

Login :: Damn Vulnerable x +

← → X ⓘ 127.0.0.1/DVWA/login.php



Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Burp Project Intruder Repeater View Help

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

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

 Request to http://127.0.0.1:80

Forward

Drop

Intercept is on

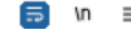
Action

Open browser

Add notes

HTTP/1 ⓘ

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: "Not(A:Brand";v="24", "Chromium";v="122"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
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
12 Gecko) Chrome/122.0.6261.112 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-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=ndgq96k4mt8j1kil0rh829l3r0
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=1a617a4e3197b075ab60c0c61be24696
```

Inspector



Request attributes

2 v

Request query parameters

0 v

Request body parameters

4 v

Request cookies

2 v

Request headers

20 v

Inspector

Notes



Search




0 highlights

Event log

All issues

Memory: 103.4MB



The screenshot shows a web browser's address bar. The address bar contains the URL `127.0.0.1/DVWA/login.php`. To the left of the address bar, the page title is visible as `Login :: Damn Vulnerable`. The browser's navigation buttons (back, forward, reload, home) and other icons (star, lock, etc.) are also visible.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder

Extensions Learn

Send Cancel < > Follow redirection

1 x +
Target: http://127.0.0.1
HTTP/1

Inspector
Request
Response
Raw
Hex
Sequencer
Decoder
Comparer
Logger
Organizer
Settings

Request

```

1 POST /DWAA/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: "Not(A:Brand";v="24",
  "Chromium";v="122"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
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/122.0.6261.112 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/DWAA/login.php
18 Accept-Encoding: gzip, deflate, br
          
```

Response

Pretty Raw Hex Render In

```

1 HTTP/1.1 302 Found
2 Date: Tue, 09 Apr 2024 20:43:09 GMT
3 Server: Apache/2.4.58 (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=o9k25g16bv948ss6o2ds6od6b; expires=Wed, 10 Apr 2024 20:43:09 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: login.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
          
```

| Inspector | | X |
|--------------------------|--|----|
| Request attributes | | 2 |
| Request query parameters | | 0 |
| Request body parameters | | 4 |
| Request cookies | | 2 |
| Request headers | | 20 |
| Response headers | | 10 |

Done
Event log All issues
439 bytes | 21 millis

