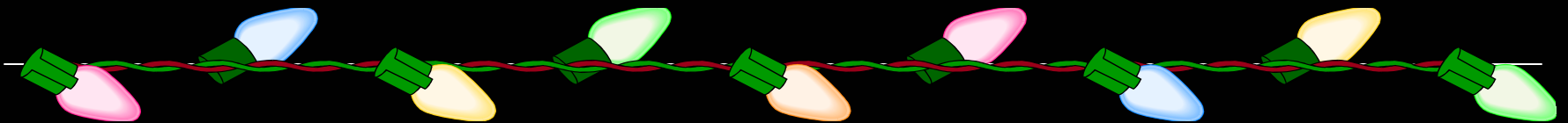

Vulnerability Summary

November/December 2004

Paul Asadoorian
Lead IT Security Specialist
Brown University



Vulnerabilities

- Web Browser Security
- Samba Buffer Overflow
- PHP Vulnerabilities
- FREE Intrusion Prevention for Windows

Web Browser Security

- Yet even more unpatched vulnerabilities in Internet Explorer
- Two problems:
 - URL re-direction
 - Buffer Overflow leading to code execution



Web Browser Security

- URL redirection
 - Presents a link to the user
 - Status bar displays the same link
 - Link really goes somewhere else

- Example

Web Browser Security

- Buffer overflow in iFRAME (again)
- Attackers finding new ways to exploit the same vulnerabilities
- Leads to execution of arbitrary code with the permissions of the user logged in

Web Browser Security

- Internet Explorer (IE) is the CIS supported web browser
- ERP applications (like ours) require IE
- Some web sites will not function with browsers other than IE
- Alternate browsers are considered just that, an alternative, and are currently unsupported by CIS

Web Browser Security

- People using Firefox as an alternative
 - Brown University Security Team
 - Cisco Technical Support Engineers
 - Everyone in Finland
 - <http://asia.cnet.com/news/software/printfriendly.htm?AT=39202962-39037051t-39000001c>

Web Browser Security

- Firefox 1.0 release in early November
- Over 5.6 million downloads in first two weeks
- Received CNET Editors Choice Award
 - *“If you're fed up with the latest Internet Explorer security patch issued from Microsoft or with the latest virus to capitalize on some flaw in IE, you should switch to Firefox--now.”*
 - http://reviews.cnet.com/Mozilla_Firefox_1_0/4505-9241_7-31117280-2.html?tag=top

Samba Buffer Overflow

- Samba versions 3.0.7 and prior are vulnerable
 - Not Samba versions 2.x
- Remotely exploitable
- Special pathnames must exist or user must have write permissions



Samba Buffer Overflow

- Upgrade to Samba version 3.0.8
- Patch available for Samba version 3.0.7
- Restrict access to NetBIOS ports
 - TCP/UDP ports 135-139, 445

PHP Vulnerabilities

- SANS issued an alert on November 28th
- Numerous web servers were compromised using PHP vulnerabilities
- Securing a web application is two fold:
 - Patching/Upgrading web server software
 - Securing the web application



PHP Vulnerabilities

- Apache and associated modules need to be kept up to date
- Latest versions are:
 - PHP 4.3.9 or 5.0.2 (www.php.net)
 - Apache 1.3.33 or 2.x (www.apache.org)
 - Mod_SSL 2.8.22 (www.modssl.org)
 - Mod_Perl 1.29 (perl.apache.org)
 - Openssl 0.9.7e (www.openssl.org)

PHP Vulnerabilities

```
# nc www.example.com 80
HEAD / http/1.0

HTTP/1.1 200 OK
Date: Wed, 01 Dec 2004 17:14:59 GMT
Server: Apache/1.3.32 (Unix)PHP/4.3.8
      mod_perl/1.29 mod_ssl/2.8.21
      OpenSSL/0.9.7d
Connection: close
Content-Type: text/html
```

PHP Vulnerabilities

- Securing the application is even more difficult
- Cross-site scripting & SQL injection are popular
- Problems are hidden in code and not easily found

PHP Vulnerabilities

- Tools to help:
 - Nikto (<http://www.cirt.net/code/nikto.shtml>)
 - Web application scanner based on whisker by RFP
 - Wikto (<http://www.sensepost.com/research/wikto/>)
 - Windows version of Nikto
 - Also runs google hacks
 - Example

PHP Vulnerabilities

- Achilles
 - <http://packetstormsecurity.org/web/achilles-0-27.zip>
 - Web application tester
 - Intercepts the session
 - Great for SSL Man-In-The-Middle
- WebScarab
 - <http://www.owasp.org/software/webscarab.html>
 - Proxy, spider, session analysis tool

FREE Intrusion Prevention for Windows

- Prevx Home edition, free for personal use
- <http://www.prevx.com>
- According to web site protects you from:
 - Memory/Buffer Overflow Attacks
 - File System Attacks
 - Registry Attacks
 - Uncontrolled Program Execution
 - Process Hijacking

/* The End */



Questions? Comments? Flame Mail? Donations?

Paul_Asadoorian@brown.edu

This presentation:

<http://www.brown.edu/Research/SysAdmins/vuln-nov-2004.pdf>

Paul's Essential Security Links

<http://packetstormsecurity.nl/>

<http://www.incidents.org>

<http://www.security.nnov.ru/>

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

<http://www.cert.org>

<http://www.l0t3k.org/>

<http://www.whitehats.com>

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

<http://rr.sans.org>