



Penetration Testing Report

Date: [Date]

Version: 0.1

By	For
zSecurity 9 Robinhood Road, Dublin, Ireland Email: info@zsecurity.org Phone: 011234567	[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 (စီမံကိန်း၏အဓိကအချက်အလက်များ).....	3
1 Engagement Summary(ထိတွေ့ဆက်ဆံမှု အကျဉ်းချုပ်).....	4 1.1
Scope(အခွင့်အလမ်း).....	4
1.2 Risk Ratings(အန္တရာယ်အဆင့်သတ်မှတ်ချက်များ).....	4
1.3 Findings Overview(တွေ့ရှိချက်များ ခြုံငုံသုံးသပ်ချက်).....	5
2 Technica Detail(နည်းပညာဆိုင်ရာအသေးစိတ်).....	6
2.1 SQL Injection	6
2.2 Cross-site Request Forgery	7
2.3 Information Disclosure(သတင်းအချက်အလက် ထုတ်ဖော်ခြင်း။)	8

Confidentiality (လျှို့ဝှက်ချက်)

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

GDPR

Disclaimers(ငြင်းဆိုချက်များ)

.....etc

Change Log

Date	Version	Comments
1/1/2021	0.1	Initial Report(ကနဦးအစီရင်ခံစာ)
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.

စီမံကိန်း၏အဓိကအချက်အလက်များ

[CompanyName] [ဝက်ဘ်ဆိုက်/အက်ပ်/ဝဘ်အက်ပလီကေးရှင်း]ကို လုံခြုံရေးအကဲဖြတ်ခြင်းနှင့် ထိုးဖောက်ဝင်ရောက်မှုစမ်းသပ်မှုပြုလုပ်ရန် zSecurity နှင့် ချိတ်ဆက်ထားသည်။ ထိတွေ့ဆက်ဆံမှု၏ အဓိကရည်ရွယ်ချက်မှာ ပလက်ဖောင်း၏လုံခြုံရေးကို အကဲဖြတ်ရန်နှင့် ဖြစ်နိုင်ချေရှိသော ခြိမ်းခြောက်မှုများနှင့် အားနည်းချက်များကို ဖော်ထုတ်ရန်ဖြစ်သည်။

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.

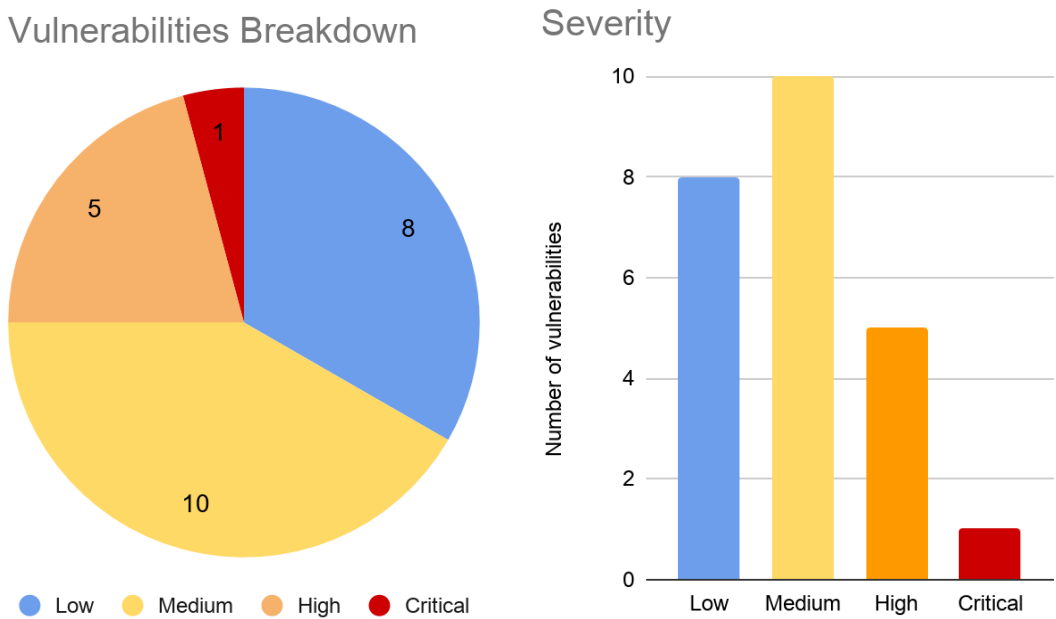
ဤအစီရင်ခံစာတွင် ပါဝင်ပတ်သက်မှုနယ်ပယ်၊ တွေ့ရှိချက်အားလုံးနှင့် အကြံပြုချက်အချို့အကြောင်း အသေးစိတ်အချက်အလက်များကို ဖော်ပြထားသည်။ အောက်ဖော်ပြပါ အကျဉ်းချုပ်သည် ထိတွေ့ဆက်ဆံမှု၏ အလုံးစုံရလဒ်များနှင့် အဓိကတွေ့ရှိချက်များကို အကြံဉာဏ်ပေးရန်အတွက် နည်းပညာမဟုတ်သော ပရိသတ်များအတွက် ရည်ရွယ်ပါသည်။ ဤအစီရင်ခံစာ၏ ဒုတိယအပိုင်းသည် ကျွန်ုပ်တို့၏တွေ့ရှိချက်အားလုံးကို အသေးစိတ်စာရင်းပြုစုထားသောကြောင့် မျိုးပွားခြင်းအဆင့်များ၊ ခွဲခြမ်းစိတ်ဖြာမှုနှင့် အကြံပြုချက်များနှင့်အတူ နည်းပညာဆိုင်ရာ ပရိသတ်များအတွက် ရည်ရွယ်ပါသည်။

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 unauthorized access to some management pages. The methodology followed is detailed in the following diagram:

[ပလက်ဖောင်း] အတွက် ကျွန်ုပ်တို့ဆောင်ရွက်ခဲ့သည့် လုံခြုံရေးအကဲဖြတ်မှုအပေါ် အခြေခံ၍ ကျွန်ုပ်တို့၏တွေ့ရှိချက်များအပေါ် အခြေခံ၍ လက်ရှိအန္တရာယ်အဆင့်သတ်မှတ်ချက်သည် မြင့်မားပါသည်။ တွေ့ရှိရသည့် အားနည်းချက်များကို ဖောက်ဖျက်မှုများဖြစ်စေရန်အတွက် အန္တရာယ်ရှိသော သရုပ်ဆောင်မှုများက အသုံးပြုနိုင်ပြီး အချို့သော စီမံခန့်ခွဲမှုစာမျက်နှာများသို့ ခွင့်ပြုချက်မရှိဘဲ ဝင်ရောက်ခွင့်ကိုပင် ရရှိနိုင်သည်။ လိုက်နာရမည့် နည်းစနစ်ကို အောက်ပါပုံတွင် အသေးစိတ်ဖော်ပြထားသည်။



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 \(CVSS v3.0\)](#) 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:

