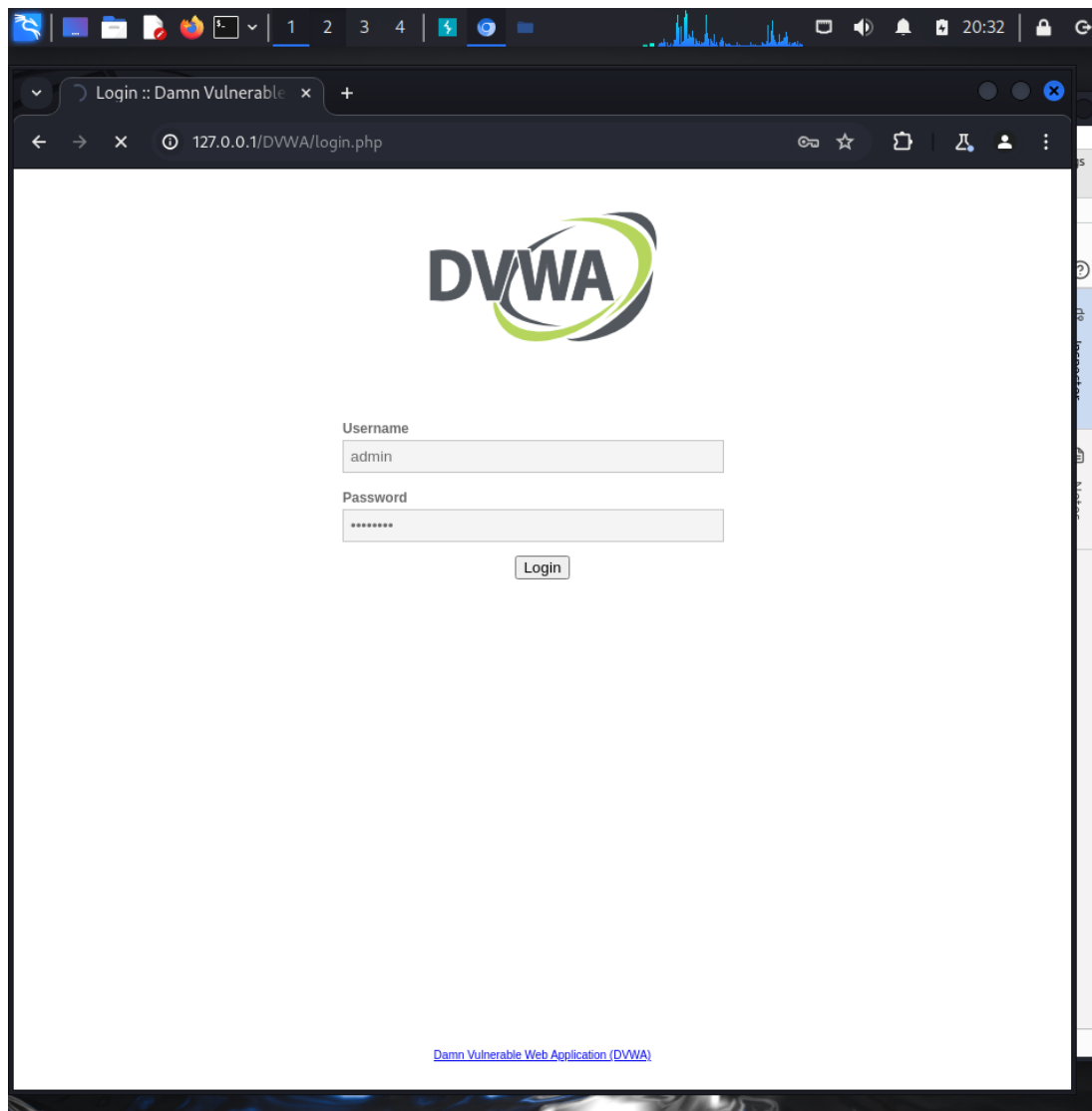


# S3L2

## Screen iniziale di login



## Screen del primo forward dopo l'inserimento dei dati di login

The screenshot displays the Burp Suite Community Edition v2024.4.5 interface. The main window shows a captured HTTP request in the 'Proxy' tab. The request is a POST to `http://127.0.0.1:80/DWA/login.php`. The 'Pretty' view of the request body shows the following data:

```
POST /DWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=dfhjdreckh1kpm752p4b6o6dfi
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=ee3507437053616e784115f3adf880cb
```

The right-hand side of the interface shows the 'Inspector' panel, which is currently empty. The bottom status bar indicates 'Memory: 105.0MB'.

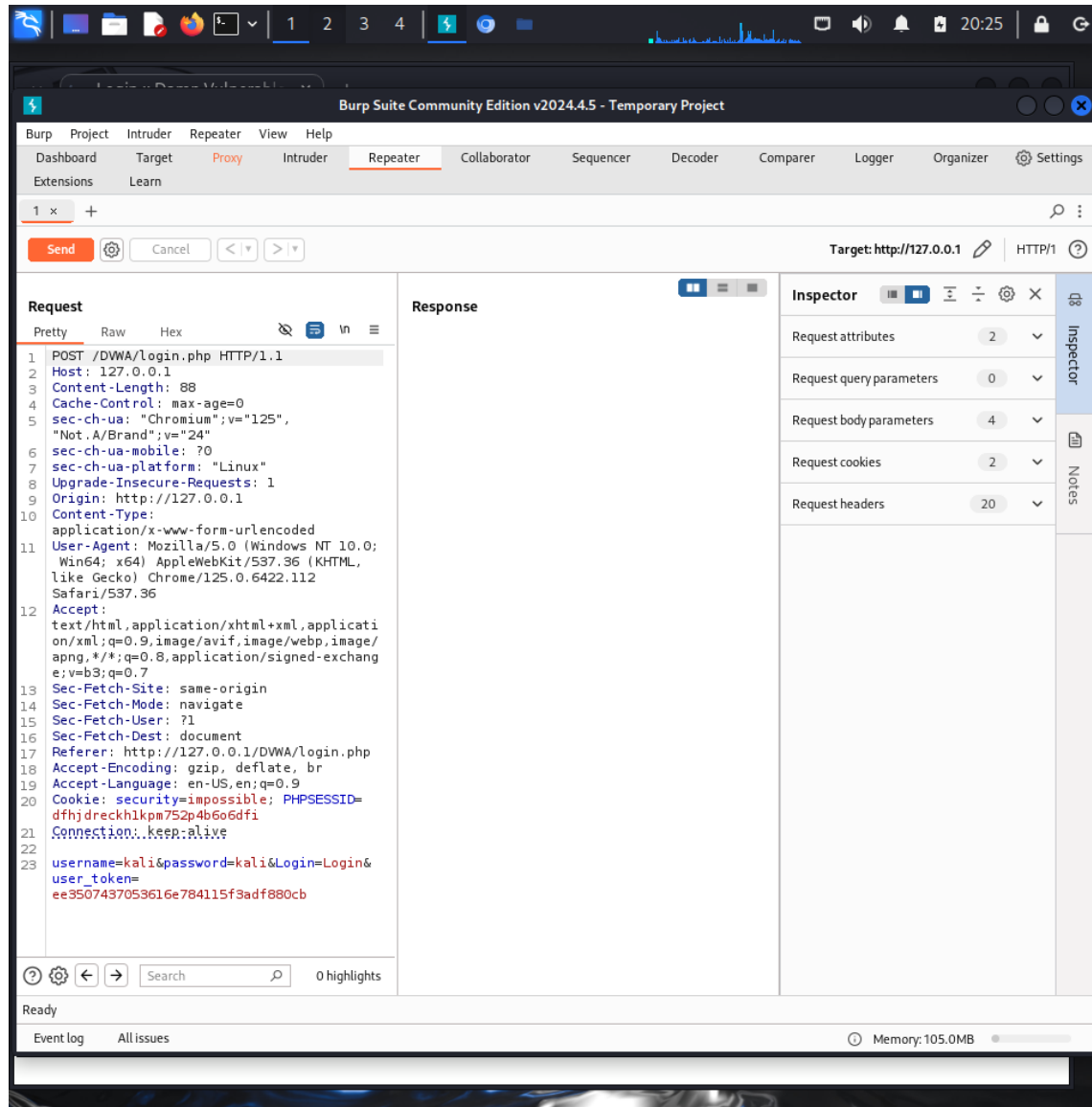
## Screen modifica dati di login prima di inviarla al repeater

The screenshot displays the Burp Suite Community Edition v2024.4.5 interface. The main workspace shows an intercepted HTTP POST request to `http://127.0.0.1:80/DWA/login.php`. The request body is visible in the Pretty tab, showing the following data:

```
POST /DWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=dfhjdreckh1kpm752p4b6o6dffi
Connection: keep-alive
username=kali&password=kali&Login=Login&user_token=ee3507437053616e784115f3adf880cb
```

The Inspector panel on the right shows the request details, including request attributes, query parameters, body parameters, cookies, and headers. The status bar at the bottom indicates the memory usage is 105.0MB.

## Screen arrivato alla sezione repeater



## Screen invio richiesta con dati errati e prima di eseguire il follow redirection

The screenshot displays the Burp Suite Community Edition v2024.4.5 interface. The 'Repeater' tab is active, showing a single request. The target is set to `http://127.0.0.1` with the method `HTTP/1`.

**Request Details:**

- Method: `POST`
- URL: `/DWA/login.php`
- Host: `127.0.0.1`
- Content-Length: `83`
- Cache-Control: `max-age=0`
- sec-ch-ua: `"Chromium";v="125", "Not.A/Brand";v="24"`
- sec-ch-ua-mobile: `0`
- sec-ch-ua-platform: `"Linux"`
- Upgrade-Insecure-Requests: `1`
- Origin: `http://127.0.0.1`
- Content-Type: `application/x-www-form-urlencoded`
- User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36`
- 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`
- Sec-Fetch-Site: `same-origin`
- Sec-Fetch-Mode: `navigate`
- Sec-Fetch-User: `?1`
- Sec-Fetch-Dest: `document`
- Referer: `http://127.0.0.1/DWA/login.php`
- Accept-Encoding: `gzip, deflate, br`
- Accept-Language: `en-US,en;q=0.9`
- Cookie: `security=impossible; PHPSESSID=dfhjdreckh1kpm752p4b6o6dfi`
- Connection: `keep-alive`
- username=kali&password=kali&Login=Login&user\_token=ee3507437053616e784115f3adf880cb

**Response Details:**

- Status: `HTTP/1.1 302 Found`
- Date: `Tue, 11 Jun 2024 18:26:00 GMT`
- Server: `Apache/2.4.59 (Debian)`
- Expires: `Thu, 19 Nov 1981 08:52:00 GMT`
- Cache-Control: `no-store, no-cache, must-revalidate`
- Pragma: `no-cache`
- Set-Cookie: `PHPSESSID=csg77mamu7alk8ngqql0apm6tn; expires=Wed, 12 Jun 2024 18:26:00 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict`
- Location: `login.php`
- Content-Length: `0`
- Keep-Alive: `timeout=5, max=100`
- Connection: `Keep-Alive`
- Content-Type: `text/html; charset=UTF-8`

The right-hand side of the interface shows the 'Inspector' panel with request attributes, query parameters, body parameters, cookies, headers, and response headers. The status bar at the bottom indicates 'Done' and '476 bytes | 1,014 millis'.

# Screen dopo il redirection 1

The screenshot displays the Burp Suite Community Edition v2024.4.5 interface. The 'Repeater' tab is active, showing a single request and response. The target is set to 'http://127.0.0.1'.

**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="125",
5 "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 User-Agent: Mozilla/5.0 (Windows NT 10.0;
11 Win64; x64) AppleWebKit/537.36 (KHTML,
12 like Gecko) Chrome/125.0.6422.112
13 Safari/537.36
14 Accept:
15 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
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Referer: http://127.0.0.1/DVWA/login.php
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-US,en;q=0.9
22 Cookie: security=impossible; PHPSESSID=
23 dfhjdreckhlpn752p4b6o6dfi
24 Connection: keep-alive
```

**Response:**

```
1 HTTP/1.1 200 OK
2 Date: Tue, 11 Jun 2024 18:27:18 GMT
3 Server: Apache/2.4.59 (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"
20 content="text/html; charset=UTF-8" />
21
22 <title>Login :: Damn Vulnerable Web
23 Application (DVWA)</title>
24
25 <link rel="stylesheet" type="text/css"
26 href="dvwa/css/login.css" />
27
28 </head>
29
30 <body>
31
32 <div id="wrapper">
33
34 <div id="header">
35
36 <br />
37
38 <p></p>
40
41 </div>
42
43 </div>
44
45 </body>
46
47 </html>
```

**Inspector:**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 18
- Response headers: 10

**Footer:**

Done 1,670 bytes | 1,010 millis

Event log All issues Memory: 105.2MB

## Screen dopo il redirection 2

The screenshot displays the Burp Suite Community Edition v2024.4.5 interface. The 'Repeater' tab is active, showing a single request and its corresponding response.

**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="125",
  "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/125.0.6422.112
  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=
  dfhjdreckh1kpm752p4b6o6dfi
19 Connection: keep-alive
20
21
```

**Response:**

```
34 <p></p>
36
37 <br />
38
39 </div> <!--div id="header">-->
40
41 <div id="content">
42
43 <form action="login.php" method="post">
44
45 <fieldset>
46
47 <label for="user">Username</label>
48 <input type="text" class="loginInput"
49 size="20" name="username"><br />
50
51 <label for="pass">Password</label>
52 <input type="password" class="loginInput"
53 AUTOCOMPLETE="off" size="20" name="
54 password"><br />
55
56 <br />
57
58 <p class="submit"><input type="
59 submit" value="Login" name="Login"></p>
60
61 </fieldset>
62
63 <input type="hidden" name='user_token'
64 value='45b1bd43dd922ba888115cac2fd6336b'
65 />
66
67 </form>
68
69 <br />
70
```

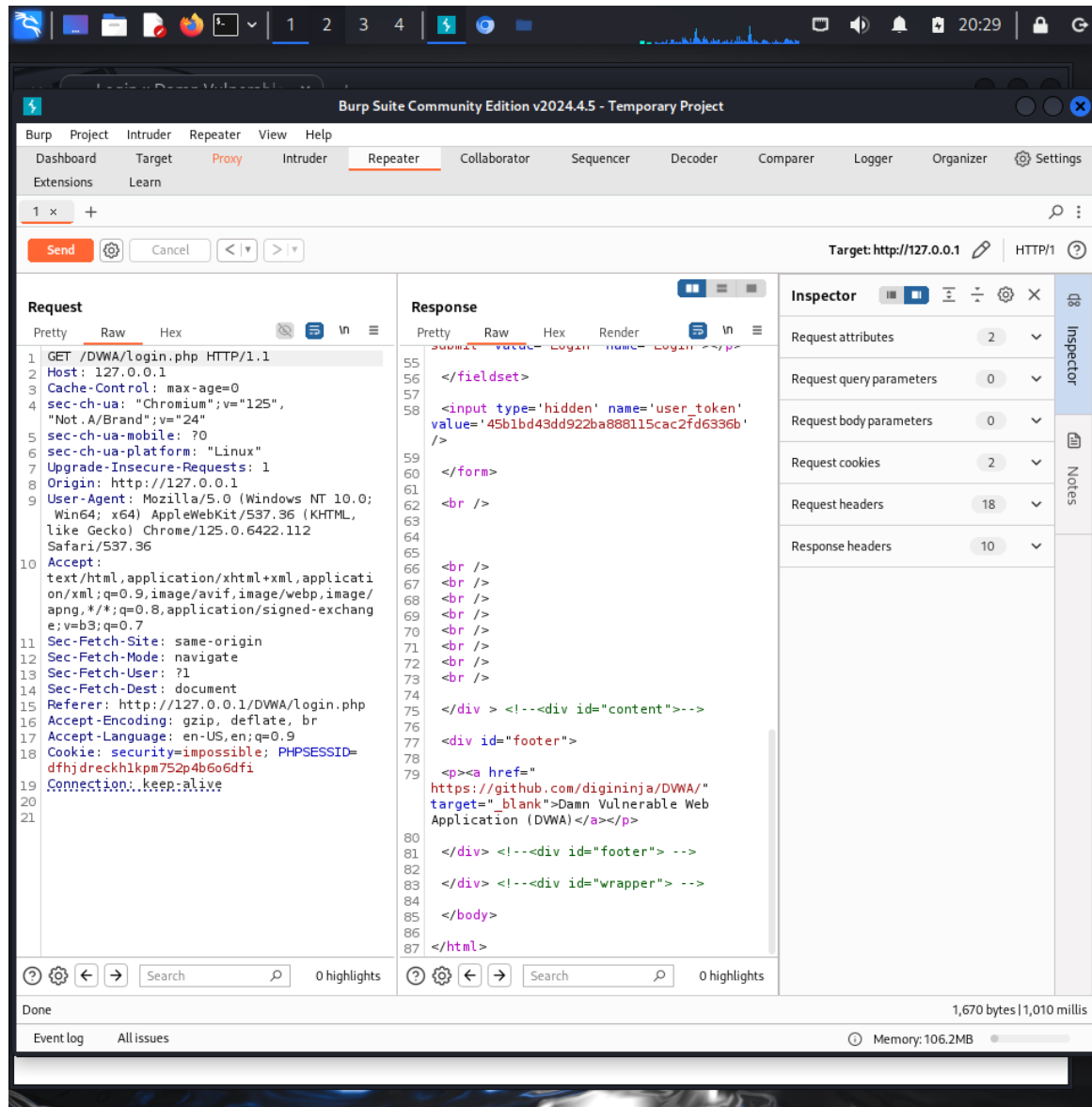
**Inspector:**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 18
- Response headers: 10

**Bottom Bar:**

- Done
- Event log
- All issues
- Memory: 106.2MB

## Screen dopo il redirection 3



**PS: Non sono riuscito a completare l'esercizio, in quanto, come può vedere nell'ultimo screen, ho riscontrato due problemi che sono: Riga 19 in basso a sinistra dove c'è scritto "connection" che non mi dava la dicitura "close" e il secondo problema è la mancanza della scritta "login failed" che continuava a non apparire e, di conseguenza, a crearmi confusione. Molto probabilmente non avrò eseguito nel modo corretto qualche passaggio. Quindi, quando correggerà l'esercizio, le sarei grato se riuscisse a darmi una dritta su questo esercizio!**