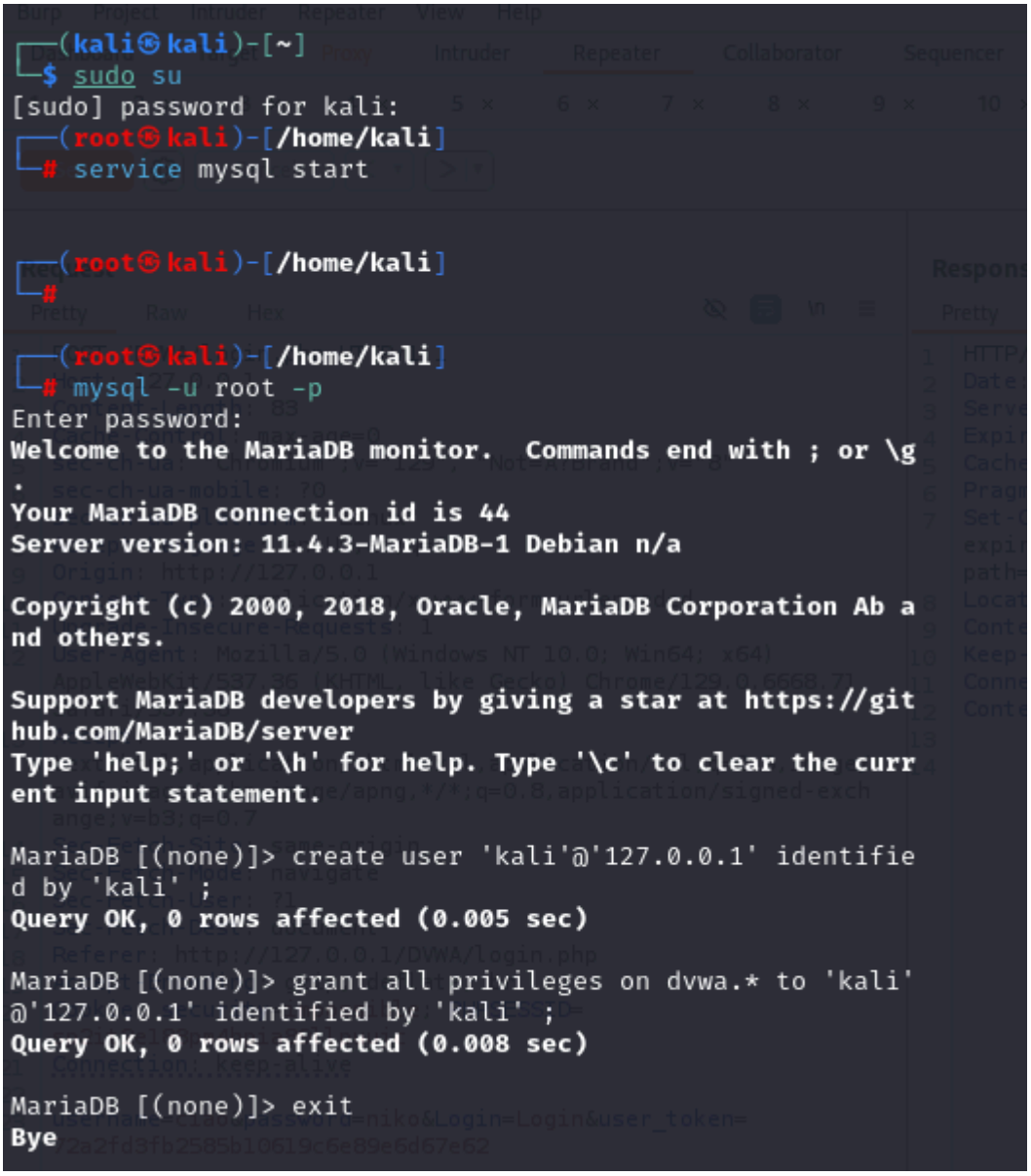
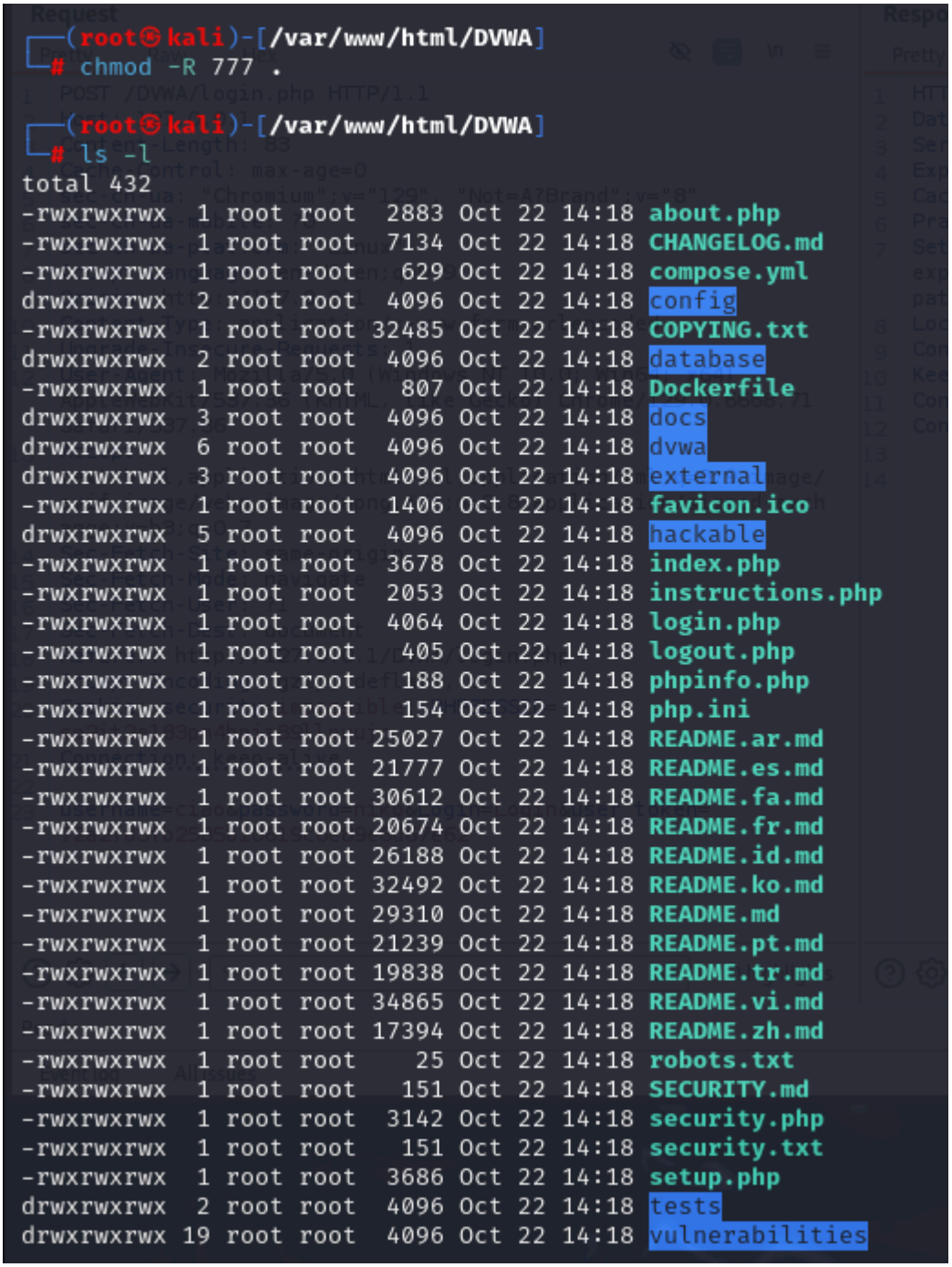
W8D1 di Pandolfi Luciano
Configurazione mysql/apache2 su shell Linux, pratica con BurpSuite:



```
┌──(root㉿kali)-[/home/kali]
└─# service apache2 start

┌──(root㉿kali)-[/home/kali]
└─# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

┌──(root㉿kali)-[/home/kali]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2
┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# nano php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# service apache2 start
```

```
┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4825, done.
remote: Counting objects: 100% (473/473), done.
remote: Compressing objects: 100% (221/221), done.
remote: Total 4825 (delta 278), reused 402 (delta 234), pack-reused 4352 (from 1)
Receiving objects: 100% (4825/4825), 2.36 MiB | 2.60 MiB/s, done.
Resolving deltas: 100% (2350/2350), done.
```


┌──(root㉿kali)-[/var/www/html/DVWA]
└─# chmod -R 777 .
┌──(root㉿kali)-[/var/www/html/DVWA]
└─# ls -l
total 432
-rwxrwxrwx 1 root root 2883 Oct 22 14:18 about.php
-rwxrwxrwx 1 root root 7134 Oct 22 14:18 CHANGELOG.md
-rwxrwxrwx 1 root root   629 Oct 22 14:18 compose.yml
drwxrwxrwx 2 root root 4096 Oct 22 14:18 config
-rwxrwxrwx 1 root root 32485 Oct 22 14:18 COPYING.txt
drwxrwxrwx 2 root root 4096 Oct 22 14:18 database
-rwxrwxrwx 1 root root   807 Oct 22 14:18 Dockerfile
drwxrwxrwx 3 root root 4096 Oct 22 14:18 docs
drwxrwxrwx 6 root root 4096 Oct 22 14:18 dvwa
drwxrwxrwx 3 root root 4096 Oct 22 14:18 external
-rwxrwxrwx 1 root root 1406 Oct 22 14:18 favicon.ico
drwxrwxrwx 5 root root 4096 Oct 22 14:18 hackable
-rwxrwxrwx 1 root root 3678 Oct 22 14:18 index.php
-rwxrwxrwx 1 root root 2053 Oct 22 14:18 instructions.php
-rwxrwxrwx 1 root root 4064 Oct 22 14:18 login.php
-rwxrwxrwx 1 root root   405 Oct 22 14:18 logout.php
-rwxrwxrwx 1 root root   188 Oct 22 14:18 phpinfo.php
-rwxrwxrwx 1 root root   154 Oct 22 14:18 php.ini
-rwxrwxrwx 1 root root 25027 Oct 22 14:18 README.ar.md
-rwxrwxrwx 1 root root 21777 Oct 22 14:18 README.es.md
-rwxrwxrwx 1 root root 30612 Oct 22 14:18 README.fa.md
-rwxrwxrwx 1 root root 20674 Oct 22 14:18 README.fr.md
-rwxrwxrwx 1 root root 26188 Oct 22 14:18 README.id.md
-rwxrwxrwx 1 root root 32492 Oct 22 14:18 README.ko.md
-rwxrwxrwx 1 root root 29310 Oct 22 14:18 README.md
-rwxrwxrwx 1 root root 21239 Oct 22 14:18 README.pt.md
-rwxrwxrwx 1 root root 19838 Oct 22 14:18 README.tr.md
-rwxrwxrwx 1 root root 34865 Oct 22 14:18 README.vi.md
-rwxrwxrwx 1 root root 17394 Oct 22 14:18 README.zh.md
-rwxrwxrwx 1 root root   25 Oct 22 14:18 robots.txt
-rwxrwxrwx 1 root root   151 Oct 22 14:18 SECURITY.md
-rwxrwxrwx 1 root root 3142 Oct 22 14:18 security.php
-rwxrwxrwx 1 root root   151 Oct 22 14:18 security.txt
-rwxrwxrwx 1 root root 3686 Oct 22 14:18 setup.php
drwxrwxrwx 2 root root 4096 Oct 22 14:18 tests
drwxrwxrwx 19 root root 4096 Oct 22 14:18 vulnerabilities

```
┌──(root㉿kali)-[/var/www/html/DVWA]
└─# cp config.inc.php.dist config.inc.php
cp: cannot stat 'config.inc.php.dist': No such file or directory

┌──(root㉿kali)-[/var/www/html/DVWA]
└─# cd config

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service apache2 restart
```

Dashboard | Target | Proxy | Intruder | Repeater | Collaborator | Sequencer | Decoder | Comparer | Logger | Organizer | Extensions

Intercept | HTTP history | WebSockets history | Match and replace | Proxy settings

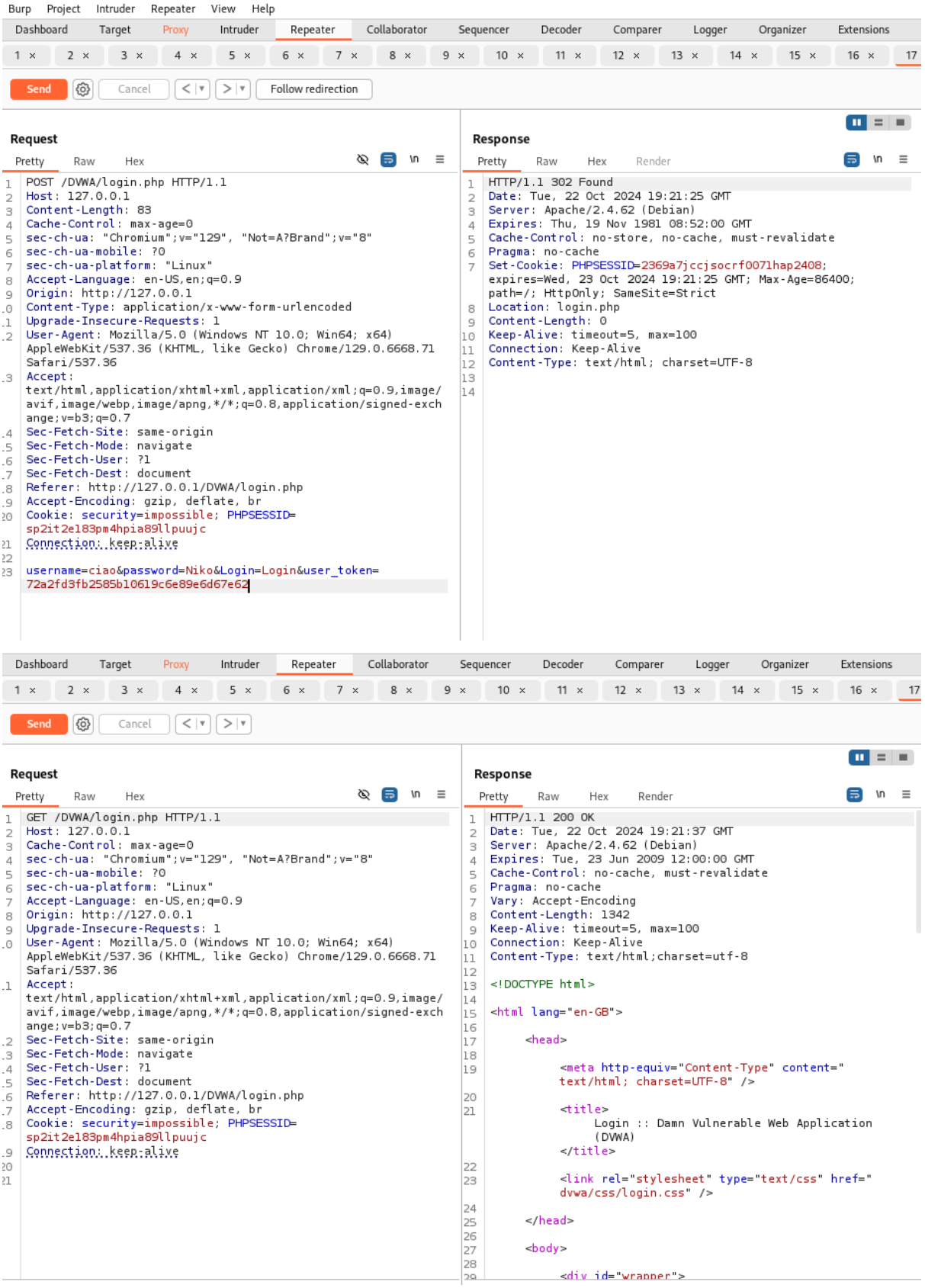
Intercept on | Forward | Drop | Request t

Time	Type	Direction	Host	Method	URL
14:46:32 22 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/DVWA/index.php
14:49:50 22 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/DVWA/index.php
15:03:26 22 Oct 2024	HTTP	→ Request	127.0.0.1	GET	http://127.0.0.1/DVWA/login.php
15:04:01 22 Oct 2024	HTTP	→ Request	127.0.0.1	POST	http://127.0.0.1/DVWA/login.php

Request

Pretty | Raw | Hex

```
1  POST /DVWA/login.php HTTP/1.1
2  Host: 127.0.0.1
3  Content-Length: 88
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Linux"
8  Accept-Language: en-US,en;q=0.9
9  Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
13 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
   b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=sp2it2el83pm4hpia89llpuujc
21 Connection: keep-alive
22
23 username=ciao&password=Niko&Login=Login&user_token=72a2fd3fb2585b10619c6e89e6d67e62
```


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 × 11 × 12 × 13 × 14 × 15 × 16 × 17
Send Cancel Follow redirection
Request
Pretty Raw Hex
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 83
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=sp2it2e183pm4hpia89llpuujc
21 Connection: keep-alive
22
23 username=ciao&password=Niko&Login=Login&user_token=72a2fd3fb2585b10619c6e89e6d67e62
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 22 Oct 2024 19:21:25 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=2369a7jccjsocrf0071hap2408; expires=Wed, 23 Oct 2024 19:21:25 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 × 11 × 12 × 13 × 14 × 15 × 16 × 17
Send Cancel
Request
Pretty Raw Hex
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Origin: http://127.0.0.1
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: http://127.0.0.1/DVWA/login.php
17 Accept-Encoding: gzip, deflate, br
18 Cookie: security=impossible; PHPSESSID=sp2it2e183pm4hpia89llpuujc
19 Connection: keep-alive
20
21
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Tue, 22 Oct 2024 19:21:37 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 1342
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html;charset=utf-8
12
13 <!DOCTYPE html>
14
15 <html lang="en-GB">
16
17 <head>
18
19 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
20
21 <title>Login :: Damn Vulnerable Web Application (DVWA)</title>
22
23 <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />
24
25 </head>
26
27 <body>
28
29