Security Assesment Finding Report

FortifyTech

Name : Nicholas Marco Weinandra
NRP: 5027221042
Date: June 1st, 2024

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Praktikan prioritized the assessment to identify the weakest security controls an attacker would exploit. Praktikan recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Assessment Overview

From May 29, 2024 to June 1, 2024, Parkitkan engaged Praktikan to evaluate the security posture of its infrastructure compared to module best practices that included an external penetration test. All testing performed is based on the Module 8-10 customized testing frameworks.

Phases of penetration testing activities include the following:
· Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
· Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
· Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Contact Information

Name	Title	Contact Information
Technology Information - ITS		
Nicholas Marco Weinandra	Pentester	5027221042

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Detail
External Penetration Test	167.172.75.216

Scope Exclusions

Per client request, Pentester did not perform any Denial of Service attacks, any activities that might disrupt the server or database, or any ilegal activities during testing.

Client Allowances

DC did not provide any allowances to assist the testing

Executive Summary

Pentester evaluated DC's external security posture through an external network penetration test from May 5th, 2024 to May 7th, 2024. By leveraging a series of recon method, SQL Injection, XSS (Cross-site Scripting), the pentester found that the website is prone to XSS (Cross-site scripting). By injecting the script in the username column, then updating the data of the account, and re-login to the account, the script was successfully executed. This kind of attack is considered to be Reflected XSS. is a type of web vulnerability that occurs when a malicious script is injected into a web application and is immediately reflected back to the user without being stored on the server. In this case, the username data that has been flushed to remove special characters is not stored on the server. It is proven that after updating the data, the username format remains raw, causing the script to be executed.

Attack Summary

The following table describes how TCMS gained internal network access, step by step:

Step	Action	Recommendation
1	**Managed to successfully run scripts** through the username column after updating the data and re-login. **Script:** </h1><script>alert(100)</script>	● **Sanitize Input**: Ensure that all user inputs are properly sanitized and encoded before reflecting them back in the response. ● **Use Content Security Policy (CSP)**: Implement CSP to restrict the sources from which scripts can be executed. ● **Validate Input**: Perform strict input validation to ensure that only expected data is accepted. ● **Escape Output**: Escape special characters in the output to prevent the execution of injected scripts.
2	**Getting user's cookies through XSS** Script: **</h1><script>alert(document.cookie)</script>**	● **HttpOnly Flag**: Set the HttpOnly attribute on cookies to prevent them from being accessible via JavaScript.

		• **Secure Flag**: Ensure the Secure attribute is set to prevent cookies from being transmitted over non-HTTPS connections. • **SameSite Attribute**: Use the SameSite attribute to protect against cross-site request forgery (CSRF) and some types of XSS attacks by controlling how cookies are sent with cross-origin requests.
3	**Redirecting Users to Malicious Websites Through XSS** Script: **<script>window.location.replace("http://evil.com");</script>**	• **Sanitize Input**: Ensure that all user inputs are properly sanitized and encoded before reflecting them back in the response.

Security Strengths

The Update Data Form is Secure from XSS and SQL Injection

During the assessment, the Pentester found that the Update data form () is secure and is not prone for SQL Injection nor XSS.

Security Weaknesses

Vulnerable to XSS attacks

The signup and login page, are prone for XSS attacks. When the pentester put a script in the username for registering and logging in, then updating the data and re-login, the script was successfully executed. If a website is vulnerable to Cross-Site Scripting (XSS) **attackers**

can steal cookies, users information, session hijacking, phishing attacks, and many more.

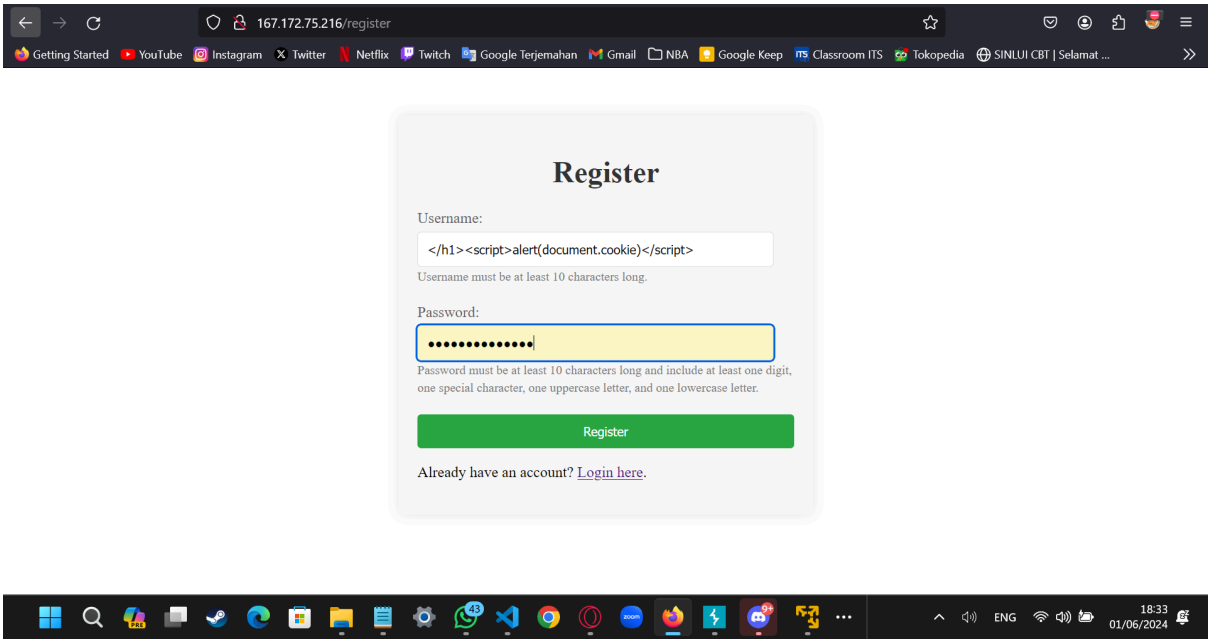
External Penetration Test Findings

XSS Vulnerability - High

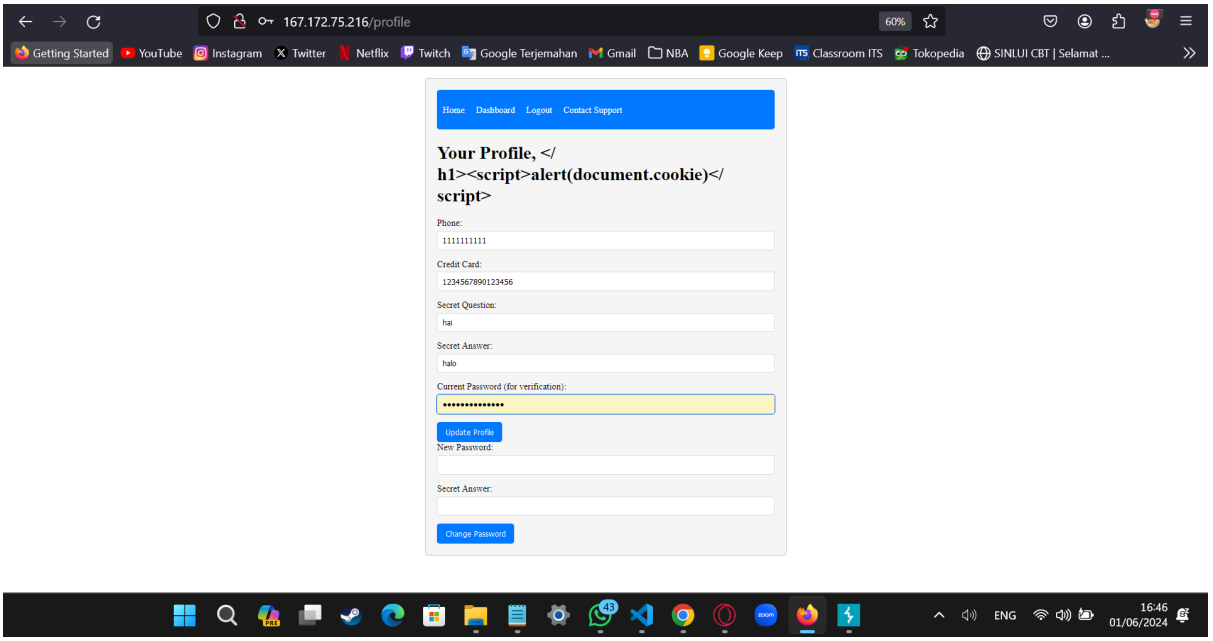
Description:	Vulnerable to Cross-site scripting (Reflected XSS)
Impact:	High
System:	167.172.75.216
References:	CVE-2021-41878 - Reflected XSS

Exploitation Proof of Concept

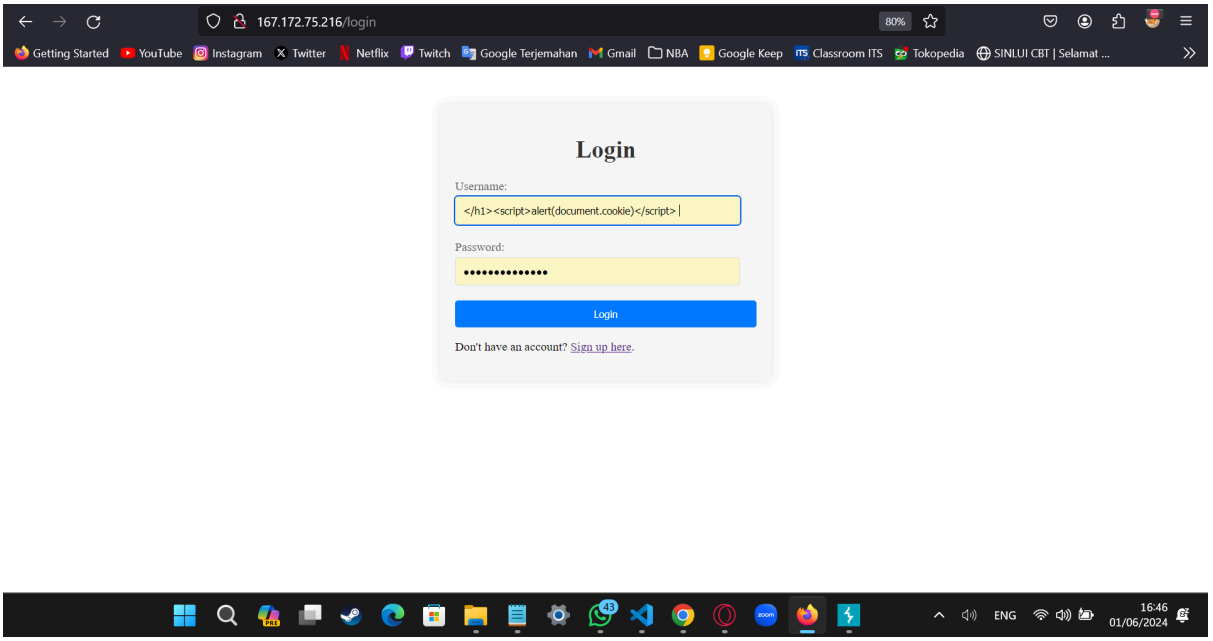
1. Register and login by inputting ***</h1><script>alert(document.cookie)</script>*** (or other malicious script) and input the password



2. After logging in, the script is not yet executed. We must first edit the profile data.

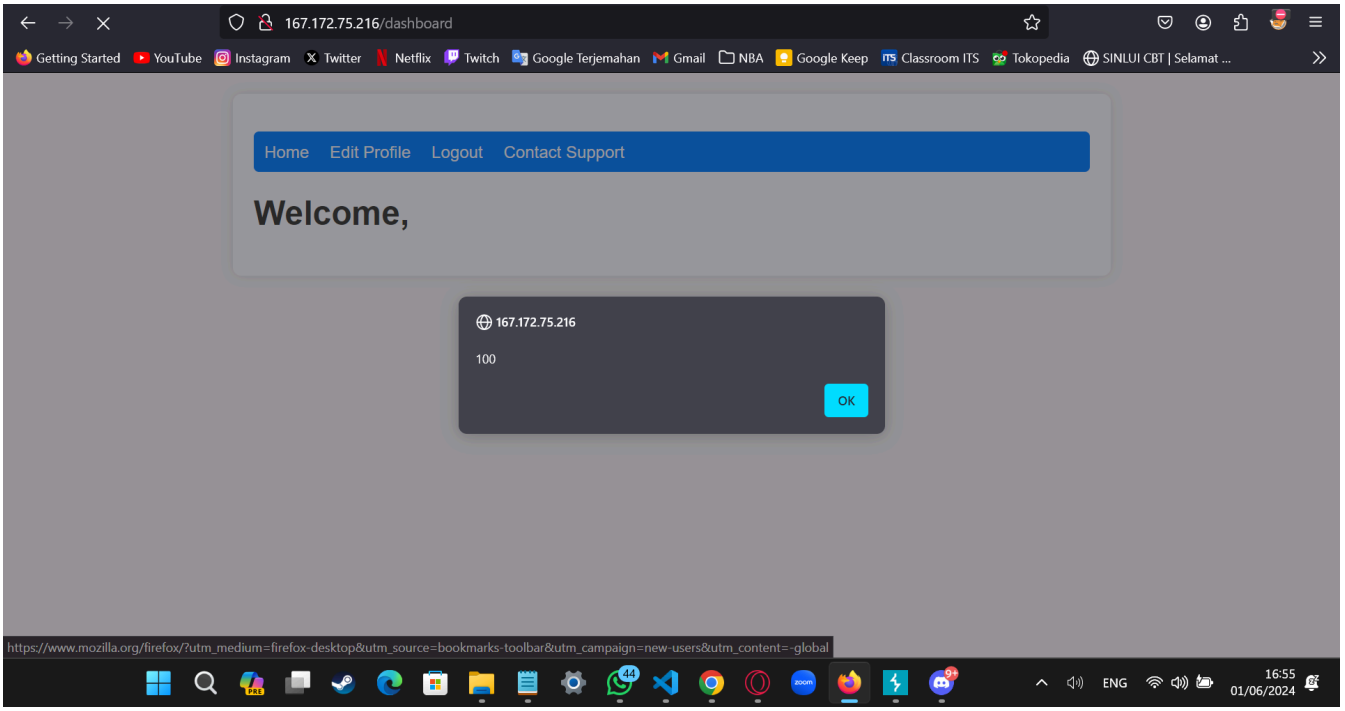


3. Log out then log in again using the same username and password.

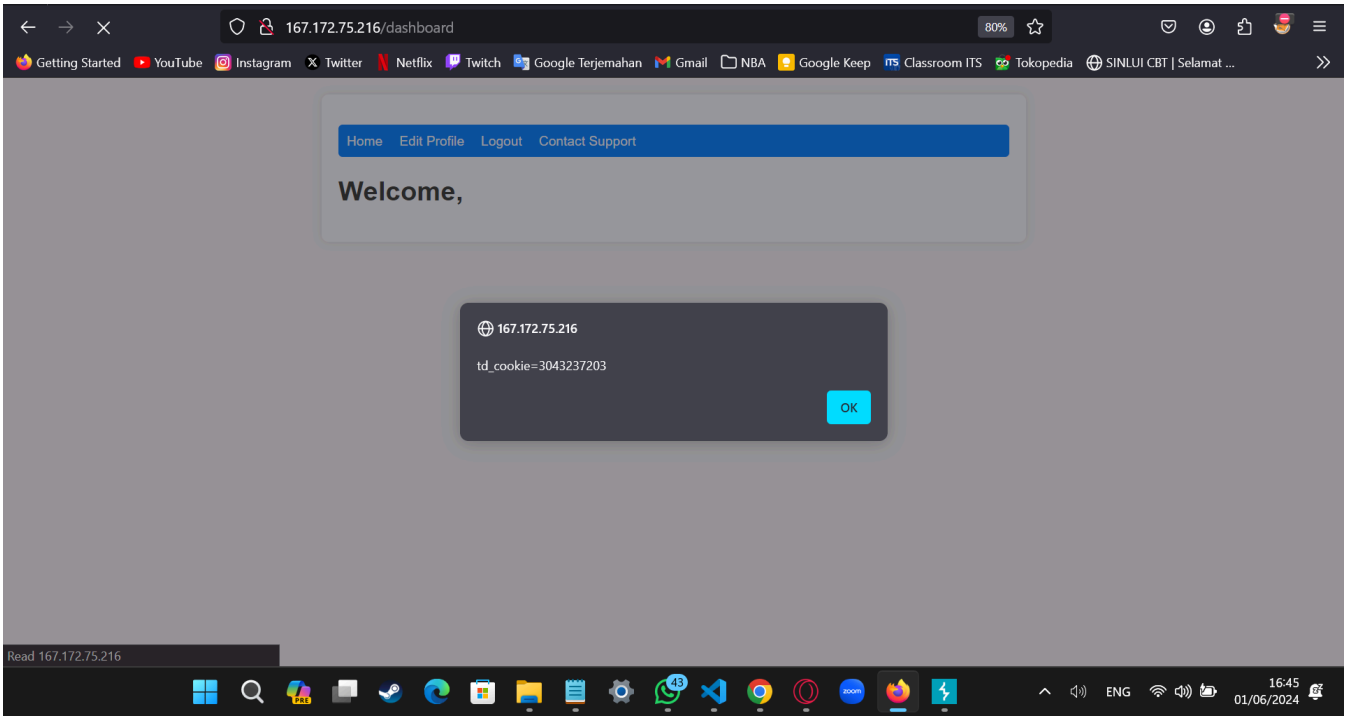


4. **The script will be executed**

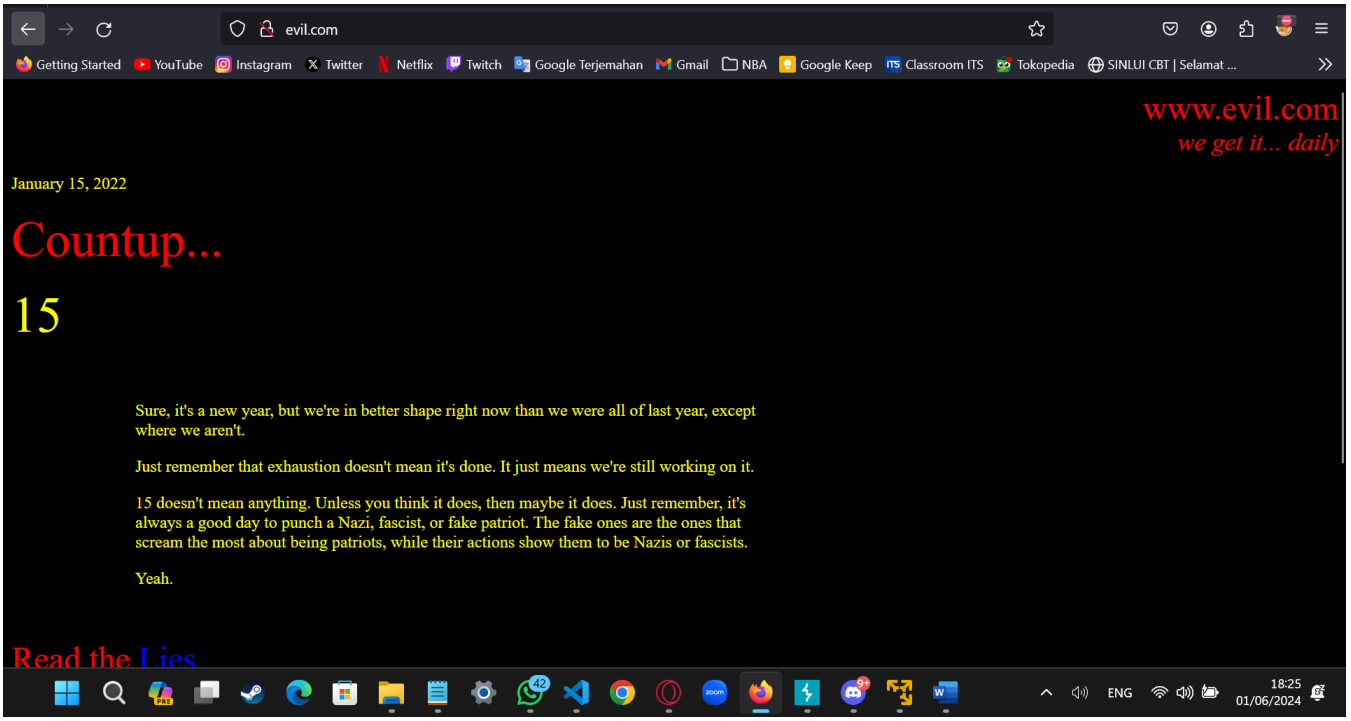
- **</h1><script>alert(100)</script> (Creating a simple alert)**



- **</h1><script>alert(document.cookie)</script> (Accessing users' cookie)**



- **<script>window.location.replace("http://evil.com");</script> (redirecting to another website)**



Additional Reports and Scans

To access additional reports, please refrain from my Github under the additional folders.