CIBERTEC

VISIÓN: Ser la institución líder de educación superior técnica en el Perú con alcance a nivel nacional.
MISIÓN: Formar profesionales íntegros y competentes brindando una educación superior de alta calidad que contribuya al desarrollo económico y ambiental del país.

I. INFORMACIÓN GENERAL DEL CURSO

Curso : Seguridad en Aplicaciones (SP2414)
Ciclo : Quinto
Período : 2023
Horas : 1 Laboratorio + 3 Virtual
Carrera(s) : Computación e Informática

II. INTRODUCCIÓN

El software inseguro está debilitando las finanzas, salud, defensa, energía y otras infraestructuras críticas. A medida que la infraestructura digital se hace cada vez más compleja e interconectada, la dificultad de lograr la seguridad en aplicaciones aumenta exponencialmente. Es por ello, que la industria de TI requiere profesionales entrenados en el desarrollo seguro de software y aplicaciones web, que aseguren la calidad del producto basándose en metodologías y estándares como el reconocido OWASP Top 10, el cual es un poderoso documento de concienciación para la seguridad en aplicaciones web y representa un amplio consenso sobre las 10 fallas de seguridad más críticas, analizadas por expertos en seguridad alrededor del mundo, quienes comparten sus experiencias para producir esta fabulosa guía. El objetivo de este curso es crear conciencia y capacitar a los estudiantes acerca de la seguridad en aplicaciones web mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. El proyecto Top 10 es referenciado por muchos estándares, libros, herramientas y organizaciones y su versión más reciente es del año 2017. Esta asignatura es de naturaleza práctica. Se inicia con la introducción a OWASP Top 10, pasando por el empleo de herramientas para auditar las aplicaciones web con la finalidad de identificar los riesgos más críticos, y culmina con la presentación de un informe de análisis de vulnerabilidades web.

III. METODOLOGÍA

El proceso de enseñanza- aprendizaje se basa en el aprendizaje a partir de la experiencia. Busca motivar al estudiante a través de situaciones cercanas a la realidad y propiciar la reflexión para la resolución de problemas en los que se aplican de forma práctica los conocimientos adquiridos. El aprendizaje del curso se consolida con el desarrollo de un proyecto de investigación aplicada asesorado por el docente. Esta metodología contribuye a que el alumno sea protagonista de su aprendizaje individual y colaborativo mientras que el docente asume un rol de planificador, facilitador y guía, creando escenarios que permiten a los alumnos la adquisición de competencias profesionales.

IV. LOGRO DEL CURSO

Al término del curso, el alumno, comprende la metodología OWASP Top 10 y emplea herramientas basadas en el estándar para analizar brechas de seguridad en las aplicaciones web y aplica contramedidas. Finalmente entrega como producto un informe de análisis de vulnerabilidades web.

V. RESULTADOS DE APRENDIZAJE DE LA CARRERA

Nro	Resultado de Aprendizaje de la Carrera	Aporte
RAC 1	Desarrollo de soluciones de software multiplataforma utilizando herramientas tecnológicas adecuadas	
RAC 2	Contribución en el aseguramiento de la calidad de las soluciones informáticas	Directo
RAC 3	Participación en la definición y diseño de las soluciones informáticas	Directo
RAC 4	Contribución en la administración de los servicios y proyectos de TI	
RAC 5	Resolución de situaciones y orientación a resultados	
RAC 6	Innovación y desarrollo de emprendimientos	
RAC 7	Compromiso con la actualización profesional y la mejora continua	Directo
RAC 8	Capacidad de liderazgo y trabajo en equipo	Directo
RAC 9	Responsabilidad ética y profesional	
RAC 10	Comunicación asertiva	

VI. UNIDADES DE APRENDIZAJE

UNIDAD 1.- Introducción a la Seguridad de Aplicaciones	**Duración: 4 horas**

Logro de la Unidad de Aprendizaje
Al término de la unidad, el alumno, identifica las metodologías y estándares de seguridad en el desarrollo de aplicaciones y reconoce las tecnologías de defensa y ataque.

Capacidades	Conocimientos
1. Identifica correctamente las metodologías para el desarrollo de software seguro. 2. Identifica los procedimientos a seguir asegurar el software en las fases del SDLC.	**Temario** **1.1. Tema 1: Introducción a la Seguridad de Aplicaciones (4 horas)** 1.1.1. Tendencias de Ataques web 1.1.2. Seguridad SDLC. 1.1.3. Metodologías y Proyectos Web 1.1.4. Tecnologías de Defensa y Ataque.

UNIDAD 2.- OWASP Top 10 2017 RC2	**Duración: 44 horas**

Logro de la Unidad de Aprendizaje
Al término de la unidad, el alumno identifica la metodología OWASP sobre los 10 riesgos más críticos de las aplicaciones web y recomienda soluciones para mitigar ataques web.

Capacidades	Conocimientos
1. Identifica la metodología OWASP Top 10. 2. Reconoce las diferencias entre versiones de OWASP. 3. Describe los diferentes tipos de análisis. 4. Describe las herramientas OWASP. 5. Describe los tipos de inyección. 6. Realiza test de análisis de vulnerabilidades de SQL Injection, Blind SQL Injection, LDAP Injection, XPath Injection y Command Injection. 7. Describe las remediaciones para mitigar los ataques de inyección. 8. Identifica los ataques de robo de sesiones. 9. Emplea técnicas de Session Fixation, Pass-the-hash y Session Hijacking. 10. Describe las remediaciones para los ataques de robo de sesiones. 11. Describe la criticidad de la exposición de datos sensibles. 12. Describe las remediaciones para la protección de datos sensibles. 13. Describe la criticidad de los ataques de Denegación de servicio. 14. Describe los ataques de RFI/LFI. 15. Describe las remediaciones para los ataques XXE. 16. Describe los ataques de rutas transversales. 17. Identifica los ataques por permisos de archivos. 18. Identifica los robos a la caché del cliente.	**Temario** **2.1. Tema 2: OWASP Top 10 (4 horas)** 2.1.1. Introducción a OWASP Top 10 2.1.2. OWASP Top 10 2013 vs OWASP Top 10 2017 RC2 2.1.3. Análisis Dinámico y Estático 2.1.4. Herramientas OWASP **2.2. Tema 3: A1 – Injection (4 horas)** 2.2.1. SQL Injection y Blind SQL Injection 2.2.2. LDAP Injection 2.2.3. XPath Injection 2.2.4. Command Injection 2.2.5. Remediaciones **2.3. Tema 4: A2 – Broken Authentication (4 horas)** 2.3.1. Session Fixation 2.3.2. Pass-the-hash 2.3.3. Session Hijacking 2.3.4. Remediaciones **2.4. Tema 5: A3 – Sensitive Data Exposure (4 horas)** 2.4.1. Validación de la capa de transporte 2.4.2. Almacenamiento criptográfico inseguro 2.4.3. Remediaciones **2.5. Tema 6: A4 – XML External Entities (XXE) (4 horas)** 2.5.1. Denegación de servicio (DDoS) 2.5.2. Acceso a archivos y servicios remotos 2.5.3. Acceso a archivos y servicios locales 2.5.4. Remediaciones

19. Describe las remediaciones para la vulnerabilidad de control de acceso inseguro. 20. Realiza el listado de directorios desprotegidos. 21. Identifica contraseñas por defecto. 22. Describe la criticidad de los backups desprotegidos. 23. Describe las remediaciones a los errores de configuración de seguridad. 24. Describe las técnicas de XSS. 25. Realiza pruebas de XSS. 26. Describe las remediaciones para los ataques XSS. 27. Describe la criticidad de los ataques de ejecución de código arbitrario y ejecución de comandos remotos. 28. Describe las remediaciones para los ataques de deserialización de archivos no confiables. 29. Describe los componentes usados con vulnerabilidades conocidas. 30. Describe las recomendaciones para la mitigación de errores comunes. 31. Describe la criticidad de no contar con software de monitoreo de logs. 32. Identifica herramientas y soluciones para monitorear eventos en servicios web.	**2.6. Tema 7: A5 – Broken Access Control (4 horas)** 2.6.1. Path Traversal 2.6.2. Permisos de archivos 2.6.3. Client Side Caching 2.6.4. Remediaciones **2.7. Tema 8: A6 – Security Misconfiguration (4 horas)** 2.7.1. Listado de directorios no deshabilitado 2.7.2. Passwords por defecto 2.7.3. Backups 2.7.4. Remediaciones **2.8. Tema 9: A7 – Cross-Site Scripting (XSS) (4 horas)** 2.8.1. Tipos y definiciones 2.8.2. Técnicas de inyección de script 2.8.3. Codificación y ofuscamiento 2.8.4. Remediaciones **2.9. Tema 10: A8 –Insecure Deserialization (4 horas)** 2.9.1. Ejecución de Código arbitrario 2.9.2. Denegación de Servicio (DoS) 2.9.3. Remote command execution 2.9.4. Remediaciones **2.10. Tema 11: A9 – Using Components with Know Vulnerabilities (4 horas)** 2.10.1. Certificados digitales 2.10.2. Protocolo HTTPS 2.10.3. Configuración defectuosa de seguridad 2.10.4. Remediaciones **2.11. Tema 12: A10 – Insufficient Logging and Monitoring (4 horas)** 2.11.1. Log & Event Manager 2.11.2. Web Application Firewall

UNIDAD 3.- Análisis de vulnerabilidades web	**Duración: 8 horas**
Logro de la Unidad de Aprendizaje Al término de la unidad, el alumno el alumno realiza análisis de código fuente, realiza test dinámico de aplicaciones y finalmente entrega como producto un informe técnico y un informe ejecutivo sobre análisis de vulnerabilidades web.	
Capacidades	**Conocimientos**
1. Describe las herramientas open source para análisis de código fuente. 2. Describe las herramientas comerciales para análisis de código fuente. 3. Realiza test de código fuente. 4. Describe las herramientas open source para análisis dinámico de aplicaciones web. 5. Describe las herramientas comerciales para análisis dinámico de aplicaciones web.	**<u>Temario</u>** **3.1. Tema 13: Análisis Estático (3 horas)** 3.1.1. Source code Analisys Tools 3.1.2. Open Source or Free Tools 3.1.3. Commercial Tools 3.1.4. Proof of Concept **3.2. Tema 14: Análisis Dinámico (3 horas)** 3.2.1. DAST - Dynamic Application Security Testing 3.2.2. Open Source or Free Tools 3.2.3. Commercial Tools 3.2.4. Proof of Concept

6. Realiza test de dinámico de aplicaciones web. 7. Documenta el análisis de vulnerabilidades en un informe técnico. 8. Documenta el análisis de vulnerabilidades en un informe ejecutivo.	**3.3. Tema 15: Documentación (2 horas)** 3.3.1. Reportes OWASP 3.3.2. Informe Ejecutivo 3.3.3. Informe Técnico

VII. EVALUACIÓN

Fórmula del Curso:

Promedio Final = 25% (T1) + 30% (T2) + 45% (EF)

Dónde:

T1: Evaluación de Laboratorio Nro 1
T2: Evaluación de Laboratorio Nro 2
EF: Evaluación Final de Laboratorio

Cronograma:

TIPO DE EVALUACIÓN	SEMANA
T1	06
T2	10
EF	14

Consideraciones:

- La nota mínima aprobatoria es 13.
- Ninguna evaluación es susceptible de eliminación.
- El desarrollo (mínimo 12) de los Minicuestionarios (MCU) en la plataforma, de estar disponibles, otorgan un punto de bonificación sobre la Evaluación Final.
- El desarrollo (al 100%) de las Actividades Virtuales (AV) en la plataforma, de estar disponibles, otorgan un punto de bonificación sobre la Evaluación Final.
- El curso SÍ permite rendir un Examen Sustitutorio que reemplace una de las evaluaciones, a excepción del Proyecto Aplicativo, si lo considerase.
- La rendición del Examen Sustitutorio se realiza en fecha posterior al fin de periodo académico y requiere una inscripción previa según el procedimiento que indique Secretaría Académica oportunamente.

VIII. BIBLIOGRAFÍA

Bibliografía Básica

- **OWASP Top 10 2017 (Español).** (2018). Owasp.org. Obtenido de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

- **OWASP Top 10 2017 RC2 (Inglés).** (2018). Owasp.org. Obtenido de https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf

Bibliografía Complementaria

- **OWASP Testing Guide 4.0 - Lanzamiento de Matteo Meucci y Andrew Muller (Paperback) - Lulu GB.** (2018) Lulu.com. Obtenido de http://www.lulu.com/shop/matteo-meucci-and-andrew-muller/testing-guide-40-release/paperback/product-22294314.html

- **OWASP.** (2018). Owasp.org. Obtenido de https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf

- **OWASP**. (2018). Owasp.org. Obtenido de https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

- **OWASP.** (2018). Owasp.org. Obtenido de https://www.owasp.org/images/1/19/OTGv4.pdf

Enlaces a páginas web

- **OWASP**. (2018). Owasp.org. Obtenido de https://www.owasp.org/index.php/Main_Page

- **OWASP.** (2018). Owasp.org. Obtenido de https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

- **OWASP.** (2018). Owasp.org. Obtenido de https://www.owasp.org/index.php/Source_Code_Analysis_Tools

- **Source Code Security Analyzers - SAMATE**. (2018). Samate.nist.gov. Obtenido de https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html