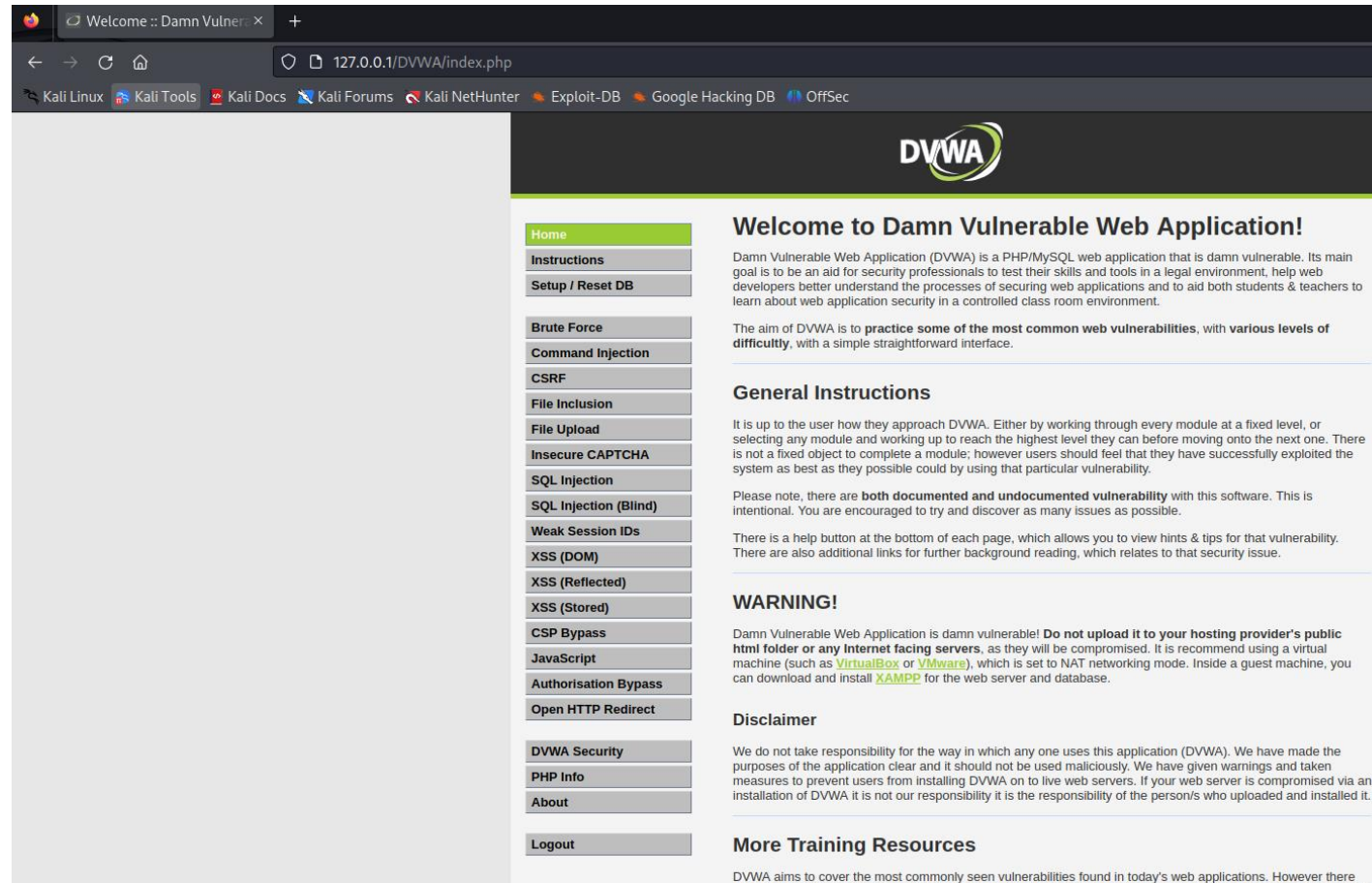


Esercizio S3 L2

Davide Andreozzi

Abbiamo installato la DVWA ovvero damn vulnerable web application in Kali Linux, per farlo abbiamo installato e configurato un Database MySql e un Web Server Apache. Una volta configurato tramite terminale inserendo nella barra di ricerca del browser l'indirizzo 127.0.0.1/DVWA/ comparirà la schermata sotto riportata.



Una volta che la configurazione è stata terminata e verificato che funzioni correttamente possiamo andare su Burp Suite, impostare su on l'intercettazione e cliccare su open browser e da lì andiamo di nuovo a inserire l'indirizzo di prima.

Da qui possiamo notare come vengono eseguite le richieste HTTP e possiamo notare principalmente due metodi:

GET: E' utilizzato per richiedere una risorsa web

POST: Quando invece andiamo a inviare parametri, ad esempio il login nella schermata in basso

The screenshot displays the Burp Suite interface with a web browser window on the left and the HTTP history/inspector on the right.

Browser Window (Left): The address bar shows "Login :: Damn Vulnerable" and "127.0.0.1/DVWA/login.php". The page content includes the DVWA logo and a login form with fields for "Username" (containing "admin") and "Password" (containing "*****"), and a "Login" button.

Burp Suite Interface (Right): The top menu bar includes "Burp", "Project", "Intruder", "Repeater", "View", and "Help". The "Proxy" tab is active, showing "Intercept" and "HTTP history" sub-tabs. The "Intercept" sub-tab is selected, displaying a request to "http://127.0.0.1:80". The "Intercept is on" button is highlighted. The "Inspector" panel on the right shows the request details.

HTTP Request Details (Inspector):

```
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:
  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
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=391j98v3lemuj0sg4erncdi79s
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=a098c8faf3465703971bc9b279acaba7
```

Inserendo una password errata come possiamo vedere dalla schermata response troveremo la dicitura Login Failed.

E il tipo di metodo sarà GET in quanto riceveremo dal server locale la schermata quasi identica a prima ma diversa in quanto troviamo in basso la dicitura «Login Failed»

A sinistra troviamo inoltre tutti i dettagli della richiesta del client a destra la risposta del server.

The image displays two side-by-side screenshots. The left screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows a GET request to /DVWA/login.php. The 'Response' pane in the center shows the server's HTML response, which includes a 'Login failed' message. The 'Inspector' pane on the right shows the request and response headers. The right screenshot shows a web browser window displaying the DVWA login page. The 'Username' field contains 'admin' and the 'Password' field is filled with asterisks. The 'Login' button is visible, and the message 'Login failed' is displayed below the form.

Burp Suite - 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:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
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/115.0.5790.171 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
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=391j98v3lemuj0sg4erncdi79s; security=impossible
19 Connection: close
20
21
```

Burp Suite - Response:

```
54 <?php
55 <fieldset>
56
57 <input type='hidden' name='
58 user_token' value='
59 51c71f972e833dd9da9724883ddf2835'
60 />
61
62 </form>
63
64 <div class="message">
65 Login failed
66 </div>
67
68 <br />
69
70 <br />
71 <br />
72 <br />
73 <br />
74 </div>
75 <!--<div id="content">-->
76
77 <div id="footer">
78
79 <p>
80 <a href="
81 https://github.com/digininja/DVWA/"
82 target="_blank">
83 Damn Vulnerable Web Application
84 (DVWA)
85 </a>
86 </p>
87
```

Web Browser - DVWA Login Page:

Username: admin

Password: *****

Login

Login failed

Damn Vulnerable Web Application (DVWA)