CÓDIGO DE ASIGNATURA
2636

ASIGNATURA: Seguridad y Calidad en Aplicaciones Web

REFERENTE DE CÁTEDRA: Mg. Lic. Walter R. Ureta

AÑO: 2020

CARGA HORARIA: 4

OBJETIVOS:

Esta materia capacita al alumno en los conocimientos necesarios para la construcción de aplicaciones Web seguras utilizando las más modernas y efectivas técnicas de defensa de ataques en aplicaciones Web.
Los docentes guiaran al alumno en el aprendizaje y resolverán todas las dudas, para lograr que se familiarice acerca de las posibles fallas y ataques de seguridad en los sistemas basados en Web para llegar a ser buenos profesionales en la materia.

Objetivos Generales:

- Familiarizar al alumno en los conceptos y términos básicos y avanzados del área de seguridad y calidad de aplicaciones Web.
- Incentivar al alumno al trabajo en equipo, lo cual lo preparará para una futura participación en proyectos de software donde los límites de tiempo, los recursos tecnológicos, físicos y humanos, los requerimientos de seguridad y calidad y las necesidades de los usuarios cumplen un rol fundamental.

Objetivos Específicos:

- Que el alumno adquiera los conocimientos necesarios para la construcción de aplicaciones Web seguras y de calidad utilizando las más modernas y efectivas técnicas de defensa de ataques
- Que el alumno se familiarice acerca de las posibles fallas, ataques a la seguridad y normas de calidad de los sistemas basados en Web.

CONTENIDOS MÍNIMOS:

Modelos de Seguridad Web. Amenazas y vulnerabilidad en aplicaciones para Internet. Conceptos de criptografía. Sistemas criptográficos. Aplicaciones de seguridad en desarrollos Web. Calidad de sitio Web. Normas y certificaciones. Definición de términos, algoritmos y normas.

Correlatividades:

- Programación Web 2 (2628)
- Diseño de Aplicaciones WEB (2629)

PROGRAMA ANALÍTICO:

Unidad N° 1. Introducción a la Seguridad

- Características de la información, conceptos y términos de seguridad.
- Seguridad física y lógica.
- Recursos y dispositivos para la seguridad.
- Recomendaciones generales de seguridad para el desarrollo de aplicaciones.
- Impacto en la organización.

Unidad N° 2. Amenazas a la Seguridad

- Vulnerabilidades.
- Prevención.
- Denegación de servicio.
- Ataques a navegadores y clientes.
- Ataques a servidores Web (servicio de HTTP o a otros servicios disponibles).
- Riesgos y controles frecuentes para aplicaciones web y móviles.
- Cross Site Scripting. CSRF, Inyección de código, técnicas de ataque a aplicaciones.

Unidad N° 3. Criptografía

- Historia de la criptografía, conceptos.
- Introducción a los sistemas criptográficos.
- Elementos teóricos de la criptografía.
- Algoritmos simétricos.
- Algoritmos asimétricos.
- Algoritmos de Hash.
- Algoritmos públicos y privados.
- Http vs Https. TLS/SSL.
- Certificados Digitales y Firma Digital.

Unidad N° 4. Aplicaciones de Seguridad

- Configuración segura de servidores HTTP.
- Validación de entrada.
- Autenticación en la Web.
- Autorización en la Web.
- Manejos de sesiones de estado.
- Web Services y Servicios REST.
- Técnicas de autenticación de Usuarios.
- Administración de Usuarios y privilegios.
- Aplicaciones de Terceros.

Unidad N° 5. Calidad

- Conceptos de Calidad. Calidad Total.
- Calidad del Software.
- Medición de Calidad.
- Calidad en los modelos de desarrollo de software.
- Calidad en SCRUM y métodos ágiles.

Unidad N° 6. Normas

- CMMi. CMM-SSE.
- Proyectos OWASP (ASVS, SAMM),
- Normativas.
- Certificaciones.

BIBLIOGRAFÍA:

BIBLIOGRAFÍA BÁSICA

(Debe existir en Biblioteca)

Autor	Título	Editorial	Año	Edición
Manuel José Lucena López	Criptografía y Seguridad en Computadoras V 5.0 http://criptografiayseguridad.blogspot.com/p/criptografia-y-seguridad-en.html		2019	Cuarta Edición

BIBLIOGRAFÍA COMPLEMENTARIA

Autor	Título	Editorial	Año	Edición
	A History and Survey of Network Firewalls. http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf			

Autor	Título	Editorial	Año	Edición
	2017 Edition; OWASP Foundation; 2017. https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf	OWASP Foundation	2017	
	OWASP Proactive Controls Version 3.0. https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf	OWASP Foundation	2018	
	OWASP Mobile Security Project – TopTen Mobile Risks https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks	OWASP Foundation	2016	
	OWASP Application Security Verification Standard; Version 4.0 https://github.com/OWASP/ASVS/raw/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0-en.pdf	OWASP Foundation	2019	
Luis Antonio Olsina	Tesis doctoral: “Metodología cuantitativa para la evaluación y Comparación de sitios Web”. UNLP, Facultad de Ciencias Exactas, 1999. http://gidis.ing.unlpam.edu.ar/home/downloads/pdfs/Website_QEM_VF.pdf		1999	
Guillermo Juan Covella	Tesis: “Medición y Evaluación de Calidad en Uso de Aplicaciones Web”. Facultad de Ingeniería de la UNLP. http://sedici.unlp.edu.ar/bitstream/handle/10915/4082/Documento_completo.pdf?sequence=1			
	Una Guía para Construir Aplicaciones y Servicios Web Seguros; The Open Web Application Security Project; 2005 https :/ / www . owasp . org / images / b / b 2 / OWASP Developmen t Guide _2.0.1_ Spanish .pdf		2005	
	Systems Security Engineering Capability Maturity Model 3.0, Carnegie Mellon University. http://www.sse-cmm.org/docs/ssecmmv3final.pdf		2003	
	OWASP Software Assurance Maturity Model 1.0. http://www.opensamm.org	OWASP Foundation	2009	

METODOLOGÍA DE ENSEÑANZA:

Metodología General de Clases

La metodología de enseñanza se focaliza en clases teóricas y clases prácticas participativas, con gran cantidad de horas en laboratorio, de manera de lograr que el alumno obtenga un conocimiento equilibrado de los componentes teóricos y prácticos de la materia.

Las clases serán dictadas a través de distintos métodos, como explicaciones a través de definiciones, ejemplos, ejercicios, lectura individual dirigida, actividades grupales de análisis, transferencia, validación colectiva y exámenes. Determinados contenidos temáticos serán presentados a los alumnos a través de proyecciones y videos.

Se desarrollarán diferentes prácticos individuales y/o grupales aplicando los contenidos dados en las diferentes unidades temáticas, para poder fijar los conocimientos de forma práctica. Se fomentará al alumno al trabajo en grupo y uso de practicas de desarrollo ágil.

El proceso de enseñanza y de aprendizaje de carácter teórico-práctico, permanente e integral, propone a los alumnos la adquisición de conocimientos, el desarrollo de actitudes y la detección de aptitudes, el aumento de la destreza y las habilidades para comprender y encontrar información relevante, y la resolución de las situaciones nuevas que se le presenten, utilizando un enfoque hacia la resolución de problemas.

El alumno debe mostrar al finalizar el curso un nivel mínimo de destreza en los conceptos y las tecnologías específicas asociadas a la materia.

Las diversas actividades teórico-prácticas planteadas favorecen la investigación, el desarrollo, el trabajo en equipo y la fijación de conocimientos.

Considerando que la adaptación a las nuevas tecnologías supone un reto fundamental actual, se le facilitará al alumno la posibilidad y los medios necesarios para que puedan acceder, conocer e investigar todos los instrumentos que las nuevas y últimas tecnologías ofrecen.

Metodología de Clases Teóricas

- Las clases teóricas están orientadas a introducir a los alumnos en los diferentes conceptos teóricos conceptuales de la materia.
- Cada tema teórico es abordado en clase brindando el profesor ejemplos de aplicación.

- La metodología de trabajo alternará entre clases expositivas donde los profesores explicarán los temas y otras haciendo participar a los alumnos mediante exposición dialogada.

Metodología de Clases Prácticas

- En las clases prácticas los alumnos podrán ejecutar ejercicios junto a los docentes, aplicar los conceptos teóricos, evacuar dudas y aclarar los conceptos necesarios.
- Los alumnos resolverán ejercicios planteados mediante trabajos en grupos o de forma individual, mientras los profesores supervisarán su realización y atenderán consultas personales.
- Las prácticas se referirán a cada núcleo temático de la materia para que el alumno tenga claro qué conceptos está ejercitando. Aquellos ejercicios donde se haga hincapié en algún concepto fundamental, deben ser supervisados por los profesores en clase, los cuáles harán una conclusión general al final de la práctica sobre los resultados y procedimientos aplicados.
- Las prácticas se basarán en ejercicios seleccionados y presentados de modo gradual en complejidad. La presentación de los ejercicios será guiada por los objetivos propuestos para el tema específico al cual la práctica se refiere. Los ejercicios serán seleccionados con un criterio que pondere lo conceptual y lo estratégico en lugar de la mecanización de procedimientos.

Trabajos Prácticos

- Se plantearán trabajos prácticos obligatorios y/o complementarios.
- Para poder realizar un seguimiento progresivo del aprendizaje, se asocian las diversas unidades temáticas a los trabajos prácticos en los que los alumnos podrán aplicar lo aprendido.
- Estos trabajos prácticos posibilitan la resolución de problemas con objetivos propios.
- Para poder realizar un aprendizaje integral de la aplicación de todos los contenidos de la materia se plantearán trabajos prácticos integradores obligatorios a los cuales se irán agregando los conceptos aprendidos durante la cursada.
- Esto trabajos estarán destinados a aplicar y medir el grado de comprensión de los temas teóricos expuestos en clase y el manejo de las definiciones y propiedades en contextos prácticos e integradores para comprobar que realmente se han incorporado los conceptos y no memorizado o mecanizado definiciones, procedimientos y demostraciones presentadas en las clases o que figuran en los libros.

- Los trabajos integradores tienen como finalidad generar la capacidad necesaria para saber interpretar claramente los objetivos del problema y poder resolverlo, aplicando una adecuada estrategia en la resolución.
- El alumno deberá ir realizando entregas parciales de avances establecidas por el docente durante la cursada. El docente hará seguimiento en cada entrega y/o exposición del práctico.
- El docente irá evaluando el progreso de cada alumno en cada entrega de los diferentes prácticos grupales o individuales.

Materiales Didácticos

- La materia cuenta con apuntes teórico-prácticos desarrollados por los profesores de la cátedra. También se utilizan los libros detallados en la sección de Bibliografía.

Sitio Web: Sharepoint

- Sitio web destinado a facilitar al alumno el acceso al programa de la materia, material de estudio, ejemplos, trabajos prácticos, entre otros archivos y el contacto directo con docentes y alumnos.

EXPERIENCIAS DE LABORATORIO/ TALLER / TRABAJOS DE CAMPO:

Prácticas en Laboratorios: Se podrán desarrollaran prácticas de laboratorios según los contenidos de cada unidad.

Trabajo Práctico Integrador: Trabajo Práctico Integrador de los contenidos de la materia, de carácter obligatorio.
La entrega del trabajo práctico será gradual ya que al mismo TP se le irán agregando los distintos tipos de consignas y entregables relacionados a la seguridad y los contenidos aprendidos. De esta forma se buscará lograr un desarrollo seguro y de calidad de acuerdo con todos los temas vistos.
El resultado de la evaluación del trabajo practico deriva en tres condiciones posibles:

1. **Reprobado**. Implica que el alumno obtendrá la calificación de Reprobado en la cursada de la materia, excluyéndolo de las instancias de Final o Promoción cualquiera sea su calificación en exámenes parciales y/o recuperatorios.
2. **Aprobado sobre objetivos de mínima**. Implica que el alumno ha cumplido con los objetivos mínimos del trabajo practico pero sin lograr satisfacer la totalidad de los objetivos. Los alumnos con esta calificación solo podrán acceder a instancias de Final, quedando excluidos de la posibilidad de Promoción cualquiera sea su calificación en exámenes parciales y/o recuperatorios.

3. **Aprobado sobre los objetivos planteados**. Implica que el alumno ha logrado cumplir los objetivos planteados y demostrar la aplicación de los conocimientos asociados. Esta condición le permite acceder a las instancias de Final y Promoción según sus calificaciones de parciales y recuperatorios.

Software Utilizado:

- Windows XP / Linux
- Lenguaje Java
- Marcos de trabajo para el entorno web
- Bases de datos
- Herramientas de desarrollo de libre acceso
- Servidores de libre acceso
- OpenSSL
- Firefox
- GPA-GPG

METODOLOGÍA DE EVALUACIÓN:

Exámenes Parciales

- Existirán dos evaluaciones parciales según lo indicado en el cronograma.
- Las evaluaciones serán escritas y/o prácticas, pudiendo la cátedra llevar a cabo evaluaciones orales y/o en la PC.
- Los exámenes serán corregidos por los docentes del curso y las notas serán entregadas a los alumnos como máximo a los 7 días hábiles de la toma del parcial.
- Por cada examen parcial existirá un examen recuperatorio en fecha de recuperación.

Porcentaje (%)	30 preguntas	50 preguntas	Nota
0-20	0-5	0-10	1 (Uno)
21-40	6-11	11-20	2 (Dos)
41-59	12-17	21-29	3 (Tres)
60-64	18-19	30-32	4 (Cuatro)
65-70	20-21	33-35	5 (Cinco)
71-76	22	36-38	6 (Seis)
77-82	23-24	39-41	7 (Siete)
83-88	25-26	42-44	8 (Ocho)
89-94	27-28	45-47	9 (Nueve)
95-100	29-30	48-50	10 (Diez)

Examen Final

- En el caso que el alumno cumpla con los requisitos establecidos en el Régimen de Cursada pero no con los criterios de promoción, deberá rendir un examen final.
- El primer llamado a examen final será al final del cuatrimestre según cronograma fijado por el Departamento de Ingeniería.
- Las fechas de examen final son fijadas por el Departamento de Ingeniería. Las condiciones de inscripción al final las establece el Departamento de Ingeniería.
- El examen final será confeccionado de forma uniforme para todas las comisiones.
- En fecha de final no se entregan trabajos prácticos.
- En el caso de exámenes libres se confeccionarán de forma especial de manera de evaluar la parte teórica/práctica con el mismo nivel que para alumnos regulares.
- Los exámenes serán corregidos por cualquier docente de la cátedra.

CRONOGRAMA ORIENTATIVO DE ACTIVIDADES

Clase	Contenido
1	Presentación. Características de la información, conceptos y términos de seguridad. Seguridad lógica. Elementos de seguridad lógica (Firewalls, Firewalls personales, firewalls móviles, IDS/IPS, Verificadores de Integridad).
2	Seguridad física. Impacto en la organización.
3	Términos generales, vulnerabilidades, clasificaciones, estadísticas, técnicas Client-Side. DoS. Áreas de riesgo.
4	Ataques, riesgos y controles frecuentes para aplicaciones.
5	Ataques, riesgos y controles frecuentes para aplicaciones. Variantes aplicadas a las tecnologías móviles
6	Introducción a los sistemas criptográficos. Historia de la criptografía. Elementos teóricos de la criptografía. Criptografía clásica y moderna.
7	1er PARCIAL
8	Algoritmos simétricos.
9	Algoritmos asimétricos. Hash, HMAC, Derivadores, Algoritmos públicos y privados.
10	Http vs Https. TLS/SSL. Certificados. Digitales y Firma Digital. Configuración de segura de servidores HTTP
11	Validaciones de buenas practicas. Técnicas de autenticación de Usuarios. Administración de Usuarios y privilegios.
12	Manejo de sesiones. Web Services y Servicios REST.

Clase	Contenido
13	Aplicaciones de terceros. Buenas practicas.
14	Calidad del Software. Perspectivas. Medición. Calidad en modelos de desarrollo y metodologías ágiles. CMMi, SSE-CMM, ASVS, SAMM. Normativas. Certificaciones
15	2do PARCIAL
16	RECUPERATORIO OPTATIVO / COLOQUIO TP

CONDICIONES DE CURSADA Y APROBACIÓN

Según lo establecido en la RHCS 054/2011 (Régimen académico integrado)

"Declaro que el presente programa de estudios de la asignatura Seguridad y Calidad en Aplicaciones Web, es el vigente para el ciclo lectivo 2020, guarda consistencia con los contenidos mínimos del Plan de Estudios"

Firma	Aclaración	Fecha