



Web Security School Lesson 3

Locking down your Web applications

Michael Cobb, Founder & Managing Director, Cobweb Applications, Ltd.



searchsecurity.com/WebSecuritySchool



Web Security School overview



- Lesson 1: How to secure a Web server and understanding risks to your Web site
- · Lesson 2: How to secure the network perimeter and defeat Web attacks
- Lesson 3:

Webcast: Locking down your Web applications

* Includes: Developer's active content delivery checklist Spyware removal checklist

Article: Top tools for testing your online security

Quiz: Test your knowledge of the materials covered in Lesson 3

Through an agreement with (ISC)2, all CISSPs and SSCPs earn one CPE credit for each Security School webcast attended.

searchsecurity.com/WebSecuritySchool



·	

Today's agenda

- Directory structures and permissions
- Web page coding essentials
- Primer on input and output validation
- Change management
- End-to-end reliability
- Phishing, adware and spyware
- Protecting your networked PCs



Active content technology

- CGI (Common Gateway Interface)
- ASP
- PHP
- Perl
- ActivePerI
- Server-Side Include (SSI) Directives



<FORM ACTION=

http://www.yourserver.com/scripts/processorder.pl
METHOD=POST>



Folder structures for active content

File Type	Folder
CGI (.exe, .dll, .cmd, .pl)	E:\inetpub\wwwroot\myserver\executable
Script files (.asp, .aspx)	E:\inetpub\wwwroot\myserver\script
Include files (.inc, .shtm, .shtml)	E:\inetpub\wwwroot\myserver\include
Static pages (.txt, .html)	E:\inetpub\wwwroot\myserver\static
Static content (.gif, .jpg)	E:\inetpub\wwwroot\myserver\images



File permissions

Appropriate ACLs on virtual directories

File type	Access control list
CGI (.exe, .dll, .cmd, .pl)	Everyone (Denied)
E:\inetpub\wwwroot\myserver\executable	Administrators (Full Control)
	System (Full Control)
Script files (.asp)	Everyone (Denied)
E:\inetpub\wwwroot\myserver\script	Administrators (Full Control)
	System (Full Control)
Include files (.inc, .shtm, .shtml)	Everyone (Denied)
E:\inetpub\wwwroot\myserver\include	Administrators (Full Control)
	System (Full Control)
Static pages (.txt, .html)	Everyone (Read)
E:\inetpub\wwwroot\myserver\static	Administrators (Full Control)
	System (Full Control)
Static content (.gif, .jpg)	Everyone (Read)
E:\inetpub\wwwroot\myserver\images	Administrators (Full Control)
	System (Full Control)



Coding essentials

- ✓ Scripting for Security
 - ✓ www.microsoft.com/technet/scriptcenter/hubs/security.mspx
- √ PHP Advisory
 - √ http://www.phpadvisory.com/



- ✓ Understanding Malicious Content
 - √ http://www.cert.org/tech_tips/malicious_code_mitigation.html



Primer on input and output validation

- √ Validate all data before it is processed either on receipt or on publication.
- √ Validate
 - ✓ Form data
 - ✓ Database content
 - √ File content





· · · · · · · · · · · · · · · · · · ·	
	

Input validation

- √ Client-side validation
 - ✓ JavaScript
 - **✓** MAXLENGTH
- √ Server-side validation
 - √ Regular expressions
 - ✓ ASP.NET validation controls
- √ Database input validation



Filtering and encoding characters

√ Filter special characters

- X < > " ' % ;) (& + -
- X <>
- √ &It; >

√ Encode special characters

- √ Set document character encoding
- √ <META http-equiv="Content-Type" con CHARSET=ISO-8859-1">
- ✓ Encode output of special characters





Hidden form fields

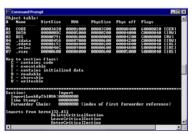
- Never use hidden form fields for sensitive data.
- Never use hidden form fields for sensitive data.

- Never use hidden form fields for sensitive data.
- Never use hidden form fields for sensitive data.



Validate third-party programs

- ISAPI DLLs can gain elevated privileges to the level of the built-in SYSTEM account.
- Inspect third party executables on your site.
- Use Microsoft's Binary
 File Dumper tool (dumpbin.exe).
- dumpbin /imports UntrustedISAPI.DLL | find "RevertToSelf"





Change management

- Use Change or Source Control
- Use a development server
- Remove .bak files
- Associate .bak files with the scripting engine
- Run cipher.exe





Protecting your data

- ✓ Don't use live production data
- ✓ Mirror data to separate servers
- ✓ Implement rollback and recovery





End-to-end reliability

Lack of reliability

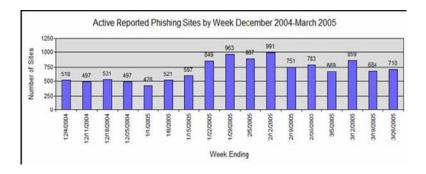
Perceived lack of security





Phishing

• www.antiphishing.org





· · · · · · · · · · · · · · · · · · ·	
	

Phishing from a corporate perspective

- Affects customer confidence
- ✓ Develop e-mail policies



- √ Google your organization
- √ Whois similar Web addresses



Identifying phishing scams

Pop

http://192.168.255.205/wood/index.htm

- "Verify your account."
- "Click the link below to gain access to your account."

 https://www.woodggovebank.com/logins
- "If you don't respond within 48 hours, your account will be closed."
- "Dear Valued Customer"



How to avoid phishing scams

- Be suspicious of any e-mail with an urgent request for personal financial information.
- Don't use the link in an e-mail to get to a Web page if you suspect the message might not be authentic.
- Always ensure that you're using a secure Web site when submitting credit card or other sensitive information via your Web browser.
- Regularly log into your online accounts.
- Ensure that your browser is up to date and security patches applied.



Adware and spyware

- Accounts for 20% or more of IT help desk efforts
- Can capture data before it is encrypted
- Has surpassed even spam as biggest threat





Antispyware checklist

- PCs are running unusually slow.
- Ads are popping up.
- Home pages have been changed.
- Unusual toolbars appear on browsers.
- Antispyware and/or AV programs not working correctly.
- There's a dramatic increase in network traffic.





Protecting your networked PCs

- Run the Benchmarks and Scoring Tool
- Create an acceptable usage policy
- Communicate it to your users
- Regularly update antivirus software
- Keep patches up to date
- Never install software via a Web browser
- Disable ActiveX
- Disable third-party cookies





Internet Explorer security checklist

- Disable ActiveX controls
- Use the Zone Management features
- Manage IE settings with IE Administrator's Kit.
- Update patches regularly
- Educate your users





Looking Ahead

- More client-side attacks
- More vulnerabilities in complex data formats
- More vulnerabilities in Web applications
- More malicious code for mobile devices





Homework



- Check all Web pages against the Developer's active content delivery checklist.
- Review your data-handling methodology.
- Check for hidden form fields in your forms.
- Run Benchmarks and Scoring Tool against all workstations.



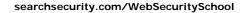
Web Security School, Lesson 3

Webcast: Locking down your Web applications

* Includes: Developer's active content delivery checklist Spyware removal checklist

Article: Top tools for testing your online security

Quiz: Test your knowledge of the materials covered in Lesson 3





Through an agreement with (ISC)2, all CISSPs and SSCPs earn one CPE credit for each Security School webcast attended.

	-	
-		-
	>	11
Searc	Secur	ty.com
acart.	13ecur	Nycom

Web Security School



- Lesson 1: How to secure a Web server and understanding risks to your Web site
- Lesson 2: How to secure the network perimeter and defeat Web attacks
- Lesson 3: How to lock down Web apps and tools for testing online security

Through an agreement with (ISC)2, all CISSPs and SSCPs earn one CPE credit for each Security School webcast attended.

searchsecurity.com/WebSecuritySchool