

SIMULAZIONE ATTACCO DI BRUTE FORCE (LOGIN, PASSWORD) come man in the middle A SERVIZIO SERVER DVWA UTILIZZANDO IL TOOL BURPSUIT CHE INTERCETTA IL TRAFFICO DI DATI TRA CLIENT (KALI) E SERVER: in base al sito a cui si vuole accedere simula un tentativo di accesso al sito tramite username e password.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A GET request to `/DWA/login.php` is displayed on the left, and the corresponding HTML response is on the right. The response shows a login form with a password field and a submit button labeled 'Login'. Below the form, a message box indicates 'Login failed'.

Request:

```
1 GET /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
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/119.0.6045.159 Safari/537.36
10 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
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/DWA/login.php
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=0stff0kuh0u7qdfjjocqk706mr
19 Connection: close
20
21
```

Response:

```
49 <label for="pass">
    Password
  </label>
  <input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="
    password">
  <br />
50
51 <br />
52
53 <p class="submit">
  <input type="submit" value="Login" name="Login">
  </p>
54
55 </fieldset>
56
57 <input type="hidden" name='user_token' value='ed8b328f1094850b22775b9b3375874e'
  />
58
59 </form>
60
61 <br />
62
63 <div class="message">
  Login failed
  </div>
64
```

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A POST request to `/DWA/login.php` is displayed on the left, and the 'Inspector' panel on the right shows the request body parameters. The request body contains a JSON object with 'username', 'password', and 'user_token' fields.

Request:

```
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 85
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
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/119.0.6045.159 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/DWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=0stff0kuh0u7qdfjjocqk706mr
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=b4c3c0eff58f262000451983181e0694
```

Inspector - Request body parameters:

Parameter	Value
username	admin
password	password
Login	Login
user_token	b4c3c0eff58f262000451983181e0694

1 x2 x+

SendCancel<>>

Target: http://127.0.0.1HTTP/1

Request

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="119", "Not?A_Brand";v="24"

5 sec-ch-ua-mobile: ?0

6 sec-ch-ua-platform: "Linux"

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/119.0.6045.159 Safari/537.36

10 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

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, br

17 Accept-Language: en-US,en;q=0.9

18 Cookie: security=impossible; PHPSESSID=0stff0kuh0u7qdfjjocqk706mr

19 Connection: close

20

21

Response

1 HTTP/1.1 200 OK

2 Date: Wed, 06 Dec 2023 21:06:07 GMT

3 Server: Apache/2.4.58 (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: 1442

9 Connection: close

10 Content-Type: text/html; charset=utf-8

11

12 <!DOCTYPE html>

13

14 <html lang="en-GB">

15

16 <head>

17

18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

19

20 <title>

21 Login :: Damn Vulnerable Web Application (DVWA)

22 </title>

23

24 <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

25

26 </head>

0 highlights

0 highlights

Done

1,733 bytes | 89 millis

CTRL (DESTRA)