Client-Side Security with Angular JS and HTML5

1-day course

Syllabus

AppSec Labs Ltd.
info@appsec-labs.com | https://appsec-labs.com | 23 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

Client-Side Security with Angular JS and HTML5

Seminar description

Our applications are under attack on a daily basis, facing sophisticated attacks targeted at security bugs in the code we develop. Exposed in the hostile internet or intranet network, our software must withstand malicious user's attempts trying breaking into it, steal its data, disable its services, or perform any other unauthorized operation. Now if you don't fully understand the risks, or even worse, not aware of - how can you know how to protect against them?

The information provided by this seminar is a MUST for every developer who deals with HTML5 Web applications. This seminar will help you understand the security attacks applications must withstand, the proper actions that must be taken to protect our own applications against such threats, and best practices of writing secure code with HTML5.

Course topics

Module 1 – HTML5 features

- Introduction to HTML5
- Introduction to hackers world
- HTML5's threats
- Local storage
- Session storage
- Indexed DB
- Web SQL
- Offline web application
- Sensitive data leakage
- Data manipulation
- Client Cross Site Scripting (DOM Based XSS)
- Client side SQL Injection
- Web Messaging
- GEO Location
- Privacy issues and user tracking

Module 2 – Java Script secure coding

- Remote resources
- External libraries
- Open redirect
- Same Origin Policy
- Cross Origin Resource Sharing
- Cross domain risks
- Remote file inclusion
- Client side input validation methods
- Client side output encoding

Module 3 – Browser manipulation and session management

- Cross Site Request Forgery (CSRF)
- Open redirect
- Sandboxing
- Auto complete feature
- Browser cache
- Click Jacking / UI Redressing
- X-XSS-Protection
- Content-Security-Policy
- Secure transport layer
- Session management techniques
- Cookie based session management
- Cookie properties
- Security attributes – HTTPONLY, Secure
- Cookies - secrets in cookies, tampering
- Exposed session variables
- Securing stateless session
- Session invalidation

Module 4 – Angular security

- Angular filters
- Remote file inclusion
- Routes and ng-include attribute
- ng-href attribute
- SCE (Strict Contextual Escaping)
- Angular – new injections
- JSON Hijacking
- Angular XSRF protection