HTM201 – DEFENDING HTML5

Course Learning Objectives

Learn about HTML5 standards and using secure programming techniques to perform cross-domain requests, JavaScript, AJAX, and more. Learn HTML5 vulnerabilities for offline storage, insecure cross-domain requests, insecure JSONP, malicious iFrames, JavaScript hijacking, and Clickjacking. Discover defensive coding techniques for HTML5 standards and learn defensive coding techniques to better protect your modern, cross-domain web applications.

Description

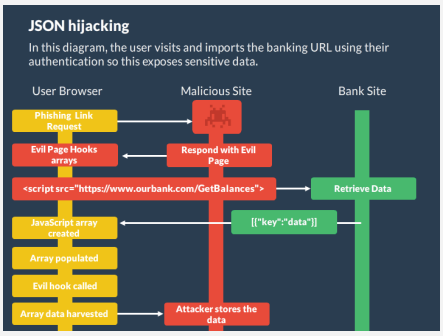
In this course, students will learn about defensive coding when it comes to HTML5 standards. Students will learn about HTML5 storage options and vulnerabilities. Students will also deep-dive into how cross-domain requests are often performed insecurely and will understand the business risk and defenses. Students will learn the risks to creating JavaScript objects insecurely and describe the difference between secure vs. insecure construction of JSON objects. Together, this course will help a student understand both the business and technical risks to creating modern, cross-domain web applications.

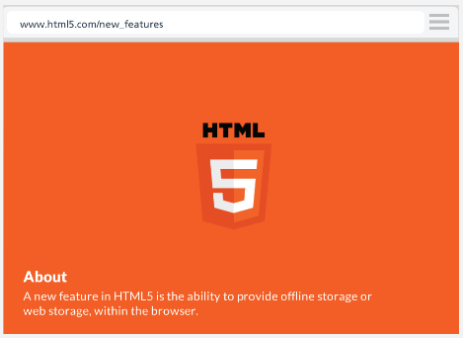
Audience

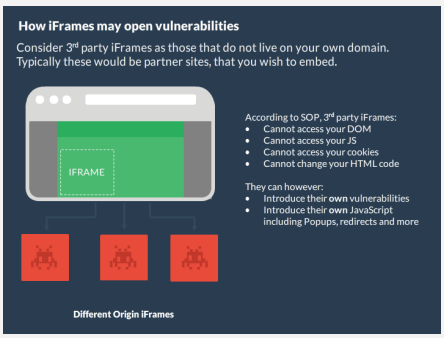
Web developers
Web application architects
JavaScript developers

Time Required

Tailored learning - 60 minutes total







Security Compass

HTM201 – DEFENDING HTML5

Course Outline

1. Same Origin Policy

- About
- What is considered same-origin?
- SOP exceptions

2. Insecure Storage

- About
- Local vs. session storage
- Vulnerabilities in offline storage
- Exploited offline storage
- Avoid storing sensitive data in offline storage
- Use session storage

3. Insecure Cross-Domain Request

- About
- Cross domain requests
- Vulnerabilities in cross-domain requests
- Web messaging API
- Web messaging code example
- Cross origin resource sharing request
- CORS response
- CORS best practices
- JSONP best practices

4. Malicious iFrames

- About
- How iFrames may open vulnerabilities
- Newsflash: Ad network affects NYT
- iFrame sandbox attribute

5. JavaScript Hijacking

- About JSON object construction
- JSON hijacking
- Reading the JSON array
- Newsflash: JSON is not as safe as people think it is
- Always return JSON as an object
- Block the Array execution

6. Clickjacking

- About the risk
- Exploiting Clickjacking
- Newsflash: Likejacking takes off
- X-Frame-Options
- Framebusting JavaScript

Security Compass