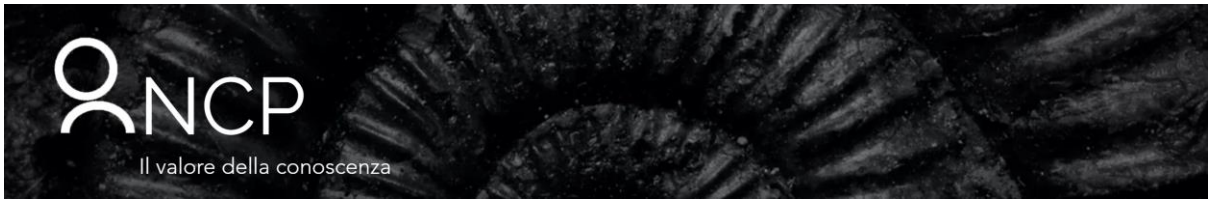
Corso specialistico di 2 giorni



Web Application Security

Introduzione

Il tema della Cybersecurity è oggi sentito in modo prioritario dai responsabili dell'IT delle imprese e da tutte le figure chiave all'interno dell'azienda ormai consapevoli dell'importanza di una corretta politica di gestione della sicurezza informatica. Uno dei capitoli più importanti è rappresentato dalla sicurezza delle applicazioni web, nota anche come Web Application Security, un campo fondamentale per proteggere le applicazioni web dai rischi e dagli attacchi informatici. Riguarda la protezione di siti web, servizi web e applicazioni web da minacce come hacking, furto di dati, attacchi di scripting e molto altro.
È essenziale per gli sviluppatori e i responsabili della sicurezza comprendere queste criticità e implementare pratiche di sviluppo sicure per ridurre al minimo le possibilità di attacchi informatici.
Una buona pratica è seguire linee guida e standard riconosciuti, come l'OWASP Top 10, che elenca le principali criticità della sicurezza delle applicazioni web. Con una corretta attenzione alla sicurezza durante tutto il ciclo di sviluppo delle applicazioni web, è possibile ridurre significativamente i rischi di violazioni e proteggere i dati degli utenti e l'infrastruttura delle applicazioni.

Agenda

- Metodologie per l'analisi del rischio: introduzione a OSSTMM e OWASP
- Approccio all'analisi dei requisiti
- Risk analysis di una applicazione
- OWASP e domini
- OWASP Top 10: i 10 maggiori rischi riconosciuti dai professionisti del settore
- **Broken Access Control**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza che consentono l'accesso non autorizzato a risorse riservate.
- **Cryptographic Failures**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza che consentono la compromissione dei dati cifrati.
- **Injection (XSS e SQL injection)**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza che consentono di iniettare codice malevolo in un'applicazione web.
- **Insecure Design**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza introdotte a causa di scelte errate o inadeguate effettuate durante la fase di progettazione di un'applicazione.
- **Security Misconfiguration**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza introdotte quando un'applicazione non è correttamente configurata per garantire una protezione adeguata.
- **Vulnerable and Outdated Components**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza presenti quando un'applicazione utilizza componenti software vulnerabili e obsoleti.
- **Identification and Authentication Failures**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza presenti quando un'applicazione non è in grado di identificare correttamente gli utenti o non riesce a fornire una corretta autenticazione per gli utenti.

- **Software and data integrity Failures**, con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza introdotte da situazioni in cui il software o i dati vengono alterati, compromessi o danneggiati in modo indesiderato o malevolo.
- **Security Logging and Mmonitor Failures**,
- **Server-Side Request Forgery**: con laboratorio incentrato sulle tecniche di mitigazione delle falle di sicurezza introdotte quando un attaccante riesce a indurre il server a effettuare richieste ad altri sistemi o risorse su Internet a nome del server stesso.

Metodologie didattiche

Il corso è teorico/pratico con numerosi laboratori studiati per dare maggiore incisività agli argomenti presentati e rafforzare la comprensione dei concetti e delle competenze apprese, si svolgerà integrando casi studio, simulazioni, demo, esempi di analisi dei rischi, discussioni sulle tecniche di difesa e sugli strumenti di prevenzione.
Le lezioni saranno svolte in modo tale da favorire al massimo il processo d'apprendimento e rendere più coinvolgente la partecipazione. Il materiale didattico comprende il manuale del corso che integra l'intera collezione delle diapositive mostrate con note, commenti, esempi e casi di studio.
Ad ogni partecipante sarà consegnato un attestato di partecipazione rilasciato da NCP.

Obiettivi

Il corso è rivolto a chi si occupa di sviluppo, gestione ed organizzazione di reti di calcolatori e di applicazioni di tipo Internet , Intranet ed Extranet.

Destinatari

Il corso è rivolto ai manager di rete, agli installatori, ai system integrator, agli operatori telefonici che si stanno movendo verso l'integrazione Voce/Dati e al personale tecnico di qualsiasi fascia che opera nel mondo delle reti.

Prerequisiti

Il corso affronta una ampia panoramica delle problematiche inerenti il mondo Internet e i suoi protocolli. E' consigliata una adeguata conoscenza di Networking e dei principi di base della Cybersecurity oltre a competenze di sviluppo applicativo.