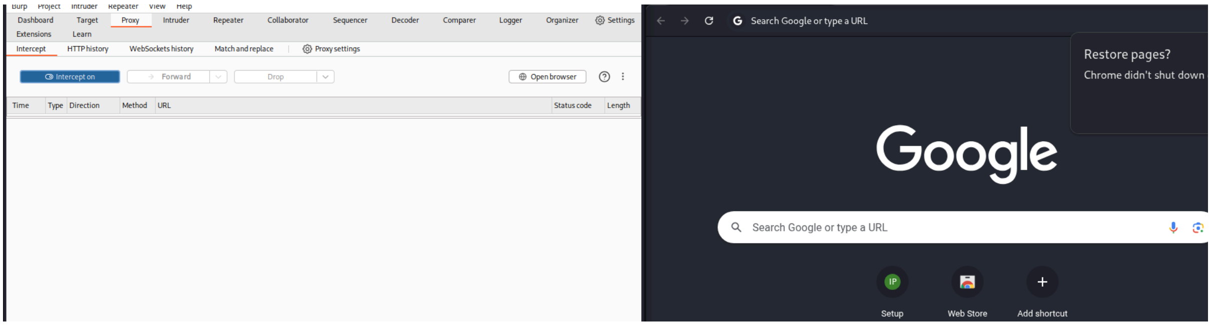
Alessandro Azzolini
M2,W3,D3

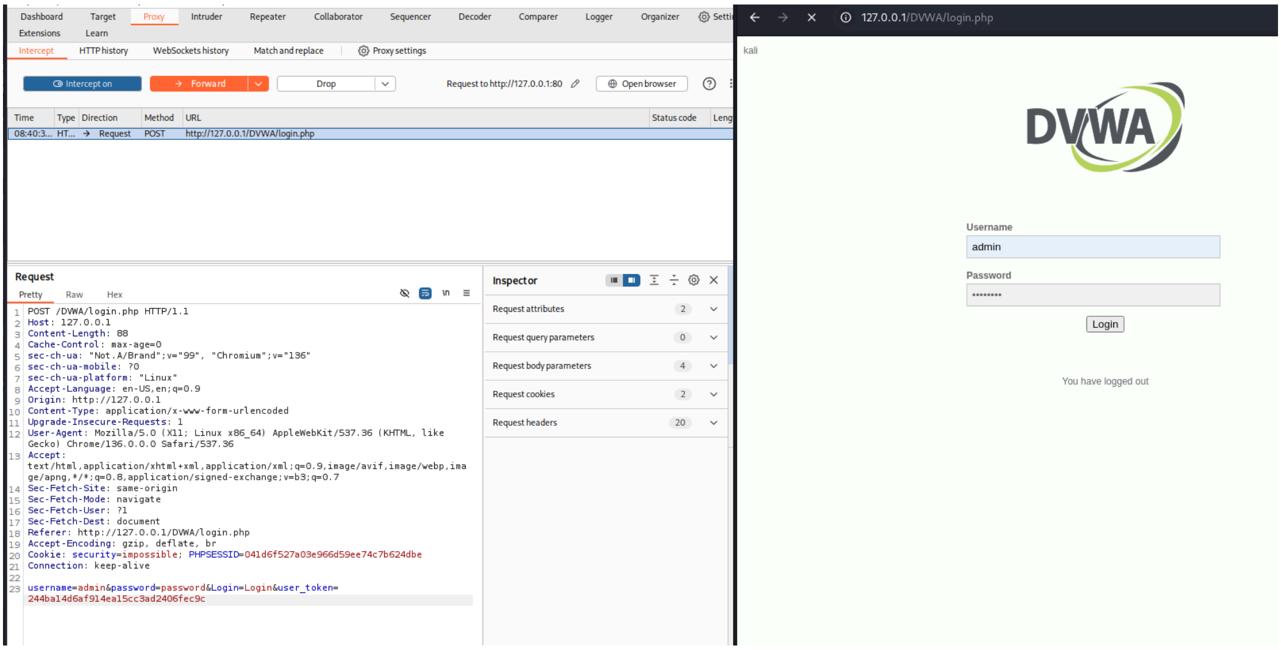
TRACCIA:

L’esercizio richiede di installare Burp Suite e il server DVWA sulla macchina virtuale Kali Linux, testando il login in modalità di sicurezza “low”, intercettando il pacchetto del client e modificando i parametri prima di spedirlo al server.

1 Come prima cosa si apra burp suite, si attivi l’interceptor e si apra una pagina web (da burp suite). Si inserisca poi l’ip della DVWA per arrivare alla pagina del login. Ad ogni passaggio si prema forward per inviare ogni singola comunicazione da client a server.



2 Dalla finestra di login si inseriscano le credenziali corrette e si prema login. Su burp suite comparirà il pacchetto post con la richiesta del client compresa di user e password. Si noti che nel pacchetto, in ultima riga ci sono proprio le credenziali appena inserite. Inoltre si noti anche che nella sezione “Cookie security” è possibile modificare il livello di sicurezza del sito.



08:40:3... HT... → Request POST http://127.0.0.1/DVWA/login.php

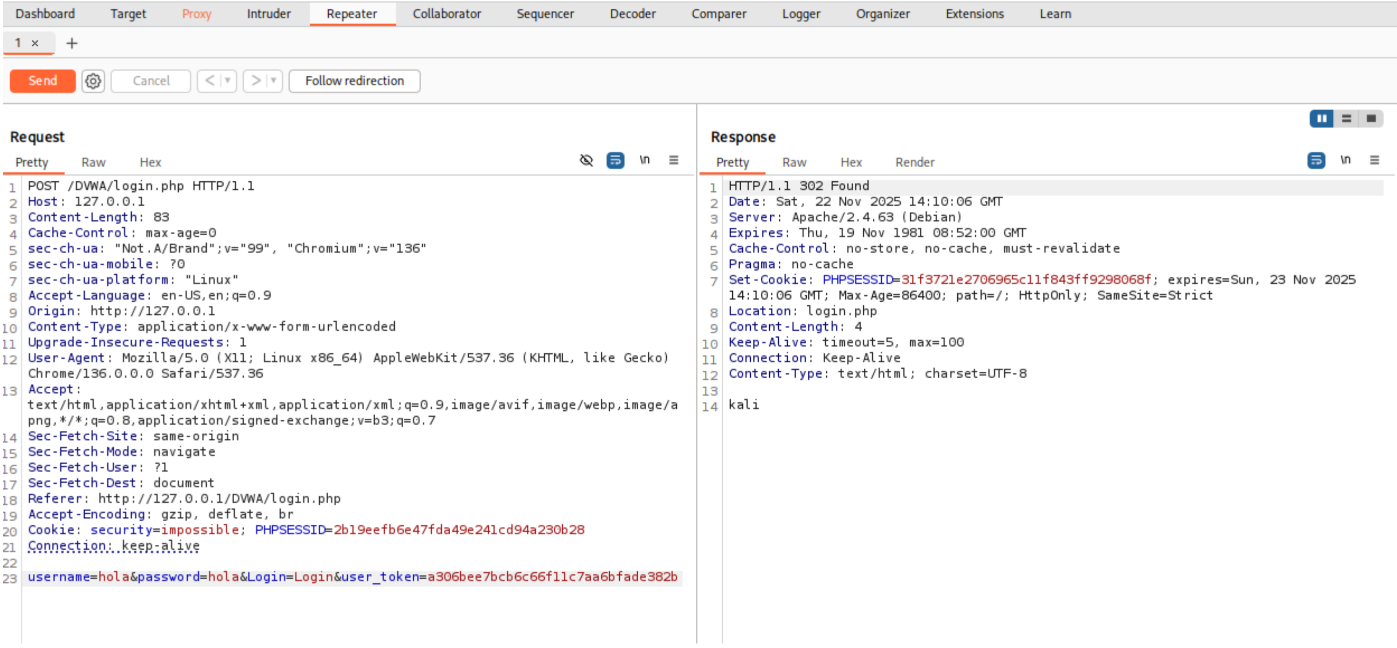
```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/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=041d6f527a03e966d59ee74c7b624dbe
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=
244ba14d6af914ea15cc3ad2406fec9c
```

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

Username: admin
Password: ********

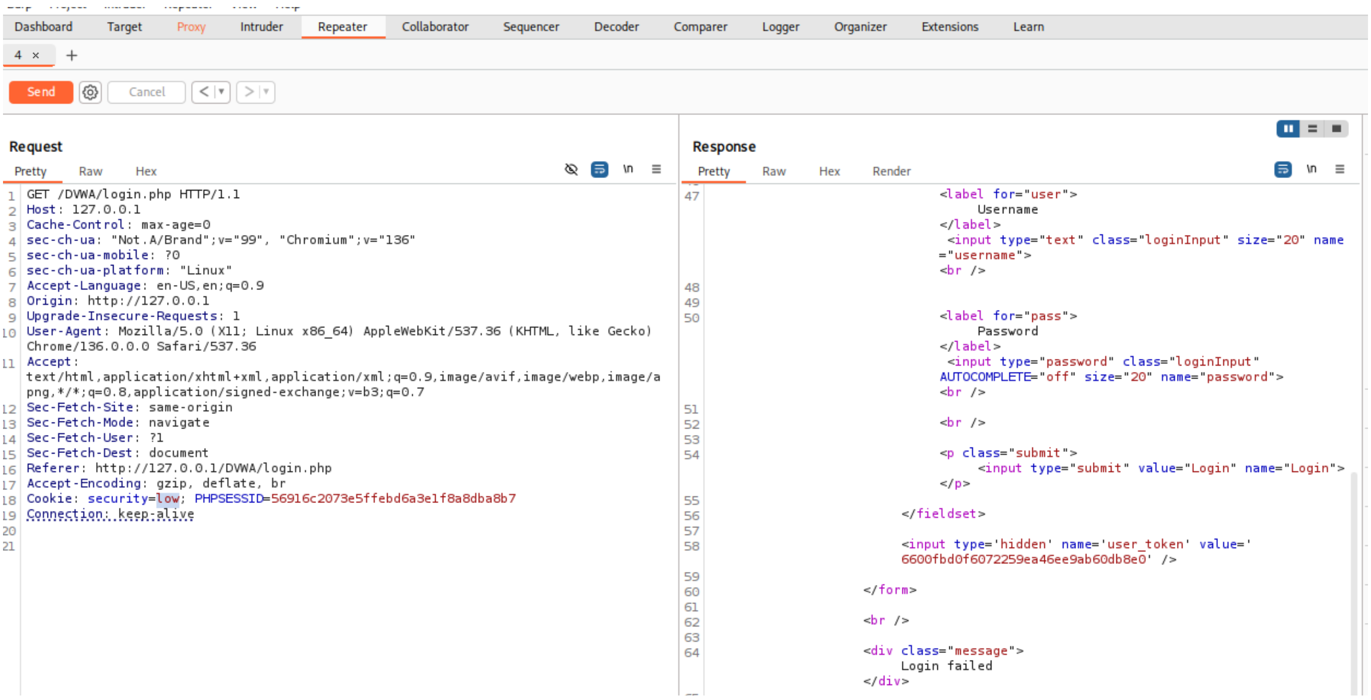
You have logged out

3 Andando su repeater possiamo modificare il pacchetto e mandarlo per vedere la risposta del server: inserendo una password errata il server risponde infatti con un “login failed”.



```
POST /DWWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 83
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;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/DWWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=2b19eefb6e47fda49e241cd94a230b28
Connection: keep-alive

username=hola&password=hola&Login=Login&user_token=a306bee7bcb6c66f11c7aa6bfade382b
```

```
HTTP/1.1 302 Found
Date: Sat, 22 Nov 2025 14:10:06 GMT
Server: Apache/2.4.63 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=31f3721e2706965c11f843ff9298068f; expires=Sun, 23 Nov 2025
14:10:06 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
Location: login.php
Content-Length: 4
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

kali
```



```
GET /DWWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;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/DWWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=56916c2073e5ffebd6a3e1f8a8dba8b7
Connection: keep-alive
```

```
                    <label for="user">
                        Username
                    </label>
                     <input type="text" class="loginInput" size="20" name
                    ="username">
                    <br />


                    <label for="pass">
                        Password
                    </label>
                     <input type="password" class="loginInput"
                    AUTOCOMPLETE="off" size="20" name="password">
                    <br />

                    <br />

                    <p class="submit">
                        <input type="submit" value="Login" name="Login">
                    </p>

                </fieldset>

                <input type='hidden' name='user_token' value='
                6600fbd0f6072259ea46ee9ab60db8e0' />

            </form>

            <br />

            <div class="message">
                Login failed
            </div>
```