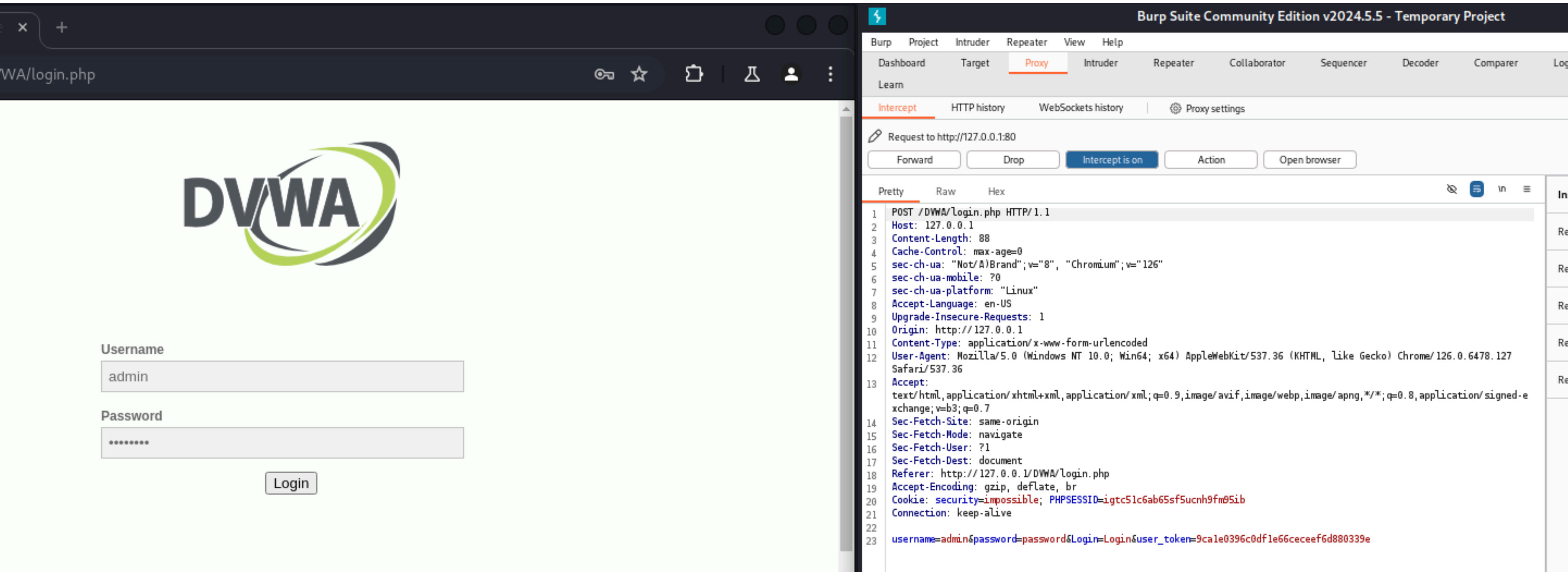


S3-E4

Verificare processo login con Burpsuite

Inserendo le CORRETTE credenziali all'interno della pagina (sinistra), intercettando Burpsuite possiamo vedere questi dati in chiaro (riga 23).



The image shows a side-by-side comparison of a web application's login page and a network traffic capture tool. On the left, the DVWA (Damn Vulnerable Web Application) login page is displayed. It features the DVWA logo at the top, followed by input fields for 'Username' (containing 'admin') and 'Password' (masked with dots). A 'Login' button is positioned below the password field. On the right, the Burp Suite Community Edition v2024.5.5 interface is shown, specifically the 'Proxy' tab. The 'Intercept' section is active, displaying a request to 'http://127.0.0.1:80'. The request details are shown in 'Pretty' format, listing various headers like 'Host', 'Content-Length', 'Cache-Control', 'sec-ch-ua', 'sec-ch-ua-mobile', 'sec-ch-ua-platform', 'Accept-Language', 'Upgrade-Insecure-Requests', 'Origin', 'Content-Type', 'User-Agent', 'Accept', 'Sec-Fetch-Site', 'Sec-Fetch-Mode', 'Sec-Fetch-User', 'Sec-Fetch-Dest', 'Referer', 'Accept-Encoding', 'Cookie', and 'Connection'. The body of the request is visible at the bottom, showing the login attempt with parameters: 'username=admin&password=password&Login=Login&user_token=9cale0396c0df1e66cecef6d880339e'.

Username
admin

Password
.....

Login

Burp Suite Community Edition v2024.5.5 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Log

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:80

Forward Drop **Intercept is on** Action Open browser

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="8", "Chromium";v="126"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 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-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=impossible; PHPSESSID=igtc51c6ab65sf5ucnh9fm05ib
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=9cale0396c0df1e66cecef6d880339e
```

Modifichiamo da Burpsuite le credenziali (corrette) inserite e per esperimento le modifichiamo con credenziali errate e utilizzando Burpsuite andiamo ad analizzare gli eventi successivi.

The image shows a web browser window on the left displaying the DVWA (Damn Vulnerable Web Application) login page. The page has a logo at the top and two input fields: 'Username' with the value 'admin' and 'Password' with masked characters. A 'Login' button is at the bottom. The browser's address bar shows '27.0.0.1/DVWA/login.php'.

On the right, the Burp Suite Community Edition v2024.5.5 interface is shown in 'Proxy' mode. It displays an intercepted HTTP POST request to 'http://127.0.0.1:80'. The request details are as follows:

- Method: POST
- URL: /DVWA/login.php
- 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/126.0.6478.127 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;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=gg8khp0cqrra7b8ar3meuou832
- Connection: keep-alive

The raw data of the request body is shown at the bottom:

```
username=SonoUn&password=BlackHat&Login=Login&user_token=f606cd289acb70a41b81f843556ce5f5
```

1 x +

SendCancel<>

Request

PrettyRawHex

1GET /DVWA/login.php HTTP/1.1

2Host: 127.0.0.1

3Cache-Control: max-age=0

4Upgrade-Insecure-Requests: 1

5User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

6Accept: 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

7Sec-Fetch-Site: same-origin

8Sec-Fetch-Mode: navigate

9Sec-Fetch-User: ?1

0Sec-Fetch-Dest: document

1sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"

2sec-ch-ua-mobile: ?0

3sec-ch-ua-platform: "Linux"

4Accept-Language: en-US

5Referer: http://127.0.0.1/DVWA/login.php

6Accept-Encoding: gzip, deflate, br

7Cookie: security=impossible; PHPSESSID=dhvhm432pgctmq96kpdbe38e07


8Connection: keep-alive

9

0

Response

PrettyRawHexRender



Username

Password

Login

Login failed

Possiamo osservare come avanzare con le credenziali errate, porterà ad un login fallito. Questo è possibile apprezzarlo osservando il render del response.