



Jay's Bank Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: DC-001
Version 1.0

Table of Contents

Table of Contents.....	2
Confidentiality Statement.....	4
Disclaimer.....	4
Contact Information	4
Assessment Overview	5
Assessment Components	5
Internal Penetration Test.....	5
Finding Severity Ratings	6
Risk Factors.....	6
Likelihood	6
Impact.....	6
Scope.....	7
Scope Exclusions	7
Client Allowances	7
Executive Summary	8
Scoping and Time Limitations	8
Testing Summary	8
Tester Notes and Recommendations	9
Key Strengths and Weaknesses	10
Vulnerability Summary & Report Card.....	11
Internal Penetration Test Findings.....	11
Technical Findings	13
Internal Penetration Test Findings.....	13
Finding IPT-001: Insufficient LLMNR Configuration (Critical)	13
Finding IPT-002: Security Misconfiguration – Local Admin Password Reuse (Critical)	14
Finding IPT-003: Security Misconfiguration – WDigest (Critical)	15
Finding IPT-004: Insufficient Hardening – Token Impersonation (Critical)	16
Finding IPT-005: Insufficient Password Complexity (Critical).....	17
Finding IPT-006: Security Misconfiguration – IPv6 (Critical).....	18
Finding IPT-007: Insufficient Hardening – SMB Signing Disabled (Critical).....	19
Finding IPT-008: Insufficient Patch Management – Software (Critical)	20
Finding IPT-009: Insufficient Patch Management – Operating Systems (Critical).....	21
Finding IPT-010: Insufficient Patching – MS08-067 - ECLIPSEDWING/NETAPI (Critical).....	22
Finding IPT-011: Insufficient Patching – MS12-020 – Remote Desktop RCE (Critical)	23
Finding IPT-012: Insufficient Patching – MS17-010 - EternalBlue (Critical)	24
Finding IPT-013: Insufficient Patching – CVE-2019-0708 - BlueKeep (Critical)	25
Finding IPT-014: Insufficient Privileged Account Management – Kerberoasting (High).....	26

Finding IPT-015: Security Misconfiguration – GPP Credentials (High)	27
Finding IPT-016: Insufficient Authentication - VNC (High).....	28
Finding IPT-017: Default Credentials on Web Services (High).....	29
Finding IPT-018: Insufficient Hardening – Listable Directories (High)	30
Finding IPT-019: Unauthenticated SMB Share Access (Moderate).....	31
Finding IPT-020: Insufficient Patch Management – SMBv1 (Moderate)	32
Finding IPT-021: IPMI Hash Disclosure (Moderate)	33
Finding IPT-022: Insufficient SNMP Community String Complexity (Moderate).....	34
Finding IPT-023: Insufficient Data in Transit Encryption - Telnet (Moderate)	35
Finding IPT-024: Insufficient Terminal Services Configuration (Moderate).....	36
Finding IPT-025: Steps to Domain Admin (Informational)	37
Additional Scans and Reports	37

Confidentiality Statement

This document is the exclusive property of Demo Corp and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Demo Corp and TCMS.

Demo Corp 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

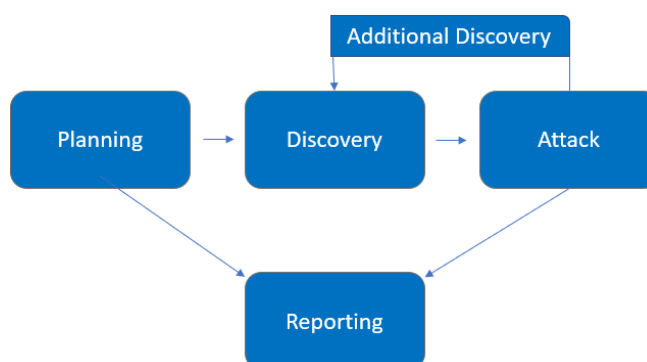
Name	Title	Contact Information
Mohammad Arkananta Radithya Taratugang	5027221003	Email: arkaradithya47@gmail.com

Assessment Overview

From May 28th, 2024 to June 1st, 2024, FortifyTech engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment*, OWASP *Testing Guide (v4)*, and customized testing frameworks.

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

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man-in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

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.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	167.172.75.216

Scope Exclusions

Per client request, TCMS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Demo Corp.

Client Allowances

Demo Corp provided TCMS the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

Safeguard Solutions evaluated Jay's Bank's internal security posture through penetration testing from February 22nd, 2021 to March 5th, 2021. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

1. Application IP Address: 167.172.75.216
2. All application functions.
3. User account and authentication mechanism.
4. Web interface and API.
5. Database interaction and data handling processes.
6. You are allowed to search for and identify vulnerabilities in Jay's Bank application.
7. Focus on application vulnerabilities such as SQL injection, XSS, and authentication/authorization issues.
8. If possible, vulnerabilities found can be exploited to access other user accounts, but only within the application (not on the server).

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)
2. Mimikatz detected on some machines
3. Service accounts were not running as domain administrators
4. Demo Corp local administrator account password was unique to each device

The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Critically out-of-date operating systems and weak patching exist within the network
3. Passwords were observed in cleartext due to WDigest
4. LLMNR is enabled within the network
5. SMB signing is disabled on all non-server devices in the work
6. IPv6 is improperly managed within the network
7. User accounts can be impersonated through token delegation
8. Local admin accounts had password re-use and were overly permissive
9. Default credentials were discovered on critical infrastructure, such as iDRACs
10. Unauthenticated share access was permitted

11. User accounts were found to be running as service accounts
12. Service accounts utilized weak passwords
13. Domain administrator utilized weak passwords

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

0	0	3	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
<u>Internal Penetration Test</u>		
Absence of Anti-SCRF Tokens	Moderate	
CSP: Wildcard Directive	Moderate	
Vulnerable to Cross Site Scripting	Moderate	

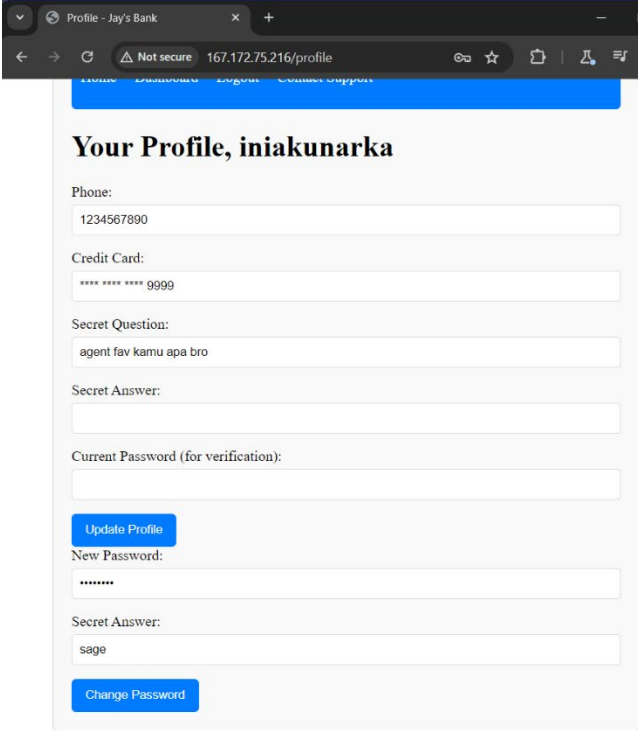
Technical Findings

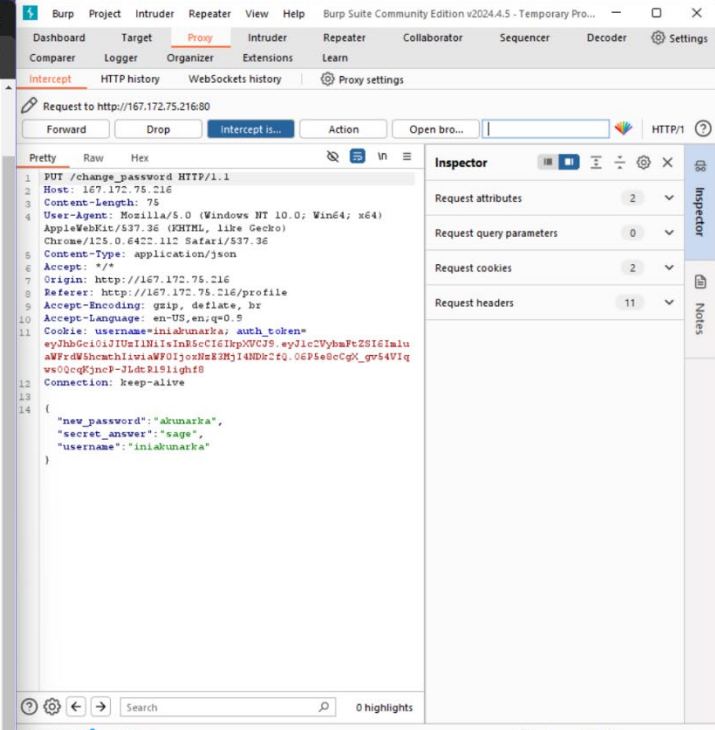
Internal Penetration Test Findings

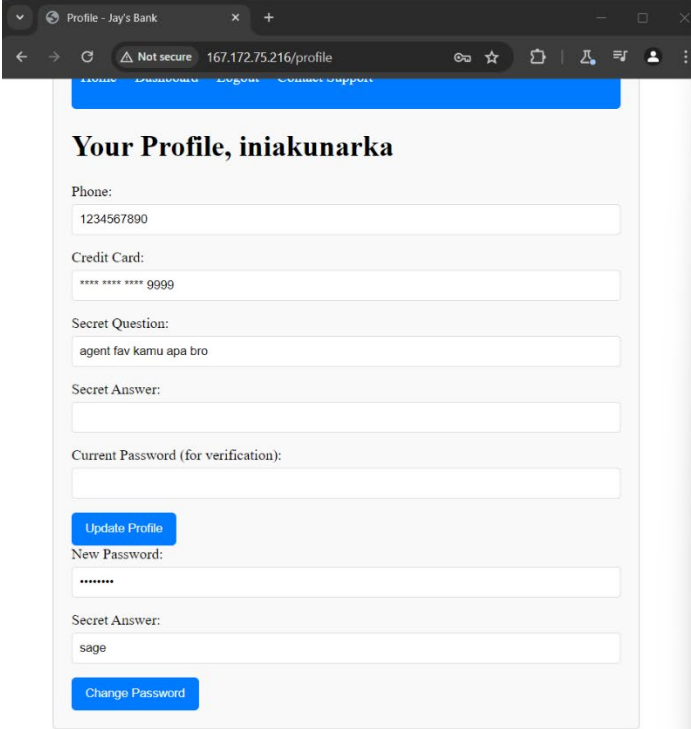
Vulnerable to Cross Site Scripting

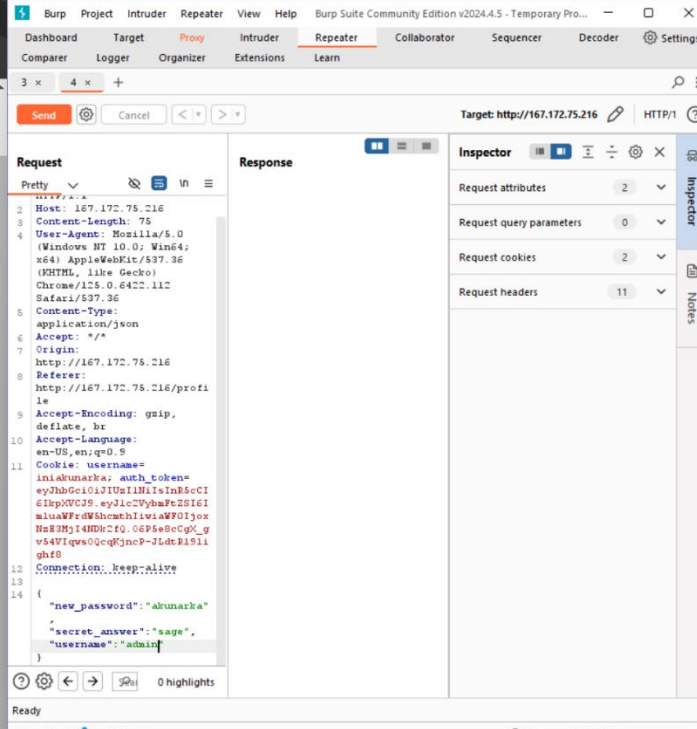
Description:	Vulnerable to Cross Site Scripting
Risk:	Moderate
System:	All
Tools Used:	Burp Suite

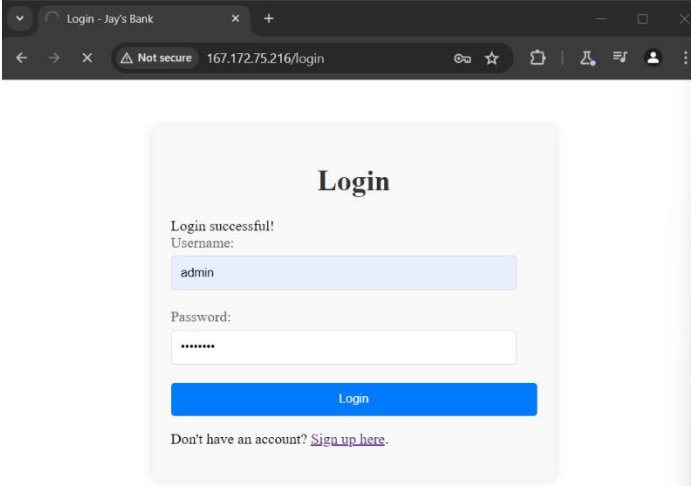
References:

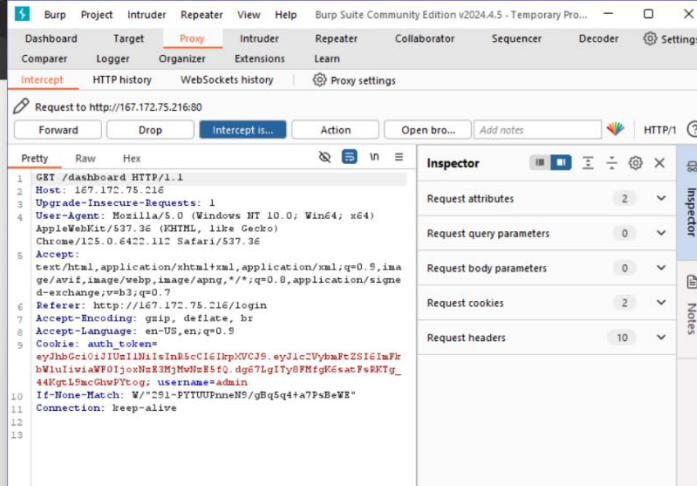


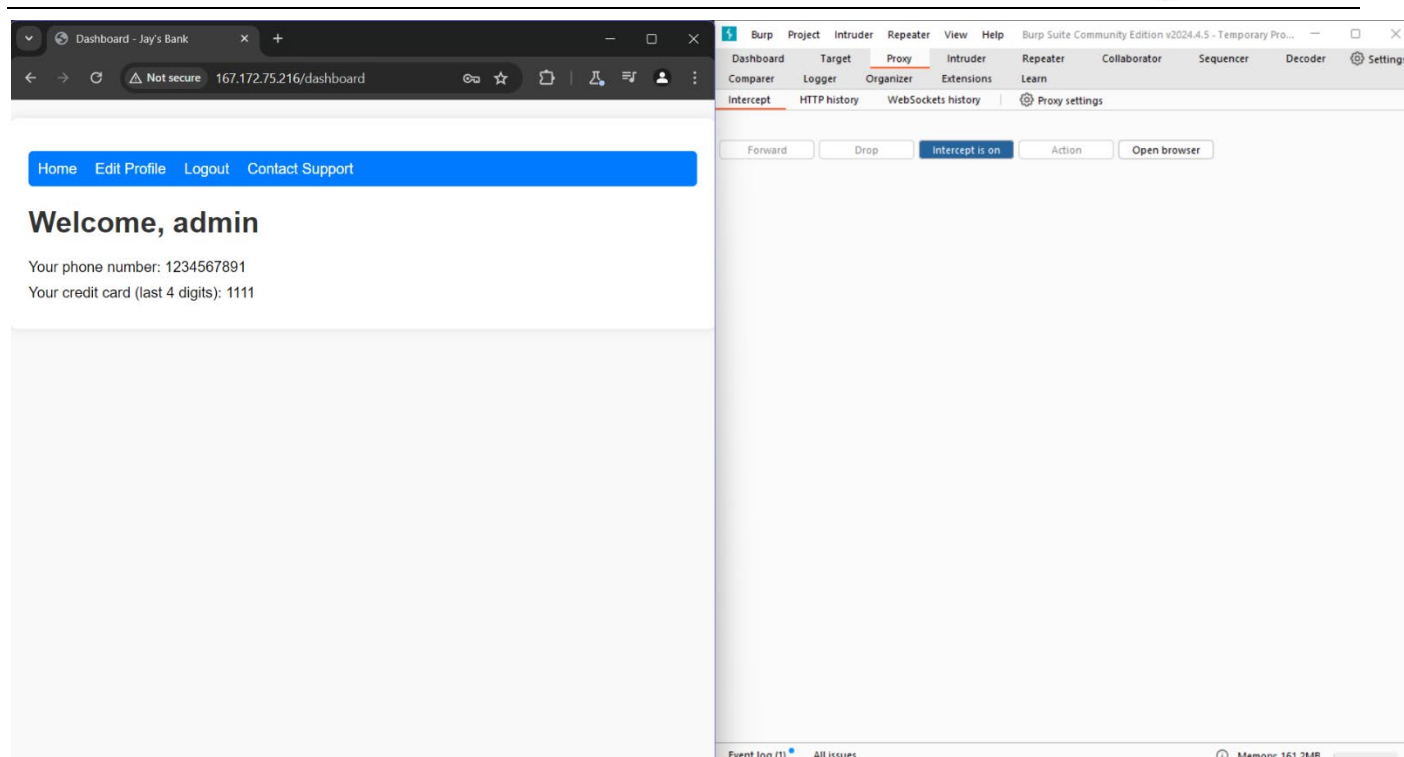












Absence of Anti-CSRF Tokens

Description:	When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, then it might be possible for an attacker to trick a client into making an unintentional request to the web server which will be treated as an authentic request. This can be done via a URL, image load, XMLHttpRequest, etc. and can result in exposure of data or unintended code execution.
Risk:	Moderate
System:	All
Tools Used:	ZAP

References:	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
-------------	--

CSP: Wildcard Directive

Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
Risk:	Moderate
System:	All
Tools Used:	ZAP
References:	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

