vulnerability was discovered by showing a parameter to the delete button. Which can delete or change data by utilizing an artificial web that can send malicious commands to the target |
| **Security Risk** | * Data abuse * Account takeover * Money laundering |
| **Recommendation** | By adding random token validation or secret token validation so that the website is more secure against crsf attacks |
| **Step to**  **Reproduce** | <body>  <center>  <h1>LASADA</h1>  <h2>SELAMAT ANDA MENDAPATKAN IPHONE</h2>  <p>  <img src="27837-iphone-13.webp"/>  </p>  <a href="http://103.250.10.97/Cross%20Site%20Request%20Forgery/2/delete-data.php?id=4" target="" rel="noopener noreferrer">Klaim Hadiahnya</a>  </center>  </body>  By inserting malicious commands on the website according to what the hacker wants. After that it is distributed to many people, including the target or victim. Thus when the victim opens the web and clicks the button, the data or what the hacker wants will be granted |
| **More Info** | https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site\_Request\_Forgery\_Prevention\_Cheat\_Sheet.html |
| **Screenshot Before** | **After** |
| **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))