

[illegible]

Name	Active Crawling with ZAPProxy
URL	<a href="https://attackdefense.com/challengedetails?cid=1897">https://attackdefense.com/challengedetails?cid=1897</a>
Type	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:** Perform Dictionary Attack on the bWAPP login page.

**Step 1:** Identifying IP address of the target machine

**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
25090: eth0@if25091: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
25093: eth1@if25094: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:c3:d6:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.195.214.2/24 brd 192.195.214.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.195.214.2. The target machine is located at the IP address 192.195.214.3

## Step 2: Identifying open ports.

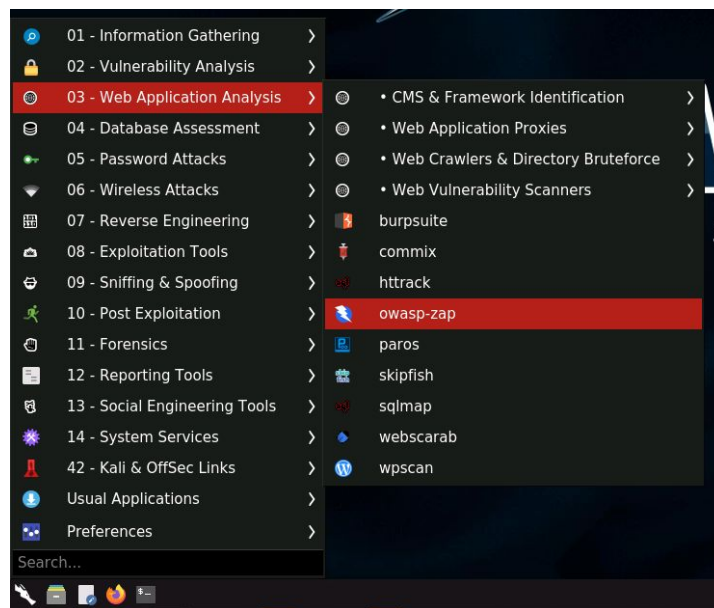
**Command:** nmap 192.195.214.3

```
root@attackdefense:~# nmap 192.195.214.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-21 05:27 IST
Nmap scan report for target-1 (192.195.214.3)
Host is up (0.000013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:C3:D6:03 (Unknown)

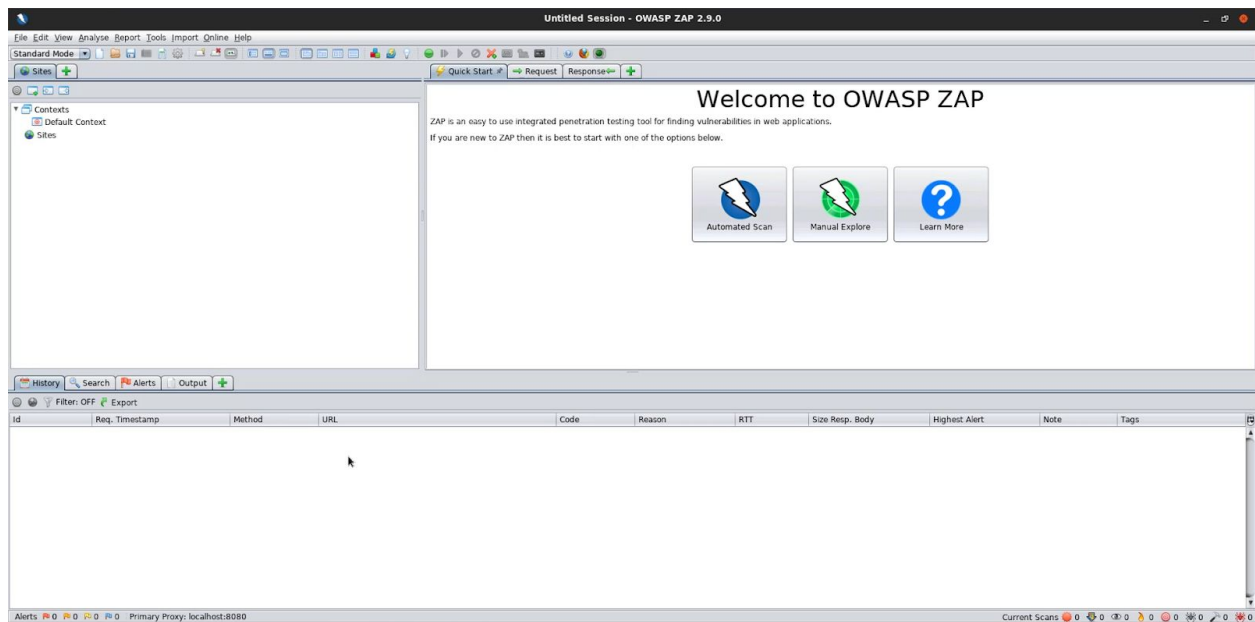
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@attackdefense:~#
```

Port 80 and 3306 are open.

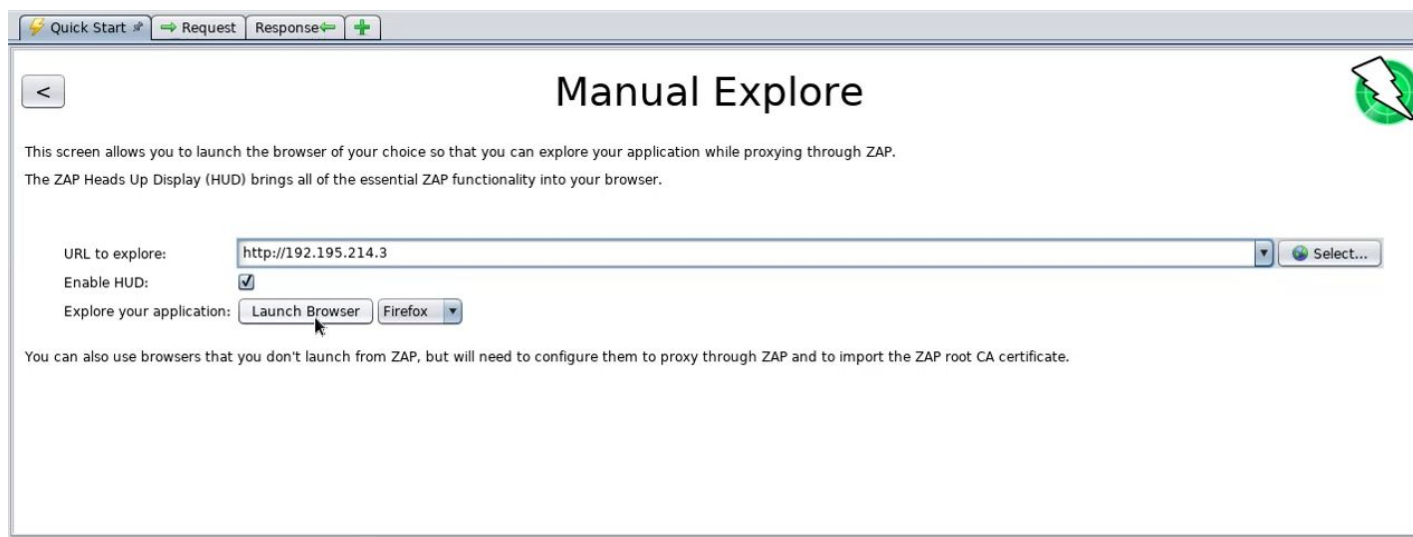
**Step 3:** Starting Burp Suite. Click on the Menu, Navigate to "Web Application Analysis" and click on "owasp-zap".



ZAP:

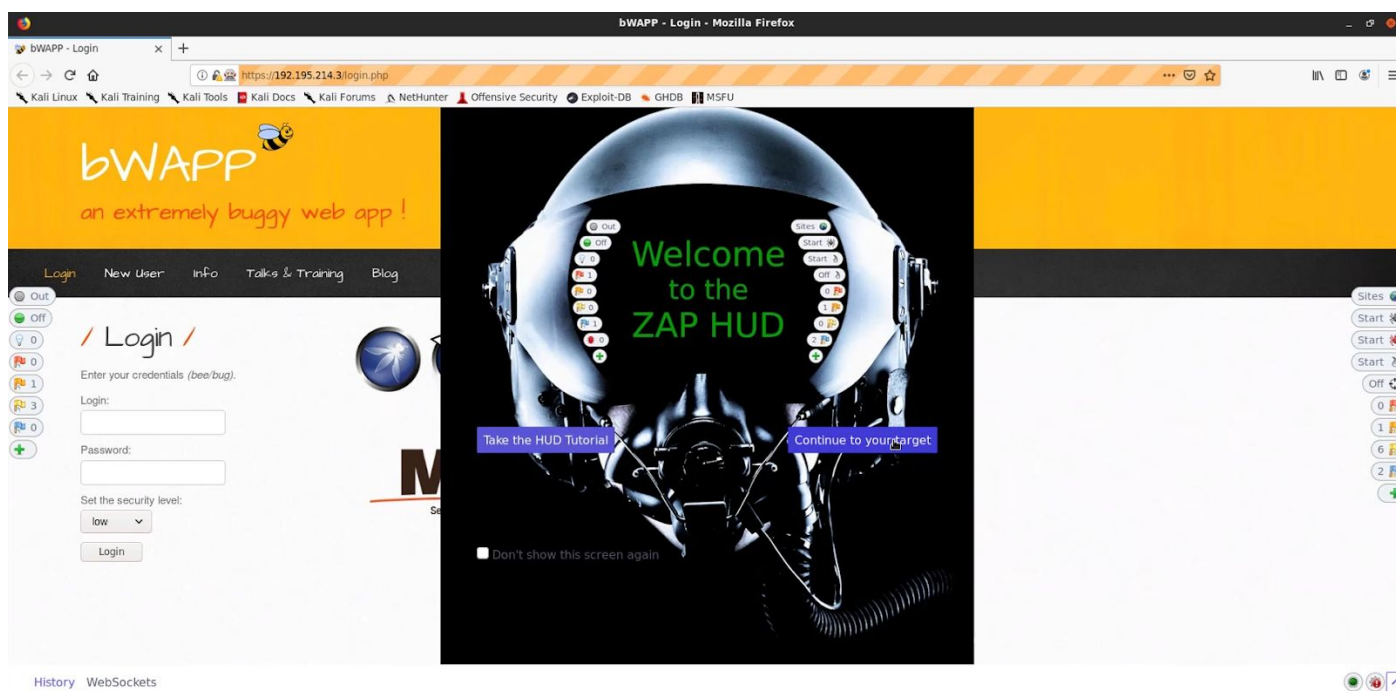


**Step 4:** Click on "Manual Explore", enter the target IP address in the Input field and click on "Launch Browser".

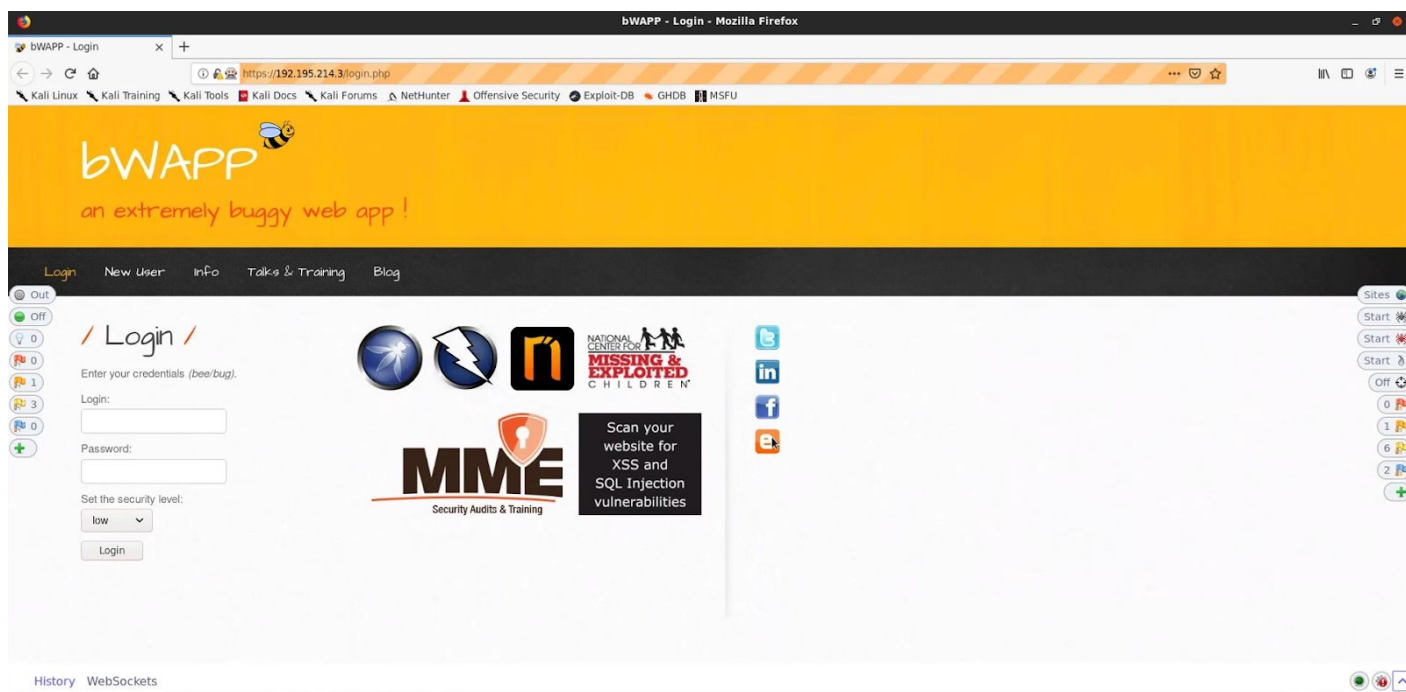


A browser session will be started with ZAP HUD.

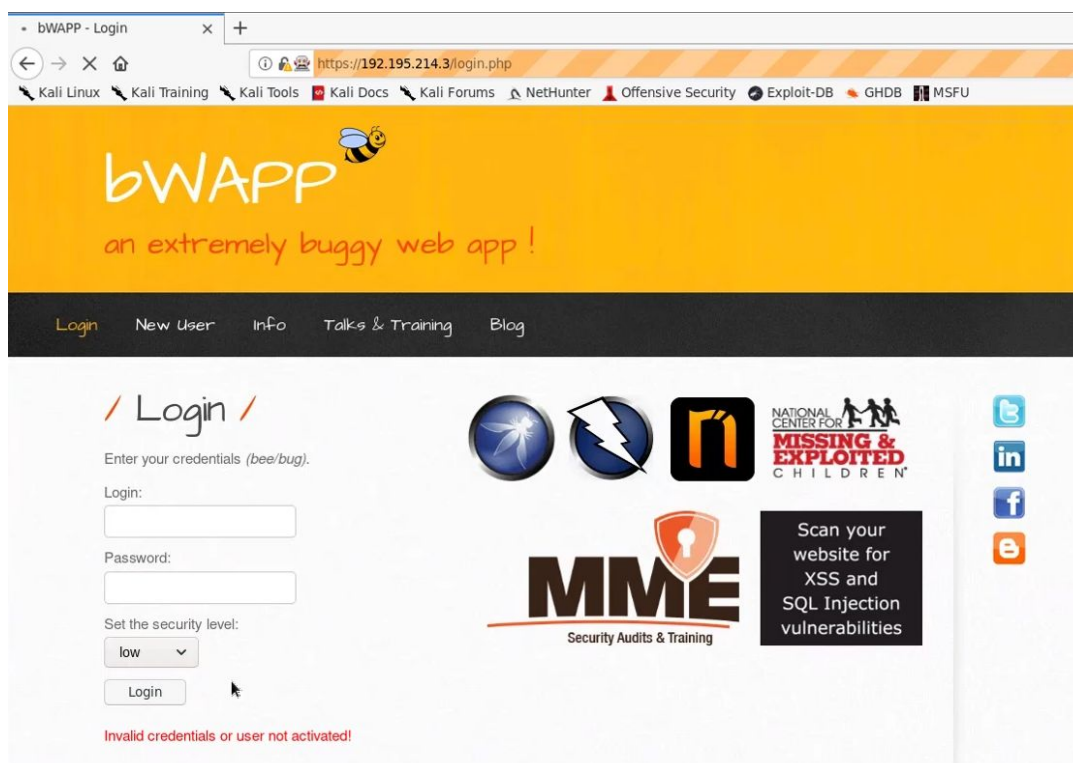




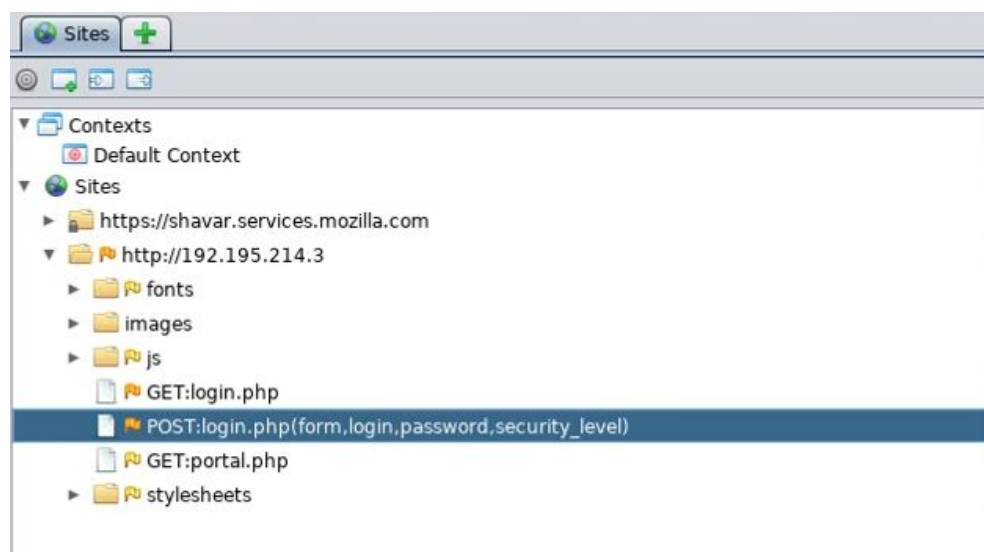
**Step 5:** Click on "Continue to your target".



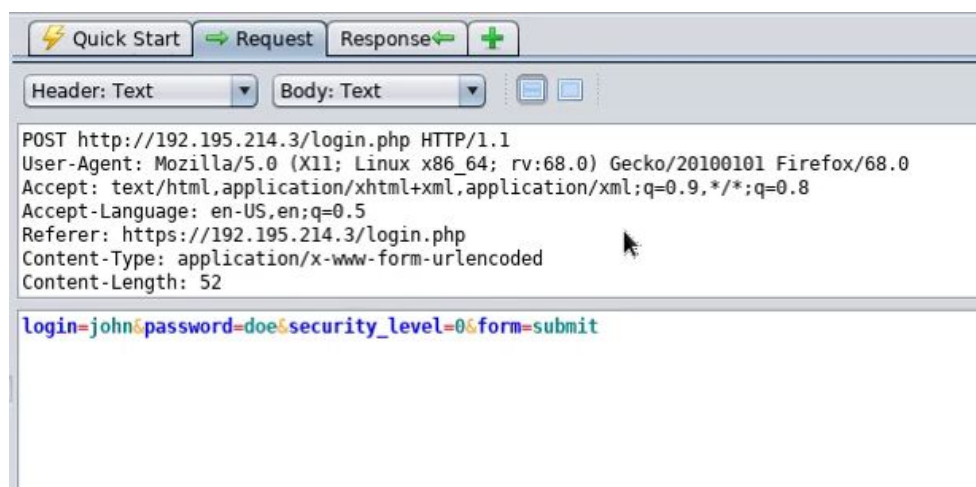
**Step 6:** Attempt login with invalid credentials.



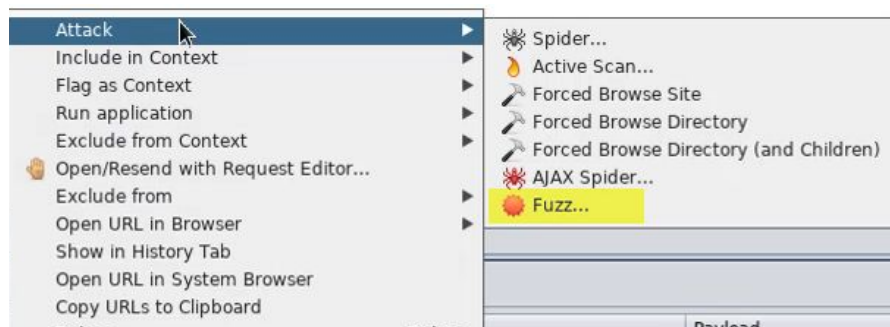
The website and the login page action will be added to the sitemap.



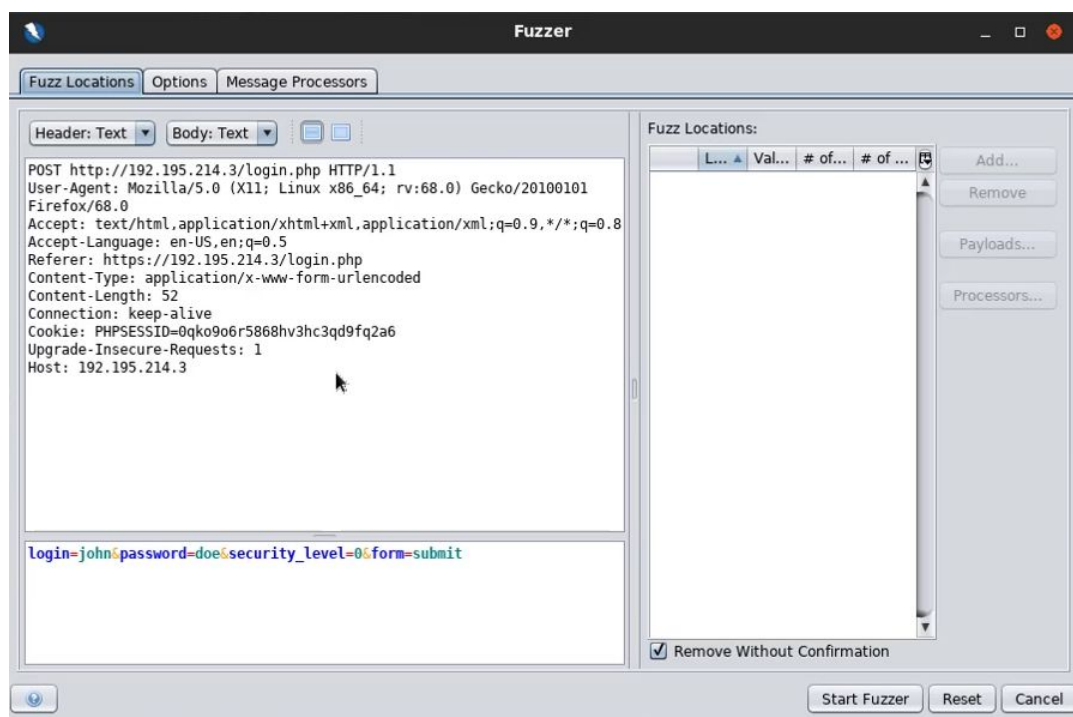
**Step 7:** Click on the POST request from the sitemap and click on the "Request" tab.



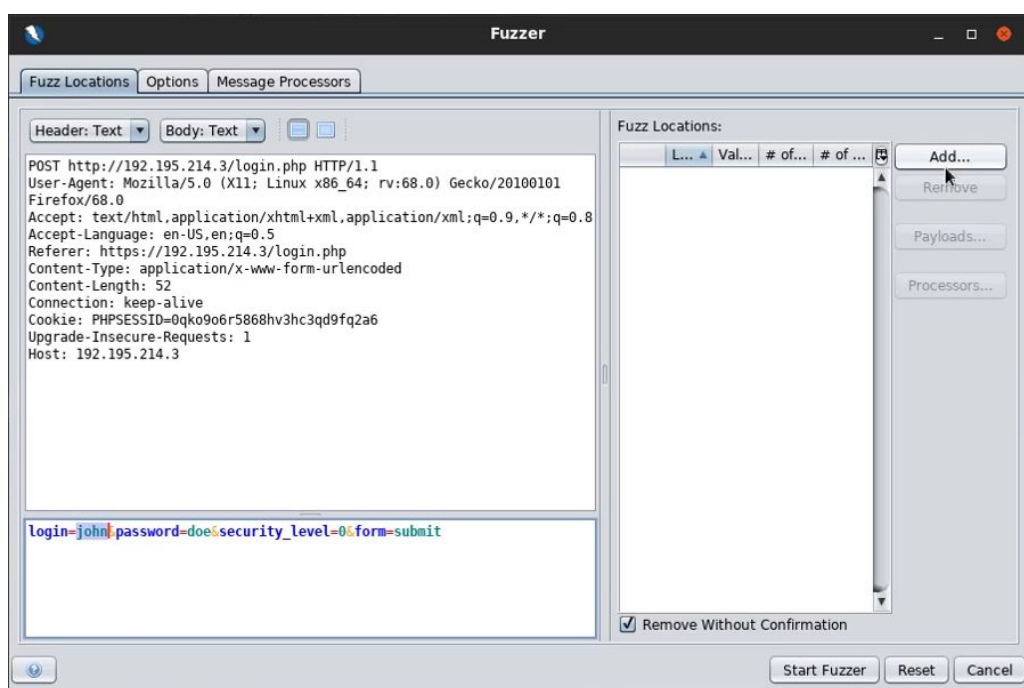
**Step 8:** Right click on the POST request, navigate to Attack and click on "Fuzz".



The Fuzzer window will appear.

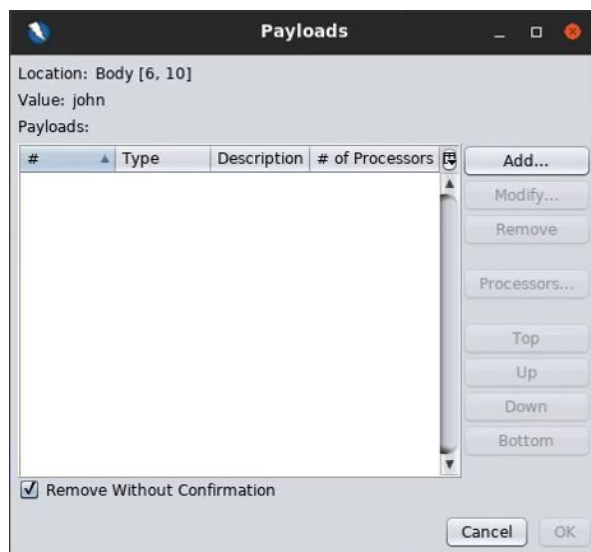


**Step 9:** Select the entered username "john" and click on the Add button.



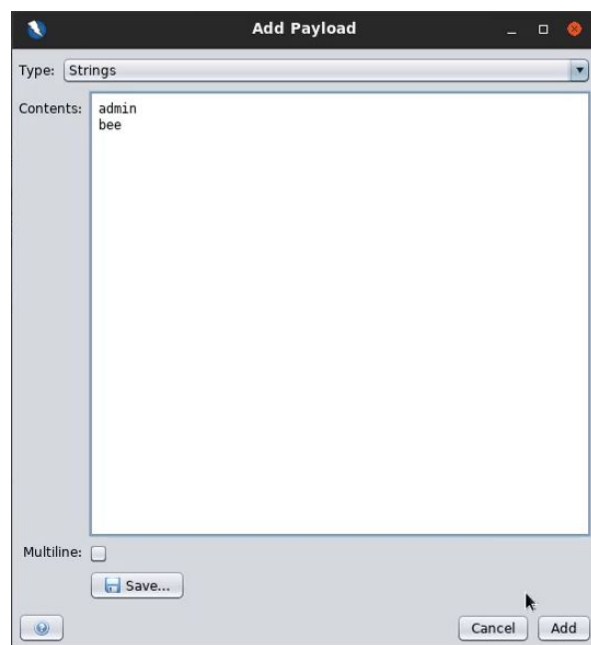


The payloads window will appear.

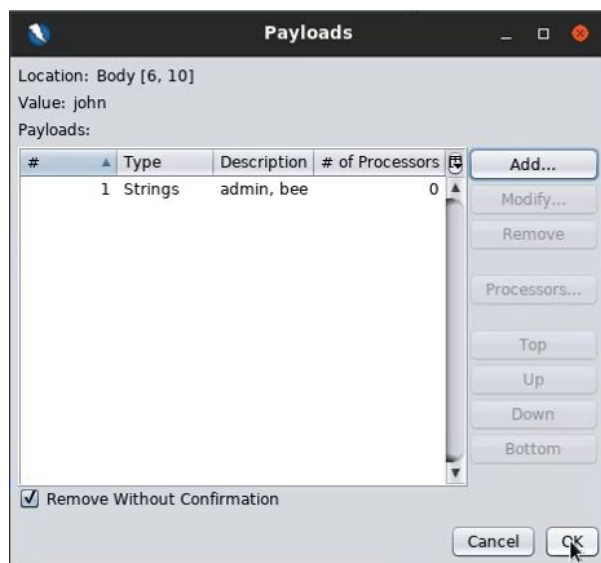


**Step 10:** Click on the Add button, enter the payloads for username. Click on the Add button.

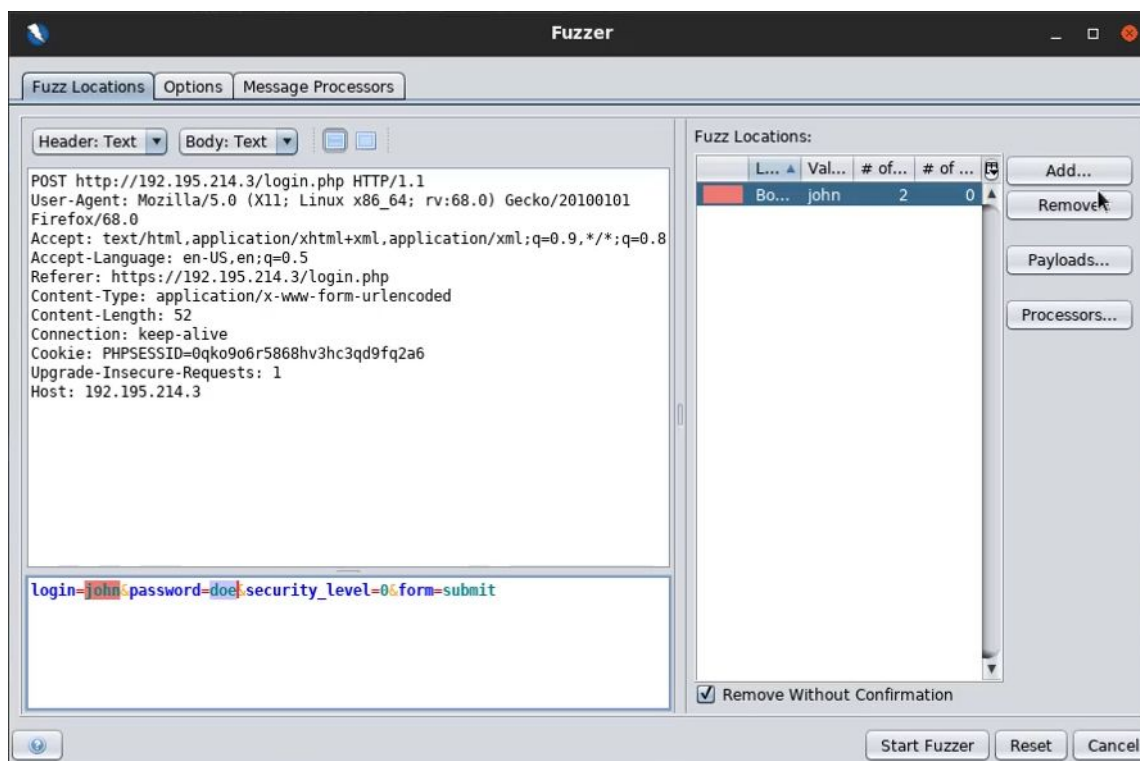
**Payloads:** admin,bee



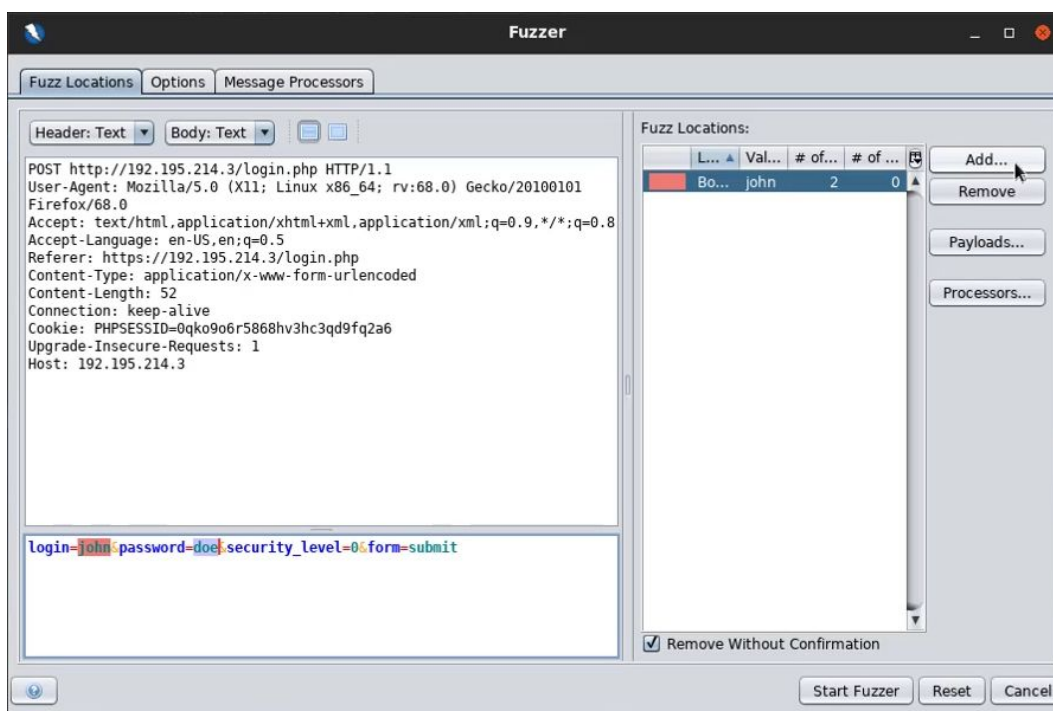
**Step 11:** Click on the "OK" button.



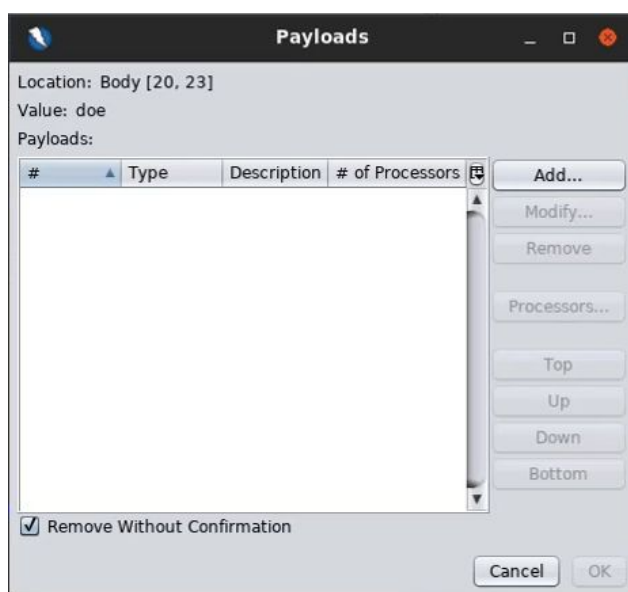
The payload will appear in the Fuzz Locations.



**Step 12:** Similarly, select the entered password "doe" and click on the Add button.



The payloads window will appear.

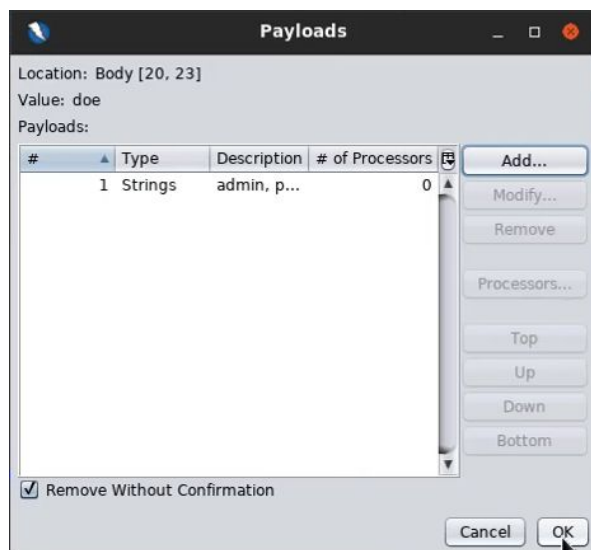


**Step 13:** Click on the Add button, enter the payloads for password. Click on the Add button.

**Payloads:** admin, password, adminpasswd, cookie, hello, world, bug, bee

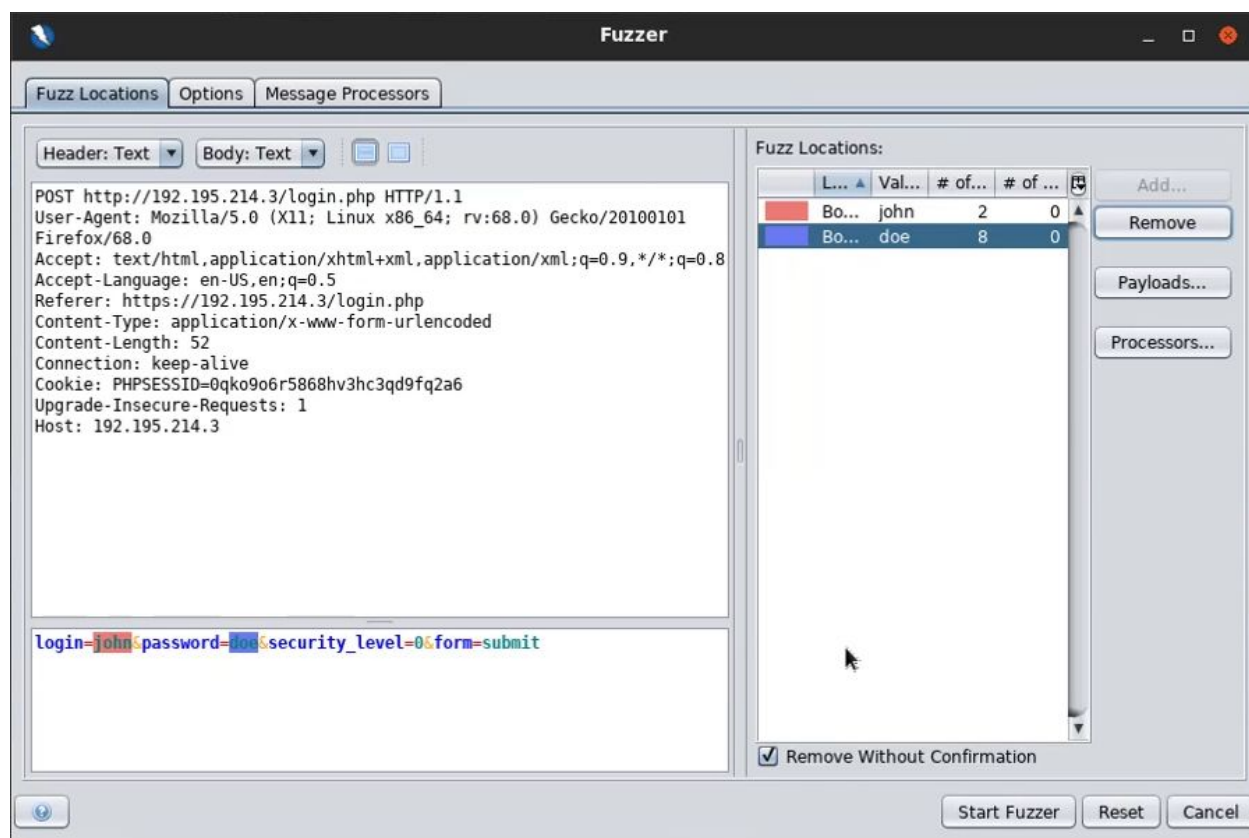


**Step 14:** Click on the OK button.





The payload will appear in the Fuzz Locations.



**Step 15:** Click on Start Fuzzer. Upon completion of the attack, compare the status code.

History Search Alerts Output WebSockets Fuzzer

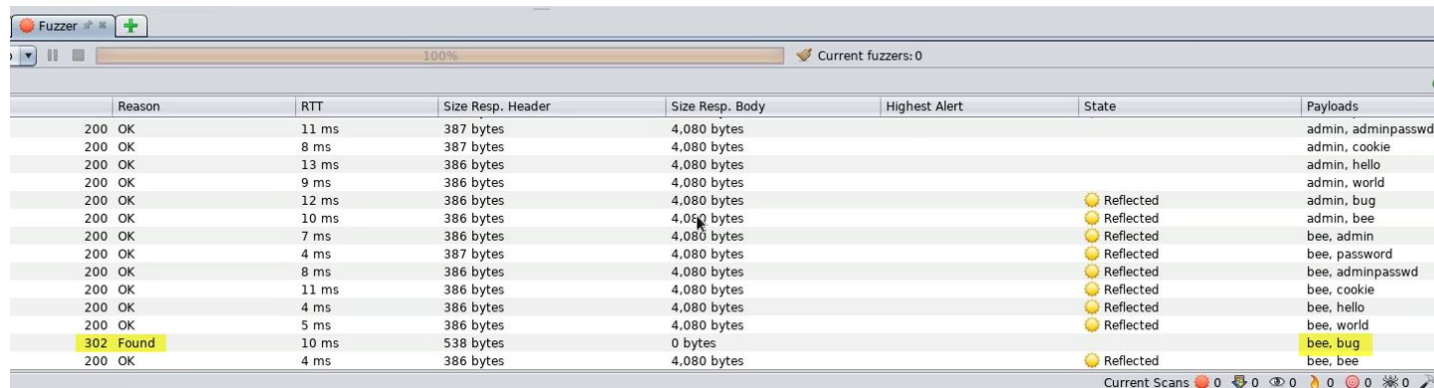
New Fuzzer Progress: 0: HTTP - http://192.195.214.3/login.php 100%

Messages Sent: 16 Errors: 0 Show Errors

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
3	Fuzzed	200	OK	11 ms	387 bytes	4,080 bytes
4	Fuzzed	200	OK	8 ms	387 bytes	4,080 bytes
5	Fuzzed	200	OK	13 ms	386 bytes	4,080 bytes
6	Fuzzed	200	OK	9 ms	386 bytes	4,080 bytes
7	Fuzzed	200	OK	12 ms	386 bytes	4,080 bytes
8	Fuzzed	200	OK	10 ms	386 bytes	4,080 bytes
9	Fuzzed	200	OK	7 ms	386 bytes	4,080 bytes
10	Fuzzed	200	OK	4 ms	387 bytes	4,080 bytes
11	Fuzzed	200	OK	8 ms	386 bytes	4,080 bytes
12	Fuzzed	200	OK	11 ms	386 bytes	4,080 bytes
13	Fuzzed	200	OK	4 ms	386 bytes	4,080 bytes
14	Fuzzed	200	OK	5 ms	386 bytes	4,080 bytes
15	Fuzzed	302	Found	10 ms	538 bytes	0 bytes
16	Fuzzed	200	OK	4 ms	386 bytes	4,080 bytes

Alerts 0 1 6 2 Primary Proxy: localhost:8080

One of the status code will be 302.

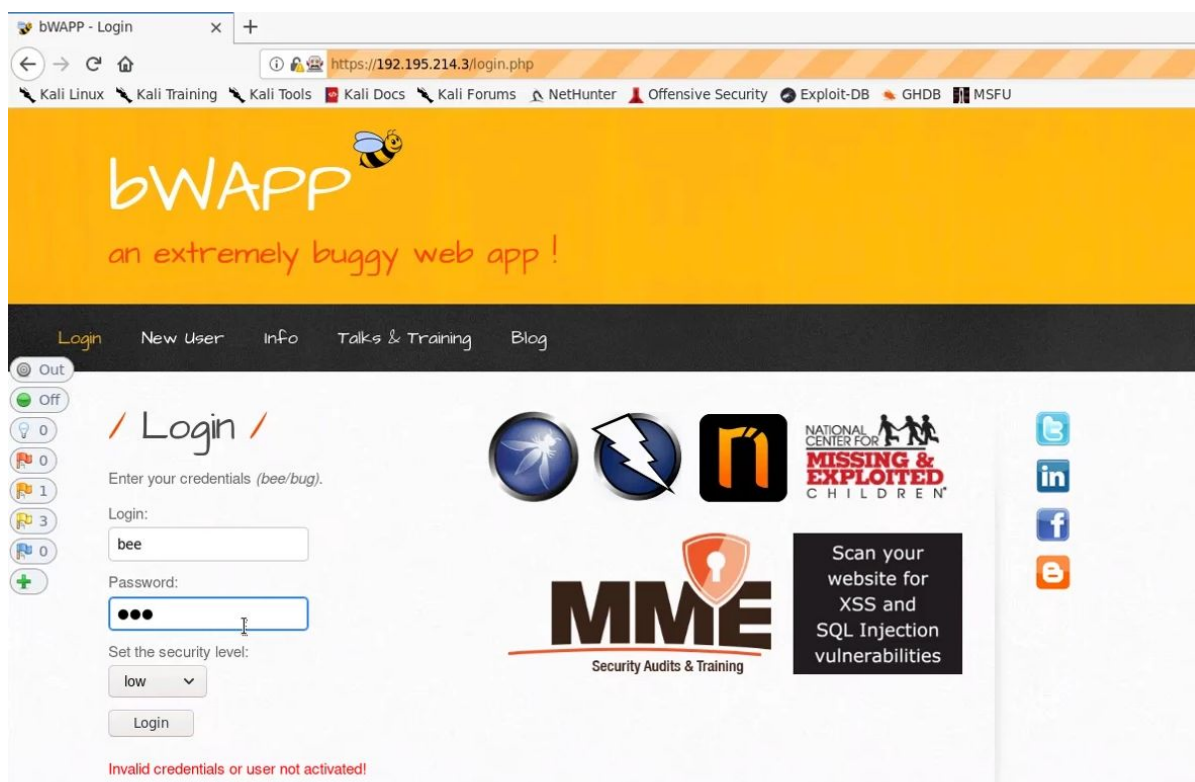


Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
200 OK	11 ms	387 bytes	4,080 bytes			admin, adminpasswd
200 OK	8 ms	387 bytes	4,080 bytes			admin, cookie
200 OK	13 ms	386 bytes	4,080 bytes			admin, hello
200 OK	9 ms	386 bytes	4,080 bytes			admin, world
200 OK	12 ms	386 bytes	4,080 bytes		Reflected	admin, bug
200 OK	10 ms	386 bytes	4,080 bytes		Reflected	admin, bee
200 OK	7 ms	386 bytes	4,080 bytes		Reflected	bee, admin
200 OK	4 ms	387 bytes	4,080 bytes		Reflected	bee, password
200 OK	8 ms	386 bytes	4,080 bytes		Reflected	bee, adminpasswd
200 OK	11 ms	386 bytes	4,080 bytes		Reflected	bee, cookie
200 OK	4 ms	386 bytes	4,080 bytes		Reflected	bee, hello
200 OK	5 ms	386 bytes	4,080 bytes		Reflected	bee, world
302 Found	10 ms	538 bytes	0 bytes		Reflected	bee, bug
200 OK	4 ms	386 bytes	4,080 bytes		Reflected	bee, bee

**Step 16:** Login to the web application. The login credentials were discovered in the previous step.

**Username:** bee

**Password:** bug



bwAPP - Login

https://192.195.214.3/login.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

bwAPP an extremely buggy web app!

Login New User Info Talks & Training Blog

Out Off 0 1 3 0

/ Login /

Enter your credentials (bee/bug).

Login: bee

Password: ●●●

Set the security level: low

Login

Invalid credentials or user not activated!

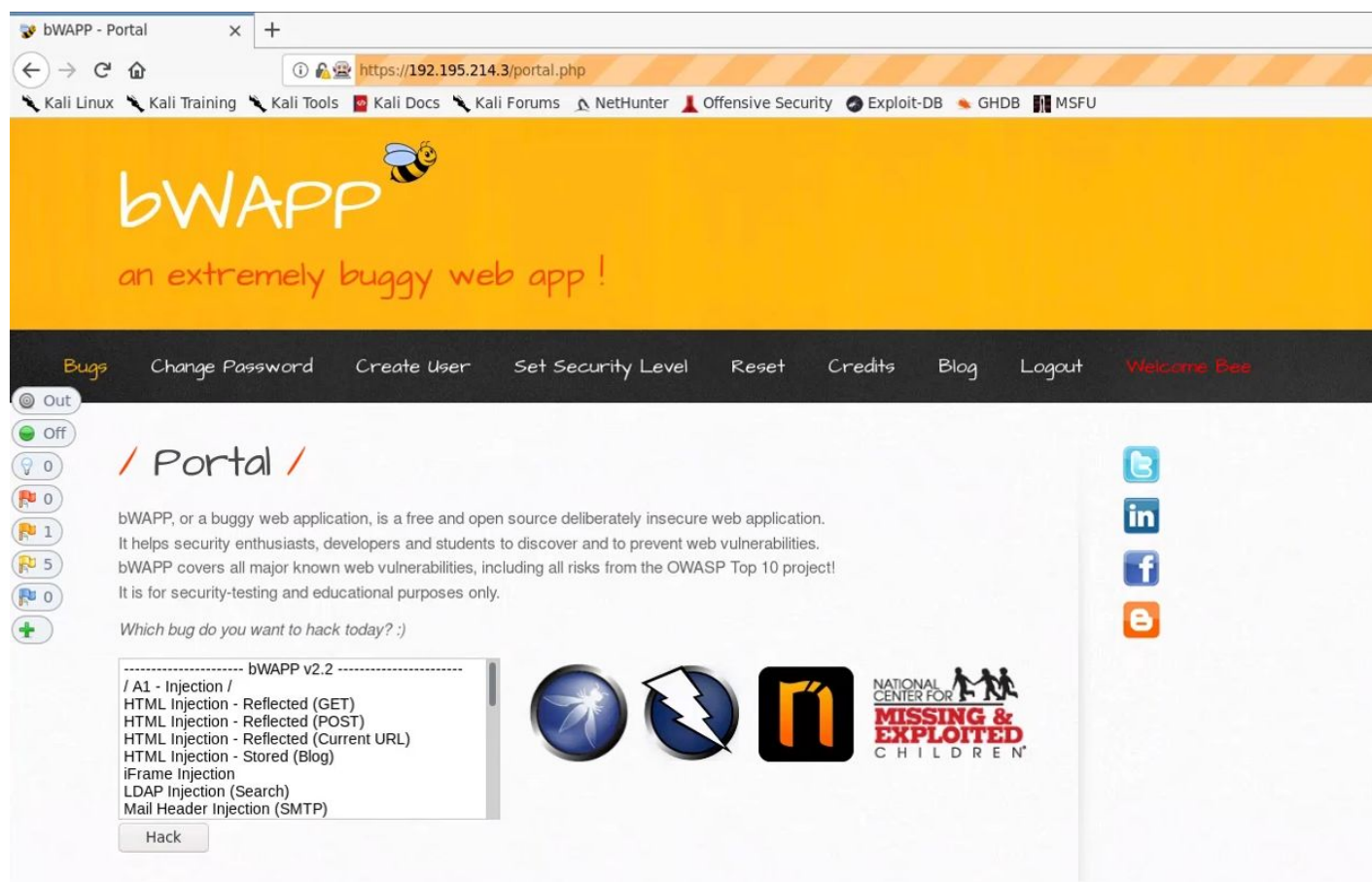
MME Security Audits & Training

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Scan your website for XSS and SQL Injection vulnerabilities

Twitter LinkedIn Facebook Email

## After Login:



## References:

1. OWASP Zed Attack Proxy (<https://www.zaproxy.org/>)
1. bWAPP (<http://www.itsecgames.com/>)