Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

ANEXO I

RESOLUCIÓN Nº...../21

ASIGNATURA:	SEGURIDAD EN APLICACIONES WEB	**CÓDIGO:**	
DEPARTAMENTO:	INGENIERÍA EN SISTEMAS DE INFORMACIÓN	**CLASE:**	Cuatrimestral
ÁREA:	INGENIERÍA EN SISTEMAS DE INFORMACIÓN	**HORAS SEM.:**	6 hs.
BLOQUE:	ELECTIVAS	**HORAS / AÑO:**	Reloj 72hs./ Cátedra 96hs

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.

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.

Programa analítico:

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?
• ¿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.
• Que herramientas aporta para el desarrollo seguro de soluciones WEB.
Que es el Top 10 de OWASP.
i.Repaso de las amenazas o vulnerabilidades planteadas.
ii.Análisis de las mismas
iii.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
Que es DevOps. Cuál es la diferencia con DevSecOps.
Herramientas utilizadas.
Que es un Pipeline.

SAST
DAST.

Distribución de carga horaria entre actividades teóricas y prácticas:

Tipo de actividad	Carga horaria total en hs. reloj	Carga horaria total en hs. cátedra
Teórica	27	36
Formación Práctica	45	60
Formación experimental	0	0
Resolución de problemas	0	0
Proyectos de diseño	0	0
Práctica supervisada	0	0
Total	72	96

Articulación Horizontal y vertical con otras materias

La asignatura Seguridad en Aplicaciones Web se articula en forma vertical con las materias de Programación y Diseño de sistemas troncales de la carrera. La Seguridad de la Información o lo relacionado con la Ciberseguridad está siempre presente ya que es transversal al ciclo de formación de los ingenieros en Sistemas de Información.
En cuanto a la articulación horizontal, Seguridad en Aplicaciones Web, brinda conocimientos que son compatibles y complementarios con conceptos y contenidos de otras asignaturas, fomentando así la interdisciplinariedad.
El equipo docente participa de reuniones inter-cátedras convocadas por el Departamento, a fin de generar acuerdos temáticos y de metodologías que faciliten la articulación horizontal y vertical entre las distintas asignaturas.

Unidad temática	Duración en horas cátedra
1	12
2	12
3	12
4	12
5	36
6	12

Bibliografía:

- Gupta, B. B. (Ed.). (2018). *Computer and cyber security: principles, algorithm, applications, and perspectives*. CRC Press.

- Hsu, T. H. C. (2019). *Practical security automation and testing: tools and techniques for automated security scanning and testing in devsecops*. Packt Publishing Ltd.
- Deshpande, V. M., Nair, D. M. K., & Shah, D. (2017). Major web application threats for data privacy & security–detection, analysis and mitigation strategies. *International Journal of Scientific Research in Science and Technology*, *3*(7), 182-198.
- ur 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* (pp. 168-180). Springer, Singapore.
- Phanindra, A. R., Narasimha, V. B., & PhaniKrishna, C. V. (2019). A review on application security management using web application security standards. In *Software Engineering* (pp. 477-486). Springer, Singapore.
- Sinha, S. (2019). Finding Command Injection Vulnerabilities. In *Bug Bounty Hunting for Web Security* (pp. 147-165). Apress, Berkeley, CA.
- Foltz, K. E., & Simpson, W. R. (2020). *Enterprise Level Security 2: Advanced Techniques for Information Technology in an Uncertain World*. CRC Press.
- Bryan Sullivan,Vincent Liu (2011) *Web Application Security, A Beginner's Guide.*
- Ivan Ristic (2010) *Modsecurity Handbook*.
- 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 (SAMI)* (pp. 000043-000048). IEEE.
- 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)* (pp. 643-648). IEEE.
- Akbar, M., & Ridha, M. A. F. (2018). SQL Injection and Cross Site Scripting Prevention using OWASP ModSecurity Web Application Firewall. *JOIV: International Journal on Informatics Visualization*, *2*(4), 286-292.
- 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* (pp. 93-107). 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
- Stack Overflow is a question and answer site for professional and enthusiast programmers. http://stackoverflow.com/

Correlativas:

Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

PARA CURSAR:

Cursadas: Administración de recursos
Redes de información
Simulación
Ingeniería de software

Aprobadas: Diseño de sistemas
Sistemas operativos
Gestión de datos

PARA RENDIR:

Aprobadas: Administración de recursos
ingeniería en software
Redes de información
Simulación