

Di seguito le intercettazioni fatte con BurpSuite verso la pagina DVWA

Richiesta POST con user e password corrette:

The screenshot displays the Burp Suite interface with a virtual machine window titled 'Login - Damn Vulnerable' showing the DVWA login page. The Burp Suite window shows the 'Intercept' tab with a request to 'http://127.0.0.1:80'. The 'Raw' tab shows the following request details:

```
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:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
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/115.0.5790.171 Safari/537.36
12 Accept:
13 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 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=cakBuqfqcT59vuhv5pfu9ga
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=8d3ce773477f23e1e68d8d8e5ec3b0
```

The 'Inspector' tab on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

Richiesta GET successiva al POST:

The screenshot displays the Burp Suite interface with the same virtual machine window. The Burp Suite window shows the 'Intercept' tab with a request to 'http://127.0.0.1:80'. The 'Raw' tab shows the following request details:

```
1 GET /DVWA/index.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
6 Accept:
7 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 sec-ch-ua:
12 sec-ch-ua-mobile: ?0
13 sec-ch-ua-platform: ""
14 Referer: http://127.0.0.1/DVWA/login.php
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: security=impossible; PHPSESSID=cakBuqfqcT59vuhv5pfu9ga
18 Connection: close
19
20
```

The 'Inspector' tab on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

Di seguito le richieste intercettate in cui ho modificato da burpsuite i parametri user e password, ricevendo il login failed, inserendo come user:admin1 e come pass:afasf :

This screenshot shows the Burp Suite interface with a POST request to `127.0.0.1/DVWA/login.php`. The request body contains the following data:

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 86
Cache-Control: max-age=0
sec-ch-ua:
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: ""
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/115.0.5790.171 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
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=cokBuqfpc59vuhvt5pfu9ga
Connection: close

username=admin1&password=afasf&Login=Loginuser_token=893c928839681c191046f70ca9145319
```

The response shows a "Login failed" message. The DVWA login page on the left shows the input fields for "admin1" and "afasf".

This screenshot shows the Burp Suite interface with a GET request to `127.0.0.1/DVWA/login.php`. The response is an HTML page with the following structure:

```
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua:
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: ""
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/115.0.5790.171 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
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=cokBuqfpc59vuhvt5pfu9ga
Connection: close
```

The response body contains the following HTML:

```
<fieldset>
<input type="hidden" name="user_token" value="06423437657c8bce6fc7a80bc5185f54" />
</form>
<div class="message">
  Login failed
</div>
 ...
</div>
<div id="content">...
</div id="footer">
  <a href="https://github.com/digininja/DVWA/" target="_blank">
    Damn Vulnerable Web Application (DVWA)
  </a>
</div id="footer"> ...
</div id="wrapper"> ...
```

The DVWA login page on the left shows the input fields for "admin1" and "afasf".