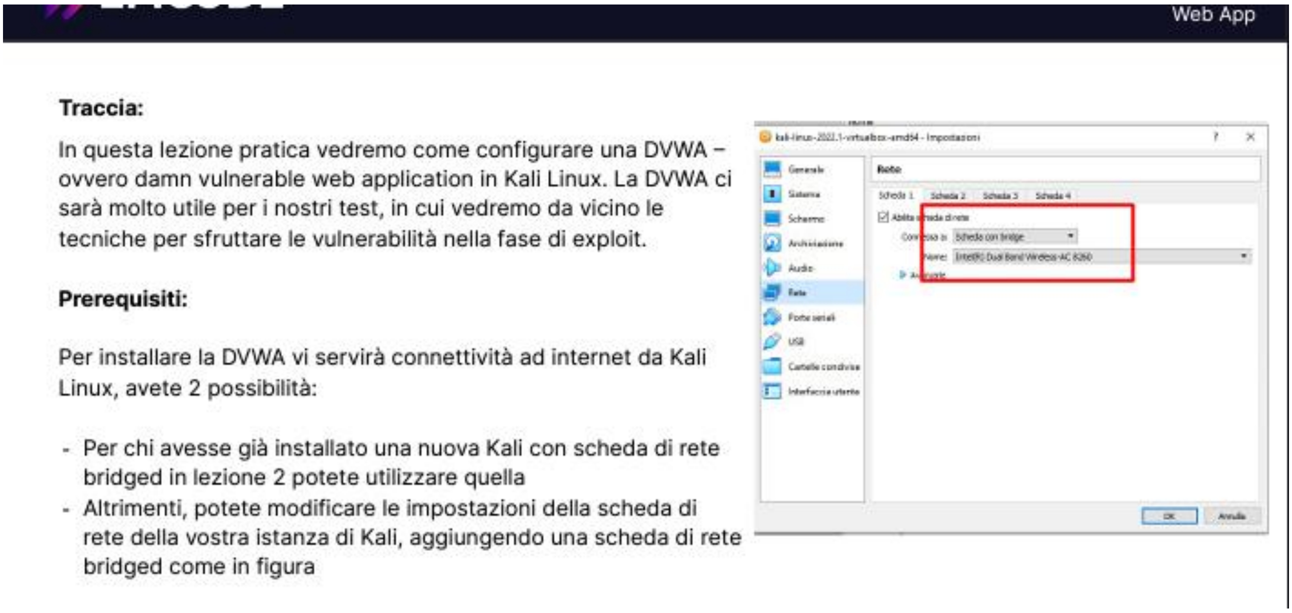


**Traccia:**

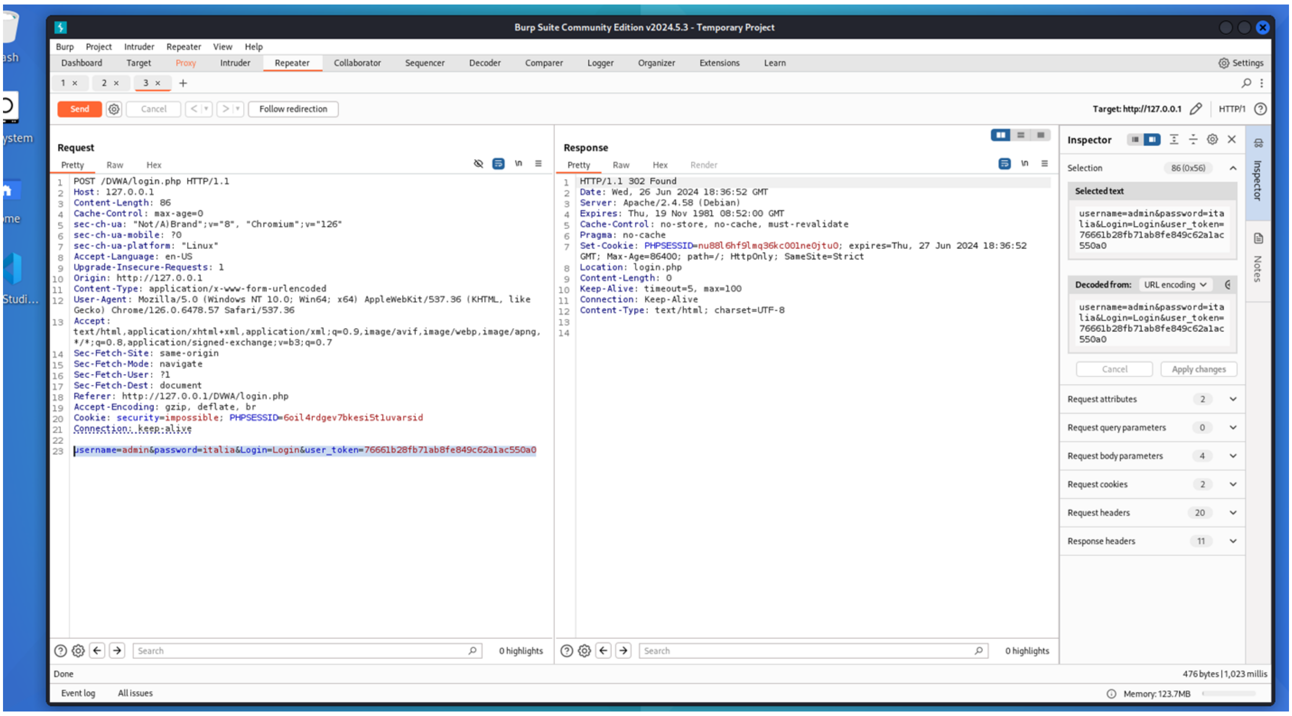
In questa lezione pratica vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test, in cui vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

**Prerequisiti:**

Per installare la DVWA vi servirà connettività ad internet da Kali Linux, avete 2 possibilità:

- Per chi avesse già installato una nuova Kali con scheda di rete bridged in lezione 2 potete utilizzare quella
- Altrimenti, potete modificare le impostazioni della scheda di rete della vostra istanza di Kali, aggiungendo una scheda di rete bridged come in figura

W8D1 -- BURPSUITE



Request

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 86
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
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/126.0.6478.57 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/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=6oil4rdgev7bkesi5t1uvarsid
Connection: keep-alive

username=admin&password=italia&Login=Login&user_token=76661b28fb71ab8fe849c62a1ac550a0
```

Response

```
HTTP/1.1 302 Found
Date: Wed, 26 Jun 2024 18:36:52 GMT
Server: Apache/2.4.58 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=nu88l6hf9lmq36kc001ne0jtu0; expires=Thu, 27 Jun 2024 18:36:52
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


```

Inspector

Selection 86 (0x56)

Selected text

```
username=admin&password=ita
lia&Login=Login&user_token=
76661b28fb71ab8fe849c62a1ac
550a0
```

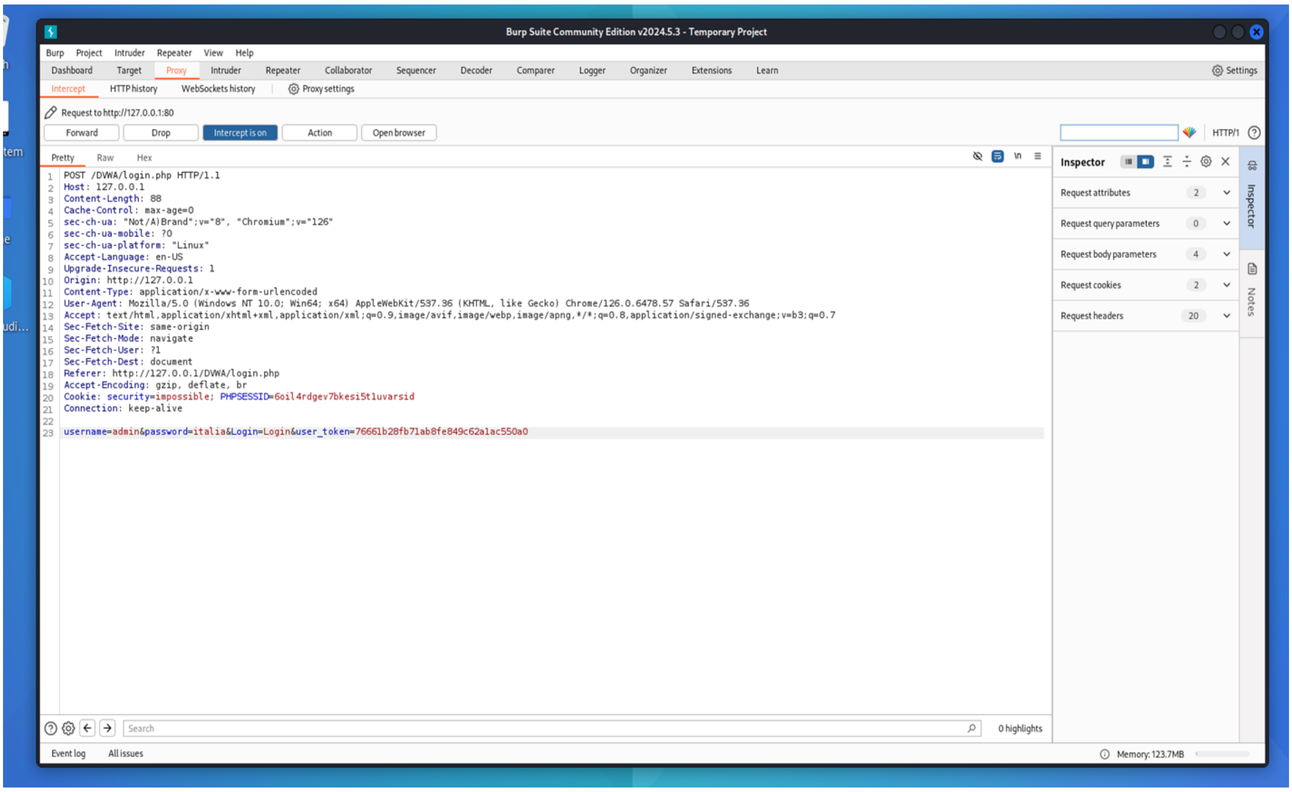
Decoded from: URL encoding

```
username=admin&password=ita
lia&Login=Login&user_token=
76661b28fb71ab8fe849c62a1ac
550a0
```

Cancel | Apply changes

| | |
|---|---|
| Request attributes | 2 |
| Request query parameters | 0 |
| Request body parameters | 4 |
| Request cookies | 2 |
| Request headers | 20 |
| Response headers | 11 |

MODIFICA PASSWORD:

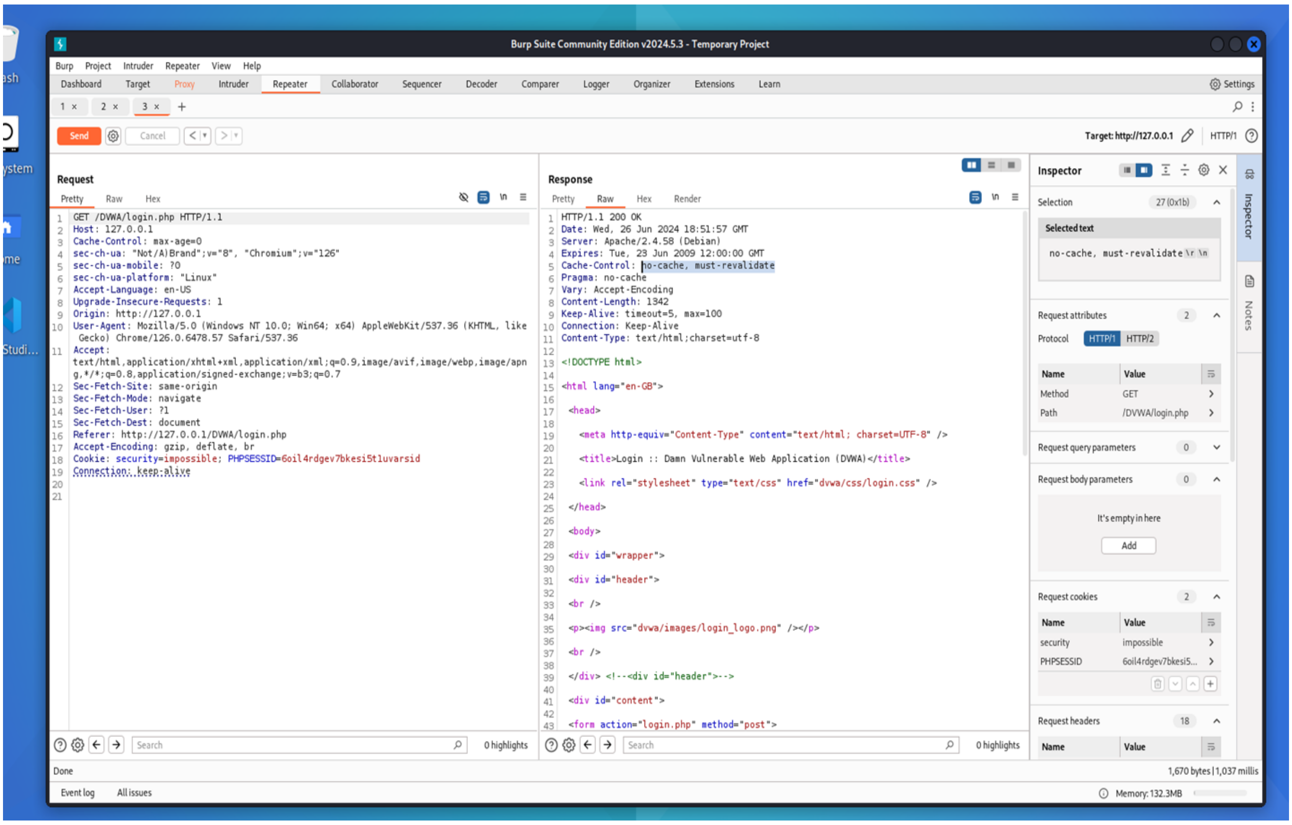

Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
HTTP/1
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log All issues
Memory: 123.7MB

Request to http://127.0.0.1:80

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
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/126.0.6478.57 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/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=6oil4rdgev7bkesi5t1uvarsid
Connection: keep-alive

username=admin&password=italia&Login=Login&user_token=76661b28fb71ab8fe849c62a1ac550a0
```

Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers 20


Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × 3 × +
Send Cancel
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes
Search
0 highlights
Event log All issues
Memory: 132.3MB

Target: http://127.0.0.1

Request

```
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/126.0.6478.57 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;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/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=6oil4rdgev7bkesi5t1uvarsid
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2024 18:51:57 GMT
Server: Apache/2.4.58 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1342
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

 <head>

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

   <title>Login :: Damn Vulnerable Web Application (DWVA)</title>

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

 </head>

 <body>

 <div id="wrapper">

 <div id="header">

 <br />

 <p><img src="dvwa/images/login_logo.png" /></p>

 <br />

 </div> <!--<div id="header">-->

 <div id="content">

 <form action="login.php" method="post">
```

Selection 27 (0x1b)

Selected text

`no-cache, must-revalidate \r \n`

Request attributes 2

Protocol HTTP/1 HTTP/2

| Name | Value |
|---|---|
| Method | GET |
| Path | /DVWA/login.php |

Request query parameters 0

Request body parameters 0

It's empty in here

Add

Request cookies 2

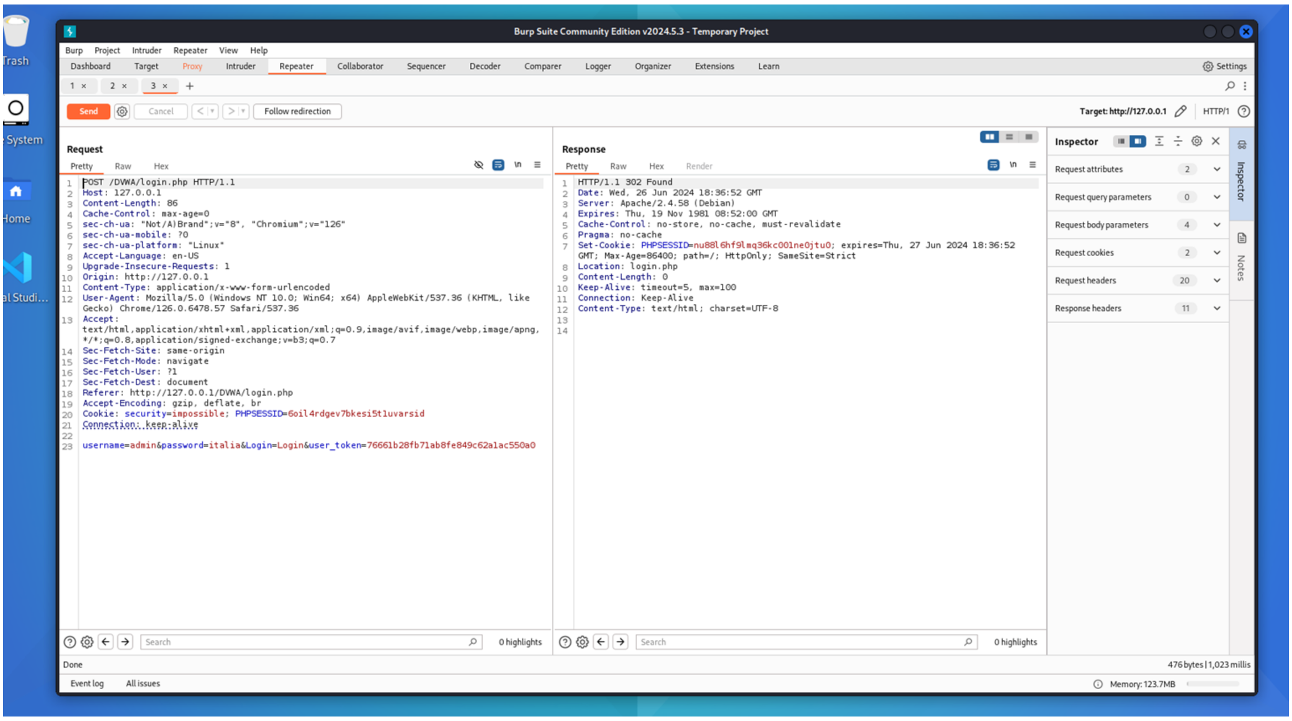
| Name | Value |
|---|---|
| security | impossible |
| PHPSESSID | 6oil4rdgev7bkesi5... |

Request headers 18

| Name | Value |
|---|---|

Done

1,670 bytes | 1,037 millis



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 86
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
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/126.0.6478.57 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/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=6oil4rdgev7bkesi5t1uvarsid
Connection: keep-alive

username=admin&password=italia&Login=Login&user_token=76661b28fb71ab8fe849c62a1ac550a0
```

```
HTTP/1.1 302 Found
Date: Wed, 26 Jun 2024 18:36:52 GMT
Server: Apache/2.4.58 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=nu88l6hf9lmq36kc001ne0jtu0; expires=Thu, 27 Jun 2024 18:36:52
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


```

Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers 20
Response headers 11

476 bytes | 1,023 millis