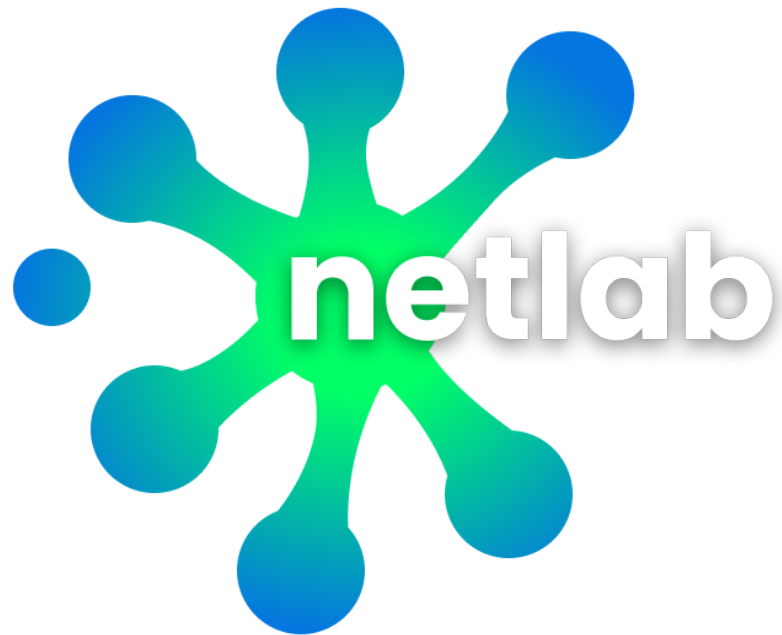


**PROYEK AKHIR
KEAMANAN JARINGAN 2023**



**Leonardo Jeremy Pong Pare Munda
2106707914**

**Mikhael Morris Hapataran Siallagan
2106731491**

BAB 1

Pendahuluan dan Latar Belakang

a. Latar Belakang

Keamanan jaringan merupakan aspek penting dalam dunia teknologi informasi. Dalam era di mana komunikasi dan pertukaran data semakin meluas, risiko keamanan juga semakin meningkat. Salah satu tantangan utama dalam keamanan jaringan adalah pemahaman dan penanganan terhadap serangan seperti Insecure Direct Object Reference (IDOR) dan Privilege Escalation.

Insecure Direct Object Reference (IDOR) merujuk pada kondisi di mana aplikasi atau sistem tidak memvalidasi dengan benar hak akses pengguna terhadap objek-objek tertentu. Serangan IDOR memungkinkan penyerang untuk mengakses atau memanipulasi objek-objek yang seharusnya tidak dapat diakses oleh pengguna yang tidak memiliki otorisasi.

Sementara itu, Privilege Escalation merupakan teknik yang digunakan oleh penyerang untuk memperoleh akses yang lebih tinggi atau hak istimewa dari yang seharusnya mereka miliki. Hal ini bisa terjadi karena adanya celah keamanan di sistem yang memungkinkan penyerang untuk mendapatkan kontrol atau hak akses yang lebih tinggi daripada yang seharusnya dimilikinya.

b. Pendahuluan

Dalam proyek akhir ini, fokus kelompok kami adalah untuk mengetahui lebih dalam mengenai serangan keamanan jaringan yang berkaitan dengan Insecure Direct Object Reference (IDOR) dan Privilege Escalation. Kami akan melakukan analisis mendalam terhadap kedua jenis serangan ini, termasuk cara kerja, potensi dampaknya terhadap sistem yang rentan, serta strategi perlindungan dan pencegahan yang dapat diimplementasikan untuk mengurangi risiko keamanan.

Dalam pengerjaan proyek ini, kami akan membuat target dummy agar terhindar dari aksi yang merugikan pihak lain. Kemudian kita akan melakukan pengujian penyerangan terhadap target tersebut. Setelah itu akan dianalisis bagaimana penyerangan tersebut dapat berhasil dan proses penyerangannya. Lalu kami akan mencari tahu bagaimana vulnerability dari target bisa diatasi. Dan akhirnya menguji coba kembali penyerangan untuk memastikan bahwa vulnerability sudah tidak ada

BAB 2 Implementasi

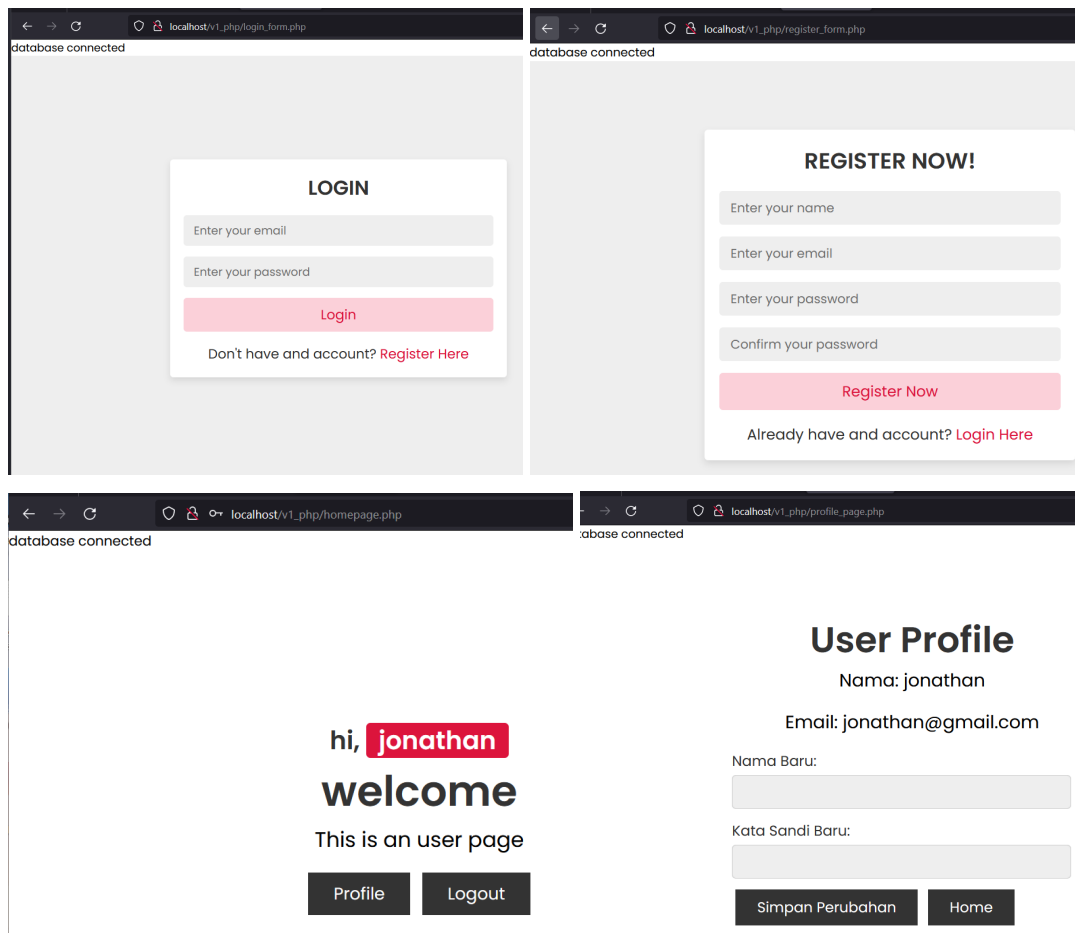
a. Target Creation

Target merupakan sebuah website dummy yang dibuat dengan bahasa PHP. Website terdiri dari login, register, user homepage, user profile, dan admin page. Untuk login admin diperlukan login menggunakan email dan password tertentu, sedangkan untuk sisi user dapat melakukan register dan bisa dilakukan login. Pada home user terdapat profile page untuk melihat profile user dan bisa mengganti nama dan password. Disini kita akan melakukan pentest dimana apakah user a dapat mengakses profile user b dan user-user lainnya, dan juga apakah user dapat mengakses admin page.

b. Enumeration

Stack website : PHP

Overview website:



The image displays four screenshots of a dummy website interface:

- Login Page:** Shows a "LOGIN" form with fields for "Enter your email" and "Enter your password", a "Login" button, and a link "Don't have an account? Register Here".
- Register Page:** Shows a "REGISTER NOW!" form with fields for "Enter your name", "Enter your email", "Enter your password", and "Confirm your password", a "Register Now" button, and a link "Already have an account? Login Here".
- Homepage:** Shows a greeting "hi, jonathan" with a red highlight on "jonathan", a "welcome" message, and the text "This is an user page". It includes "Profile" and "Logout" buttons.
- User Profile Page:** Shows a "User Profile" section with "Nama: jonathan" and "Email: jonathan@gmail.com". It includes input fields for "Nama Baru:" and "Kata Sandi Baru:", and "Simpan Perubahan" and "Home" buttons.

Kemungkinan vulnerabilities: IDOR, Privilege Escalation,

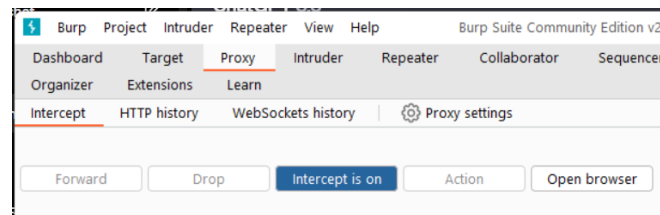
c. Vulnerabilities:

1. IDOR

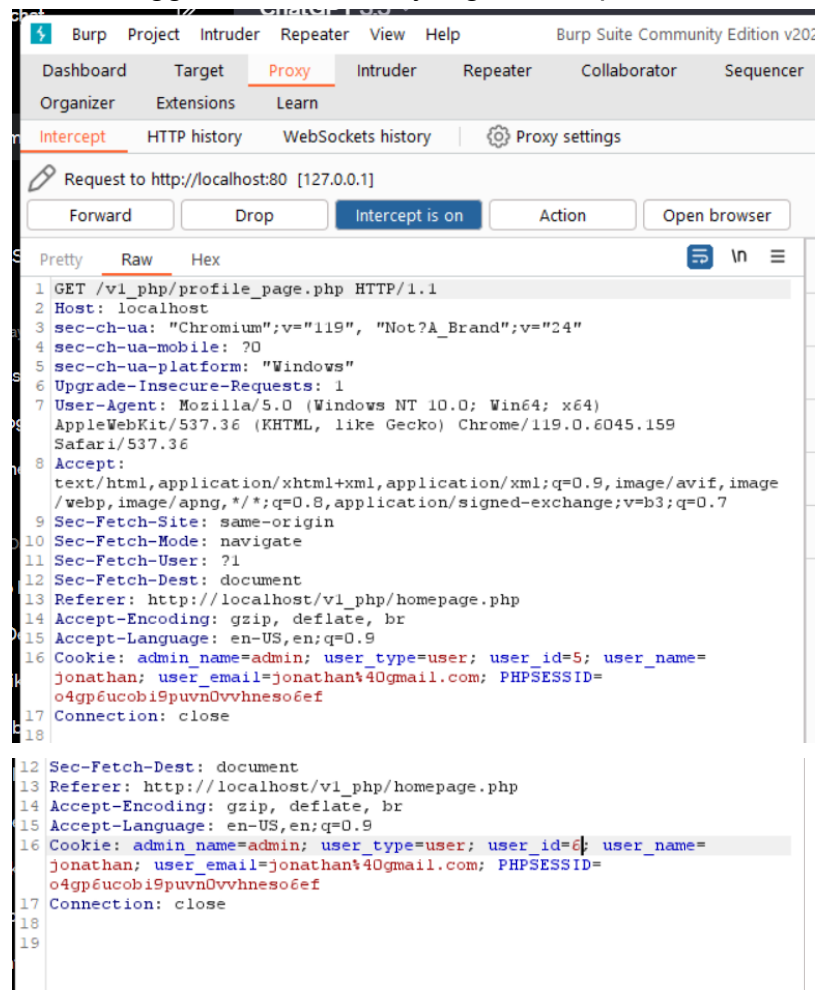
a. Exploitation

Tools yang akan dimanfaatkan untuk exploit adalah menggunakan Burp Suite.

Pertama kita akan melakukan intercept pada localhost, jalankan website pada browser yang sudah terintegrasi dengan Burp Suite, lakukan login hingga masuk ke user profile.



Saat men-click Profile, lakukan intercept burp suite. Dimana kita akan mengganti id dari user yang berada pada cookie tersebut.



Mari kita ganti user_id, misal menjadi 6, maka profile yang akan ditampilkan bukan profile akun jonathan, melainkan profile dari user dengan id 6.

User Profile

Nama: banserUI

Email: banser@banser.co.id

Nama Baru:

Kata Sandi Baru:

Simpan Perubahan

Home

Seharusnya jika login sebagai jonathan, maka kita hanya bisa melihat user profile akun jonathan. Lalu kita coba ganti nama dan katasandi baru untuk akun dengan id 6. Jika berganti maka bisa dibilang IDOR ini berjalan.

User Profile

Nama: banserUI

Email: banser@banser.co.id

Nama Baru:

banser kota depok

Kata Sandi Baru:

.....

Simpan Perubahan

Home

← → ↺ ⓘ localhost/v1_php/update_profile.php

database connectedPerubahan disimpan!

Mari kita login ulang untuk user id = 6 dan lihat user profilnya.

hi, **banser kota depok**

welcome

This is an user page

[Profile](#)[Logout](#)

User Profile

Nama: banser kota depok

Email: banser@banser.co.id

Nama Baru:

Kata Sandi Baru:

[Simpan Perubahan](#)[Home](#)

Dapat dilihat hasilnya user dengan id jika dilakukan login ulang dengan password yang telah di-set baru sebelumnya dapat dilakukan dan juga nama dari user juga ikut berubah.

b. Remediation

Terdapat beberapa langkah yang dapat dilakukan, seperti:

- Validasi jika ingin masuk ke homepage, profile page

```
<?php
@include 'config.php';

session_start();

if (!isset($_SESSION['user_id'])) {
    header('Location: login_form.php');
    exit();
}
```

```
<?php
// Masukkan file konfigurasi
@include 'config.php';

session_start();

// // Periksa apakah user sudah login...

if (!isset($_SESSION['user_id'])) {
    header('Location: login_form.php');
    exit();
}
```

- Menerapkan Cookie + Session

```

<?php
@include 'config.php';

session_start();

if(isset($_POST['submit'])){
    $email = mysqli_real_escape_string($conn, $_POST['email']);
    // $pass = $_POST['password'];
    $pass = password_hash($_POST['password'], PASSWORD_DEFAULT);

    $select = " SELECT * FROM users WHERE email = '$email'";
    $result = mysqli_query($conn, $select);

    if(mysqli_num_rows($result) > 0){
        $row = mysqli_fetch_array($result);

        if(password_verify($password, $row['password'])){
            $_SESSION['user_id'] = $row['id'];
            $_SESSION['user_type'] = ($row['email'] === 'admin@admin.com') ? 'admin' : 'user';
            $_SESSION['user_name'] = $row['name'];
            $_SESSION['user_email'] = $row['email'];

            if ($_SESSION['user_type'] === 'admin') {
                setcookie('user_type', 'admin', time() + (86400 * 30), "/");
                setcookie('admin_name', $row['name'], time() + (86400 * 30), "/");
                header('Location: admin_page.php');
            } else {
                setcookie('user_type', 'user', time() + (86400 * 30), "/");
                setcookie('user_name', $row['name'], time() + (86400 * 30), "/");
                setcookie('user_email', $row['email'], time() + (86400 * 30), "/");
                header('Location: homepage.php');
            }
            exit();
        } else {
            $error[] = 'Incorrect email or password!';
        }
    } else {
        $error[] = 'User not found!';
    }
}

// if(mysqli_num_rows($result) > 0){ ...
}
}

```

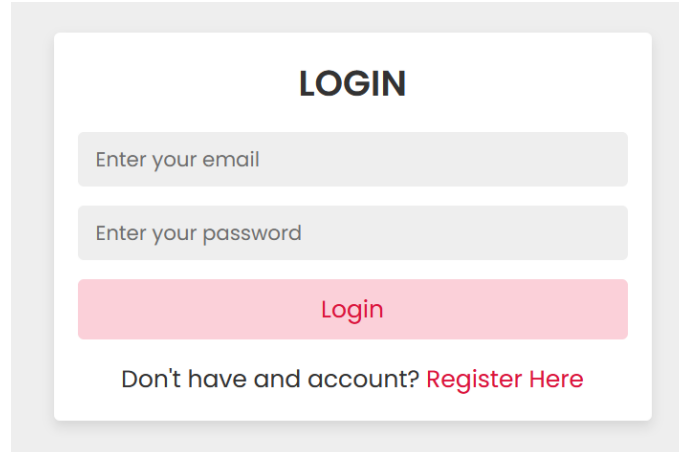
c. Proof

- Validasi jika ingin masuk ke homepage, profile page
Mencoba mengakses /homepage.php tanpa login

LOGIN

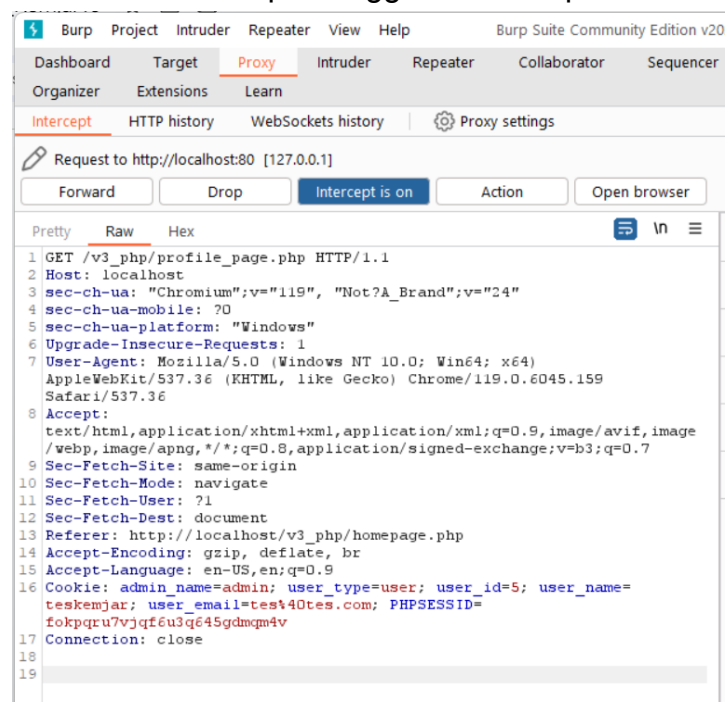
Don't have an account? [Register Here](#)

Mencoba mengakses /profile_page.php tanpa login



Jika dilihat, ketika mengakses kedua route tersebut akan di-return pada page login karena belum ada session yang terbentuk.

- Menerapkan cookies dan session
Melakukan intercept menggunakan Burp Suite.



Dan jika di-forward, maka akan tetap pada profile tes1 yang muncul, bukan profile id 5. (id tes1 adalah 6)

User Profile

Nama: tes1

Email: tes1@tes.com

Nama Baru:

Kata Sandi Baru:

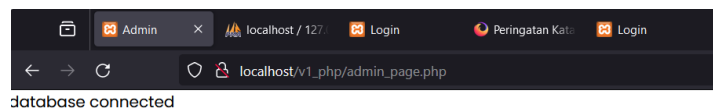
Simpan Perubahan

Home

2. Privilege Escalation

a. Exploitation

Metode eksploitasi pertama adalah langsung mengakses link `localhost/v1_php/admin_page.php` tanpa melakukan login. Dapat dilihat bahwa kita dapat mengakses langsung `admin_page.php` tanpa adanya login.

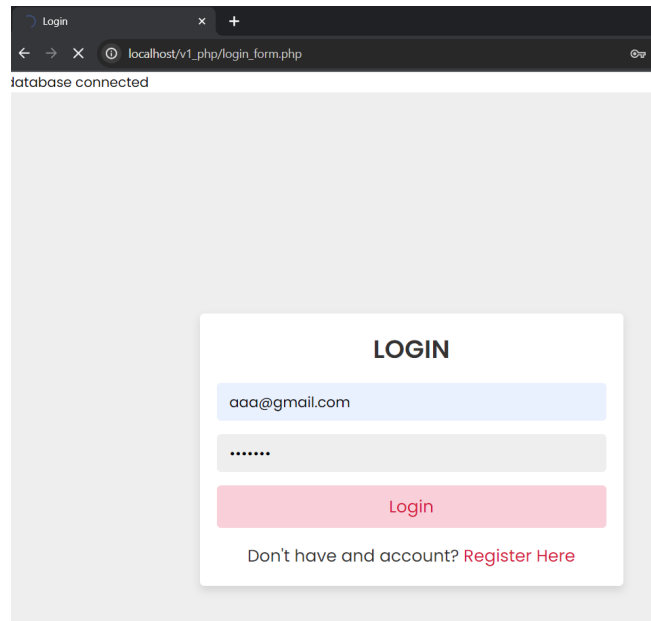


hi, **admin**

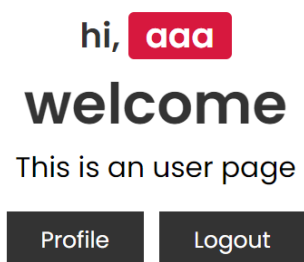
welcome admin

This is an admin page

Logout



Metode kedua adalah dengan memanfaatkan IDOR vulnerability untuk mengakses id dari admin. Attacker dapat memanfaatkan dengan mencoba brute force id secara satu per satu hingga mendapatkan akun admin dan bisa memanfaatkan fitur ganti password admin dan bisa mengakses privilege admin.



User Profile

Nama: admin

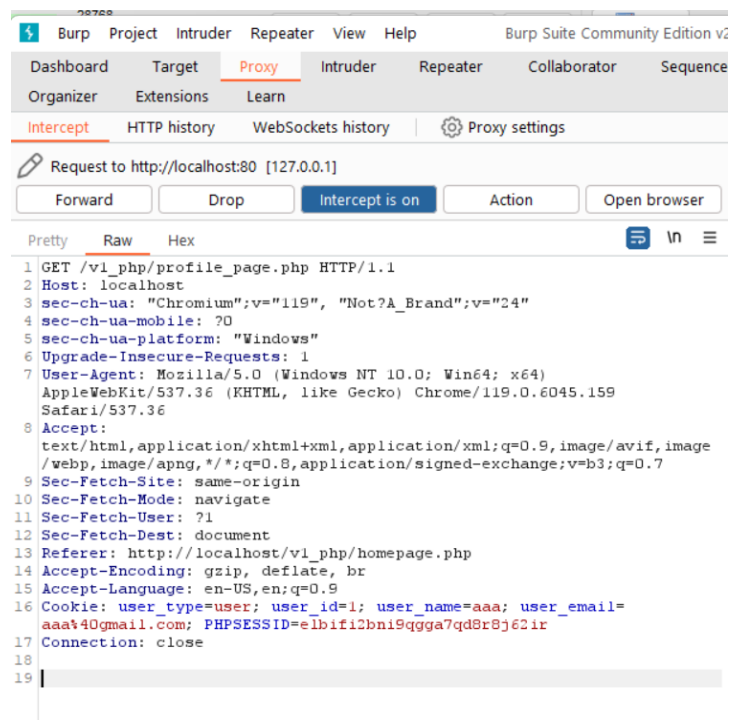
Email: admin@admin.com

Nama Baru:

Kata Sandi Baru:

Simpan Perubahan

Home



b. Remediation

Langkah pencegahan yang dapat dilakukan secara bersamaan dengan IDOR. Hal ini dikarenakan kedua vulnerability bisa saling terkait, dimana jika ada IDOR maka ada kemungkinan Privilege Escalation dapat dilakukan. Berikut tindakan pencegahannya:

- Validasi admin_page agar login terlebih dahulu.

```

in_page.php > html > body
<?php

@include 'config.php';

session_start();
session_regenerate_id(true);

// Periksa apakah session user_type sudah ditandai sebagai admin
if (!isset($_COOKIE['user_type']) || $_COOKIE['user_type'] !== 'admin') {
    header('Location: login_form.php');
    exit();
}
?>

```

- Menggunakan cookies/session

```

if(isset($_POST['submit'])) {
    $email = mysqli_real_escape_string($conn, $_POST['email']);
    $pass = $_POST['password'];
    //$hashedPass = password_hash($pass, PASSWORD_BCRYPT);

    $select = "SELECT * FROM user1 WHERE email = '$email'";
    $result = mysqli_query($conn, $select);

    if($result && mysqli_num_rows($result) > 0) {
        $row = mysqli_fetch_assoc($result);
        $dbPass = $row['password'];

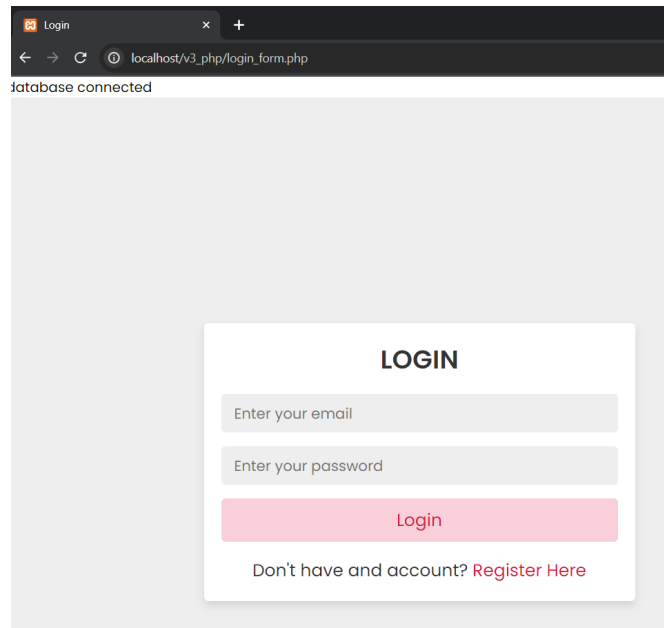
        if(password_verify($pass, $dbPass)) {
            $_SESSION['user_id'] = $row['id'];
            $_SESSION['user_type'] = ($row['email'] === 'admin@admin.com') ? 'admin' : 'user';
            $_SESSION['user_name'] = $row['name'];
            $_SESSION['user_email'] = $row['email'];

            if ($_SESSION['user_type'] === 'admin') {
                setcookie('user_type', 'admin', time() + 3600, "/");
                setcookie('admin_name', $row['name'], time() + 3600, "/");
                header('Location: admin_page.php');
            } else {
                //setcookie('user_type', 'user', time() + (86400 * 30), "/");
                //setcookie('user_name', $row['name'], time() + (86400 * 30), "/");
                //setcookie('user_email', $row['email'], time() + (86400 * 30), "/");
                header('Location: homepage.php');
            }
            exit();
        } else {
            $error[] = 'Incorrect email or password!';
        }
    } else {
        $error[] = 'User not found!';
    }
}
?>

```

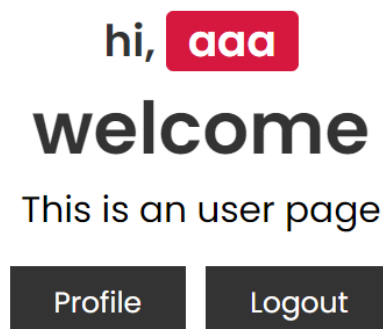
c. Proof

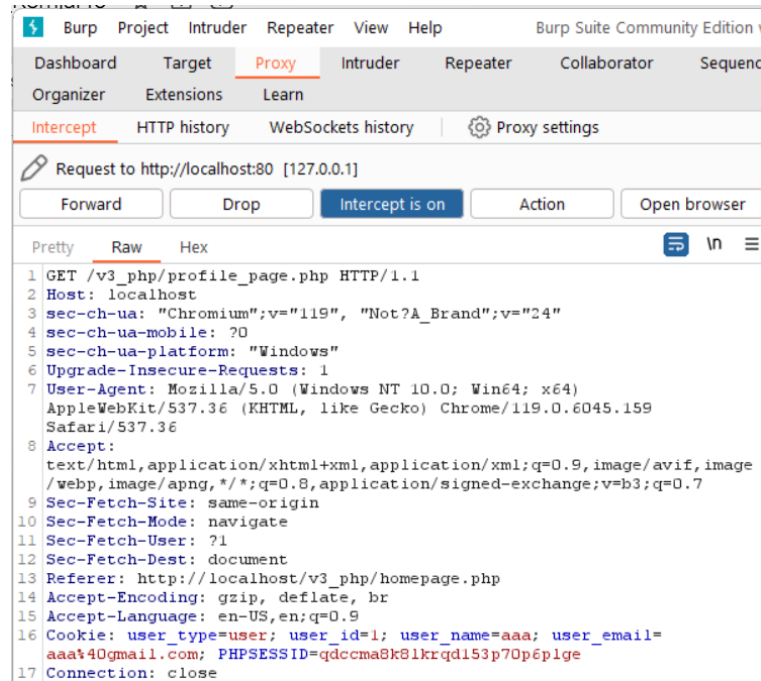
Pertama kita akan mencoba mengakses langsung melalui route `localhost/v3_php/admin_page.php`, tanpa melakukan login terlebih dahulu.



Dapat dilihat bahwa, ketika mengakses `admin_page` secara langsung tanpa login tidak bisa dan langsung diarahkan ke login page agar login terlebih dahulu.

Lalu kita akan melakukan intercept menggunakan Burp Suite untuk mencoba mengganti id dari user menjadi id admin dan melihat apakah bisa dilakukan kembali.





```

1 GET /v3_php/profile_page.php HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: http://localhost/v3_php/homepage.php
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Cookie: user_type=user; user_id=1; user_name=aaa; user_email=
  aaa@gmail.com; PHPSESSID=qdcccma8k8lkrqdl53p7Op6plge
17 Connection: close
  
```

Dapat dilihat, ketika mengganti user id menjadi 1 yang menjadi id dari admin. Lalu dilakukan forward, dan dapat dilihat ketika melihat profile akan tetap pada user profile akun dengan email aaa@gmail.com

User Profile

Nama: aaa

Email: aaa@gmail.com

Nama Baru:

Kata Sandi Baru:

Simpan Perubahan

Home

BAB 3

Kesimpulan

Pada proyek akhir untuk praktikum keamanan jaringan ini, dilakukan percobaan dan analisis untuk 2 jenis vulnerabilities, yaitu Insecure Direct Object Reference (IDOR) dan Privilege Escalation. Untuk melakukan percobaan ini, telah dibuat target berupa website dummy dengan bahasa PHP yang terdiri dari login, register, user homepage, user profile, dan admin page. Target yang telah dibuat disengajai agar memiliki vulnerabilities IDOR dan Privilege Escalation.

Setelah itu dilakukanlah eksploitasi dengan memanfaatkan tools Burp Suite. Disini Burp Suite akan melakukan intercept pada localhost dan mengganti id dari user yang berada pada cookie yang telah di-intercept. Dengan mengganti id pada cookie, user dapat mengakses profile user lain yang bukan miliknya hanya dengan mengganti id user-nya. Disini user juga dapat mengganti nama dan password dari user yang idnya diserang. Untuk mengatasi vulnerability IDOR ini, perlu dilakukan pemberian validasi jika akan mengakses homepage dan profile page serta menerapkan cookie dan session. Setelah menerapkan perbaikan tersebut, jika penyerang mencoba untuk mengakses profile page atau homepage tanpa melakukan login, ia akan dikembalikan ke page untuk login karena belum ada session yang terbentuk sehingga tidak bisa mengakses page lain. Selain itu jika diuji menggunakan intercept dari burp suite, user tidak dapat mengakses user dengan id lain dan akan tetap pada id dari user yang saat ini sedang login.

Untuk percobaan kedua, digunakan kembali website yang belum diberikan perbaikan. Awalnya diuji untuk mengakses page admin tanpa melakukan login dan berhasil mengakses page admin. Disini maka dikatakan bahwa penyerang telah mendapatkan privilege dari seorang admin tanpa harus login sebagai admin. Setelah itu diuji dengan melakukan brute force user id secara satu per satu menggunakan intercept burp suite sampai bisa menemukan id yang merupakan admin. Untuk mengatasi vulnerability ini, dapat diaplikasikan juga solusi dari percobaan sebelumnya yaitu dengan memberikan validasi saat ingin mengakses admin_page agar user perlu login terlebih dahulu sebagai admin untuk bisa

mengakses page tersebut. Selain itu juga bisa dengan menerapkan cookies atau session. Setelah page diperbaiki dengan menerapkan solusi-solusi tadi, admin page tidak lagi bisa diakses tanpa melakukan login sebagai admin terlebih dahulu. Dan ketika dicoba di-intercept dengan burp suite untuk mengganti id user menjadi ke id admin, profile akan tetap di id user yang sedang login saat ini.

Dari seluruh kesimpulan dari hasil percobaan proyek akhir ini, dapat dikatakan hal yang paling penting dari website yang memiliki fitur login dan user dengan privilege yang berbeda, adalah perlu diberikan validasi dan verifikasi agar keamanan dan integritas dari user dapat terjaga. Selain itu perlu juga diterapkan cookies atau session agar user tidak dapat mengakses data dari user lain dengan memanfaatkan celah pada kerentanan website