Training: SCADEMY
CL-ARF Angular, React and Front-end Security Follow Up

TRAINING GOALS:

This course is the next step for our participants, who completed either our OWASP Top 10, Java Secure Coding or C# Fundamentals course. This is a follow up training, meaning that in order to attend this, everyone must already have the knowledge that is covered in the Fundamentals.

This follow-up course is tailored to participants working as full-stack or frontend developers using Angular and React. The course dives into modern browser security features, as well as framework specific countermeasures and mitigation techniques.

At the end of the training everyone has the possibility to take an exam, where they are able to measure their level of the gained knowledge.

Participants attending this course will:

- Learn client-side vulnerabilities and secure coding practices
- Understand Content Security Policy
- Explore the security features of Angular
- Understand Angular's countermeasures against XSS
- Understand Angular's countermeasures against HTTP-level vulnerabilities
- Learn about the security of ReactJS
- Understand React's countermeasures against XSS
- Learn about JSON security

Audience:

- Frontend developers

CONSPECT:

- Client-side security
  - JavaScript security
  - Same Origin Policy
  - Simple requests
  - Preflight requests

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- JavaScript usage
- JavaScript Global Object
- Dangers of JavaScript
- Clickjacking
    - Exercise – IFrame, Where is My Car?
    - Protection against Clickjacking
    - Anti frame-busting – dismissing protection scripts
    - Protection against busting frame busting
- AJAX security
    - XSS in AJAX
    - Script injection attack in AJAX
    - Exercise – XSS in AJAX
    - XSS protection in AJAX
    - iCloud worm
    - AJAX security guidelines

- Modern browser security features
    - SameSite Attribute
        - 3rd party cookies
    - Certificate Transparency
        - Exercise – HTTP Response Headers
    - Content Security Policy
        - Directives
        - Sources
        - Extensions
        - Exercise – CSP in Action

- Introduction to Angular security
    - Versions of Angular
    - Data binding
    - Templating
    - Built-in security features
    - Best practices by Angular
- Protection against XSS in Angular
    - XSS in a nutshell
    - Trusted and untrusted values
        - Inserting values into the DOM
        - Handling of templates

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- AOT template compiler
- Ahead-of-time compilation
- Ahead-of-time compilation phases
- Sanitization and security contexts
  - Sanitization
  - Security contexts
  - Exercise: Security Contexts
  - Interacting with the DOM
  - Marking values as trusted
  - Exercise: Marking values as trusted
- Enforcing Trusted Types
  - Configuring HTTP headers
- Server-side XSS protection
  - Server-side template generation
- Protection against HTTP-level vulnerabilities
  - Cross-site request forgery protection in Angular
  - Angular's XSRF protection in practice
  - XSSI protection in Angular
    - Cross-site script inclusion protection in Angular
    - Angular's XSSI protection in practice
- Introduction to React security
- Introduction to ReactJS
- Protection against XSS in React
  - Cross Site Scripting (XSS) in React - 1
  - Cross Site Scripting (XSS) in React - 2
  - Cross Site Scripting (XSS) in React - 3
  - Cross Site Scripting (XSS) in React - 4
  - Case study – XSS via spoofed JSON element
    - Advanced attack abusing dangerouslySetInnerHTML

REQUIREMENTS:

General JS development

Difficulty level



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CERTIFICATE:

The participants will obtain certificates signed by SCADEMY (course completion).

TRAINER:

Authorized SCADEMY Trainer.

ADDITIONAL INFORMATION:

Related courses:

- CL-WTS Web application security testing
- CL-WSC - Web application security
- CL-WSM - Web application security master course
- CL-NJS - Node.js and Web application security

Note: Training come with a number of easy-to-understand exercises providing live hacking fun. By accomplishing these exercises with the lead of the trainer, participants can analyze vulnerable code snippets and commit attacks against them in order to fully understand the root causes of certain security problems. All exercises are prepared in a plug-and-play manner by using a pre-set desktop virtual machine, which provides a uniform development environment.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007