Penetration Testing Report

**Date:** [Date]

**Version:** 0.1

|  |  |
| --- | --- |
| **By** | **For** |
|  | [Company Name]  ID#11111 |
| Pentester 1 - pentester1@zsecuritu.org  Pentester 2 - pentester2@zsecurity.org | John Doe (CTO) - john@companyname.com  Jane Doe (IT Manager) - jane@company.com |

Table of Contents

Executive Summary ............................................................................................................................... 3

1 Engagement Summary.......................................................................................................... 4 1.1 Scope.......................................................................................................................................... 4

1.2 Risk Ratings................................................................................................................................. 4

1.3 Findings Overview....................................................................................................................... 5

2 Technical Details.................................................................................................................. 6 2.1 SQL Injection ……………………………………….......................................................................... 6 2.2 Cross-site Request Forgery ………………………………………….............................................. 7 2.3 Information Disclosure ........................................................................................................................ 8

Legal

Confidentiality

This document contains sensitive and confidential information, it should not be shared with any other 3rd parties without written permission.

GDPR

Disclaimers

…..etc

Change Log

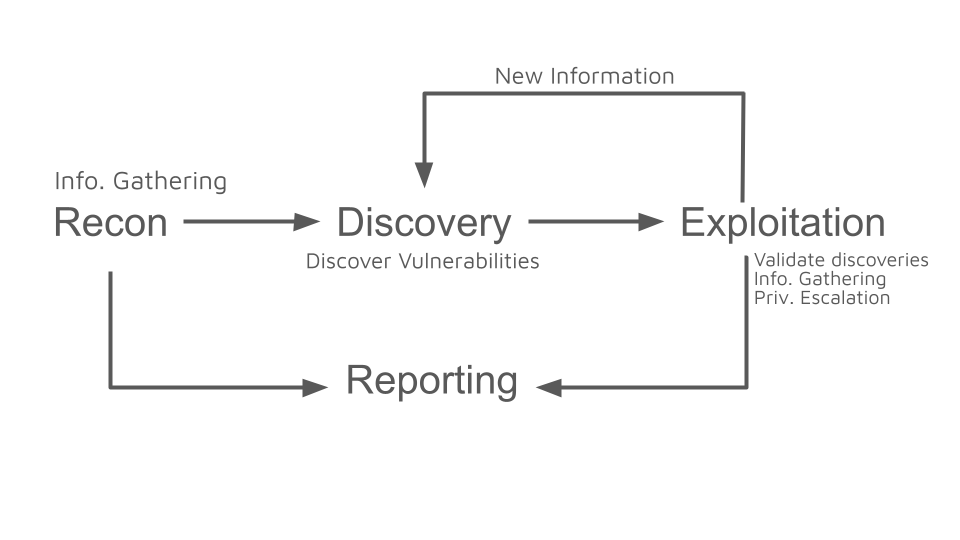
|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Comments** |
| 1/1/2021 | 0.1 | Initial Report |
| 10/1/2021 | 0.2 | Recon Stage |

Executive Summary

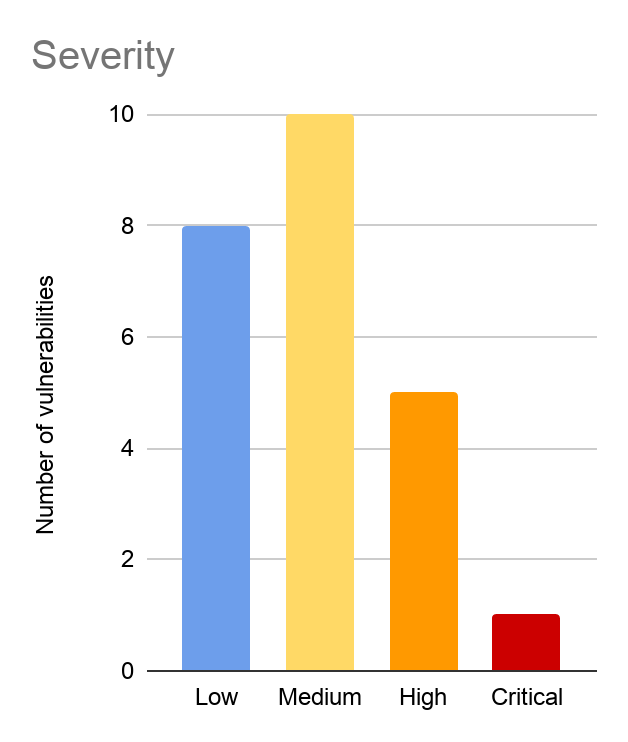
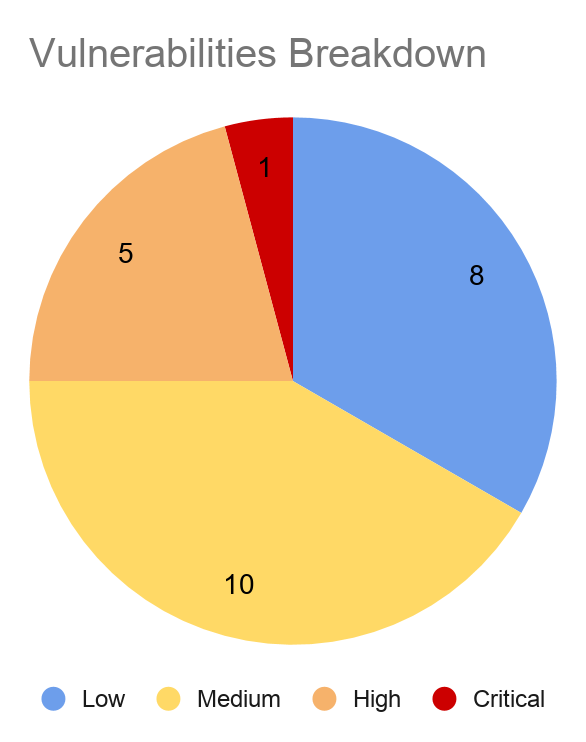
[CompanyName] engaged zSecurity to conduct a security assessment and penetration testing against a [website / app / web application]. The main goal of the engagement was to evaluate the security of the platform and identify possible threats and vulnerabilities.

This report details the scope of the engagement, detailed information about all of the findings and some recommendations. The summary below is intended for non-technical audiences to give an idea of the overall results of the engagement and the key findings. The second section of this report is intended for a technical audience as it lists all of our findings in detail, along with reproduction steps, analysis and recommendations.

Based on the security assessment we carried for [platform] and based on our findings, the current risk rating is high . The vulnerabilities discovered can be used by malicious actors to cause breaches and even gain unauthorised access to some management pages. The methodology followed is detailed in the following diagram:



The following charts summarize the findings grouped by severity of the threat:



1 Engagement Summary

1.1 Scope

As requested the security assessment was only carried out on the following targets:

IP

Domain.com

Subdomain.domain.com

Subdomain2.domain.com

…...etc

1.2 Risk Ratings

The vulnerability risk was calculated based on the [Common Vulnerability Scoring System (CVSS v3.0)](https://nvd.nist.gov/vuln-metrics/cvss) which is the industry standard for assessing the severity of security vulnerabilities.

The table below gives a key to the risk naming and colours used throughout this report to provide a clear and concise risk scoring system.

|  |  |  |
| --- | --- | --- |
| **Risk** | **CVSS v3.0 Score** | **Recommendation** |
| None | 0.0 | N/A |
| Low | 0.1 - 3.9 | Fix at the next update cycle. |
| Medium | 4.0 - 6.9 | Fix immediately if there are 0 medium risk vulnerabilities. |
| High | 7.0 - 8.9 | Fix immediately if there are 0 critical vulnerabilities. |
| Critical | 9.0 - 10.0 | Fix immediately. |

1.3 Findings Overview

Below is a list of all the issues found during the engagement along with a brief description, its impact and the risk rating associated with it. Please refer to the “Risk Ratings” section for more information on how this is calculated.

|  |  |  |
| --- | --- | --- |
| **ID** | **Risk** | **Description** |
| 1 | Critical | SQL Injection leading to unauthorised database access. |
| 2 | Medium | CSRF -Clients can be forced to submit certain non-critical requests. |
| 3 | Low | PHP version disclosure - Can help develop attacks for this specific version. |

2 Technical Details

2.1 SQL Injection **CRITICAL ID:** 1

We discovered that using specially crafted requests a malicious actor can communicate with the database and query it to retrieve stored data including data stored in the *users* tables.

|  |  |
| --- | --- |
| **URL** | https://domain.com/news/post.php |
| **Parameter** | id |
| **References** | https://owasp.org/www-community/attacks/SQL\_Injection |
| **Request** | POST /news/post.php HTTP/1.1  Host: domain.com  Accept: application/json, text/plain, \*/\*  ……………………….. |
| **Response** | HTTP/1.1 200 OK  Content-Type: application/json; charset=utf-8  Vary: Accept-Encoding  ………….... |

**Impact:**

As a result of this vulnerability, a malicious actor can:

1. Query the database and get the database engine, its version and the database user.

2. Retrieve user data.

3. Retrieve hashed passwords from the *users* table.

**Mitigation:**

Use prepared statements with parameterized queries.

Refernces - <https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>.

2.2 Cross-site Request Forgery  **Medium ID:** 2

Description

|  |  |
| --- | --- |
| **URL** |  |
| **Parameter** |  |
| **References** |  |
| **Request** |  |
| **Response** |  |

**Impact:**

**Mitigation:**

2.3 Information Disclosure  **Low ID:** 3

Description

|  |  |
| --- | --- |
| **URL** |  |
| **Parameter** |  |
| **References** |  |
| **Request** |  |
| **Response** |  |

**Impact:**

**Mitigation:**

**CRITICAL**