****

**SiberTren ID**

**BLACKBOX PENTEST REPORT INTERNAL**

**I. Introduction**

This report contains the results of penetration testing documentation. The goal of the project contract is to identify and validate the findings of the vulnerability in scope

specified in the Non-Disclosure Agreement.

(berisikan detail report pengujian dan goals nya seperti apa)

**II. Security Information**

**Team**

|  |  |
| --- | --- |
| **Role** | **Name** |
| Pentester | Anggi Gunawan |

(Siapakah pelakunya???)

**Scope of Work**

Scope of this Penetration testing project

* Web Application

(Jangkauannya apasaja, seperti web app semua fitur, atau fitur tertentu)

**Time Line**

The timeline of this test is as follows:

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

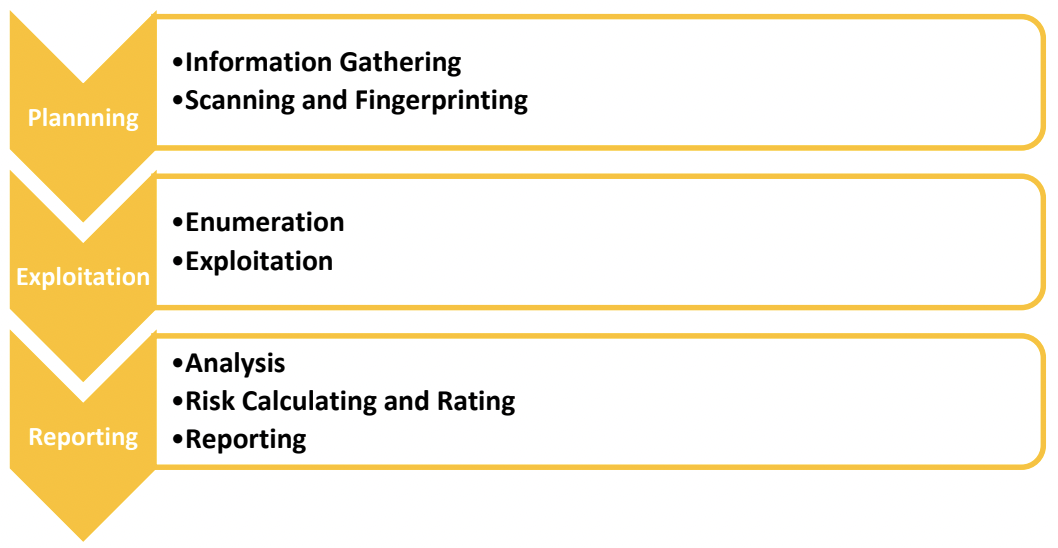
(Waktu pengerjaannya berapa lama)

Version Log

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **State** |
| 1 | 24 Oktober 2022 | Initial Reporting |

(Report tiap versi berisikan tanggal dan lapoae)

**III. Methodology**



(Apa yang sudah dilakukan ketika melakukan Pentesting)

Nb:

- Enumeration adalah memahami aplikasi lebih dalam

- Risk Calculating and Rating adalah melakukan kalkulasi resiko dan rating pada kerusakan yang dialami oleh aplikasi

**Security Reference**

Application testing uses references based on OWASP 2017.



(Apa rekomendasi Owaspnya dari th brp??)

**IV. Vulnerability Findings**

|  |  |
| --- | --- |
| **Total Findings** | **Severity** |
| 2 | Medium |
|  |  |

(Total temuan cela keamanan ada berapa dan levelnya bagaimana?)

1. [api.redacted.com] XSS labs 1

(Disini menjelaskan detail cela keamanan)

|  |  |
| --- | --- |
| **Bug ID** | SEC-001 (Berisikan ID bisa bebas atau menyesuaikan dari perusahaan juga bisa) |
| **Date Found** | 24 Oktober 2022 (Tanggal ditemukan Bugnya) |
| **Status** | OPEN (Apakah bug masih terbuka atau tidak) |
| **Severity by CVSS 3.1** | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N 4.3 (Medium) (Didapatkan dari cara menentukannya pada penjelasan OWASP) |
| **Endpoint** | <http://103.250.10.97/Cross%20Site%20Scripting/1/>  (Berisikan Url ditemukan bug) |
| **Method** | POST (Berisi method GET atau POST) |
| **Description** | Cross site scripting vulnerabilities have been found in the Search feature, where one can enter malicious scripts/payloads into the search field  (Berisikan deskripsi kerentanan) |
| **Security Risk** | * cookie Stealing (Berisi Impactnya apa?) |
| **Recommendation** | sanitize search fields using limit certain characters such  as < > alert  (Berisikan Rekomendasi biar aman) |
| **Step to**  **Reproduce** | 1. Input this payloads <img src=x onerror=prompt(1);> to field Search   when the payloads input is sent it will produce an error message that returns xss popup  (Berisikan referensi bug) |
| **More Info** | * <https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html>   (Link konsepnya) |
| **Screenshot Before** | (Berisikan Video Screenshootnya) |
| **Video Proof of Concept** | (Berisikan Video Konsep) |
| **Close Date** | (Berisi kapan bug ditutup) |

2. [api.redacted.com] File Inclusion labs 1

(Keterangan sama dengan diatas)

|  |  |
| --- | --- |
| **Bug ID** | SEC-002 |
| **Date Found** | 24 Oktober 2022 |
| **Status** | OPEN |
| **Severity by CVSS 3.1** | <https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N> 9.3 (Critical) |
| **Endpoint** | http://103.250.10.97/File%20Inclusion/1/index.php?lang=../../../../../etc/passwd |
| **Method** | GET |
| **Description** | someone can make a call to the /etc/passwd file by exploiting the file inclusion vulnerability |
| **Security Risk** |  |
| **Recommendation** | limit direct calls to endpoints or files directly via url |
| **Step to**  **Reproduce** | 1. Request to url http://103.250.10.97/File%20Inclusion/1/index.php?lang=../../../../../etc/passwd |
| **More Info** |  |
| **Screenshot Before** |  |
| **Video Proof of Concept** |  |
| **Close Date** |  |

**V. Closing**

sibertren.id grateful for the opportunity to perform penetration

testing, we hope that the information in this document will be useful for your

company. If you have any questions or require further information please contact

one of the following :

* Anggi Gunawan ([suling.ninja16@gmail.com](mailto:suling.ninja16@gmail.com))

(Berisikan penjelasan perasaan dan kata2 penutup dan kontak apabila ada bug)