

Esercizio S3/L3

Web App - Preparazione ambiente

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

Per l'esercizio di oggi configuriamo una DVWA. Il primo passaggio è installare e configurare il database MySQL e il Web Server Apache. Alla fine dei vari passaggi, potremo accedere al DVWA.

```
root@kali: /etc/php/8.2/apache2
# service apache2 start

(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php

(root@kali)-[/etc/php]
# ls
8.2

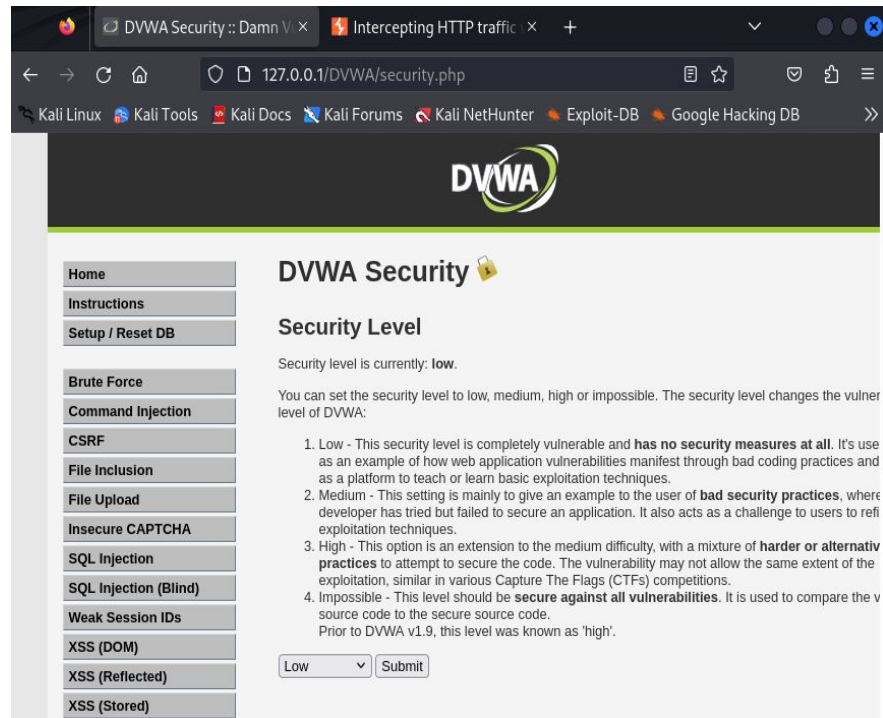
(root@kali)-[/etc/php]
# cd /etc/php/8.2/apache2

(root@kali)-[/etc/php/8.2/apache2]
# nano php.ini

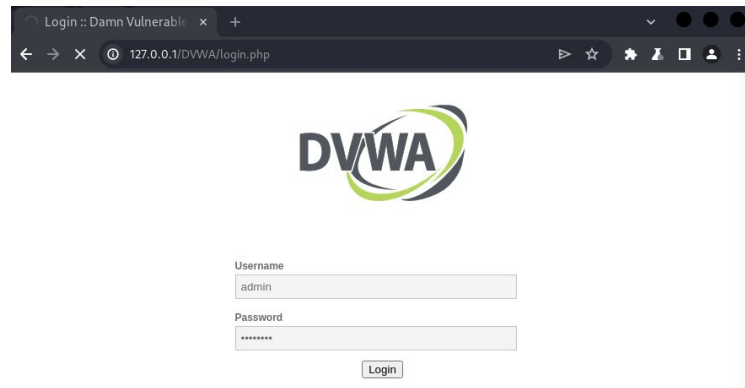
(root@kali)-[/etc/php/8.2/apache2]
# service apache2 start

(root@kali)-[/etc/php/8.2/apache2]
#
```

Aprendo il browser web, accediamo a 127.0.0.1/DVWA/setup.php, accediamo ed impostiamo il livello di sicurezza.



Fatto questo, avviamo BurpSuite, andiamo su Proxy, attiviamo l'intercept, apriamo il browser del programma ed intercettiamo l'accesso al sito.



Effettuato il login e vedremo i dati inseriti visualizzati sul programma. Prima di inviare i dati ci spostiamo sul repeater e li modifichiamo in maniera errata. Come previsto, il login fallirà.

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows an HTTP GET request to `/DWA/login.php`. The 'Response' pane on the right shows the HTML response, where a red circle highlights the message `<div class="message">Login failed</div>`. The 'Inspector' pane on the far right shows the 'Request attributes' section with 2 items.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

1 x +

Send Cancel < >

Target: <http://127.0.0.1> HTTP/1

Request

Pretty Raw Hex

```
1 GET /DWA/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/DWA/Login.php
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=
  gs308ug4FF03q6upaogq2mp8jq
19 Connection: close
20
21
```

Response

Pretty Raw Hex Render

```
58 '='cbe62c3c14999a1ccb2c6c7badbb34a7' />
59
60 <form>
61 <br />
62 <div class="message">
63   Login failed
64 </div>
65 <br />
66 <br />
67 <br />
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73
74 <div>
75   <!--div id="content"-->
76   <div id="footer">
77     <p>
78       <a href="https://github.com/digininja/DWA/"
  target="_blank">
  Damn Vulnerable Web Application (DWA)
79     </a>
80   </p>
81   <!--div id="footer"-->
82 </div>
  <!--div id="banner"-->
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

Done

1,672 bytes | 34 millis