Universitat Autònoma de Barcelona

2021/2022

Seguretat i Vulnerabilitat del Programari

Codi: 104376
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2503758 Enginyeria de Dades	OT	4	0

La metodologia docent i l'avaluació proposades a la guia poden experimentar alguna modificació en funció de les restriccions a la presencialitat que imposin les autoritats sanitàries.

Professor/a de contacte

Nom: Elisa Ruth Heymann Pignolo
Correu electrònic: Elisa.Heymann@uab.cat

Utilització d'idiomes a l'assignatura

Llengua vehicular majoritària: espanyol (spa)
Grup íntegre en anglès: No
Grup íntegre en català: No
Grup íntegre en espanyol: Sí

Prerequisits

Domini d'algun llenguatge de programació: Java, Python o C/C++.

Objectius

L'alumne aprendrà sobre la seguretat del software durant totes les etapes del cicle de desenvolupament de programari (SDLC): Metodologies per al disseny de programació segura, tècniques de programació segura, metodologies d'avaluació de vulnerabilitats en profunditat (auditoria de programari), eines d'anàlisi de codi estàtic i dinàmic per detectar vulnerabilitats i defenses del sistema per reduir amenaces de seguretat.

Competències

- Concebre, dissenyar i implementar sistemes demmagatzematge de dades de forma eficient i segura.
- Prevenir i solucionar problemes, adaptar-se a situacions imprevistes i prendre decisions.
- Que els estudiants hagin desenvolupat aquelles habilitats d'aprenentatge necessàries per emprendre estudis posteriors amb un alt grau d'autonomia.
- Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes destacats d'índole social, científica o ètica.
- Treballar cooperativament, en entorns complexos o incerts i amb recursos limitats, en un context multidisciplinari, assumint i respectant el rol dels diferents membres de lequip.

Resultats d'aprenentatge

1. Estudiar les adaptacions que es fan als algoritmes d'anàlisi i consulta de dades perquè preservin la privadesa de les dades d'entrada, dels models apresos o de les sortides dels models utilitzats en l'àmbit de la intel·ligència empresarial.
2. Prevenir i solucionar problemes, adaptar-se a situacions imprevistes i prendre decisions.
3. Que els estudiants hagin desenvolupat aquelles habilitats d'aprenentatge necessàries per emprendre estudis posteriors amb un alt grau d'autonomia.

4. Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes destacats d'índole social, científica o ètica.
5. Treballar cooperativament, en entorns complexos o incerts i amb recursos limitats, en un context multidisciplinari, assumint i respectant el rol dels diferents membres de lequip.

Continguts

1. Introducció i terminologia bàsica.
2. Pensar com un atacant.
3. Programació segura:
3.1. Desbordament de buffers.
3.2. Errors numèrics.
3.3. Serialització.
3.4. Excepcions.
3.5. Atacs d'injecció.
3.5.1.Injeccion SQL.
3.5.2. Injecció d'ordres.
3.5.3. Injescció XML.
3.5.4. Injecció de codi.
3.6. Travessia del directoris.
3.7. Atacs Web.
3.7.1. XSS
3.7.2. CSRF.
3.7.3. Gestió de sessions.
3.7.4. Redireccions.
3.8. Seguretat en dispositius mòbils.
4. Disseny segur. Modelització de riscos.
5. Detecció de vulnerabilitats. Metodologia FPVA.
6. Eines de detecció de vulnerabilitats.
7. Fuzz testing.

Metodologia

Hi ha 4 hores de docència setmanals, dividides en 2 sessions de 2 hores. Durant cada sessió s'exposarà un tema teòric i es realitzaran exercicis pràctics relacionats amb el tema exposat. Això requereix que els estudiants tinguin el seu propi portàtil. El contingut de cada classe es detallarà en el programa que estarà disponible al campus virtual abans del primer dia de classe.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Activitas autonomes	100	4	1, 2, 3, 4, 5
Classes teoriques amb exercisis practics.	44	1,76	1, 2, 3, 4, 5

Avaluació

Hi haurà 2 o 3 proves escrites durant el semestre. Aquestes proves tindran un pes del 60% del total de la qualificació de l'assignatura.

Cada tema tindrà un exercici pràctic. Associat a cada exercici l'alumne haurà de presentar una petita memòria. El pes d'aquests exercicis és del 40%

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
2 o 3 controls de teoria	60%	3	0,12	1, 2, 3, 4, 5
Exercisis de practiques	40%	3	0,12	1, 2, 3, 4, 5

Bibliografia

Introduction to Software Security per Loren Kohnfelder, Elisa Heymann and Barton Miller. Disponible en: http://research.cs.wisc.edu/mist/SoftwareSecurityCourse/

Programari

Els estudiants rebran una imatge de VirualBox que contindrà tot el programari necessari per realitzar la majoria d'exercicis de l'assignatura. Aquest programari inclou llenguatges de programació i múltiples eines. Els estudiants hauran de descarregar i instal·lar Android Studio per programar dispositius mòbils. També hauran de descarregar-se l'eina Microsoft Thread Modeling Tool.