



Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

PROGRAMA ANALÍTICO DE ASIGNATURA

DEPARTAMENTO: Ingeniería en Sistemas de Información

CARRERA: Ingeniería en Sistemas de Información

NOMBRE DE LA ACTIVIDAD CURRICULAR: Seguridad en aplicaciones web

Año Académico: 2023

Área: Gestión Ingenieril

Bloque: Electivas

Nivel: 5º

Tipo: Electiva

Modalidad: Cuatrimestral

Cargas horarias totales:

<i>Horas reloj</i>	<i>Horas cátedra</i>	<i>Horas cátedra semanales</i>
72	96	6

COMPOSICIÓN DEL EQUIPO DE CÁTEDRA:

Profesor Adjunto: Ing. Vilanova Gonzalo

FUNDAMENTACIÓN

El avance de Internet como medio de comunicación, haciendo de la plataforma WEB el estándar de interfaz entre el usuario final y las aplicaciones, generó un incremento significativo en su exposición al mundo de este nuevo estándar de comunicación transformándolo en la mayor superficie disponible para ataques y denegaciones de servicio.

La asignatura tiene como finalidad instruir a los alumnos en las herramientas disponibles actuales para la comprensión, prevención, solución o mitigación de las amenazas, adoptando diversos enfoques y estrategias.



*Universidad Tecnológica Nacional
Facultad Regional Buenos Aires*

OBJETIVOS

- Reconocer el contexto actual del desarrollo de soluciones que utilizan la plataforma WEB (http/https) para su comunicación con el usuario u otros servicios (WebServices).
- Identificar las vulnerabilidades que afectan a las aplicaciones WEB, las causas que las generan y cómo es posible explotarlas.
- Reconocer la evolución de la tecnología en los últimos años y el contexto en el cual surgen las vulnerabilidades.
- Reconocer riesgos y alcances de las vulnerabilidades de cada caso trabajado en clase.
- Reconocer el concepto de ciberseguridad para debatir en un ambiente laboral.
- Desarrollar un criterio crítico sobre el desarrollo de aplicaciones WEB y su seguridad.
- Distinguir buenas prácticas de programación y las herramientas que componen un ciclo de vida seguro.
- Utilizar herramientas que permitan mantener plataformas WEB con adecuados niveles de seguridad.

CONTENIDOS

Contenidos analíticos

Unidad Temática 1: Contexto.

Historia. Estado del arte en la construcción de soluciones WEB. Avance y cambios en la tecnología. Tendencias. Desafíos presentes y futuros del desarrollador y su responsabilidad en la seguridad.

Unidad Temática 2: Nociones fundamentales.

Conocimientos sobre vulnerabilidades y cómo explotarlas. Conocimientos sobre exploits. Riesgos de las vulnerabilidades, su impacto. Por qué una aplicación es vulnerable. Que produce una vulnerabilidad. Ejemplos de codificaciones que hacen a las aplicaciones vulnerables. ¿Qué es el rol de Security Champion? Y su importancia en las organizaciones.

Unidad Temática 3: Implementación e infraestructura.

Repaso de las infraestructuras más habituales. Debate sobre las mismas para concluir en una infraestructura segura por diseño. Componentes habituales: Balanceador de carga. Terminador de túneles SSL. Proxys Reversos. WAF. Web Server. App Server. Bases de Datos (tipos). Concepto de confianza en terceros. Uso de Certificados públicos y privados. Que es un certificado auto firmado.

Unidad Temática 4: Firewall de Aplicaciones.

Presentación de soluciones como Firewall de Aplicaciones:

- ¿Qué es? ¿Cómo funciona?



Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

- ¿Qué alcance tiene?
- ¿Qué limitantes tiene? ¿Por qué?
- ¿Cómo se implementa?
- ¿Cómo se mantiene?

Firewall de aplicaciones (web y de base de datos).

Armado de los Laboratorios. WAF. Aplicaciones Web Vulnerables. Herramientas de investigación y explotación de vulnerabilidades.

Unidad Temática 5: OWASP.

- Que es la fundación OWASP.
- Qué herramientas aporta para el desarrollo seguro de soluciones WEB.
- Que es el Top 10 de OWASP.
 - Repaso de las amenazas o vulnerabilidades planteadas.
 - Análisis de las mismas
 - Pruebas de concepto sobre las mismas.
- Que son:
- OWASP Web Security Testing Guide
- OWASP Application Security Verification Standard (ASVS)
- Software Assurance Maturity Model (SAMM)
- Coding Quick Reference

Unidad Temática 6: Automatización – DevOps – DevSecOps

- Qué es DevOps.Cuál es la diferencia con DevSecOps.
- Herramientas utilizadas.
- Que es un Pipeline.
- SAST
- DAST



*Universidad Tecnológica Nacional
Facultad Regional Buenos Aires*

BIBLIOGRAFÍA OBLIGATORIA

- Akbar, M., & Ridha, M. A. F. (2018). SQL Injection and Cross Site Scripting Prevention using OWASP ModSecurity Web Application Firewall. Ed. *JOIV (International Journal on Informatics Visualization)*.
- Baláž, A., Ádám, N., Pietriková, E., & Madoš, B. (2018, February). ModSecurity IDMEF module. In *2018 IEEE 16th World Symposium on Applied Machine Intelligence and Informatics (SAMII)*. Ed. IEEE.
- Deshpande, V. M., Nair, D. M. K., & Shah, D. (2017). Major web application threats for data privacy & security—detection, analysis and mitigation strategies. Ed. *International Journal of Scientific Research in Science and Technology*.
- Foltz, K. E., & Simpson, W. R. (2020). *Enterprise Level Security 2: Advanced Techniques for Information Technology in an Uncertain World*. Ed. CRC Press.
- Gupta, B. B. (Ed.). (2018). *Computer and cyber security: principles, algorithm, applications, and perspectives*. Ed. CRC Press.
- Hsu, T. H. C. (2019). *Practical security automation and testing: tools and techniques for automated security scanning and testing in devsecops*. Ed. Packt Publishing Ltd.
- Jain, T., & Jain, N. (2019, March). Framework for Web Application Vulnerability Discovery and Mitigation by Customizing Rules Through ModSecurity. In *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*. Ed. IEEE.
- Phanindra, A. R., Narasimha, V. B., & PhaniKrishna, C. V. (2019). A review on application security management using web application security standards. In *Software Engineering*. Ed. Springer Singapore.
- Rehman, H., Nazir, M., & Mustafa, K. (2017, May). Security of web application: state of the art. In *International Conference on Information, Communication and Computing Technology*. Ed. Springer Singapore.
- Ristic, I. (2010) *Modsecurity Handbook*. Ed. Feisty Duck.
- Sinha, S. (2019). Finding Command Injection Vulnerabilities. In *Bug Bounty Hunting for Web Security*. Ed. Apress, Berkeley, CA.
- Tran, N. T., Nguyen, V. H., Nguyen-Le, T., & Nguyen-An, K. (2020, November). Improving ModSecurity WAF with Machine Learning Methods. In *International Conference on Future Data and Security Engineering*. Ed. Springer, Singapore.

PÁGINAS WEB DE INTERÉS

- Backtrack Academy. <http://www.backtrackacademy.com>
- Open Web Application Security Project. <https://www.owasp.org/>
- SpiderLabs® is Trustwave's elite team of ethical hackers, forensic investigators and researchers helping organizations fight cybercrime, protect data and reduce risk. <https://www.trustwave.com/Resources/SpiderLabs-Blog>



Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

- Stack Overflow is a question and answer site for professional and enthusiast programmers. <http://stackoverflow.com/>

CORRELATIVAS

Para cursar y rendir

- Cursadas:
 - Redes de Datos
 - Administración de Sistemas de Información
 - Simulación
 - Ingeniería y Calidad de Software
- Aprobadas:
 - Diseño de Sistemas de Información
 - Sistemas Operativos
 - Bases de Datos