Ca' Foscari
Summer
School

San Sebastiano
Dorsoduro 1686
30123 Venezia

T +39 0412347376-78-15
F +39 0412347375
summer.school@unive.it

LABORATORI DI ARTE, SCIENZA, ECONOMIA E CULTURA

Edizione 2014

Nome e cognome docenti: Riccardo Focardi, Mauro Bregolin, Orillo Narduzzo

Indirizzo di riferimento: Riccardo Focardi, DAIS, via Torino, Mestre
Indirizzo e-mail: focardi@dsi.unive.it

Struttura di afferenza:

- ☑ Riccardo Focardi (riferimento): Università Ca' Foscari: DAIS
- ☑ Mauro Bregolin: Kima Projects & Services (si allega CV)
- ☑ Orillo Narduzzo: Presidente ISACA VENICE Chapter (si allega CV)

Descrizione del laboratorio: lezioni teoriche con esercitazioni pratiche su applicazioni vulnerabili. Le esercitazioni si svolgeranno su PC.

Scopo del laboratorio: affrontare sperimentalmente temi di sicurezza applicativa per ottenere una comprensione delle modalità di test di un'applicazione dal punto di vista della sicurezza. Saranno esaminate le principali categorie di vulnerabilità applicative

Durata: 15 ore

Possibili date svolgimento (comprese tra il 17 giugno e il 2 agosto 2014): mercoledì 9 e giovedì 10 luglio

Articolazione contenuti:

I. Presentazione del corso (1 ora)
II. Introduzione alla Security (2 ore)
    - Proprietà di sicurezza, attacchi tipici
III. Web application assessment (1 ora)
    - Tipologie: Black / Gray / White box
    - Come effettuare un assessment black / gray box
    - Strumenti
IV. Cenni su classificazioni di vulnerabilità (1 ora)
    - OWASP Top Ten (+ Mobile)
    - CWE/SANS
    - OWASP Testing Guide
V. Categorie di vulnerabilità applicative (3,5 ore)

Ca' Foscari
Summer
School

San Sebastiano
Dorsoduro 1686
30123 Venezia

T +39 0412347376-78-15
F +39 0412347375
summer.school@unive.it

- Injection
  - SQL Injection
  - O.S.
  - Altri: XML, CRLF, etc
- XSS
  - Tipologie di XSS
- Broken Authentication and Session Management
- Insecure Direct Object References
- CSRF
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards
- Altre
  - Malicious File Execution, Information Leakage and Improper Error Handling, Buffer Overflow, DoS, Business logic testing

VI. Esercizi pratici sulle tipologie di vulnerabilità più significative utilizzando applicazioni volutamente vulnerabili (3,5 ore; vi. viene svolto in parallelo a v.)
VII. Riferimenti ad incidenti reali. (1 ora)
VIII. Sistemi reali per il 'role-based' access control (2 ore)

Numero di partecipanti: min 10 – max 12

Prerequisiti:

☑ **si, specificare quali:** TCP/IP, http, conoscenza di base di architetture e tecnologie utilizzate per applicazioni web

☐ **no**

Lingua di insegnamento:

☐ **Inglese** ☐ **Italiano** ☐ **altra:**

(indifferente inglese / italiano; il materiale è in inglese)

Attrezzature necessarie: PC (per esercitazioni)