

# Best Practices - The Upload

2013/01/13 @ WebConf

*<Orange@chroot.org>*

# About Me

- 蔡政達 aka Orange
- 2009 台灣駭客年會競賽冠軍
- 2011, 2012 全國資安競賽金盾獎冠軍
- 2011 東京 AVTOKYO 講師
- 2012 台灣 PHP Conf 講師
- 2012 香港 VXRLConf 講師



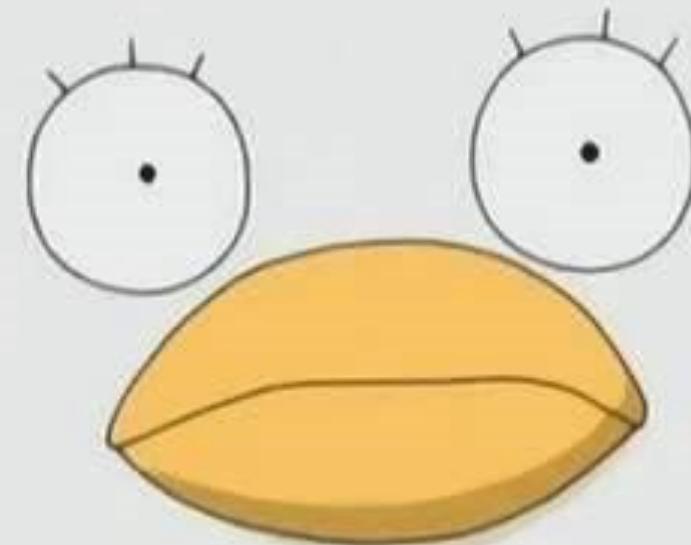
- 專精於
  - 駭客攻擊手法
  - Web Security
  - Windows Vulnerability Exploitation

# About Me

- CHROOT Security Group 成員
- NISRA 資訊安全研究會 成員
- Disclosed
  - MS12-071 / CVE-2012-4775
- <http://blog.orange.tw/>

upload

啊~不露的>//<



# Hacker's Best Practices

今天的主題是關於上傳的最佳實踐



# 駭客攻擊流程

## 1. Reconnaissance

- Google Hacking, Reversed Whois, AXFR .....

## 2. Scanning

- SYN/ACK Scan, TCP NULL/FIN/Xmas/Mainmon/Window Scan, SCTP INIT Scan, Hydra, Nessus .....

## 3. Gaining Access

- Heap/Stack/V-table Overflow, ROP, Heap Spray, System Misconfiguration, Metasploit, Exploit Database .....

## 4. Maintaining Access

- Privilege Escalation, Trojan, Backdoor, Rootkit, Code/DLL Injection, API Hook, LD\_PRELOAD, Anti AV/Debugger .....

## 5. Clearing Tracks

- Syslog, WTMP/UTMP, Event Log, Shell(Bash/Explorer) .....

# 聽不懂嗎？

其實有份簡單版的啦



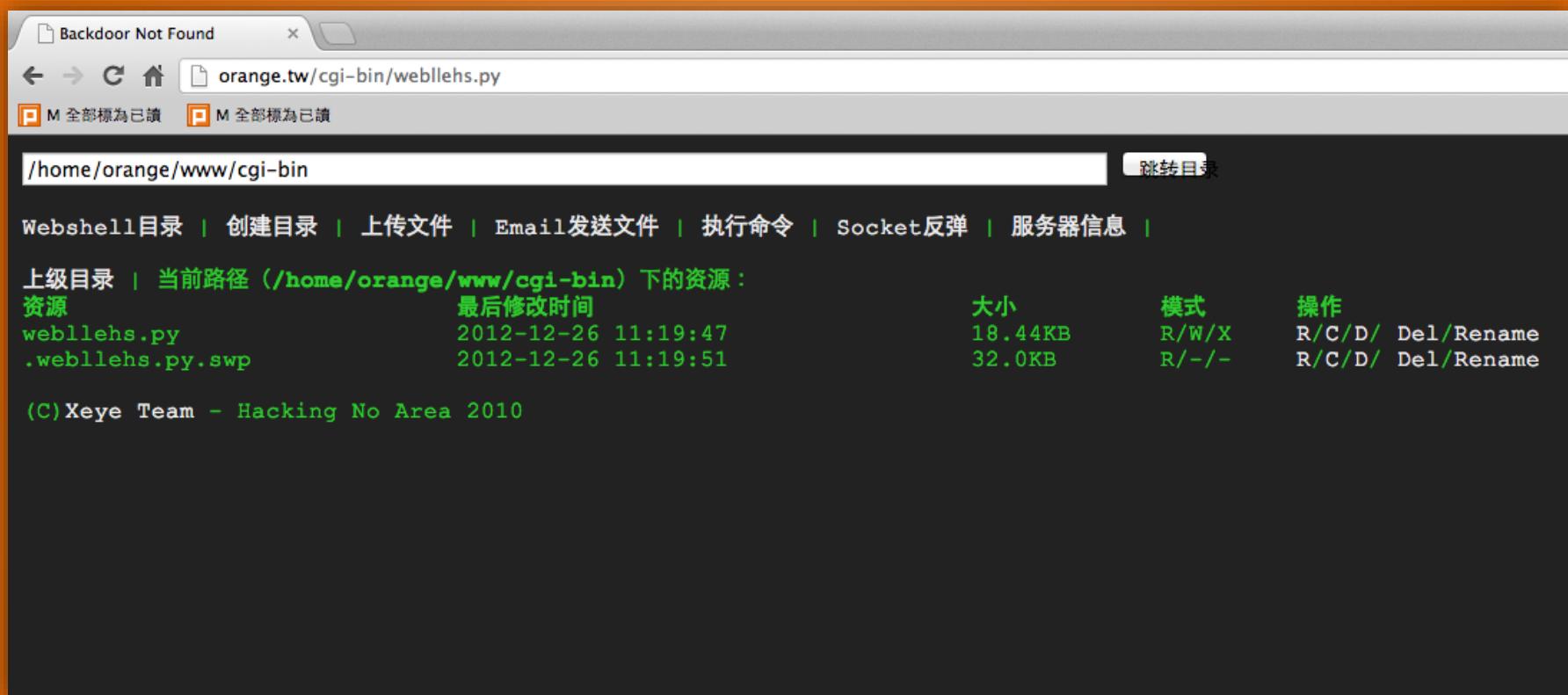
# 駭客攻擊流程 (2013 WebConf 簡單版)

1. 觀察尋找漏洞
2. 透過漏洞上傳後門取得控制權
  - Upload?
3. 清理足跡
  - Web log? Database log?

# 上傳後門 - Webshell

- 一段網頁後端語言寫的小程式
- 具有讀, 寫, 執行命令的功能讓駭客更方便控制受害主機
  - <?php eval( \$\_REQUEST[cmd] );?>
  - Runtime.getRuntime().exec( cmd )
  - <%eval request("cmd") %>
  - \_\_import\_\_('os').system(cmd)

# e.g. Python Webshell



<https://github.com/evilcos/python-webshell/>

# 來看個小案例

## 模擬駭客入侵手法

# 論壇架站？以 Discuz 為例

伊莉討論區

www03.eyny.com/index.php

註冊 登錄

简体 濱覽工具 設為首頁 收藏本站

eyny Enjoy Your Life

NARUKO 牛爾 親研 想不老？就要HOLD住年

論壇 | 羣組 | 空間 | 影片 | 百科 | 排行 | 搜尋 | 自助升級 | 尊貴會員 | 快捷導航

帖子 | 搜索

尊貴會員無限使用任何功能 | 尊貴會員無限下載附件 | 今天就來逛逛永慶房仲網

論壇索引

julia	航海王	武動乾坤	觸手	rio	紳士的品	真愛趁現
九鼎	初音島	三仙	土城	說狠話又	輔仁大學	小森美玉

休閒聊天	興趣交流	學術文化	旅遊交流	飲食交流	家庭事務	PC GAME	連線遊戲
TV GAME	熱門線上	其他線上	感情感性	寵物交流	家族門派	動漫交流	貼圖分享
BL/GL	音樂世界	影視娛樂	女性頻道	潮流資訊	BT下載區	GB下載區	下載分享
短片	電腦資訊	數碼產品	手機交流	交易廣場	網站事務	長篇小說	體育運動
時事經濟	上班一族	成人話題	博彩娛樂				

搞笑車禍(笑點低了點~) | 褥屁片場第3集..(共5) | 正妹跳舞[星間飛行]

即刻救援2-DVD高畫質 | 內衣就是要..... | 天地風雲錄之九龍變03

熱門話題

加分活動

[加分活動] 2012-13 足總杯重點賽  
喔喔~這場比賽活生生就是弟子與師傅的對決啊~ 斯旺西這審判到目前

神劍闖江湖/浪客劍心 Rurouni Kenshin  
【檔案名稱】：神劍闖江湖/浪客劍心Rurouni Kenshin [hackscale]

[港]十二生肖 Chinese Zodiac DVDscr  
電影名稱：十二生肖 Chinese Zodiac DVDscr

可能用到了

Discuz!



不是說上述網站有漏洞啦…

# 駭客註冊帳號

Firefox ▾

立即註冊 - Discuz! Board - Powered b... +

webconf.orange.tw/discuz/member.php?mod=register

設為首頁 收藏本站 切換到寬版

社區動力  
**DISCUZ!**

論壇 快捷導航

請輸入搜尋內容 帖子 搜索 熱搜：活動 交友 discuz

立即註冊 已有帳號？現在登錄

\*用戶名： ✓

\*密碼： ✓

\*確認密碼： ✓

\*Email： 請輸入正確的郵箱地址

提交

# 駭客上傳自己的大頭貼



# 駭客看看自己的大頭貼

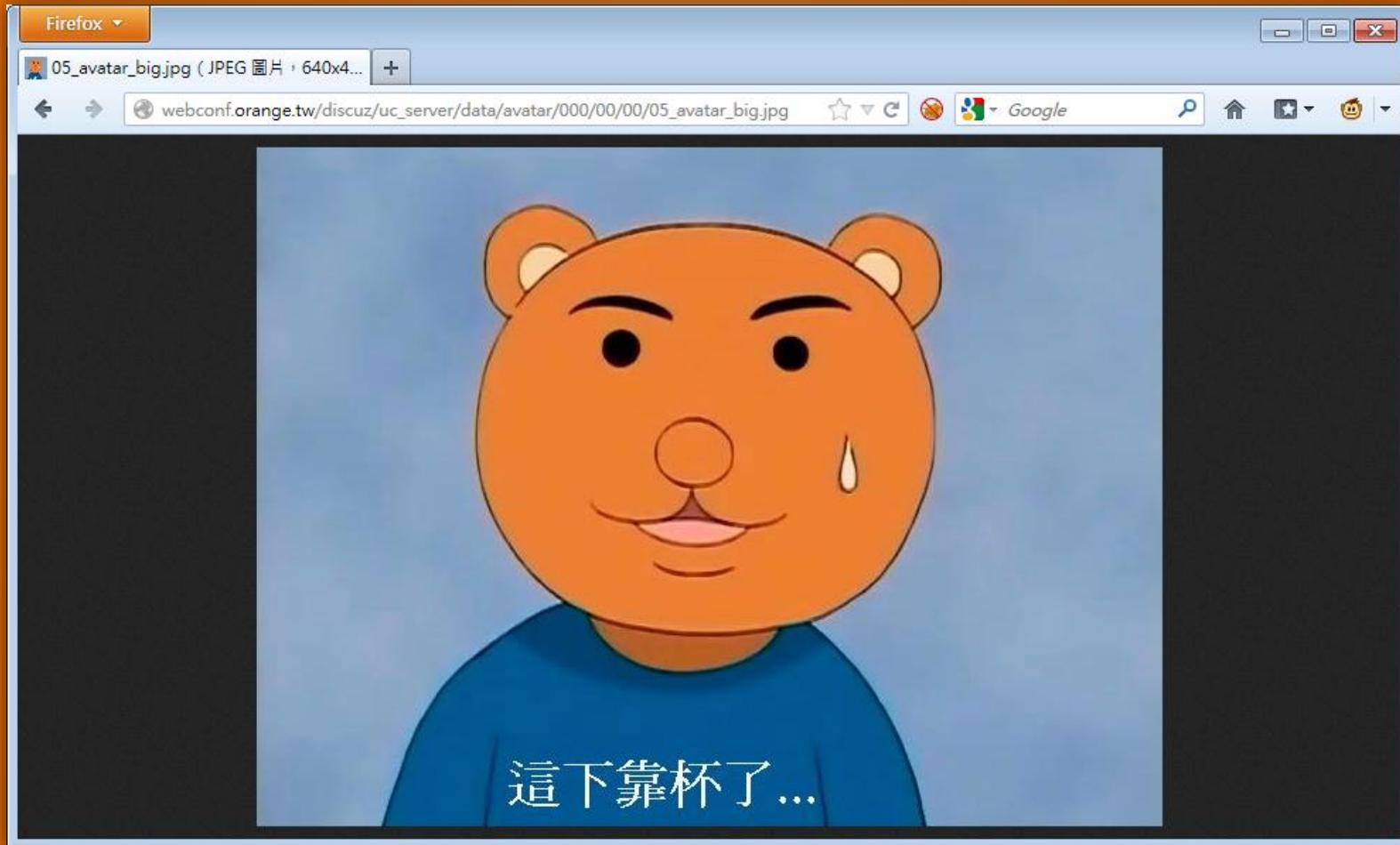




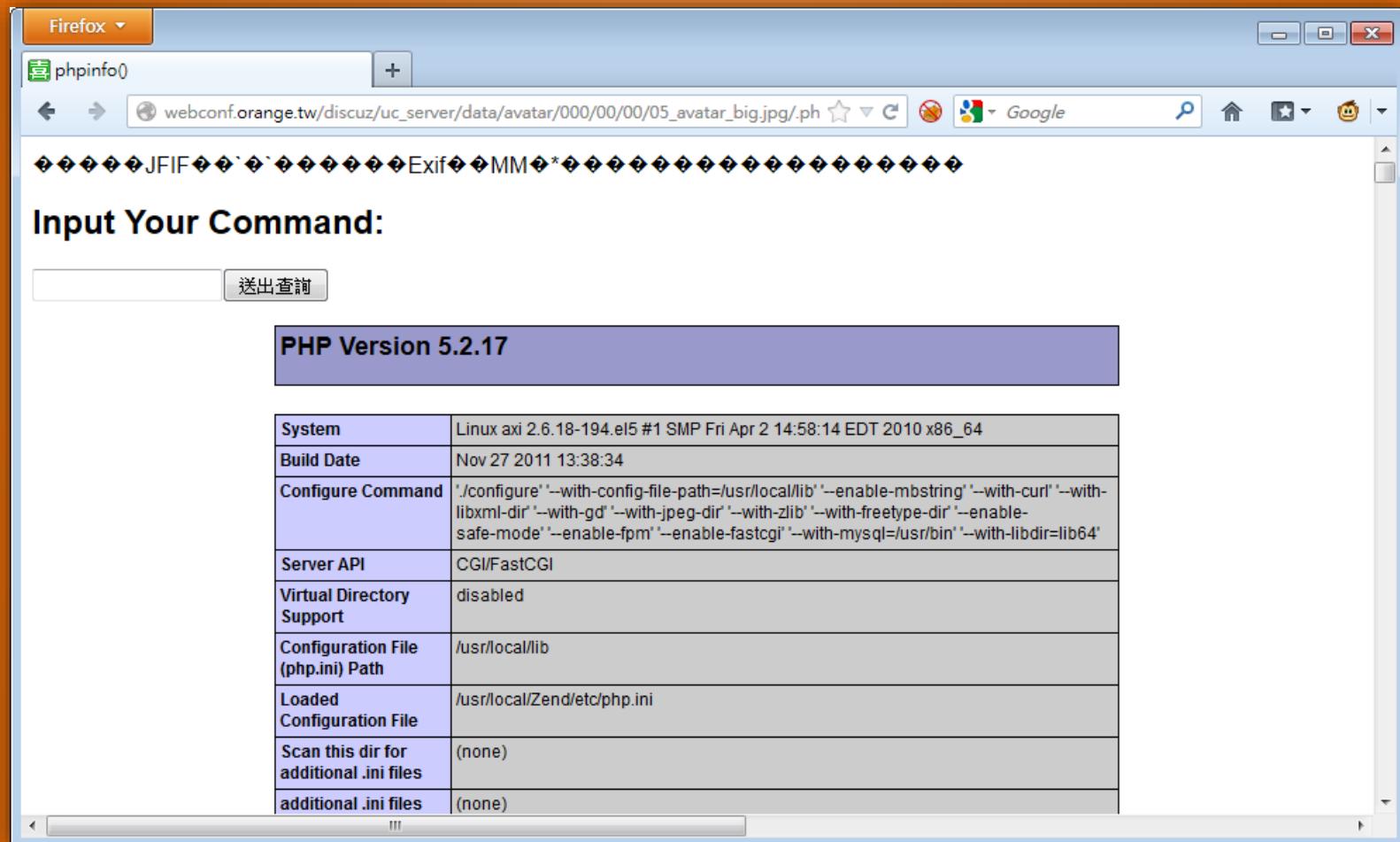
接下来，就是見證奇蹟的時刻

<http://www.lu-chen.com/>

[http://webconf.orange.tw  
/discuz/uc\\_server/data/avatar/000/  
00/00/05\\_avatar\\_big.jpg](http://webconf.orange.tw/discuz/uc_server/data/avatar/000/00/00/05_avatar_big.jpg)



[http://webconf.orange.tw  
/discuz\uc\\_server\data\avatar\000\00\00\05\\_avatar\\_big.jpg/.php](http://webconf.orange.tw/discuz\uc_server\data\avatar\000\00\00\05_avatar_big.jpg/.php)



# Nginx 文件解析漏洞

- 難道 Nginx 錯了嗎？
  - 實際上是 PHP CGI 處理 PATH\_INFO 的問題
- 什麼是 PATH\_INFO ?
  - /index.php/module/login
  - /index/module/login
- 只要駭客上傳一張經過設計的圖片
  - /userfiles/mypic.jpg
  - /userfiles/mypic.jpg/nihao.php

# 經過設計的圖片怎麼來？

- 一張圖片很多地方可藏
  - Huffman table
  - EXIF
- 老招也可以拿出來用
  - copy /b rst.jpg+backdoor.php dst.jpg
- 範例圖片
  - <http://orange.tw/exif.jpg>

**所以上傳這件事安不安全呢？**



# 翁浩正 (Allen Own)

你們都誤解了，網路是很安全的！  
(駭客入侵什麼的，都是電影特效啦)

# 上傳檔案

- 沒檢查
- 黑名單 vs. 白名單
- 如何判斷檔案類型？
- 如何做出讓駭客頭痛的上傳功能？

# 黑名單 vs. 白名單

- 防護目前最頭痛問題
  - 沒有防不了的東西
  - 不知道的東西防不了
  - 游走邊緣的東西防不了
- 常見禁止上傳附檔名
  - php phtml php3 php4 php5
  - asp asa cer cdx shtml
  - aspx asax ascx ashx asmx

# 1. 沒有防不了的東西

「程式設計師用黑名單禁止了所有他知道不可以上傳的副檔名」

# 沒有防不了的東西

1. 建立個檔案上傳， 檔案名叫做 .htaccess
    - AddHandler application/x-httpd-php .jpg
  2. 上傳經過設計的 jpg , 駭客取得控制權
- 
- Apache 的個別目錄使用者定義設定檔
    - 打破典型只認為 .php\* 有害的思考框框

# 遇過 網站管理者 說：

「這個是伺服器提供的功能不是漏洞， 沒有人會這樣子搞啦， 你以為每個人都駭客唷」

# 無恥

管理者需要悔改

9 : 0 9



笨蛋是不见棺材不落泪的

<https://www.facebook.com/TWWDB>

## 2. 不知道的東西防不了

「程式設計師用黑名單禁止了所有他知道不可以上傳的副檔名」  
(htaccess也加上了喔 ^\_\_^)

# 不知道的東西防不了

- Apache 文件解析 feature
- 未在 mime.types 定義的副檔名，會從檔名後方依序往前尋找副檔名做為解析
  - user.jpg → .jpg
  - user.php.jpg → .jpg
  - user.php.xxx → .php
  - user.php.xxx.ooo → .php

### 3. 遊走邊緣的東西防不了

「後端攻城師換了白名單的方式  
只允許 jpg 的圖片才可以上傳」

# 游走邊緣的東西防不了

- IIS 文件解析 feature
  - IIS < 7
  - Asp.net 也是一樣 ^\_\_^
- 以 \*.asp 取名的資料夾下檔案會以 asp 解析
  - <http://webconf.orange.tw/files/a.asp/user.jpg>
- IIS 檔名解析時會被分號截斷
  - <http://webconf.orange.tw/files/user.asp;aa.jpg>



user.asp;aa.jpg

用黑名單  
要注意的東西好多…



怪我囉？…  
↖(˘ ³˘)↗…

# 後端程式如何取得檔案類型？

# 這是一張圖片上傳時會送出的資訊

```
POST /up.php HTTP/1.1
Host: orange.tw
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=hvqtdjc033ck5gd34oj09j9ai7; path=/
Content-Type: multipart/form-data; boundary=myBoun
Content-Length: 12905
myBoun--
Content-Disposition: form-data; name="file";
filename="1.jpg" ③ filename
Content-Type: image/jpeg ② Content-Type
```

.....JFIF.....`.....Exif..MM.\*.....>.i  
.....X..... ① File header .....

**事實上，多數錯誤的程式碼來自搜尋引擎  
網路寫什麼就貼上，你是（逼）就是了。**

# 寫出安全的上傳功能

- Update your sense and software.
- User controlled filename is always dangerous.
  - Whatever filename, extension or temporary filename.
- Use Image library to valid or strip the image.
- Disabled the directory's execution permission you uploaded to.

# Summary

- Nginx(PHP) 文件解析漏洞
- 黑名單 vs. 白名單
  - htaccess
- 文件解析問題
  - Apache 文件解析
  - IIS 文件解析
- 檔案類型的判斷
- 撰寫上傳功能時要注意的點

# 深夜問題多… 刑法36章358~363條，妨害電腦使用罪



# 問與答

Q & A

# Thanks.

*<Orange@chroot.org>*