Website Vulnerabilities Revealed

Jeremiah Grossman
WhiteHat Security founder & CTO
Jeremiah Grossman

WhiteHat Security Founder & CTO
Technology R&D and industry evangelist
(InfoWorld's CTO Top 25 for 2007)
Frequent international conference speaker
Co-founder of the Web Application Security Consortium
Co-author: Cross-Site Scripting Attacks
Former Yahoo! information security officer
Custom Web Applications, Custom Vulnerabilities

Data is unique from reports distributed by Symantec, Mitre (CVE), IBM (ISS) X-Force, SANS, and others. These organizations track publicly disclosed vulnerabilities in commercial and open source software products, which may contain Web application flaws as well. WhiteHat Security’s data is different because it focuses solely on previously unknown vulnerabilities in custom web applications, code unique to that organization, on real-world websites.

© 2008 WhiteHat Security, Inc.
Global Scale

9 out of 10 Websites Have Serious Vulnerabilities

- Obtained between January 1, 2006 and February 22, 2008
- Classified according to the WASC Threat Classification
- Over 600 public-facing and pre-production websites
- Vast majority of websites are assessed weekly for vulnerabilities
- Currently 4,488 unresolved vulnerabilities
- Nine out of ten websites have at least one significant vulnerability
- Average of 7 vulnerabilities per website
But how bad is it really?

Likelihood that a website has a vulnerability, by severity

Websites with Urgent, Critical, or High severity issues technically would not pass PCI compliance
Samy opens new front in worm war

By Muñir Katcha
Staff Writer, CNET News.com
Published: October 17, 2005 11:40 AM PDT

Welcome Google user!
More headlines related to "F:
- Harnessing the power of wind and waves
- Police Baiter: Armed robbers nabbed through text messages
- Microsoft-Yahoo: the mother of all clusterbombs
- Week in review: Apple goes into thin 'Air'
- More interesting headlines

The newly discovered Samy worm is one of the first to exploit a cross-site scripting vulnerability, a technique security experts fear could be used to open a new front in attacks.

Italian Bank's XSS Opportunity Seized by Fraudsters

An extremely convincing phishing attack is using a cross-site scripting vulnerability on an Italian bank's own website to attempt to steal customers' bank account details. Fraudsters are currently sending phishing mails which use a specially-crafted URL to inject a modified login form onto the bank's login page.

The vulnerable page is served over SSL with a bona fide SSL certificate issued to Banca Italsider S.p.A. in Italy. Nonetheless, the Italian security firm IncidentID has discovered that the bank's login page has been hacked and is being used as a phishing site.

In an effort to prevent the fraudsters from stealing users' account data, the bank has temporarily removed the vulnerable login page from its website.

40 Million Credit Card Numbers Hacked
Data Breach at Processing Center

By Jonathan Kim and Michael Barbar
Washington Post Staff Writers
Saturday, June 18, 2005, Page A01

More than 40 million credit card numbers belonging to U.S. consumers were accessed by a computer hacker and are at risk of being used for fraud, MasterCard International Inc. said yesterday.

In the largest security breach of its kind, MasterCard officials said all credit card brands were affected, including 13.9 million cards bearing the MasterCard label. A spokeswoman for Visa USA Inc. confirmed that 22 million of its card numbers may have been breached, while Discover Financial Services Inc. said it did not yet know if its cards were affected.
Another way to look at the badness

Percentage of vulnerabilities ranked by severity

- 18% HIGH
- 72% URGENT
- 10% CRITICAL
WhiteHat Security: Top 10

**Likelihood that a website has a vulnerability, by Class**

- Cross-Site Scripting: 65%
- Information Leakage: 40%
- Content Spoofing: 23%
- Predictable Resource Location: 17%
- SQL Injection: 16%
- Insufficient Authentication: 15%
- Insufficient Authorization: 14%
- Abuse of Functionality: 10%
- HTTP Response Splitting: 8%
- Directory Indexing: 4%

© 2008 WhiteHat Security, Inc.
Overall vulnerability population

- Cross-Site Scripting: 70%
- Content Spoofing: 7%
- SQL Injection: 4%
- Predictable Res. Loc.: 5%
- Information Leakage: 4%
- HTTP Response Splitting: 5%

© 2008 WhiteHat Security, Inc.
Technology Breakdown

FILE EXTENSIONS

- ASP: 25%
- ASPX: 9%
- JSP: 8%
- DO: 4%
- Other: 12%
- Unknown: 41%
- PHP: 1%
What’s not there

Obviously we’re not going to find buffer overflows or format string issues in custom web applications

We’re also not looking for the well-known php issues and the like

Cross-Site Request Forgery remains VERY DIFFICULT to scan for and we only report the most egregious cases identified by hand

We keep finding new and cool ways of performing XSS filter-evasions

HTTP Response Splitting pushed XPath Injection off the list
Industry Verticals

Percentage of websites with either URGENT, CRITICAL or HIGH severity vulnerabilities ranked by industry

- Retail: 52%
- Financial Services: 60%
- Insurance: 84%
- Healthcare: 64%
- IT: 72%
Worst of the Worst

Percentage of vulnerability classes in overall population ranked by industry
Average inputs per website: 154
Ratio of vulnerability/inputs: 2.2%
Time to Fix

<table>
<thead>
<tr>
<th>Issue</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Injection</td>
<td>138</td>
</tr>
<tr>
<td>Insufficient Authorization</td>
<td>59</td>
</tr>
<tr>
<td>HTTP Response Splitting</td>
<td>104</td>
</tr>
<tr>
<td>Directory Traversal</td>
<td>105</td>
</tr>
<tr>
<td>Insufficient Authentication</td>
<td>160</td>
</tr>
<tr>
<td>Insufficient Authentication</td>
<td>88</td>
</tr>
<tr>
<td>Cross Site Scripting</td>
<td>92</td>
</tr>
<tr>
<td>Abuse of Functionality</td>
<td>123</td>
</tr>
<tr>
<td>Session Fixation</td>
<td>28</td>
</tr>
<tr>
<td>Cross Site Request Forgery</td>
<td>17</td>
</tr>
<tr>
<td>HTTP Response Splitting</td>
<td>36</td>
</tr>
<tr>
<td>Information Leakage</td>
<td>114</td>
</tr>
<tr>
<td>Content Spoofing</td>
<td>85</td>
</tr>
<tr>
<td>Predictable Resource Location</td>
<td>128</td>
</tr>
<tr>
<td>Directory Indexing</td>
<td>87</td>
</tr>
</tbody>
</table>

URGENT
CRITICAL
HIGH

© 2008 WhiteHat Security, Inc.
Lessons Learned

Vertical Comparisons – IT Security is extremely curious about how their security compares to others in their market. When behind the curve, justification for additional resources. When ahead, outside validation and assurance of their security program.

Remediation/Mitigation – IT Security is responsible for website security, but has no control over it (can’t patch, no firewalls). The developers don’t work for them and have other priorities other than security. This environment causes lengthy time-to-fix cycles.

Possible vs. Probable – Just because a vulnerability is found doesn’t mean it’ll be exploited. Not all vulnerabilities are created equal, some are easier to take advantage of others, and the bad guys will take the path of least resistance.

Assignment of blame – When an incident occurs exploiting a vulnerability previously reported, it’s the developers fault. When exploited by a vulnerability not found, it’s IT Security’s fault.
Those that are more "secure" have:

Use of modern development frameworks with security configs turned on (.NET, J2EE, Rails, etc.)

Vulnerability remediation prioritized by severity/threat rating (High: 1 - 7 days, Medium: < 30 days, Low: Next Update)

At least some security involvement in the SDLC (awareness training, threat modeling, QA testing, etc.)
Thank You!

For more information visit:  www.whitehatsec.com/

Jeremiah Grossman, founder and CTO
blog: http://jeremiahgrossman.blogspot.com/
email: jeremiah@whitehatsec.com