

# Information Security - Web Security

Department of Information Management  
National Taiwan University

Information Security  
Fall 2014

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
- OWASP WebGoat Project

# Introduction

- If you were a ...
  - General Web User.
    - using PC, tablet, smart phone, wearable 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 **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**
  - OWASP **WebGoat** Project

# 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 Ten Project
    - [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
  - OWASP WebGoat Project
    - [https://www.owasp.org/index.php/Category:OWASP\\_WebGoat\\_Project](https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)
- Ajax Security
  - Billy Hoffman and Bryan Sullivan, Addison-Wesley Professional, Dec. 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:  
A 157.166.240.11  
A 157.166.240.13  
A 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

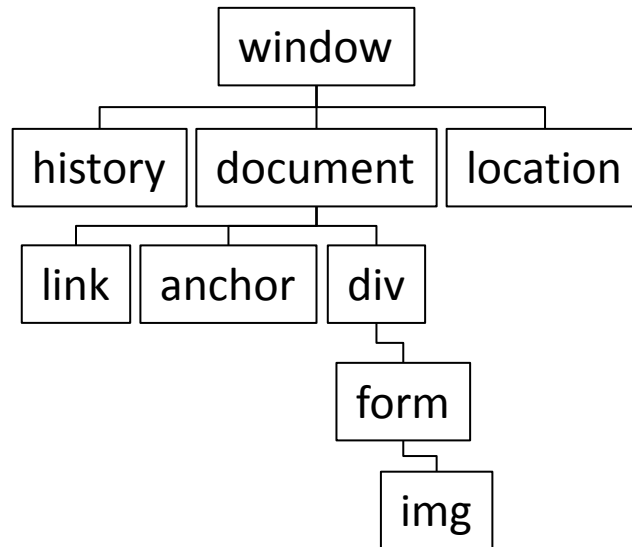
- A **web browser engine**, (sometimes called **layout engine** or **rendering engine**), is a software component that takes **marked up content** (such as HTML, XML, image files, etc.) and **formatting information** (such as CSS, XSL, etc.), and displays the formatted content on the screen.

HTML + CSS

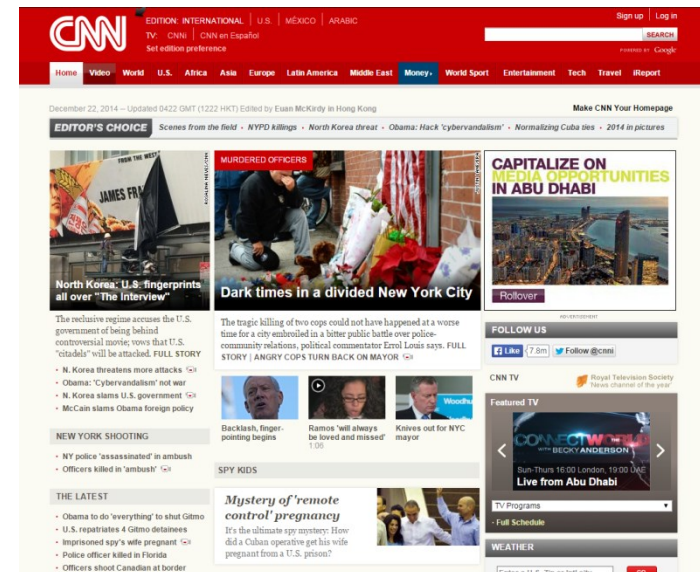
```
<html>
<head>
</head>
<body>
<div>
<form>
<img />
...
</div></body>
</html>
```



DOM

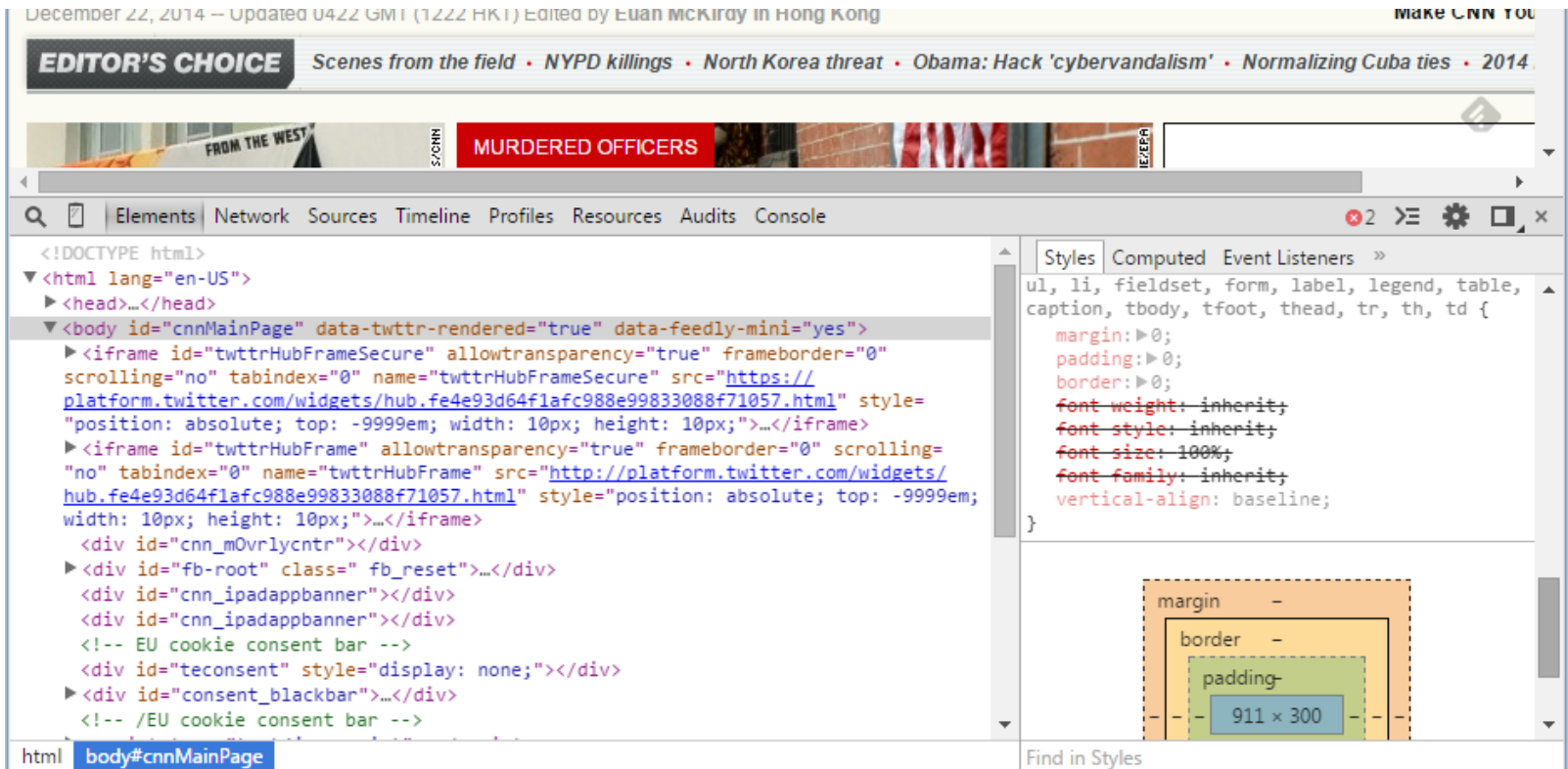


Display



# 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.

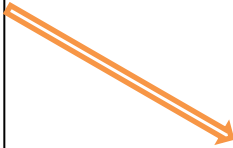


An example of DOM in Chrome web developer tool.

# 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.

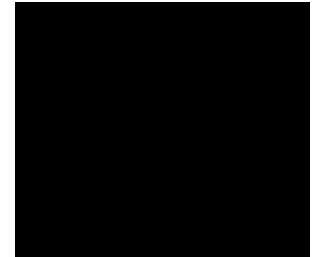
Handel Window Event



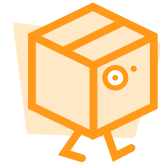
Set/Trigger Timer



Modify DOM



Send HTTP Request



:

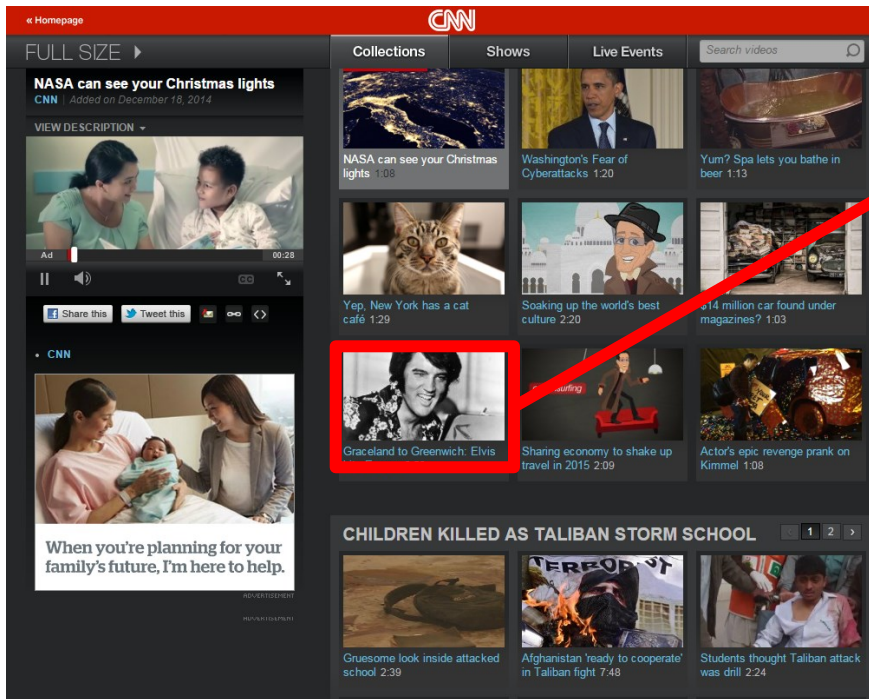
# Browser Extension

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.
  - A smart or stupid browser?



動物玩iPad大合輯 40

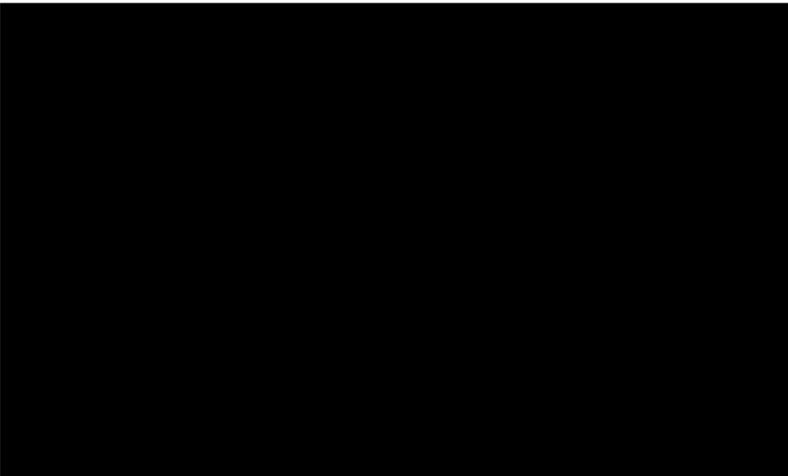
廣告

**最殺遊戲徵才，16歲可申請**

[www.loonnet.com.tw](http://www.loonnet.com.tw)

遊戲公司徵才培訓，挑戰月薪3-6萬 夠熱血，會一點電腦，請立即接受挑戰

facebook 分享 分享到 Google+



廣告

**免費下載超人氣英語教材**

[www.tutorabc.com](http://www.tutorabc.com)

每天45分鐘，輕鬆開口學英文！24小時彈性上課，立即把英文學好。

40 人說過讚 - 趕快註冊來看看朋友對那些內容投票 -

回應

Facebook 社群外圍元件

最新留言

房威志 發表了回應 · 校區雲霧



4個女生拆開1個女生...  
[www.ccfunny.com](http://www.ccfunny.com)  
這是哪國人啊? 可悲...

登入 留言 收藏

Google 自訂搜尋

這裡有最棒的新奇搞笑影片，趕快點點一下，推薦給更多人。

廣告

聯成電腦

神啊!! 請實現我的願望!!

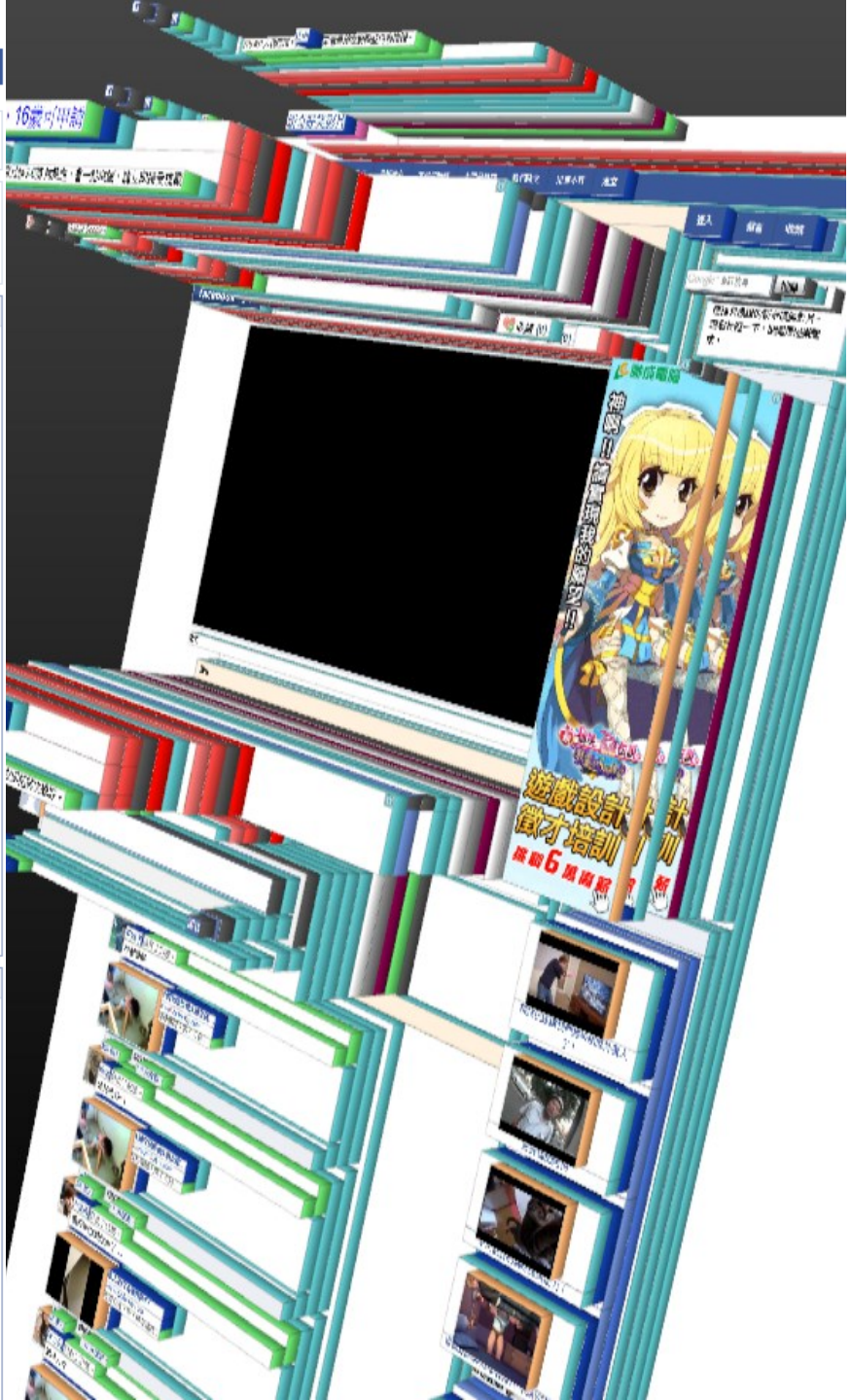
遊戲設計徵才培訓

挑戰6星高新

本週是熱門

科技已經讓我們越來越像外星人了!

好兇猛的阿伯

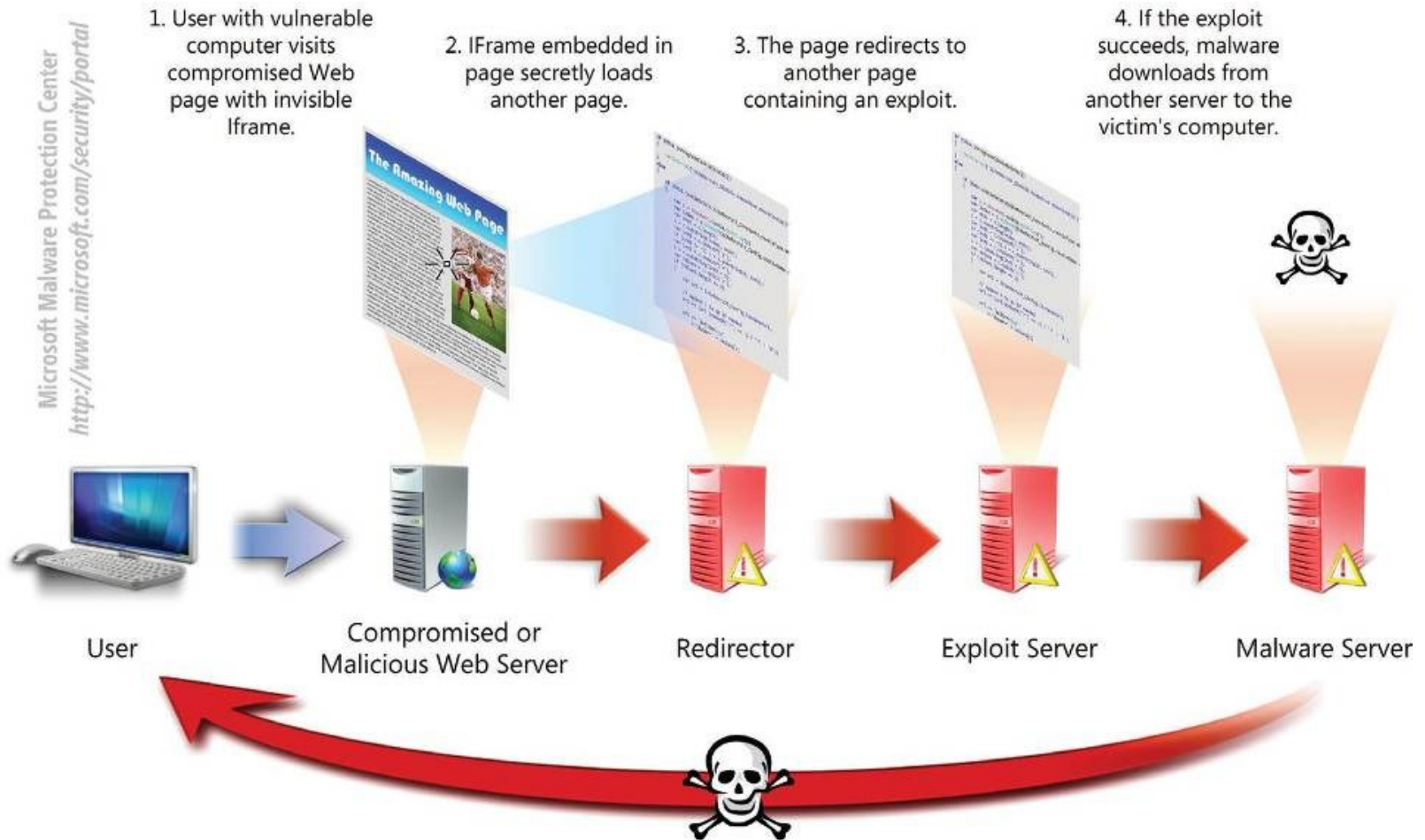




# Client-Side Attack: Drive-By Exploit

- 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, e.g., ActiveX, PDF plugin, 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

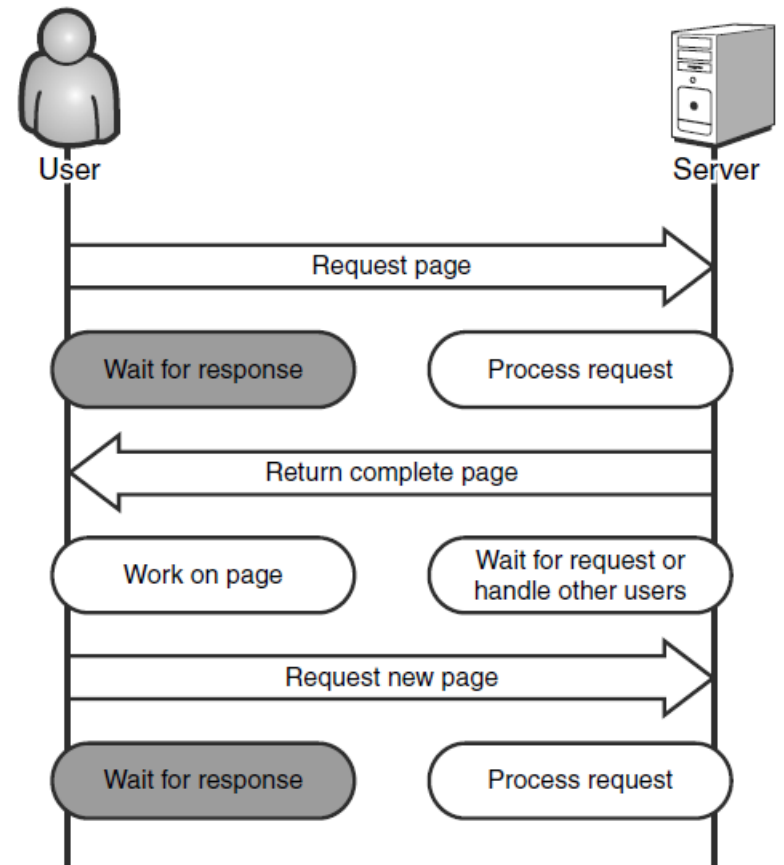
# Example of Drive-By Exploit



# **WEB HACKER - THE HEIST**

# Web Request/Response Model

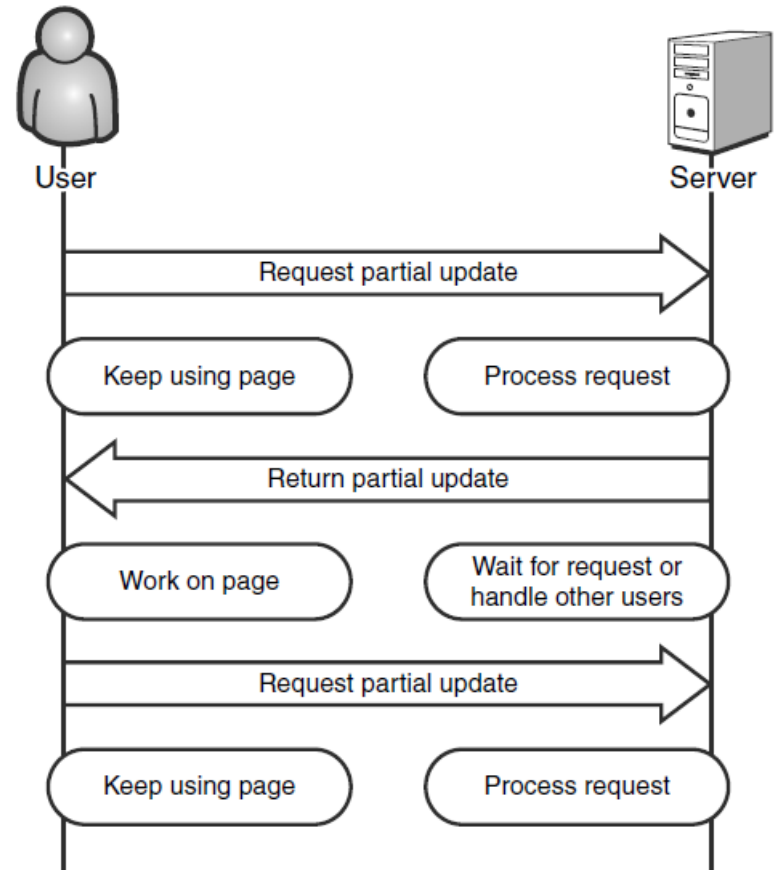
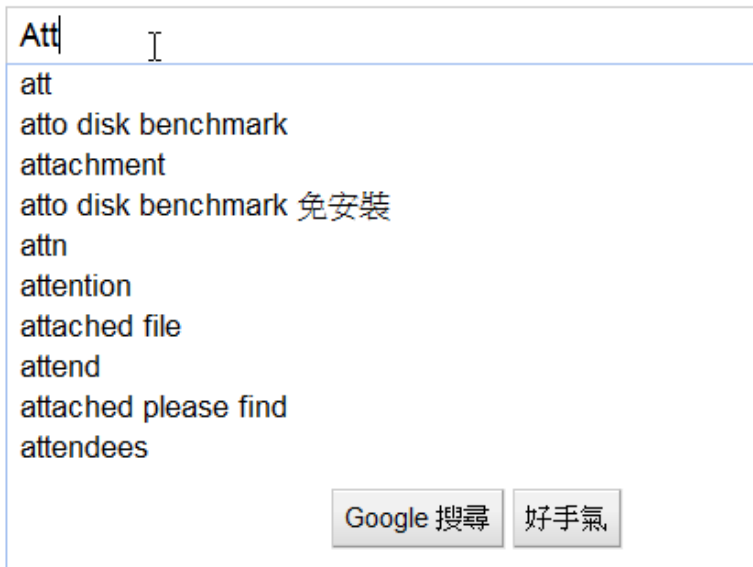
- Request
  - URL (get, post, ...)
- Response
  - HTML, CCS, JS, XML, ...
- Static Web Page
- Dynamic Web Page
  - Server-Side Scripting
  - Client-Side Scripting
    - HTML, JS, CSS, DOM



Classic synchronous Web request/response model

# Asynchronous JavaScript and XML (Ajax)

Example: Google Search!  
Facebook Wall



Asynchronous Ajax request/response model

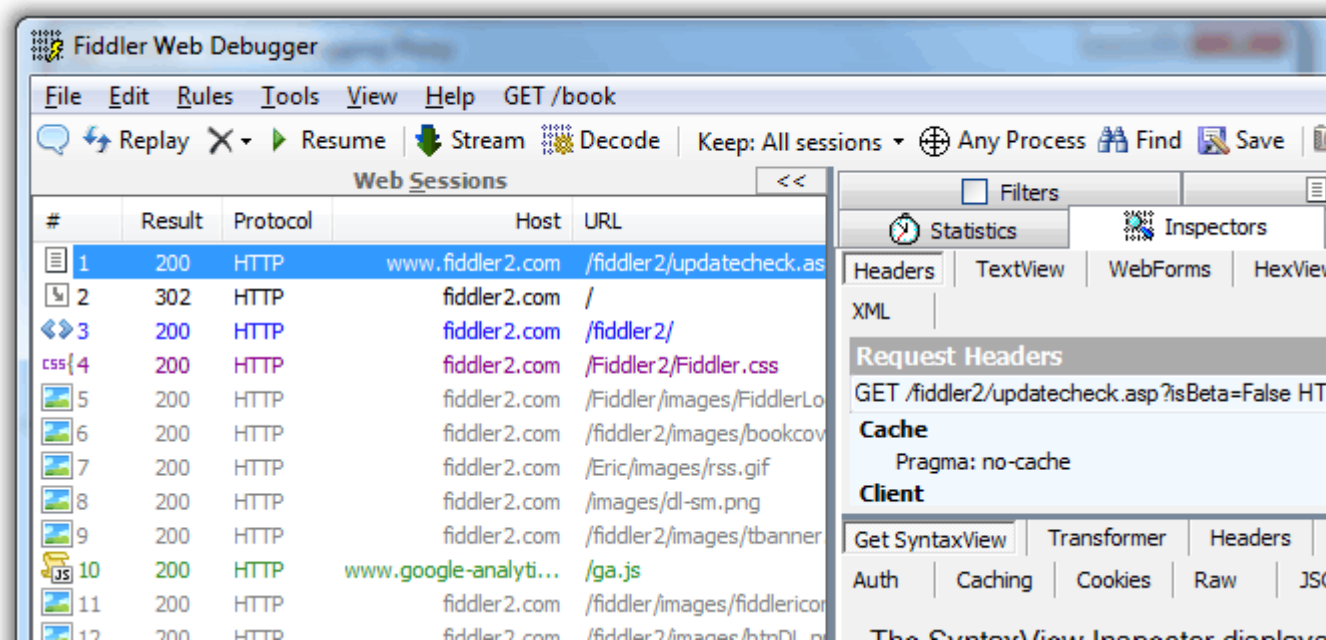
# The Heist

- 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 free Web Debugging Proxy which logs all HTTP/HTTPS traffic between your computer and the Internet.



# 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身份資料，例如由您電腦信任的第三方驗證過的憑證。如果該憑證就能驗證您的通訊對象是您想要的網站，而非其他網站，則該憑證就是可信的。

在此情況下，憑證並未經過您的電腦所信任的第三方驗證。這表示該憑證自己不是某某網站，這就是為什麼憑證需經過受信任的第三方驗證。您的身分資訊不具任何意義，這意味著沒有人可以確定您的身分資訊是與自行建立憑證並宣稱是 **oper.cc.ntu.edu.tw** 的。

如果您任職的機構使用自行產生的憑證，而您嘗試訪問該網站時，您可以解決這個問題，並且絕對安全：將貴機構的憑證安裝到您的電腦，並發行或認證的憑證，並允許您連至內部網站，不與外部世界。請與貴機構的協助人員聯絡。

← → ↻ [jsc.cc.ntu.edu.tw/ntucc/email/](https://jsc.cc.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](#)
  - [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 \[GTE CyberTru\]](#)
  - [各式郵件軟體設定說明](#)
  - [利用 gmail 收取臺大信件](#)
  - [廣告信過濾](#)

# Network Tap

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

<pre> ⊕ Frame 3671: 1249 bytes on wire (9992 bits), 1249 bytes captured on interface 0 ⊕ Ethernet II, Src: JuniperN_99:54:01 (84:18:88:99:54:01), Dst: JuniperN_99:54:01 (84:18:88:99:54:01) ⊕ Internet Protocol Version 4, Src: 74.125.101.210 (74.125.101.210), Dst: 64.233.187.113 (64.233.187.113) ⊖ Transmission Control Protocol, Src Port: http (80), Dst Port: https (443)   Source port: http (80)   Destination port: 55313 (55313)   [Stream index: 33]   Sequence number: 2072290 (relative sequence number)   [Next sequence number: 2073485 (relative sequence number)]   Acknowledgment number: 1386 (relative ack number)   Header length: 20 bytes ⊕ Flags: 0x018 (PSH, ACK)   Window size value: 250   [Calculated window size: 32000]   [Window size scaling factor: 128] ⊕ Checksum: 0xa0d3 [validation disabled] ⊖ [SEQ/ACK analysis]   [Bytes in flight: 8495]   TCP segment data (1195 bytes) ⊕ [1431 Reassembled TCP segments (2073484 bytes): #1853(549) ⊖ Hypertext Transfer Protocol   HTTP/1.1 200 OK\r\n   Last-Modified: Sun, 21 Dec 2014 15:37:08 GMT\r\n   Content-Type: video/mp4\r\n   Date: Mon, 22 Dec 2014 05:28:05 GMT\r\n   Expires: Mon, 22 Dec 2014 05:28:05 GMT\r\n </pre>	<pre> ⊕ Frame 167: 111 bytes on wire (888 bits), 111 bytes captured on interface 0 ⊕ Ethernet II, Src: JuniperN_99:54:01 (84:18:88:99:54:01), Dst: JuniperN_99:54:01 (84:18:88:99:54:01) ⊕ Internet Protocol Version 4, Src: 64.233.187.113 (64.233.187.113), Dst: 74.125.101.210 (74.125.101.210) ⊖ Transmission Control Protocol, Src Port: https (443), Dst Port: http (80)   Source port: https (443)   Destination port: 55292 (55292)   [Stream index: 4]   Sequence number: 4214 (relative sequence number)   [Next sequence number: 4271 (relative sequence number)]   Acknowledgment number: 489 (relative ack number)   Header length: 20 bytes ⊕ Flags: 0x018 (PSH, ACK)   Window size value: 352   [Calculated window size: 45056]   [Window size scaling factor: 128] ⊕ Checksum: 0xaa0c [validation disabled] ⊖ [SEQ/ACK analysis]   [Bytes in flight: 351] ⊖ Secure Sockets Layer   TLSv1.2 Record Layer: Application Data Protocol: http   Content Type: Application Data (23)   Version: TLS 1.2 (0x0303)   Length: 52   Encrypted Application Data: 000000000000000157de0a85 </pre>
--	---

HTTP

HTTPS

# 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.

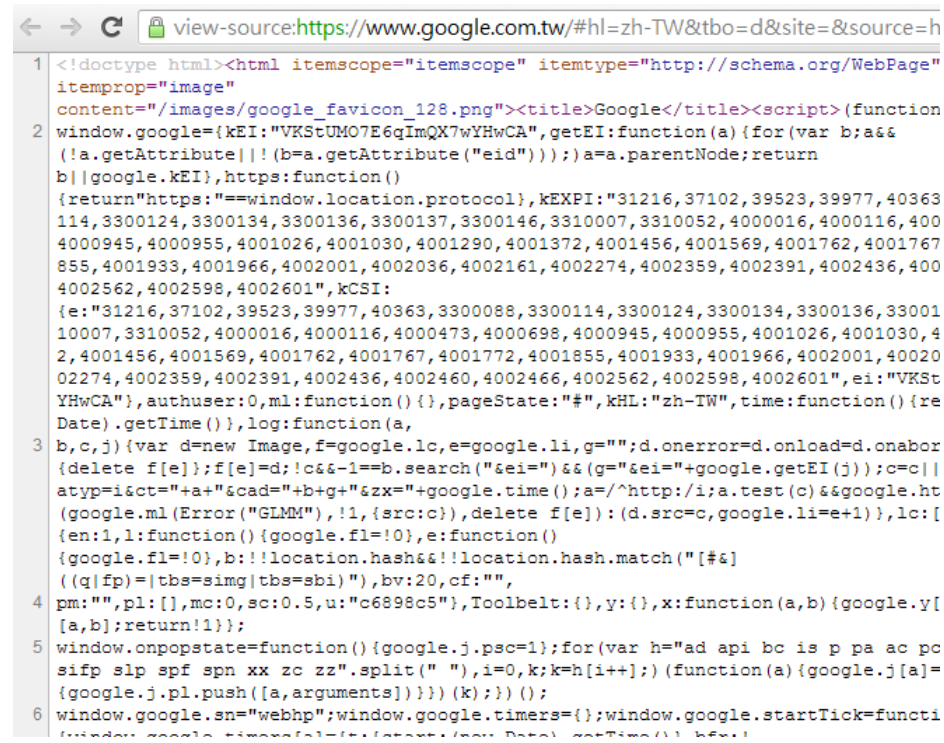
[attack 是什么意思 翻译 解释 读音 用法 例句 柯林斯 爱词霸在线词典](#)  
www.iciba.com/attack - 頁庫存檔 - 轉為繁體網頁  
高频词, 一定要记住哦! 常见度: at-tack. attack. [英] [ə'tæk] [美] [ə'tæk].  
生词本. 简明释义. 词根词缀. 词组习语. 同反义词. 同义词辨析. 更多资料. vt. & vi.

[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,雙主唱吶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(),k)}
```

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

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 ()]
- [SYMBOL {}]
- [KEYWORD if]
- [SYMBOL ()]
- [VARIABLE document]
- [SYMBOL .]
- [VARIABLE getElementBy]

Variables/Functions

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

Literals

- application/x-www-form-utle
- close
- Connection
- Content-length
- Content-type
- ERROR!
- GET
- Handler could not be attach
- load
- Msxml2.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
```

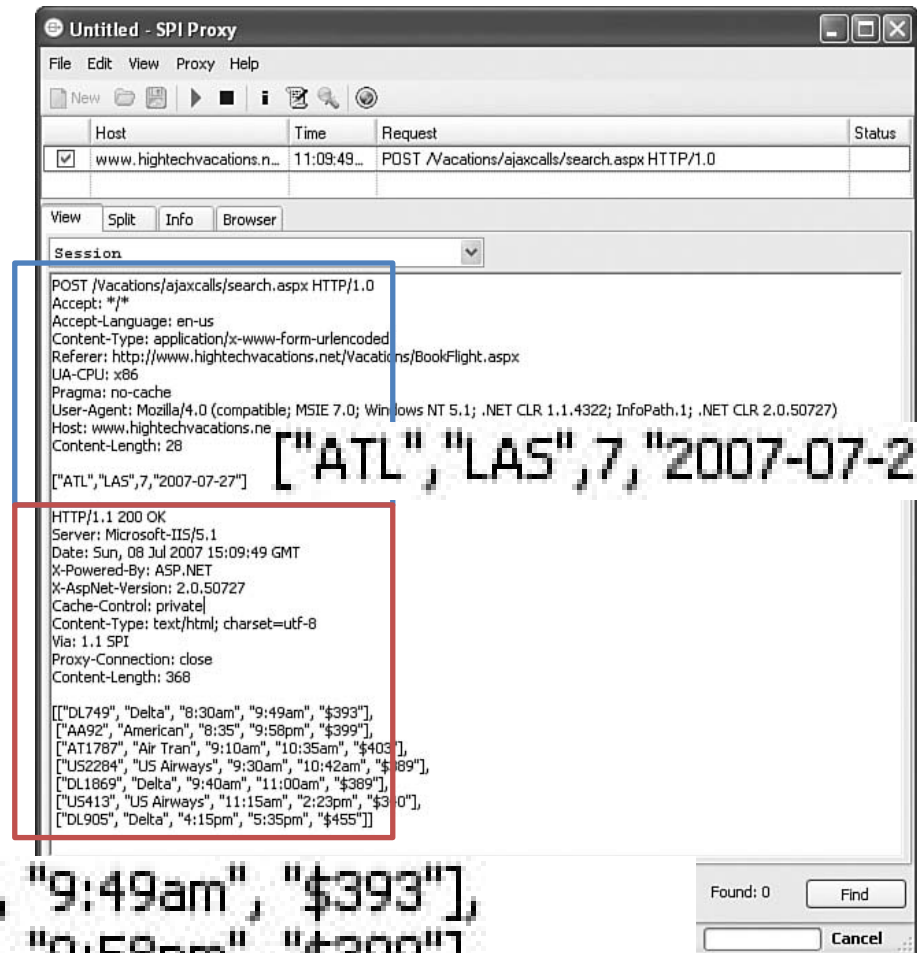


# The Heist – attacking client-side data

- 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"],  
["US2284", "US Airways", "9:30am", "10:42am", "$389"],  
["DL1869", "Delta", "9:40am", "11:00am", "$389"],  
["U5413", "US Airways", "11:15am", "2:23pm", "$380"],  
["DL905", "Delta", "4:15pm", "5:35pm", "$455"]]
```

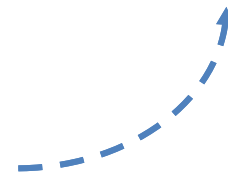
# The Heist – attacking client-side data

- 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
```

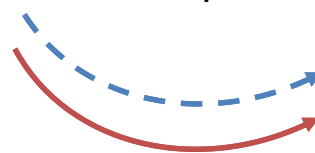
```
["ATL","LAS",7,"2007-07-27"]; SELECT 'STEAL',* FROM sysobjects WHERE type='u']
```

```
= ["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 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 does 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 wrote these 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. They are not enough.



# **THE OWASP TOP 10 WEB APPLICATION SECURITY RISKS FOR 2013**

[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 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

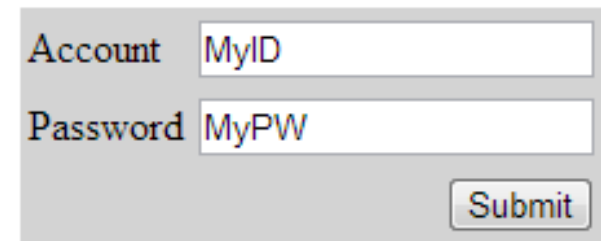
# A1: Injection

- 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 byte 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=admin'](http://example.com/app/accountView?id=admin)  
or *'1'='1'*

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

# A1: Injection (cont'd)



# A2: 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.)

# A2: 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)

## Scenario #1

An authenticated user of the site wants to let his friends know about the web page. He **e-mails the link** without knowing he is also giving away his session ID. When his friends use the link they will use his session and credit card.

## Scenario #2

Application's **timeouts** aren't set properly. User uses a **public computer** to access site. Instead of selecting "logout" the user simply closes the browser tab and walks away. Attacker uses the same browser an hour later, and that browser is still authenticated.

# A3: Cross-Site Scripting (XSS)

- XSS flaws occur whenever an application takes **untrusted raw data** and sends it **to another 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



# A3: Cross-Site Scripting (cont'd)

## 1 Attacker sets the trap

```
<tr><td>Name: </td></tr>
<tr><td>Msg: Nice Day!</td></tr>
<script>
// Send document.cookie to
// malicious web site using
onmouseover
</script>
<iframe src='xxx.net' height="0">
</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: Att  
Msg: Nice Day

⋮

# 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.
  - E.g., <https://www.onlinebank.com/user?acct=606>
    - How about changing the acct number?
  - E.g., <https://www.file.com/download?fid=gerlse>

**Recommendations:** Replace them with a temporary mapping value.

Validate the direct object reference.

# A5: 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.

# A5: Security Misconfiguration (cont'd)

- Examples

- default accounts, initial accounts, installation accounts
- default settings: directory traversal, source code directory (java, php, c)
- error messages, panic information, exception handling messages
- demonstration examples

# A6: Sensitive Data Exposure

- Scenario #1
  - An application encrypts credit card numbers in a database using **automatic database encryption**. However, this means it also decrypts this data automatically when retrieved, allowing an SQL injection flaw to retrieve credit card numbers in clear text. The system should have encrypted the credit card numbers using a public key, and only allowed back-end applications to decrypt them with the private key.
- Scenario #2
  - A site simply **doesn't use SSL** for all authenticated pages. Attacker simply monitors network traffic (like an open wireless network), and steals the user's session cookie. Attacker then replays this cookie and hijacks the user's session, accessing the user's private data.
- Scenario #3
  - The password database uses **unsalted hashes** to store everyone's passwords. A file upload flaw allows an attacker to retrieve the password file. All of the unsalted hashes can be exposed.

# A7: Missing Function Access Control

- 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

# A7: Missing Function Access Control (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.

# A8: 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?



# A8: 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.

# A9: Using Components with Known Vulnerabilities

- Virtually every application has these issues because most development teams don't focus on ensuring their components/libraries are **up to date**.
- In many cases, the developers don't even know all the components they are using, never mind their versions.
- Component dependencies make things even worse.

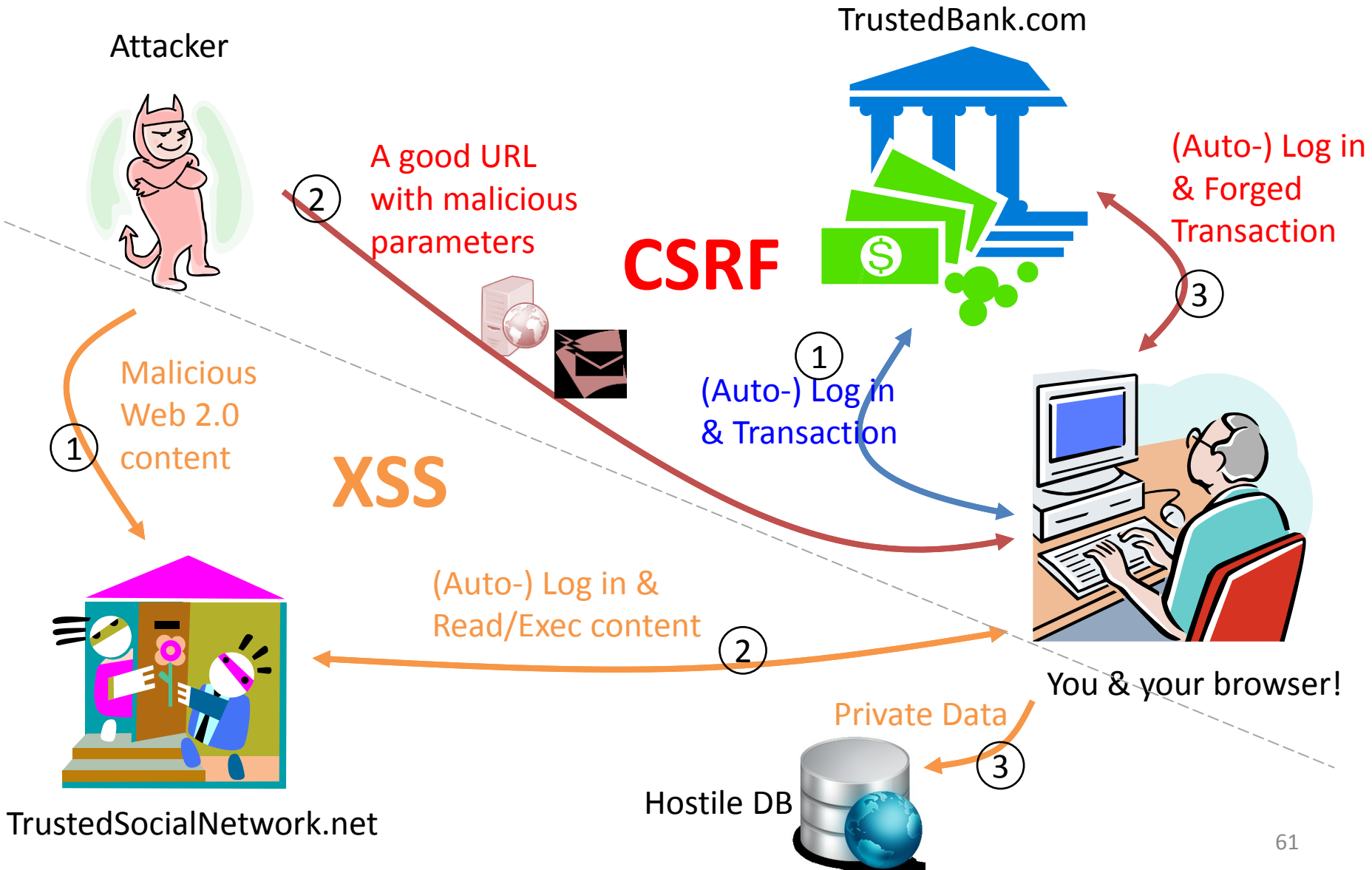
# A10: Unvalidated Redirects and Forwards

- 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>

# XSS vs. CSRF

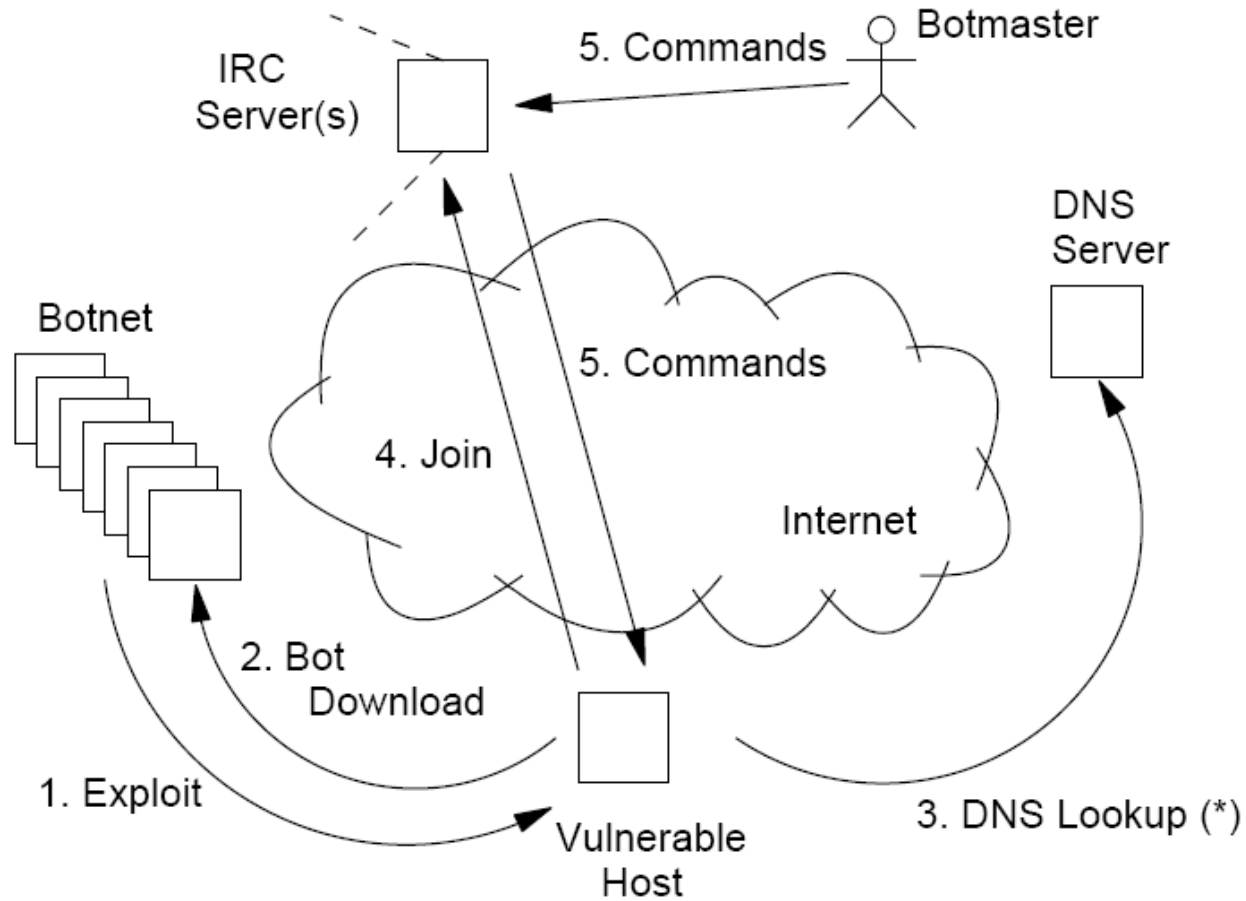


# **BOTNET**

# 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
?	Bobax	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
?	Donbot	80,000	500 million/day	
?	Grum	50,000	2 billion/day	Tedroo
?	Onewordsub	40,000	1.8 billion/day	?
?	<a href="#">Mega-D</a>	35,000	10 billion/day	Ozdok
?	Nucrypt	20,000	5 billion/day	Loosky, Locksky
?	Wopla	20,000	600 million/day	Pokier, Slogger, Cryptic
?	Spamthru	12,000	350 million/day	Spam-DComServ, Covesmer, Xmiler
?	Attack Team	10,000	250 million/day	Elite[B0tN3t]
August 14, 1996	<a href="#">SilverNet</a>	Unknown	Unknown	DataStream, doomNET

# Botnet as a Service

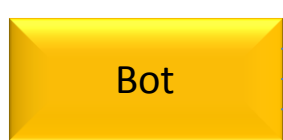
The screenshot displays a web-based interface for managing a botnet. At the top left, there is a dropdown menu with asterisks and a green 'Disconnect' button. Below this, a 'socks on port:' field shows '9099'. A green box highlights the selected bot: 'US 68.251.34.7 Chicago IL ID: 229'. To the right, account information is shown: 'Account : tst', 'group : admin', and 'time left : 19:59.25 +358d'. A green line graph shows data usage, with '30 Kb' and '15 Kb' markers. Below the graph are buttons for 'Select', 'Test HTTP Speed', and 'SBL Test'. A navigation bar includes '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



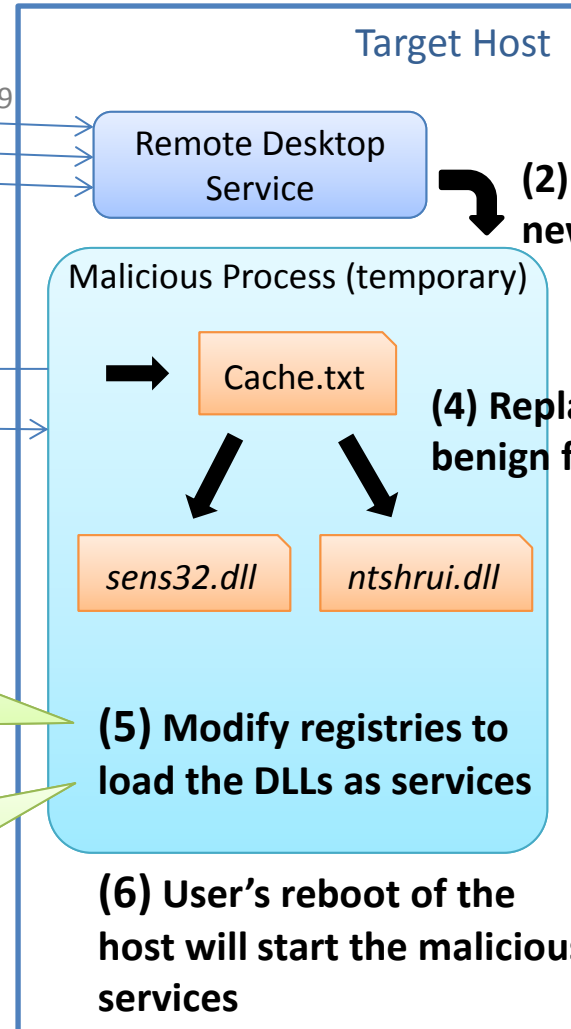
- (1) (a) Initiate RDP connection
- (b) Crack the password
- (c) Take control of the target host (encrypted)

RDP  
Port 3389



- (3) Request & download bot binary

HTTP  
Port 80



- (2) Create a new process

- (4) Replace benign files

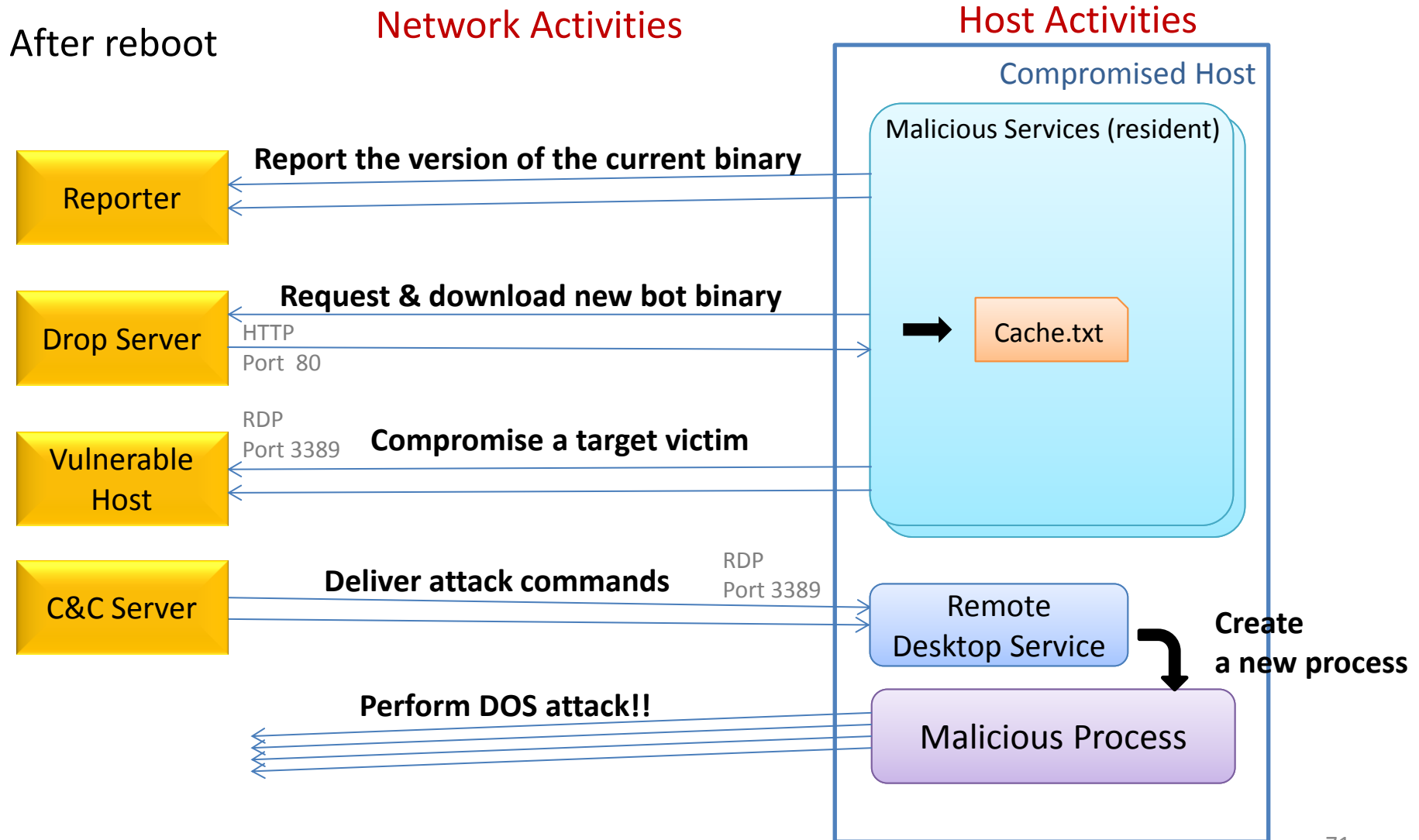
- (5) Modify registries to load the DLLs as services

- (6) User's reboot of the host will start the malicious services

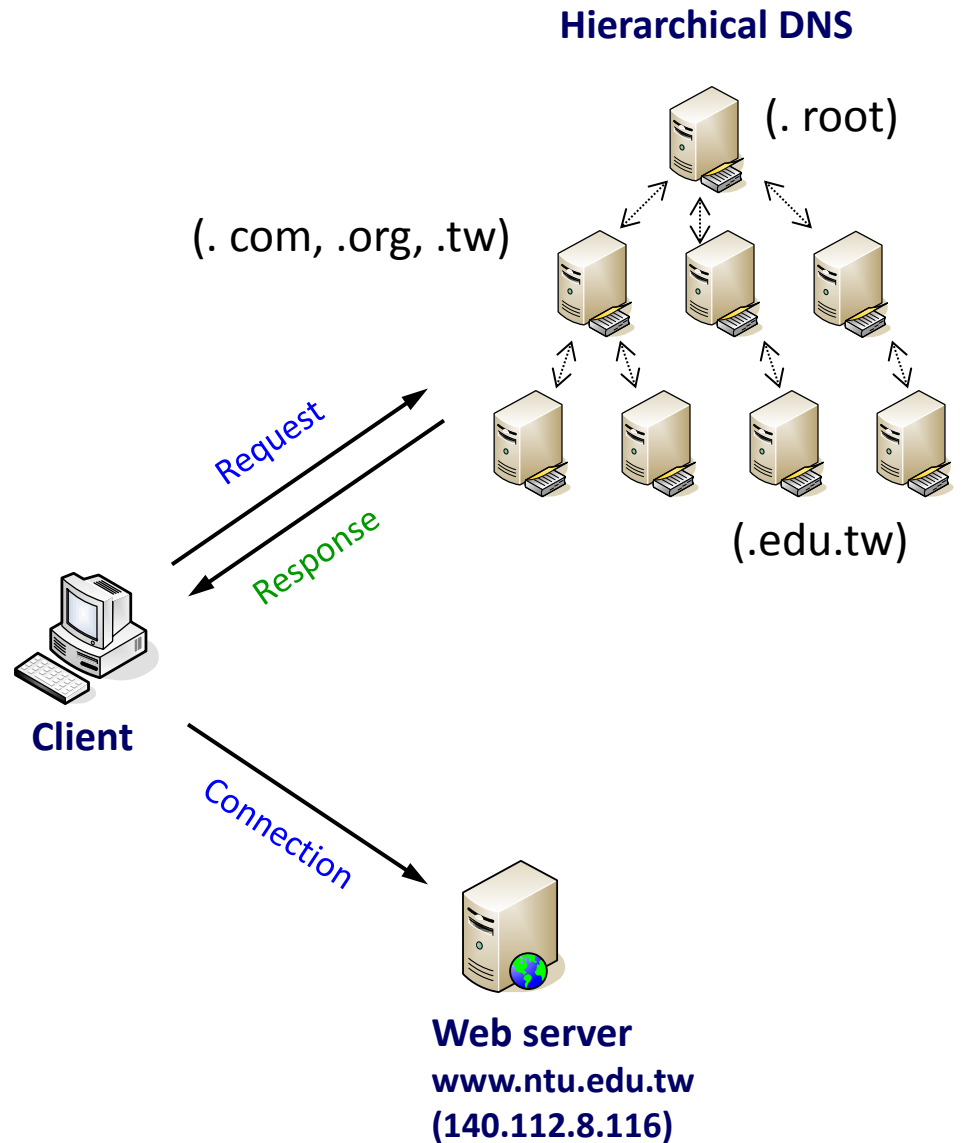
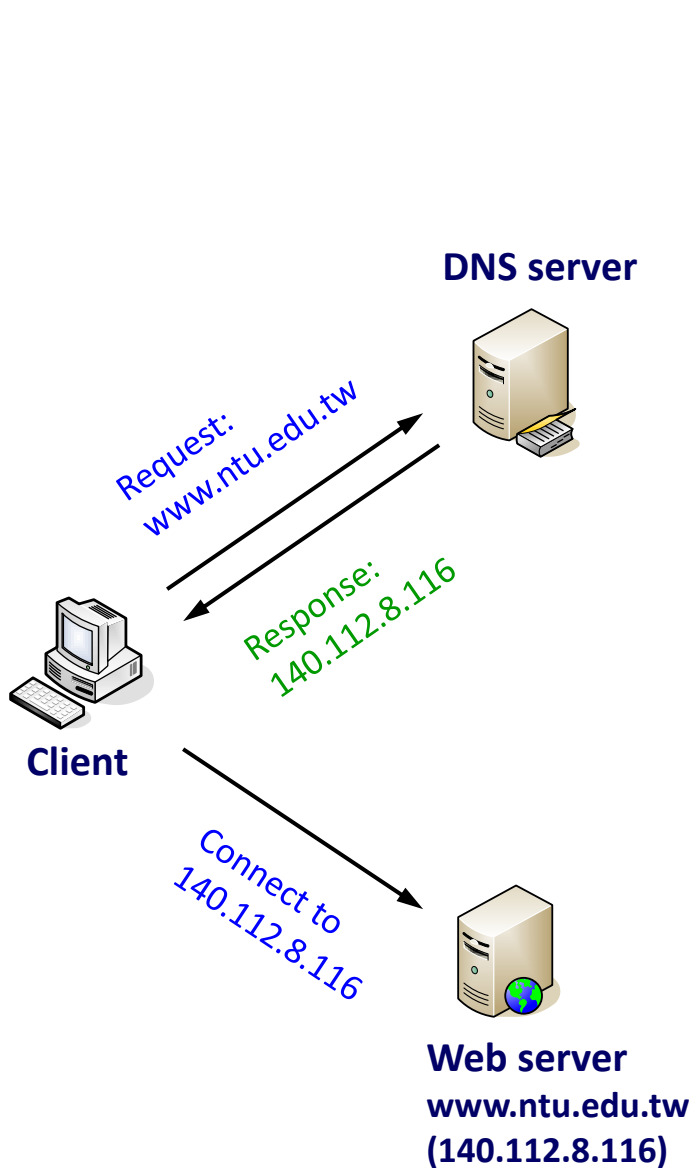
KLM\SYSTEM\CurrentControlSet\Services\Sens\Parameters  
"ServiceDll" = "<system folder>\sens32.dll"

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

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



# DNS and Fast-Flux



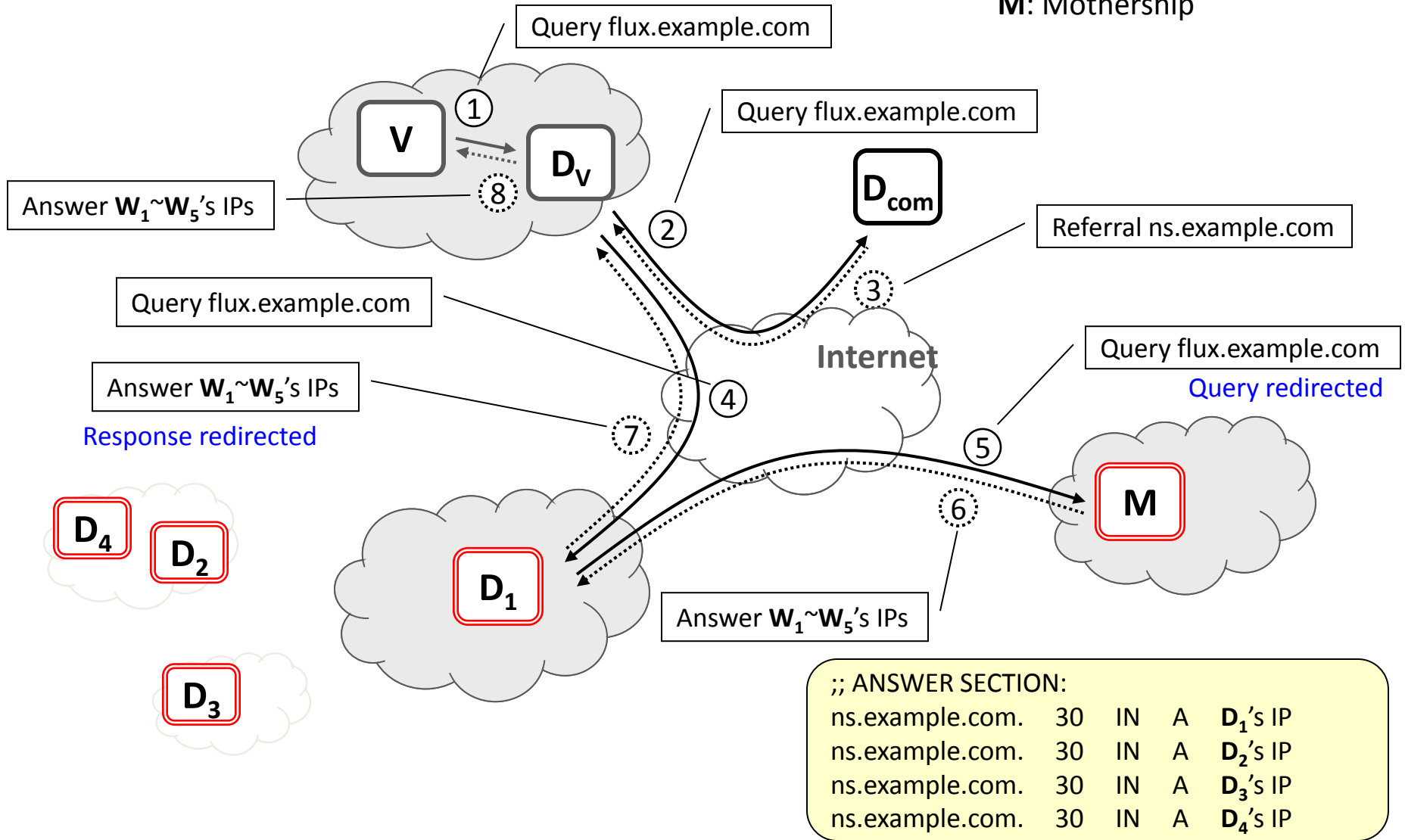


# DNS and Fast-Flux (cont'd)












- 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>	
2014/12/18_11:17	andreyzakharov.com/wp-content/plugins/wp-no-category-base/generic/	77.222.56.213	vh87.sweb.ru.	redirects to AppleId phishing	Registrar Abuse Contact onlinenic-enduser@onlinenic.com	44112	
2014/12/18_11:17	www.matecocinas.com/productos/mesas/mesa-brenda/4rfv/	213.162.195.146	matecocinas.com.	AppleId phishing	Registrar Abuse Contact abuse@registrar.eu	13287	
2014/12/18_06:50	austr-post.net/open/get_files.php?action=0.4786563355593916	37.230.116.108	molotov.genadij.example.com.	Trojan	Registrar Abuse Contact abuse-contact@publicdomainregistry.com	29182	
2014/12/18_06:50	austr-post.net/open/scripts.js	37.230.116.108	molotov.genadij.example.com.	AusPost Phish, Leads to trojan	Registrar Abuse Contact abuse-contact@publicdomainregistry.com	29182	
2014/12/18_06:50	austr-post.net/open/index.php	37.230.116.108	molotov.genadij.example.com.	AusPost Phish, Leads to trojan	Registrar Abuse Contact abuse-contact@publicdomainregistry.com	29182	
2014/12/17_23:45	my-screenshot.net/Image17398.png	62.76.74.228	-	Trojan.Downloader	Registrar Abuse Contact abuse@reg.ru	51408	
2014/12/17_23:45	my-screenshot.net/Image84726.png	62.76.74.228	-	Trojan.Downloader	Registrar Abuse Contact abuse@reg.ru	51408	
2014/12/17_23:45	my-screenshot.net/Image6542.png	62.76.74.228	-	Trojan.Downloader	Registrar Abuse Contact abuse@reg.ru	51408	
2014/12/17_23:45	my-screenshot.net/Image6542.png/	62.76.74.228	-	Trojan.Downloader	Registrar Abuse Contact abuse@reg.ru	51408	
2014/12/17_23:45	my-screenshot.net/Image6542.png	62.76.74.228	-	Trojan.Downloader	Registrar Abuse Contact abuse@reg.ru	51408	
2014/12/17_23:45	my-screenshot.net	62.76.74.228	-	Trojan.Downloader	Registrar Abuse Contact abuse@reg.ru	51408	
2014/12/17_21:01	whitehorsetechnologies.net/images/clients/x/mail.php	208.91.199.150	bh-7.webhostbox.net.	Destination of banking phishing	Registrar Abuse Contact abuse-contact@publicdomainregistry.com	19905	

# **SESSION HIJACKING AND CROSS SITE SCRIPT**

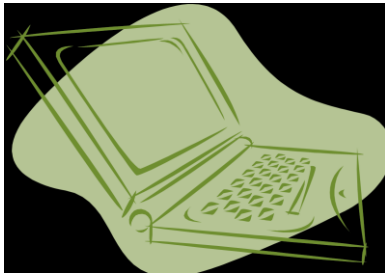
# HTTP Cookies & Sessions

- 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
```

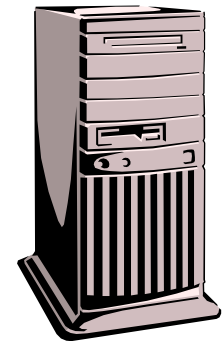
```
Cookie: id=123
```



HTTP Response

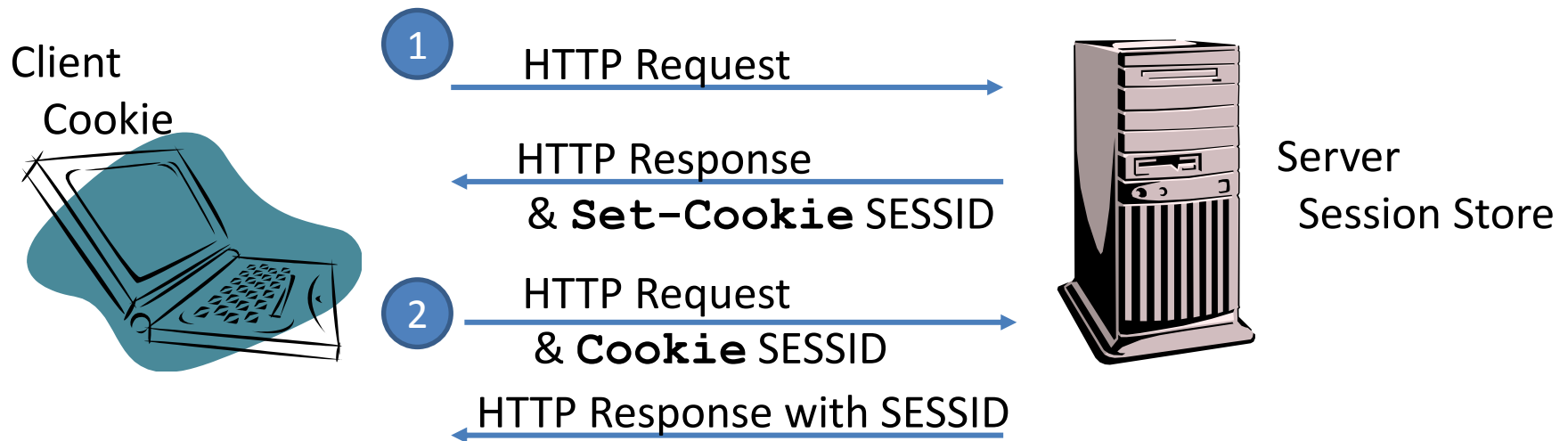
```
HTTP/1.1 200 OK
```

```
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 message in Chinese: "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 about girl suicide, it will execute an FBAutoLike script). Below the message is a large yellow question mark. The right sidebar contains advertisements for "Hottest Game on Facebook!" and "Play MMA Pro Fighter". A red box highlights the top navigation bar and the advertisement area. Another red box highlights the advertisement area.

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

Facebook Gmail - 「重要訊息發送...」

https://mail.google.com/mail/?hl=zh-tw&shva=1#label/Announce/12ca5f1a463cb8c2

Gmail Calendar Documents Reader Web more

@gmail.com | Settings | Help | Sign out

label:announce Search Mail Search the Web Show search options Create a filter

Mail Contacts Tasks

Compose mail

Priority Inbox Inbox Buzz Sent Mail Drafts All Mail Spam (92) Trash

Announce

« Back to "Announce" Remove label "Announce" Report spam Delete

Move to Labels More actions

« Newer 2 of 3531 Older »

「重要訊息發送」音樂會、網路與榮譽! Announce X

馮燕學務長 show details Dec 2 (2 days ago) Reply

計算機及資訊網路中心校內訊息轉送服務  
委託單位：學務長室  
委託人：馮燕學務長  
聯絡電話：33662995

各位同學大家好：  
時值初冬，但仍然風... 各種活動運動勃發盎然充滿生  
趣。相信同學們午間走... 到國家交響樂團破天荒在  
本校校園的野台表演... 春風的愉悅。別忘了12月  
11日晚間在總圖前草... 呂紹嘉指揮NSO的精彩草地音  
樂會，歡迎全校師生參加。

另外，近來常見學生於網路上發生「網路偏差行為」，同學們  
都知道網際網路快速發展，網際網路的使用已生活化、大眾化及  
普及化，給大眾帶來更多的便利，但請同學們注意使用網路時的  
行為。  
現今網路所產生的偏差問題更勝以往，如：網路色情、網路誹  
謗、網路成癮、網路一夜情、電腦病毒、下載非法MP3音樂、隱  
私權... 這些行為均能造成各種法律問題...

Ads

soapkitchen Australia  
Huge range of 100% Natural, Organic & Safe Skincare with Integrity  
www.soapkitchen.com.au

Nonin Pulse Oximeters  
Complete Nonin Product Line  
Great prices and fast delivery  
www.PmedicalOnline.com

Discount OPI, Essie.lbd  
All newest collections, best choice at best price! Offers and Sales  
www.beauty4nails-body.co.uk

Private Label Skin Care  
for Salons, Spa, and Bulk

# Mashups

flash

首頁 > 即時 > 自由時報 > 社會

熱門社會新聞

## 「保證非詐騙」網購90萬保時捷真上當

自由時報-2014年12月22日 上午06:38

f讚 8 g+1 0

字級：小 中 大 特 | 列印 | 轉寄 | 分享

〔自由時報記者林嘉東／基隆報導〕詐騙新手法！許姓男子在露天拍賣網看上一輛一生夢想的保時捷二手車，賣家願意減價賣他 90萬元，還寄來車主存簿、提款卡、印章擔保，讓他以為確實撿到便宜，依約匯90萬至車主帳戶後，沒想到賣方馬上辦掛失，讓許「夢想沒了、錢也沒了」。

基隆警方指出，這一週來，另有5件在露天拍賣網站上購買3C產品的買家，被詐騙集團以「誤勾到分期付款」傳統詐騙手法，騙走2萬到5萬元不等；警方呼籲買家別貪小便宜，或是選擇貨到付款自保。

警方指出，許男與妻子收入穩定、育有一子，夢想有朝一日能開著保時捷跑車，載著妻小馳騁逍遙。

許男在露天拍賣網站看上一輛保時捷997，出價不到150萬，公里數僅6萬公里，更讓他心動的是，賣方說為了衝高評價與降低保時捷折舊，帳面上成交價還是150萬元，但願意私下賣他90萬元。

賣方為取信許男，保證「絕對不是詐騙集團」，把車主的存款簿、提款卡與印章都寄給許做為擔保，許不疑有他，便把90萬元匯入車主帳戶。

登入 / 註冊

電子報 樂透 發票 回蕃薯藤

政治專欄

廣告

momo 購物網

### 即期良品

—全面3折up—

flash

廣告

2014 愛老人 年華

邀請你一同關懷角落中的弱勢長輩，讓愛團圓。

# 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

## ■ 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
- 搶便宜! 38度高粱就賣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

Glam 巨匠密碼

**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

星座七宮看配備

- 歐萊特1週年慶 買4000送1000 [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

## ■ 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
- 威寶印務: 明年協助衝高機 [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.

# **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, ...





# 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 you to access the form.

[Access The Form](#)

Thank you for your patience  
USAA

Internet Bank

Internet Banking user

Create your own digital certificate  
To begin the digital certificate process

Legal Information | Accessibility

Valued eBay Member,

**Update Your Account Information Within 24 Hours**

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 hours.

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

Establish your proof of identity with ID Verify (free of charge) - an easy way to become a trading partner. The process takes about 5 minutes to complete and involves updating your 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 trade. 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

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

# 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

網頁 地圖 新聞 圖片 影片 更多 ▾ 搜尋工具

約有 331,000 項結果 (搜尋時間: 0.40 秒)

## 資訊管理學系所 - 國立臺灣大學

[www.im.ntu.edu.tw/](http://www.im.ntu.edu.tw/) ▾

由於這個網站的 robots.txt，因此無法提供此結果的說明 - 瞭解詳情。

## 2014台大資管落點分析系統-ImWhatIM - 台灣大學資管系學生會

[union.im.ntu.edu.tw/ImWhatIM/](http://union.im.ntu.edu.tw/ImWhatIM/) ▾

最新消息. 2014-08-08 目前已經將實際分數取代估計分數了，歡迎繼續使用. 2014-07-22

目前已經使用103年的組合人數表做落點預測！歡迎大家多多使用，若有 ...

## Bing-Yu Chen

[graphics.csie.ntu.edu.tw/~robin/](http://graphics.csie.ntu.edu.tw/~robin/) ▾ 翻譯這個網頁

2014年12月6日 - Email, robin(AT)ntu.edu.tw, Web,

<http://graphics.csie.ntu.edu.tw/~robin/> ... Spring 2013 IM Ph.D. Forum (with Hsin-Min Lu) also in Fall 2009 (with ...

## 孔令傑 - 國立臺灣大學管理學院

[exp.management.ntu.edu.tw/zh-TW/IM/teachers/26](http://exp.management.ntu.edu.tw/zh-TW/IM/teachers/26) ▾

研究室, 二館413室, 電話, (02)33661176. 手機, 傳真, 個人網頁, <http://www.im.ntu.edu.tw/~lckung>.

E-mail, lckung(AT)ntu.edu.tw. 研究領域, 資訊經濟, 醫療照護管理 ...

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

[goal.im.ntu.edu.tw/](http://goal.im.ntu.edu.tw/) ▾ 翻譯這個網頁

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

## 登入確認頁

<https://intranet.im.ntu.edu.tw/> ▾

歡迎使用IM Intranet，本系統提供台大資管系教職員、學生、畢業生、系友，... 請用工作站帳號登入，此帳號終身有效；如有任何問題，歡迎來信指教: [imta@im.ntu.edu.tw](mailto:imta@im.ntu.edu.tw).

## 系電腦實驗室 - 國立臺灣大學資訊管理學系暨研究所

[exp.management.ntu.edu.tw/IM/服務資源/系電腦實驗室](http://exp.management.ntu.edu.tw/IM/服務資源/系電腦實驗室) ▾

聯絡方式：電話：(02)3366-1198 電子郵件：imta(AT)im.ntu.edu.tw. 實驗室使用印表機使用 掃描器使用. 實驗室內所有個人電腦，均由SAMBA PDC 網域控制伺服器 ...

site: im.ntu.edu.tw

網頁 圖片 新聞 地圖 影片 更多 ▾ 搜尋工具

約有 603,000 項結果 (搜尋時間: 0.30 秒)

## 2014台大資管落點分析系統-ImWhatIM - 台灣大學資管系學生會

[union.im.ntu.edu.tw/ImWhatIM/](http://union.im.ntu.edu.tw/ImWhatIM/) ▾

最新消息. 2014-08-08 目前已經將實際分數取代估計分數了，歡迎繼續使用. 2014-07-22

目前已經使用103年的組合人數表做落點預測！歡迎大家多多使用，若有 ...

## [PDF] IBM Solutions Grid for Business Partners

[jyoung.im.ntu.edu.tw/teaching/.../IBM\\_grid\\_wp.pdf](http://jyoung.im.ntu.edu.tw/teaching/.../IBM_grid_wp.pdf) ▾ 翻譯這個網頁

on site or through a VPN connection. Business Partners will be able to run Grid applications using ^ hardware and simulated virtual machines under. Linux and ...

## Pacific Graphics 2006 in Taipei

[graphics.im.ntu.edu.tw/pg2006/](http://graphics.im.ntu.edu.tw/pg2006/) ▾ 翻譯這個網頁

The 14th Pacific Conference on Computer Graphics and Applications (Pacific Graphics 2006) will be held on October 11 to 13, 2006 in Taipei, Taiwan. Taipei is ...

## [PDF] 參賽作品說明書 - 國立臺灣大學

[weal.im.ntu.edu.tw/report/BooMiner.pdf](http://weal.im.ntu.edu.tw/report/BooMiner.pdf) ▾

圖5 BooMiner 網頁架構圖(Site Map). 網頁的8大功能: 1、分數圖與關鍵報導：即人氣漲跌分析網頁。BooMiner 以折線圖呈現名人的人氣、變化，Boom Index 是反映 ...

## [PDF] Protein Function Prediction By Matching 3D ... - NTUR

[ntur.lib.ntu.edu.tw/retrieve/170793/11.pdf](http://ntur.lib.ntu.edu.tw/retrieve/170793/11.pdf) ▾ 翻譯這個網頁

由 CC Chen 著作 - 2003 - 被引用 4 次 - 相關文章

{ccchen, magicct, zick, liang}@cmlab.csie.ntu.edu.tw, {robin@ntu.edu.tw, \*ming@csie.ntu.edu.tw} ... where the protein matches the selected site can be con-

## [PDF] <http://www.im.ntu.edu.tw/frontiers2013/>

[frontiers2013.im.ntu.edu.tw/sites/.../Conference%20Progra...](http://frontiers2013.im.ntu.edu.tw/sites/.../Conference%20Progra...) ▾ 翻譯這個網頁

2013年7月6日 - Page 1. <http://www.im.ntu.edu.tw/frontiers2013/> ..... "Web Site Engagement: Behavioural or Attitudinal?" Enrique Bigné, University of Valencia, ...

## [PDF] FLoD: A Framework for Peer-to-Peer 3D Streaming

[graphics.im.ntu.edu.tw/docs/infocom08.pdf](http://graphics.im.ntu.edu.tw/docs/infocom08.pdf) ▾ 翻譯這個網頁

由 SY Hu 著作 - 被引用 88 次 - 相關文章

3D sites were to exist, prior installations for each one of them would be frustratingly ... Scalable and efficient 3D streaming thus may be an im- portant enabler for ...

