

kali 1 [In esecuzione] - Oracle VM VirtualBox

1 2 3 4

Trash

File System

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

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:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=6t0ck82o47ce8q6jp8f48co83f; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=466275d69f7720bbcc1656419b244497
```

0 highlights

Login :: Damn Vulnerable x

127.0.0.1/DVWA/login.php

DVWA

Username

admin

Password

\*\*\*\*\*

Login

[Damn Vulnerable Web Application \(DVWA\)](#)

kali 1 [In esecuzione] - Oracle VM VirtualBox

Trash

File System

Login :: Damn Vulnerable x +

127.0.0.1/DVWA/login.php

DVWA

Burp Suite Community Edition v2023.9.1 - Temporary Project

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

1 x +

Send Cancel < >

Target: http://127.0.0.1 HTTP/1

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:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/115.0.5790.171 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,ima
  ge/avif,image/webp,image/apng,*/*;q=0.8,application/sign
  d-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=6t0ck82o47ce8q6jp8f48co83f; security=
  impossible
19 Connection: close
20
21
```

Response

Pretty Raw Hex Render

```
50 <input type="password" class="loginInput"
51   AUTOCOMPLETE="off" size="20" name="password">
52 <br />
53 <p class="submit">
54   <input type="submit" value="Login" name="
55   Login">
56 </p>
57 </fieldset>
58
59 </form>
60
61 <br />
62
63 <div class="message">
64   Login failed
65 </div>
66
67 <br />
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73
74 </div>
75 <!--<div id="content">-->
76
77 <div id="footer">
78 <p>
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

Done

1,672 bytes | 85 millis