

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, followed by 'Username' and 'Password' input fields. The username field contains 'admin' and the password field contains '*****'. A 'Login' button is below the fields. Below the button, it says 'Login failed'. At the bottom, there is a link 'Damn Vulnerable Web Application (DVWA)'.

On the right, the Burp Suite interface is shown. The 'Intercept' tab is active, and a request to 'http://127.0.0.1:80' is being intercepted. The 'Forward' button is highlighted. The 'Raw' tab is selected, showing the raw HTTP request. The request is a POST to '/DVWA/login.php' with the following headers and body:

```
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: "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/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=14d5500e1f7eddfbdd4c7e6b5ed2833
21 Connection: close
22
23 username=ciao&password=ciao&Login=Login&user_token=afdf41d8827af251a18d3b6da9cbd9bc
```

The body of the request is highlighted in grey. The words 'ciao' and 'ciao' in the body are circled in red. The 'Inspector' panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

In questo esercizio abbiamo utilizzato l'app Burp Suite per intercettare request da un client a un server. Con le impostazioni default, il login di DVWA dovrebbe essere un esito se il server riceve un input di "admin" come username, e "password" come password. In questo caso abbiamo intercettato questo pacchetto, e abbiamo modificato gli input che riceverà il nostro server. mettendo ciao e ciao, che sono sbagliate

Login :: Damn Vulnerable x +

127.0.0.1/DVWA/login.php

DVWA

Username

admin

Password

Login

Login failed

Damn Vulnerable Web Application (DVWA)

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send Cancel < >

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=14d5500e1f7edd4c7e6b5ed2839
19 Connection: close
20
21

Response

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

<input type="submit" value="Login" name="Login"></p></fieldset><input type="hidden" name="user_token" value="b59890e8138847b11c5be01f918194d2" /></form>
<div class="message"><div>Login failed</div>

</div><!--div id="content"--><div id="footer">_blank Damn Vulnerable Web Application (DVWA)</div></div>

Inspector

Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 18
Response headers 9

Qua possiamo vedere la risposta del server. Ci spunta un messaggio di login failed, ed esegue il codice corrispondente.