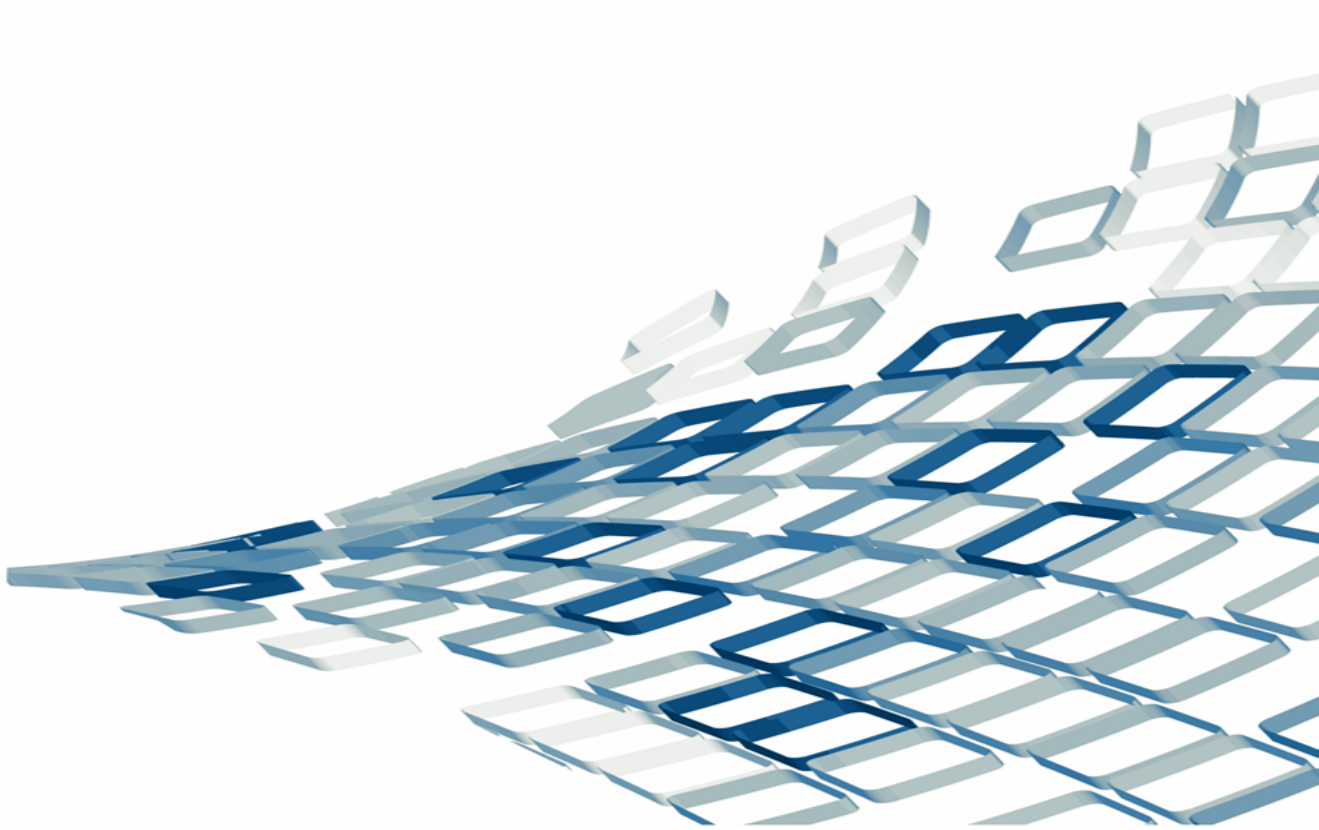
Certified Internet Web Professional



Lesson 8:
JavaScript Security

Objectives

- Distinguish between the browser and the operating system in relation to the elements responsible for security
- Discuss browser security issues relevant to JavaScript
- Define signed scripts
- Perform client-side browser detection and determine browser compatibility
- Identify common issues and procedures for creating secure JavaScript code
- Define cross-site scripting and the associated security risks
- Define the functions of cookies and manipulate them effectively
- Assign a cookie using JavaScript
- Use cookies and passwords to restrict entry to a page

Introduction to JavaScript Security Issues

- JavaScript is an open scripting language
- JavaScript does not protect data passed between browser and server
- JavaScript does not protect the Web site owner
- For true security, ensure that your Web pages use SSL/TLS (HTTPS) and that your server has all the checks in place

Browser vs. Operating System

- Browser vs. operating system
  - The operating system allows the computer to interface directly with users
  - The browser connects your operating system to the unprotected network that is the Internet
- Securing operating systems and browsers

Browser-Specific Security Issues

- Example issues with older browsers
- Example issues with recent browsers
- Helper application problems
- What users and developers can do

Browser Compatibility and Client-Side Detection

- Standards-based browsers
- Problems with browser detection
- Alternative coding for browser compatibility
- Browser detection and security

Script Blocking

- How script blocking affects developers
- Blocking JavaScript from your browser

Differences in *document.write* Among Browsers

- The *document.write* method
  - Provides the simplest way to use JavaScript to write text onto a Web page
  - Incompatibility issues with XHTML and Internet Explorer
- What JavaScript developers can do

Malicious and Accidental Coding

- Every developer makes some mistakes while coding
- Ill-advised or malicious users sometimes upload such scripts to the Web deliberately
- Locking the browser with an infinite loop

Frame-to-Frame URL Changing

- How frames work
  - Cloaking
  - Inline frames
- Browser restrictions
  - Same origin policy
- What JavaScript developers can do

Signed Scripts

- Signed script
  - A script validated by a certificate authority that can request extended privileges and abilities
- How signed scripts work
- Creating a signed script

Cross-Site Scripting (XSS)

- Cross-site scripting (XSS)
  - A security vulnerability in which an attacker embeds malicious script into a link that appears to be from a trusted site
- How XSS works
- Types of XSS
- Code and servers in XSS
- What JavaScript developers can do
- OWASP and XSS

Cookies and Security in JavaScript

- What are cookies?
- How are cookies sent?
- Who can send cookies?
- Why use cookies?
- Storing cookies
- Cookies and specific browsers
- Users deleting or disabling cookie files
- Assigning a cookie with JavaScript
- Testing for cookie presence
- Clearing a cookie
- Users controlling cookies in the browser
- Cookies and passwords

Creating Secure JavaScript Code

- Test, test, test your scripts
- Keep current in your knowledge about JavaScript and its security
- Do not use deprecated code
- Use proper encoding and validation practices
- Know the code you are using before putting it on a Web site
- Write your code consistently
- Comment your code liberally
- Keep security patches up-to-date
- Keep your operating system up-to-date

Summary

- ✓Distinguish between the browser and the operating system in relation to the elements responsible for security
- ✓Discuss browser security issues relevant to JavaScript
- ✓Define signed scripts
- ✓Perform client-side browser detection and determine browser compatibility
- ✓Identify common issues and procedures for creating secure JavaScript code
- ✓Define cross-site scripting and the associated security risks
- ✓Define the functions of cookies and manipulate them effectively
- ✓Assign a cookie using JavaScript
- ✓Use cookies and passwords to restrict entry to a page

Lesson 8 Quiz

1. Which of the following is true in relation to security?

a. The operating system can be secured but the browser cannot.

b. The browser can be secured but the operating system cannot.

c. The operating system provides a doorway to the browser for security threats.

d. Both the operating system and the browser can be secured with anti-virus software.

Lesson 8 Quiz

1. Which of the following is true in relation to security?

a. The operating system can be secured but the browser cannot.

b. The browser can be secured but the operating system cannot.

c. The operating system provides a doorway to the browser for security threats.

d. Both the operating system and the browser can be secured with anti-virus software.

Lesson 8 Quiz

2. In cross-site scripting, malicious code is generally embedded in:

a. the victim's e-mail application.

b. the attacker's Web page code.

c. an executable file.

d. a hyperlink.

Lesson 8 Quiz

2. In cross-site scripting, malicious code is generally embedded in:

a. the victim's e-mail application.

b. the attacker's Web page code.

c. an executable file.

d. a hyperlink.

Lesson 8 Quiz

3. Which JavaScript method is used for client-side browser detection?

a. AppName

b. navigator

c. UserAgent

d. BrowserType

Lesson 8 Quiz

3. Which JavaScript method is used for client-side browser detection?

a. AppName

b. navigator

c. UserAgent

d. BrowserType

Lesson 8 Quiz

4. Which example demonstrates proper JavaScript syntax to test for the presence of a cookie?

a. document.cookie = "name = value";

b. confirm(cookie);

c. alert(document.cookie);

d. window.cookie = "name = value";

Lesson 8 Quiz

4. Which example demonstrates proper JavaScript syntax to test for the presence of a cookie?

a. document.cookie = "name = value";

b. confirm(cookie);

c. alert(document.cookie);

d. window.cookie = "name = value";

Lesson 8 Quiz

5. You have just reassigned a cookie with an expiration date that has already passed. What will occur?

a. The cookie will expire and generate a same-named replacement.

b. The cookie will expire and be cleared.

c. The cookie will send a request for update to its server.

d. Nothing. You cannot reassign a cookie in this way.

Lesson 8 Quiz

5. You have just reassigned a cookie with an expiration date that has already passed. What will occur?

a. The cookie will expire and generate a same-named replacement.

b. The cookie will expire and be cleared.

c. The cookie will send a request for update to its server.

d. Nothing. You cannot reassign a cookie in this way.

Lesson 8 Quiz

6. How does a cookie appear in an HTTP response header?

Lesson 8 Quiz

6. How does a cookie appear in an HTTP response header?

Set-Cookie: name=value; expires=date; path=path; domain=domain; secure