UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

PROGRAMACIÓN SEGURA

- Introducción a la seguridad de la información: se presenta la seguridad en relación a los proyectos de desarrollo de software y los conceptos fundamentales a tener en cuenta para el abordaje de los temas avanzados.

- Aplicaciones y vulnerabilidades: definiciones, clasificación y métricas de las vulnerabilidades del software, y búsqueda de vulnerabilidades como tarea profesional.

- Diseño de software seguro: procesos de diseño seguro, interconectividad, modelado de amenazas, arquitecturas de aplicación y técnicas aplicables.

- Tipos de ataques al software: presentación de los distintos tipos de ataques, escenarios de existencia, ejemplos, protecciones y propuestas de mitigación ante cada uno.

- Criptografía: usos de la criptografía en el contexto del software. Procedimientos y técnicas seguras, uso de algoritmos y protocolos de cifrado confiables.

- Análisis de código fuente: revisión estática y dinámica de código, uso de herramientas, técnicas ofensivas

- Seguridad en Aplicaciones Web: técnicas específicas de seguridad ofensiva aplicadas a plataformas y arquitecturas web. Estándares, herramientas y técnicas de defensa.

- Software Testing: tipos de testing, técnicas utilizadas, evaluaciones de seguridad en software, generación y contenido de informes.

- Governance, Risk and Compliance (GRC): regulaciones y cumplimiento, propiedad intelectual, notificación de brechas, estándares y mejores prácticas, y gestión de riesgos

asociados al software.

- Procesos finales de gestión del software: Software Acceptance y riesgo, adquisición de software y supply chain, gestión de vulnerabilidades, deployment, operación y retiro.

12. Cronograma de clases

Temario por clase

Clase 1
Introducción al software seguro

- Evolución de la Seguridad Informática

- Proyectos de desarrollo de software

- Estadísticas y métricas mensuales

- Conceptos Fundamentales
  - Confidencialidad, Integridad y Disponibilidad
  - Autenticación y Autorización
  - Accounting y No repudio
  - Privacidad: Anonimización de datos y consentimiento de usuario
  - Defensa en profundidad
  - Atacantes: perfiles, objetivos y operatoria

- Principios de diseño seguro
  - Mínimo privilegio
  - Código limpio - KISS
  - Mantenimiento y actualización de recursos externos
  - Cifrado de comunicaciones
  - Requerimientos para nuevas funcionalidades
  - Data at rest
  - Documentación de cambios
  - Separación de tareas
  - Falla segura
  - Economía de mecanismo
  - Mediación completa
  - Diseño abierto
  - Mecanismo menos común
  - Aceptabilidad psicológica
  - Eslabón más débil

- Soporte de componentes heredados

- Metodologías de Desarrollo

- Estándares de Programación Segura
  - SEI (Software Engineering Institute) CERT Secure Coding Standards
  - Oracle Secure Coding Guidelines for Java SE
  - Apple Secure Coding Guide
  - Mozilla WebAppSec / Secure Coding Guide
  - Microsoft Secure Coding Guidelines

Requerimientos del software seguro

- Fuentes de requerimientos y descomposición de políticas
- Requerimientos internos y externos
- Clasificación y categorización de datos
- Requerimientos funcionales y operacionales

Clase 2

Aplicaciones y vulnerabilidades

- Definición de vulnerabilidad
- Tipos de vulnerabilidades
- Bug hunting
- Mercado de vulnerabilidades
- Reporte y divulgación ética de vulnerabilidades
- Bases de datos de vulnerabilidades
- Common Vulnerability Scoring System (CVSS)
  - Enumeración de vulnerabilidades
  - CVSS versión 2
  - CVSS versión 3
  - Ejemplos prácticos

- Seguridad en el canal de comunicación
  - Secure Socket Layer
  - Transport Layer Security
  - Vulnerabilidades conocidas
  - Mejores prácticas de implementación

Diseño de software seguro

- Procesos de diseño seguro

- Evaluación de superficie de ataque
- Modelado de amenazas
- Identificación y priorización de controles
- Documentación

- Consideraciones de diseño
  - Métodos de recuperación
  - Autenticación multi factores
  - Interconectividad
  - Interfaces de gestión de seguridad
  - Gestión de identidades

- Arquitectura de aplicación
  - Sistemas distribuidos
  - Service-Oriented Architecture (SOA)
  - Rich Internet Applications (RIA)
  - Pervasive computing
  - Integración con arquitecturas existentes
  - Software as a Service (SaaS)

- Tecnologías disponibles
  - Autenticación y gestión de identidades
  - Gestión de credenciales
  - Control de flujos de red
  - Auditoría y logs
  - Protección de datos, DLP y seguridad en bases de datos
  - Entornos y ambientes operativos
  - Digital Rights Management (DRM)
  - Integridad y firmado de código

Clase 3

Ataques de inyección

- Comandos
  - Escalación de privilegios
  - Ejemplos de ataque y defensa
  - Propuestas de mitigación

- SQL
  - Blind SQL Injection
  - Implicancias de seguridad
  - Herramientas de automatización de ataques (SQLMap)
  - Ejemplos de ataque y defensa
  - Propuestas de mitigación

- Sanitización de datos de entrada y salida

- Prácticas y controles defensivos
  - Concurrencia
  - Configuración
  - Manejo de errores
  - Logging & Auditoría
  - Gestión de sesiones
  - Gestión de excepciones
  - APIs seguras
  - Seguridad de tipos
  - Gestión de memoria
  - Gestión de parámetros de configuración
  - Tokenización
  - Sandboxing
  - Anti-tampering

Clase 4

- Broken Authentication and Session Management

- Cross-Site Scripting (XSS)
  - Reflejado
  - Persistente
  - Ejemplos de ataque y defensa
  - Propuestas de mitigación
  - Detección en Aplicaciones Web

Seguridad en Aplicaciones Web

- Conceptos específicos
- Modelos de ataque en aplicaciones web
- Herramientas defensivas
  - Web Application Firewalls (WAF)
  - Distributed Web Honeypots

- Herramientas ofensivas
  - Web scanners
  - Security proxies
  - Web Fuzzers

Clase 5

- Insecure Direct Object References

- Security Misconfiguration
  - Servidor de aplicaciones y Servidor Web
  - Servidor de Base de datos
  - Definición y mantenimiento de recursos externos

- Sensitive Data Exposure
  - Manejo Seguro de Errores
  - Comentarios en código productivo
  - Habilitación de funciones de DEBUG en producción
  - Exposición de arquitectura / plataforma

Clase 6

- Missing Function Level Access Control

- Cross-Site Request Forgery (CSRF)
  - Ejemplos de ataque y defensa
  - Mitigación: Políticas de navegadores (Same origin policy) y CSRF Token

- Uso de componentes con vulnerabilidades conocidas

- Redirecciones y reenvíos no validados

- Buffer overflow
  - Ejemplos de ataque y defensa
  - Propuestas de mitigación

Clase 7

Criptografía

- Aplicaciones y usos
- Tipos de algoritmos criptográficos
- Cifrado simétrico y asimétrico
- Funciones hash
- Funciones de encripción
- Cifrado vs. Encoding
- Esteganografía

- Mejores prácticas
- Cifrado de datos sensibles y Data at rest
- Firma digital
- Public Key Infrastructure (PKI)
- Usos de criptografía en programación
- Protocolos y estándares

Clase 8

Herramientas de análisis

- Análisis estático de código
  - Automático: Asserts y Unit Testing
  - Manual: Comprensión de código y Peer review

- Análisis dinámico de código
  - Debugging
  - Ingeniería inversa

- Frameworks de búsqueda de vulnerabilidades
  - Aplicaciones Web
  - Utilización de memoria RAM

Clase 9

- Web Application Security Consortium (WASC)

- W3C Web Application Security Working Group

- Open Web Application Security Project (OWASP)
  - Development Guide
  - Top 10
  - Testing Guide
  - Code Review Guide
  - Developers Cheat Sheets
  - Application Security Verification Standard (ASVS)
  - Enterprise Security API (ESAPI)
  - Otros proyectos OWASP

Clase 10

Software Testing

- Artefactos de testing
  - Testing y Quality Assurance (QA)
  - Testing funcional y no funcional (confiabilidad, rendimiento y escalabilidad)
  - Security Testing
  - Entornos: Bug tracking, defectos, errores y vulnerabilidades
  - Validación de superficie de ataque
  - Estándares

- Tipos de testing específico
  - Penetration testing
  - Fuzzing
  - Scanning
  - Simulación
  - Fallas: Fault Injection, Stress Testing y Break Testing
  - Validación criptográfica
  - Regresión
  - Testing continuo

- Penetration Testing
  - Concepto y definiciones
  - Tipos de evaluaciones
  - Metodología de evaluación
  - Testeo interno vs externo

Clase 11

Informe de revisión

- Presentación de informe
  - Destinatarios
  - Contenido mínimo
  - Resumen ejecutivo
  - Detalles técnicos

- Tipos de informe
  - Interno
  - Externo

Governance, Risk and Compliance (GRC)

- Regulaciones y cumplimiento
- Propiedad intelectual
- Notificación de brechas
- Estándares y mejores prácticas

- Gestión de riesgos

- BSIMM: Building Security In Maturity Model

Clase 12
Software Acceptance

- Pre-Release y Pre-Deployment
  - Completion Criteria: Documentación, DRP y BCP

- Aceptación del riesgo

- Post-Release
  - Validación y Verificación: FIPS y Common Criteria
  - Testing independiente

Adquisición de software y supply chain

- Supplier Risk Assessment
  - Reutilización de código
  - Propiedad intelectual
  - Cumplimientos legales

- Fuentes de proveedores
  - Controles de integridad contractual
  - Controles de integridad técnica de vendors
  - Managed Services
  - Service Level Agreements (SLAs)

- Desarrollo y pruebas
  - Controles técnicos
  - Testing de código y verificación
  - Controles de testing de seguridad
  - Requisitos de verificación y validación

- Software Delivery, operaciones y mantenimiento
  - Cadena de custodia
  - Publicación y controles de diseminación
  - Integración de sistemas
  - Autenticidad e integridad de productos
  - Desarrollo de productos y controles sostenidos
  - Monitoreo y gestión de incidentes
  - Gestión de vulnerabilidades

- Transición de proveedores

Deployment, operación y retiro

- Instalación y Deployment
  - Bootstrapping: Key Generation, acceso y gestión
  - Gestión de configuración: privilegios elevados, hardening y cambio de plataforma
  - Gestión de versiones

- Operaciones y mantenimiento
  - Monitoreo de métricas, auditorías y SLA
  - Gestión de incidentes, problemas y cambios
  - Backup, Recovery y Archiving

- Software disposal y retiro
  - Políticas de fin de ciclo de vida
  - Decommissioning