JONATHAN ADITHYA BASWARA
5027221062

Demo Pratikum
Security Assessment Findings Report

Business Confidential

Date: May 08th, 2024
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) and JOJO SECURITY (JS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

TCMS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

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. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

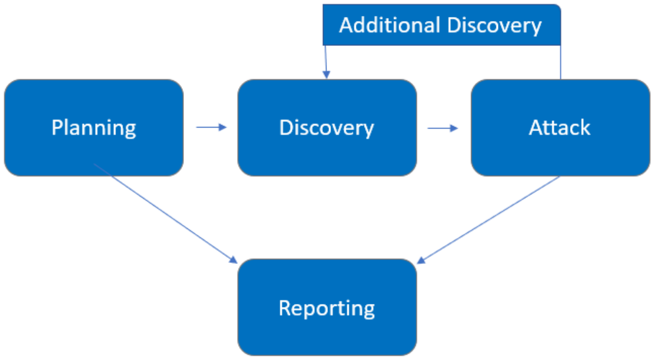
Name	Title	Contact Information
Demo Company		
Jonathan	VP, Information Security (CISO)	Office: (555) 555-5555 Email: jojo@demo.com
Jonathan	IT Manager	Office: (555) 555-5555 Email: jojo@demo.com
Jonathan	Network Engineer	Office: (555) 555-5555 Email: jojo@demo.com
TCM Security		
Jonathan	Lead Penetration Tester	Office: (555) 555-5555 Email: jojo@tcm-sec.com
Jonathan	Penetration Tester	Office: (555) 555-5555 Email: jojo@tcm-sec.com
Jonathan	Account Manager	Office: (555) 555-5555 Email: jojo@tcm-sec.com

Assessment Overview

From May 07th, 2024 to May 08th, 2024, DC engaged JS to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the Modul Pratikum

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- 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.



Assessment Components

External Penetration Test

A JS engineer attempts to recon information using Nmap. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Risk 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/High	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	Details
External Penetration Test	10.15.42.36 10.15.42.7

Scope Exclusions

Per client request, JS did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

Summary 10.15.42.7 Vulnerability Report

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (8.3%)	1 (8.3%)	1 (8.3%)	3 (25.0%)
	Low	0 (0.0%)	1 (8.3%)	4 (33.3%)	0 (0.0%)	5 (41.7%)
	Informational	0 (0.0%)	0 (0.0%)	2 (16.7%)	2 (16.7%)	4 (33.3%)
	Total	0 (0.0%)	2 (16.7%)	7 (58.3%)	3 (25.0%)	12 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

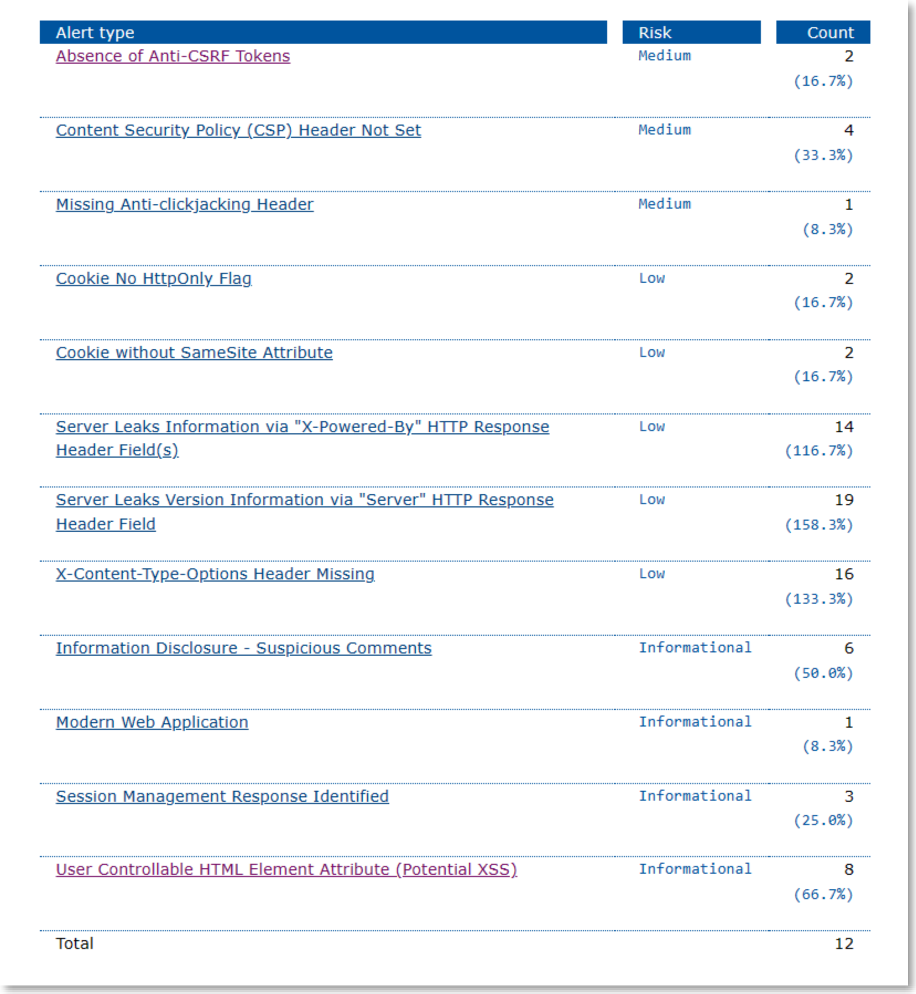
(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://10.15.42.7	0 (0)	3 (3)	5 (8)	4 (12)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)



Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	2 (16.7%)
Content Security Policy (CSP) Header Not Set	Medium	4 (33.3%)
Missing Anti-clickjacking Header	Medium	1 (8.3%)
Cookie No HttpOnly Flag	Low	2 (16.7%)
Cookie without SameSite Attribute	Low	2 (16.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	14 (116.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	19 (158.3%)
X-Content-Type-Options Header Missing	Low	16 (133.3%)
Information Disclosure - Suspicious Comments	Informational	6 (50.0%)
Modern Web Application	Informational	1 (8.3%)
Session Management Response Identified	Informational	3 (25.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	8 (66.7%)
Total		12

Summary 10.15.42.36 Vulnerability Report

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	3 (37.5%)
	Low	0 (0.0%)	1 (12.5%)	2 (25.0%)	0 (0.0%)	3 (37.5%)
	Informational	0 (0.0%)	1 (12.5%)	0 (0.0%)	1 (12.5%)	2 (25.0%)
	Total	0 (0.0%)	3 (37.5%)	3 (37.5%)	2 (25.0%)	8 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://10.15.42.36:8888	0 (0)	2 (2)	2 (4)	0 (4)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	2 (25.0%)
Content Security Policy (CSP) Header Not Set	Medium	4 (50.0%)
Missing Anti-clickjacking Header	Medium	2 (25.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	2 (25.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4 (50.0%)
X-Content-Type-Options Header Missing	Low	2 (25.0%)
Authentication Request Identified	Informational	1 (12.5%)
GET for POST	Informational	1 (12.5%)
Total		8

Additional Reports and Scans (Informational)

JOJO SECURITY provides all clients with all report information gathered during testing. This includes vulnerability scans and a solution to the detailed findings. For more information, please see the html file in the included folder

JOJO SECURITY

Last Page