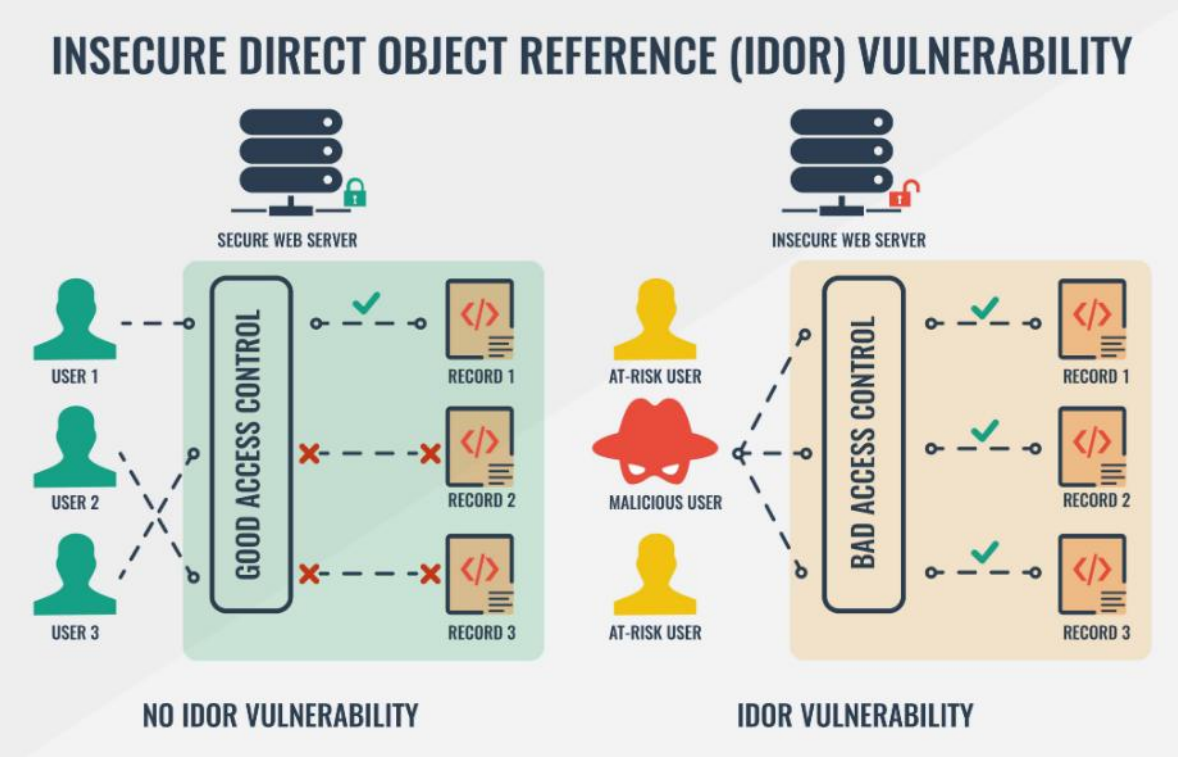
OWASP TOP 10 VULNERABILITIES

Manuel Ramos Leite Carvalho Neto – up202108744
Maria Sousa Carreira – up202408787
Matilde Isabel da Silva Simões – up202108782

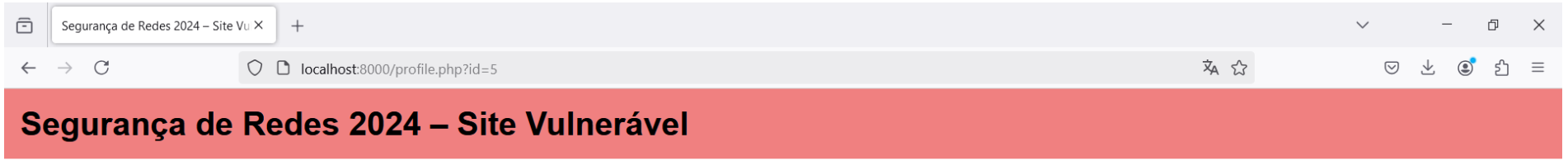
A01:2021 – Broken Access Control

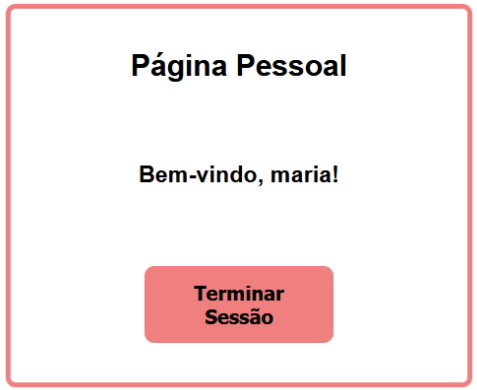
IDOR (Insecure Direct Object Reference)

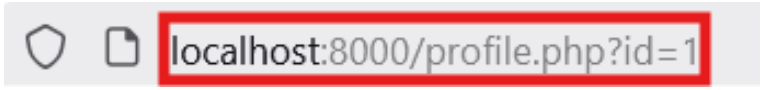
IDOR ocorre quando uma aplicação **não valida adequadamente as permissões de acesso,** permitindo que os atacantes **acedam ou manipulem dados** de outros utilizadores. Explorando parâmetros como **IDs** no **URL** ou nos **pedidos,** um atacante pode **obter informações** ou **realizar ações não autorizadas**.



IDOR (Insecure Direct Object Reference)





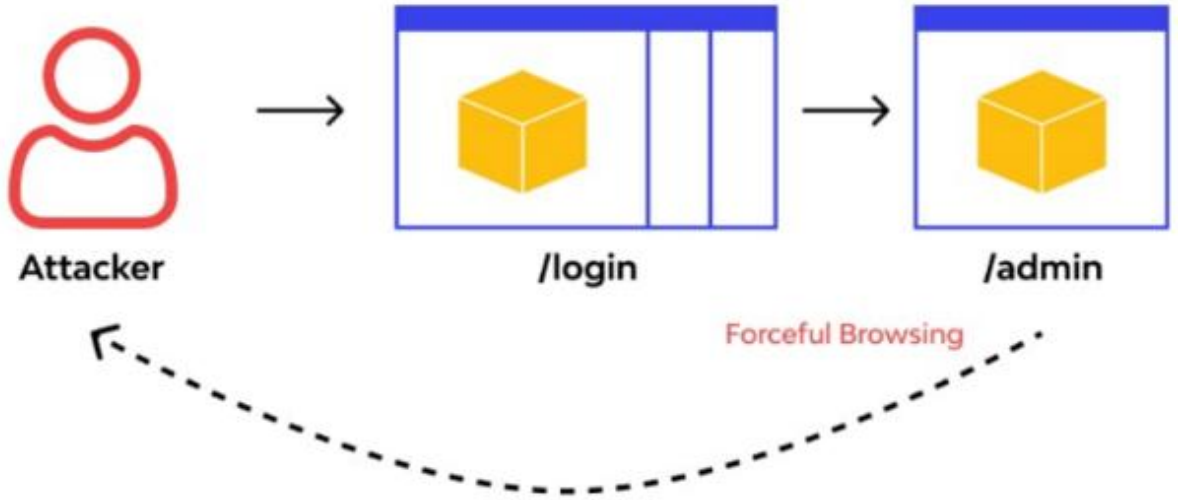


IDOR – Mitigação

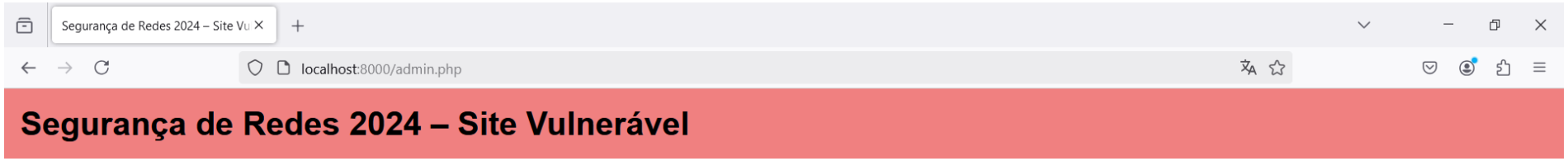
```php
<?php
    declare(strict_types = 1);
    require_once(__DIR__ . '/user.php');
    require_once(__DIR__ . '/templates.php');

    session_set_cookie_params(0, '/', 'localhost', true, true);
    session_start();

    if (!isset($_SESSION['id'])) {
        header("Location: index.php");
        die();
    }

    $db = new PDO('sqlite:' . __DIR__ . '/database.db');
    $db->setAttribute(PDO::ATTR_DEFAULT_FETCH_MODE, PDO::FETCH_ASSOC);

    $id = (int) $_GET['id'];

    if ($id !== $_SESSION['id']) {
        header("Location: profile.php?id=" . $_SESSION['id']);
        die();
    }

    $user = User::getUser($db, $id);

    profile(false, $user);
?>
```

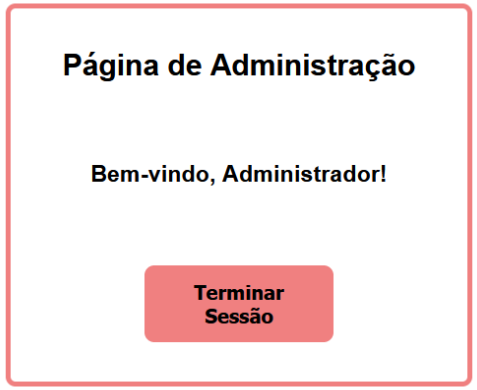
Forced Browsing

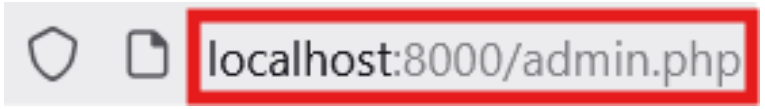
Forced Browsing é um ataque que **explora falhas de configuração** do servidor para aceder a ficheiros ou diretórios sensíveis que não são diretamente acessíveis pela interface da aplicação. O atacante **manipula URLs ou os caminhos dos diretórios** para forçar o **acesso a recursos internos,** como **logs** ou **ficheiros de configuração.**



Forced Browsing



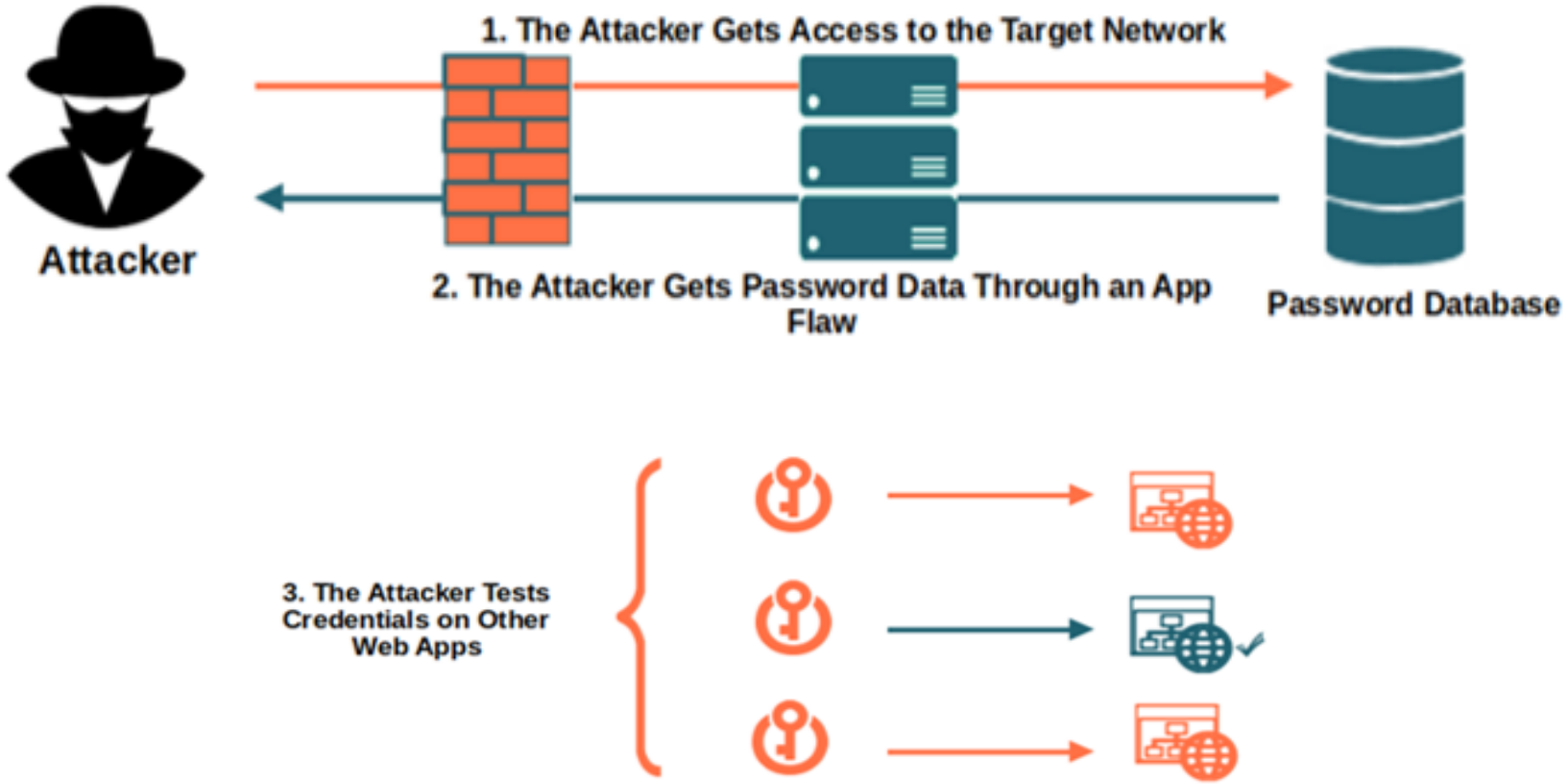




Forced Browsing – Mitigação

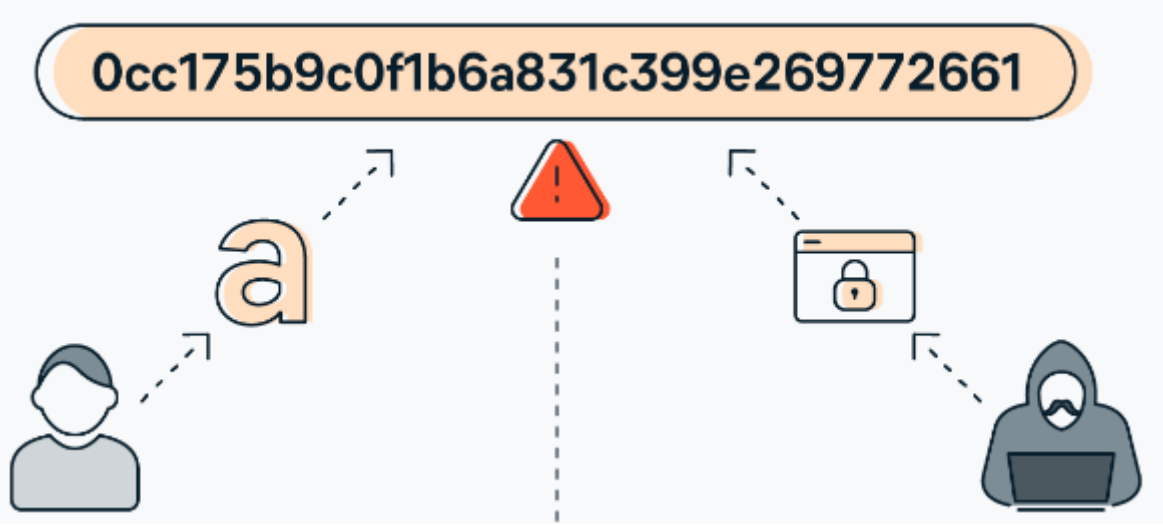
```php
<?php
    declare(strict_types = 1);
    require_once(__DIR__ . '/user.php');
    require_once(__DIR__ . '/templates.php');

    session_set_cookie_params(0, '/', 'localhost', true, true);
    session_start();

    if (!isset($_SESSION['id'])) {
        header("Location: index.php");
        die();
    }

    $db = new PDO('sqlite:' . __DIR__ . '/database.db');
    $db->setAttribute(PDO::ATTR_DEFAULT_FETCH_MODE, PDO::FETCH_ASSOC);

    $id = $_SESSION['id'];
    $user = User::getUser($db, $id);

    if (!$user->isAdmin()) {
        header("Location: profile.php?id=" . $user->getId());
        die();
    }

    admin(false);
?>
```

A02:2021 – Cryptographic Failures



Falha na Base de Dados

Falhas criptográficas nas **bases de dados,** como o **uso de algoritmos de hash inseguros** (MD5, SHA-1) e a **ausência de *salt*,** expõem informações sensíveis a ataques como ***brute force***.



Na base de dados

```php
public static function register(PDo $db, string $username, string
$password) : ?User {
    $stmt = $db->prepare('
        INSERT INTO users (username, password)
        VALUES (?, ?)
    ');

    try {
        $stmt->execute(array(strtolower($username), md5($password)));
    } catch (PDOException $e) {
        return null;
    }

    return User::login($db, $username, $password);
}
```

```php
public static function login(PDO $db, string $username, string
$password) : ?User {
    $stmt = $db->prepare('
        SELECT id, username, password, admin
        FROM users
        WHERE lower(username) = ?
    ');

    $stmt->execute(array(strtolower($username)));
    $user = $stmt->fetch();

    if ($user && md5($password) === $user['password'])
        return new User((int) $user['id'], $user['username'], (bool)
$user['admin']);

    return null;
}
```

Na base de dados

```
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite> .tables
users
sqlite> PRAGMA table_info(users);
0|id|INTEGER|0||1
1|username|VARCHAR(255)|1||0
2|password|VARCHAR(255)|1||0
3|admin|INTEGER|0|0|0
sqlite> SELECT * FROM users;
1|vulnerable|25890deab1075e916c06b9e1efc2e25f|1
2|mitigated|$2y$12$LIqlGBmRo3fE1iZZCcWrROyAb7gPqJPiOopk9frLtL0li7.WfuD72|1
3|matilde|641a3af3fd54d3a81d47e23376dcc90a|0
4|manel|95ab6cdfaa9d646f83061a936bfb8996|0
5|maria|263bce650e68ab4e23f28263760b9fa5|0
```

Hash	Type	Result
25890deab1075e916c06b9e1efc2e25f	md5	vulnerable
641a3af3fd54d3a81d47e23376dcc90a	md5	matilde
95ab6cdfaa9d646f83061a936bfb8996	md5	manel
263bce650e68ab4e23f28263760b9fa5	md5	maria

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Na base de dados – Mitigação

```php
public static function register(PDO $db, string $username, string
$password) : ?User {
    $stmt = $db->prepare('
        INSERT INTO users (username, password)
        VALUES (?, ?)
    ');

    $options = ['cost' => 12];
    $hashedPassword = password_hash($password, PASSWORD_BCRYPT,
$options);

    try {
        $stmt->execute(array(strtolower($username), $hashedPassword));
    } catch (PDOException $e) {
        return null;
    }

    return User::login($db, $username, $password);
}
```

```php
public static function login(PDO $db, string $username, string
$password) : ?User {
    $stmt = $db->prepare('
        SELECT id, username, password, admin
        FROM users
        WHERE lower(username) = ?
    ');

    $stmt->execute(array(strtolower($username)));
    $user = $stmt->fetch();

    if ($user && password_verify($password, $user['password']))
        return new User((int) $user['id'], $user['username'], (bool)
$user['admin']);

    return null;
}
```

Falha na Comunicação

A **ausência de encriptação nas conexões HTTP** permite que atacantes **intersetem dados sensíveis,** como credenciais, através de ataques **Man-in-the-Middle**. Um atacante que monitore o tráfego pode **capturar pacotes contendo informações confidenciais,** explorando a vulnerabilidade.

Na comunicação

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::1	::1	TCP	76	60118 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
2	0.000542	::1	::1	TCP	76	8000 → 60118 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
3	0.000623	::1	::1	TCP	64	60118 → 8000 [ACK] Seq=1 Ack=1 Win=65280 Len=0
4	0.001514	::1	::1	HTTP	997	POST /register.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.001660	::1	::1	TCP	64	8000 → 60118 [ACK] Seq=1 Ack=934 Win=64512 Len=0
6	0.004600	::1	::1	TCP	76	60119 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
7	0.005044	::1	::1	TCP	76	8000 → 60119 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
8	0.005124	::1	::1	TCP	64	60119 → 8000 [ACK] Seq=1 Ack=1 Win=65280 Len=0
9	0.055104	::1	::1	HTTP	434	HTTP/1.1 302 Found
10	0.055155	::1	::1	TCP	64	60118 → 8000 [ACK] Seq=934 Ack=371 Win=65024 Len=0
11	0.059741	::1	::1	HTTP	871	GET /profile.php?id=3 HTTP/1.1
12	0.059823	::1	::1	TCP	64	8000 → 60118 [ACK] Seq=371 Ack=1741 Win=63744 Len=0
13	0.064528	::1	::1	HTTP	865	HTTP/1.1 200 OK (text/html)
14	0.064586	::1	::1	TCP	64	60118 → 8000 [ACK] Seq=1741 Ack=1172 Win=64256 Len=0
15	0.104469	::1	::1	HTTP	774	GET /style.css HTTP/1.1
16	0.104527	::1	::1	TCP	64	8000 → 60118 [ACK] Seq=1172 Ack=2451 Win=62976 Len=0
17	0.107031	::1	::1	HTTP	877	HTTP/1.1 200 OK (text/css)
18	0.107075	::1	::1	TCP	64	60118 → 8000 [ACK] Seq=2451 Ack=1985 Win=63488 Len=0

```
> Frame 4: 997 bytes on wire (7976 bits), 997 bytes captured (7976 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 60118, Dst Port: 8000, Seq: 1, Ack: 1, Len: 933
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "username" = "manel"
      Key: username
      Value: manel
  v Form item: "password" = "manel"
      Key: password
      Value: manel
```

Na comunicação – Mitigação

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/server.crt
    SSLCertificateKeyFile /etc/ssl/private/server.key

    <Directory /var/www/html>
        AllowOverride All
    </Directory>
</VirtualHost>
```

```
RewriteEngine On

RewriteRule ^users/([0-9]+)$ profile.php?id=$1 [L,QSA]

RewriteCond %{HTTPS} !=on
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Na comunicação – Mitigação

No.	Time	Source	Destination	Protocol	Length	Info
5	0.001962	::1	::1	TCP	64	64602 → 8001 [ACK] Seq=1 Ack=1 Win=65280 Len=0
6	0.003525	::1	::1	TLSv1.3	1926	Client Hello (SNI=localhost)
7	0.003588	::1	::1	TCP	64	8001 → 64602 [ACK] Seq=1 Ack=1863 Win=63488 Len=0
8	0.010172	::1	::1	TCP	76	64603 → 8001 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
9	0.010704	::1	::1	TCP	76	8001 → 64603 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
10	0.010844	::1	::1	TCP	64	64603 → 8001 [ACK] Seq=1 Ack=1 Win=65280 Len=0
11	0.012867	::1	::1	TLSv1.3	1926	Client Hello (SNI=localhost)
12	0.012965	::1	::1	TCP	64	8001 → 64603 [ACK] Seq=1 Ack=1863 Win=63488 Len=0
13	0.015303	::1	::1	TLSv1.3	304	Server Hello, Change Cipher Spec, Application Data, Application Data
14	0.015390	::1	::1	TCP	64	64602 → 8001 [ACK] Seq=1863 Ack=241 Win=65280 Len=0
15	0.016952	::1	::1	TLSv1.3	94	Change Cipher Spec, Application Data
16	0.017033	::1	::1	TCP	64	8001 → 64602 [ACK] Seq=241 Ack=1893 Win=63488 Len=0
17	0.017657	::1	::1	TCP	64	64602 → 8001 [FIN, ACK] Seq=1893 Ack=241 Win=65280 Len=0
18	0.017733	::1	::1	TCP	64	8001 → 64602 [ACK] Seq=241 Ack=1894 Win=63488 Len=0
19	0.018218	::1	::1	TCP	64	8001 → 64602 [FIN, ACK] Seq=241 Ack=1894 Win=63488 Len=0
20	0.018291	::1	::1	TCP	64	64602 → 8001 [ACK] Seq=1894 Ack=242 Win=65280 Len=0
21	0.021961	::1	::1	TLSv1.3	304	Server Hello, Change Cipher Spec, Application Data, Application Data
22	0.022034	::1	::1	TCP	64	64603 → 8001 [ACK] Seq=1863 Ack=241 Win=65280 Len=0
23	0.022789	::1	::1	TLSv1.3	94	Change Cipher Spec, Application Data
24	0.022875	::1	::1	TCP	64	8001 → 64603 [ACK] Seq=241 Ack=1893 Win=63488 Len=0
25	0.023240	::1	::1	TCP	64	64603 → 8001 [FIN, ACK] Seq=1893 Ack=241 Win=65280 Len=0
26	0.023287	::1	::1	TCP	64	8001 → 64603 [ACK] Seq=241 Ack=1894 Win=63488 Len=0
27	0.023825	::1	::1	TCP	64	8001 → 64603 [FIN, ACK] Seq=241 Ack=1894 Win=63488 Len=0
28	0.023915	::1	::1	TCP	64	64603 → 8001 [ACK] Seq=1894 Ack=242 Win=65280 Len=0
29	0.025520	::1	::1	TCP	76	64604 → 8001 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
30	0.026175	::1	::1	TCP	76	8001 → 64604 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
31	0.026310	::1	::1	TCP	64	64604 → 8001 [ACK] Seq=1 Ack=1 Win=65280 Len=0
32	0.027951	::1	::1	TLSv1.3	1783	Client Hello (SNI=localhost)
33	0.028022	::1	::1	TCP	64	8001 → 64604 [ACK] Seq=1 Ack=1720 Win=63744 Len=0
34	0.034638	::1	::1	TLSv1.3	1828	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
35	0.034687	::1	::1	TCP	64	64604 → 8001 [ACK] Seq=1720 Ack=1765 Win=63744 Len=0
36	0.035459	::1	::1	TLSv1.3	128	Change Cipher Spec, Application Data
37	0.035554	::1	::1	TCP	64	8001 → 64604 [ACK] Seq=1765 Ack=1784 Win=63744 Len=0
38	0.035927	::1	::1	TLSv1.3	1021	Application Data
39	0.035966	::1	::1	TCP	64	8001 → 64604 [ACK] Seq=1765 Ack=2741 Win=62720 Len=0
40	0.037045	::1	::1	TLSv1.3	222	Application Data, Application Data
41	0.037086	::1	::1	TCP	64	64604 → 8001 [ACK] Seq=2741 Ack=1923 Win=63488 Len=0
42	0.845895	::1	::1	TLSv1.3	456	Application Data
43	0.845944	::1	::1	TCP	64	64604 → 8001 [ACK] Seq=2741 Ack=2315 Win=62976 Len=0
44	0.850840	::1	::1	TLSv1.3	894	Application Data
45	0.850902	::1	::1	TCP	64	8001 → 64604 [ACK] Seq=2315 Ack=3571 Win=61952 Len=0