Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**Secure Software Engineering**
Corso di studio	Laurea Magistrale in Computer Science (Curriculum Security Engineering)
Anno Accademico	2022/23
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	9 CFU
Settore Scientifico Disciplinare	ING-INF 05
Lingua di erogazione	Inglese
Anno di corso	Primo
Periodo di erogazione	2^ semestre, le date esatte sono riportate nel manifesto/regolamento
Obbligo di frequenza	La frequenza è fortemente raccomandata
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/computer-science/computer-science

Docente/i

Nome e cognome	Danilo Caivano
Indirizzo mail	danilo.caivano@uniba.it
Telefono	080 5443270
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n. 622, VI piano.
Sede virtuale	Piattaforma ADA - https://elearning.di.uniba.it/
Sito web del docente	https://serlab.di.uniba.it/people/danilo-caivano
Ricevimento (giorni, orari e modalità, es. su appuntamento)	(da confermare) martedì dalle 15:00 alle 16:00 (previo appuntamento)

Docente/i

Nome e cognome	Vita Santa Barletta
Indirizzo mail	vita.barletta@uniba.it

Telefono	080 5443270
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n. 616, VI piano.
Sede virtuale	Piattaforma ADA - https://elearning.di.uniba.it/
Sito web del docente	https://serlab.di.uniba.it/people/vita-barletta
Ricevimento (giorni, orari e modalità, es. su appuntamento)	(da confermare) martedì dalle 15:00 alle 16:00 (previo appuntamento)

Syllabus

Obiettivi formativi	L'insegnamento di Secure Software Engineering si propone di fornire strumenti e tecniche per lo sviluppo sicuro del software e di conseguenza orientato alla privacy. Ciò include lo sviluppo di un'applicazione che integri in ogni fase del ciclo di vita appropriati elementi di sicurezza.
Prerequisiti	Lo studente deve avere familiarità con almeno un linguaggio di programmazione e con le strutture dati fondamentali, metodologie di sviluppo software.

Contenuti di insegnamento (Programma)	**Introduzione (ore 4)**
	- Scenario Cyber
	- Security Life Cycle
	- Secure Software Application
	
	Concetti fondamentali (ore 6)
	- Asset
	- Threat
	  o Modellazione delle minacce
	  o Threat Hunting
	- Threat Actors/Agent
	- Threat Intelligence
	- Vulnerabilità
	- Rischio
	- Exploit
	- Attacco
	- CIA Triade: Confidenzialità, Integrità e Disponibilità
	- CVE (Common Vulnerabilities and Exposure)
	- CVSS (Common Vulnerabilities Score System)
	- Attacchi alla sicurezza
	  o Attacchi Passivi
	  o Attacchi attivi
	  o Mitigazione e Controllo
	
	Access Control (ore 4 + 1 esercitazione)
	- Subject e Object
	- Processi
	  o Identificazione
	  o Autenticazione
	  o Autorizzazione
	  o Accounting
	- Tipologie di Access Control
	  o Controlli Amministrativi
	  o Controlli Fisici

	o Controlli Tecnici - Modelli di Access Control o DAC – Discretionary Access Control o MAC – Mandatory Access Control o RBAC – Role-Based Access Control o ABAC – Attribute-Based Access Control **Cyber Kill Chain (ore 4 + 2 esercitazione)** - Fasi della Kill Chain o Reconnaissance o Weaponization o Delivery o Exploit o Installation o Command & Control - Indicatori Kill Chain o Atomico o Computed o Behavioral **Red Team (ore 5 + 2 esercitazione)** - Penetration Testing o Black Box o White Box o Grey Box - Network Penetration Testing - Application Penetration Testing - Web Application Penetration Testing - Physical Penetration Testing - Social Engineering Testing - Vulnerability Assessment o Pianificazione o Fasi **Blue Team (ore 5 + 2 esercitazione)** - Security Operation Centre (SOC) o Struttura o Funzioni o Responsabilità e Ruoli o Modelli o Security Monitoring System o Servizi - Computer Security Incident Response Team (CSIRT) o Struttura o Funzioni o Servizi - Application Penetration Testing - Web Application Penetration Testing - Physical Penetration Testing - Social Engineering Testing - Vulnerability Assessment o Pianificazione o Fasi **Sicurezza Organizzativa (ore 4 + 1 esercitazione)** - Ciclo di vita della Sicurezza o Funzioni: Identify, Protect, Detect, Respond e Recover o Controlli essenziali di Cybersecurity - Unità Organizzative di Sicurezza - The Hack-Space

MITRE ATT&CK (ore 4 + 1 esercitazione)

- Tattiche e Tecniche
- Threat Based Model
- Casi d'uso
  - Adversary Emulation
  - Red Teaming
  - Behavioral Analytics Development
  - Defensive Gap Assessment
  - SOC Maturity Assessment
  - Cyber Threat Intelligence Enrichment
- Domini tecnologici

Sviluppo del software orientato alla privacy (ore 5 + 1 esercitazione)

- General Data Protection Regulation (GDPR)
  - Privacy by Design and by Default
  - Data Protection
- Privacy Knowledge Base
  - Principi della Privacy by Design
  - Strategie di progettazione orientate alla Privacy
  - Privacy Patterns
  - Vulnerabilità
  - Contesto: Requisiti Architetturali, Casi d'uso e scenari, Privacy Enhancing Technologies
- Sviluppo del software orientato alla privacy (POSD: Privacy Oriented Software Development)
  - Fasi per lo sviluppo di software orientato alla privacy (Forward)
  - Fasi per la reingegnerizzazione di software (Backward)
- Vulnerabilità
  - Access Violation
    - Access Control: Authorization Bypass
  - Indirect Access to Sensitive Data
    - Command Injection
    - Cookie Security: HTTPOnly not Set
  - Insufficient Data Protection
    - Insecure Storage
  - Privacy Violation
    - Credential Management

Security by Design (ore 4 + 1 esercitazione)

- Privacy vs Security
- Principi della Security by Design

Vulnerabilità delle Web Application e Security Flaws (ore 3 + 1 esercitazione)

- OWASP Top 10
- Threat Modeling e Application Security Risks

Sicurezza Applicativa (ore 5 + 1 esercitazione)

- Vulnerabilità
  - Buffer overflows
  - Race Conditions
  - Input validation attacks
  - Authentication attacks
  - Authorization attacks
  - Cryptographic attacks
  - SQL Injection
    - Error Based
    - Blind Based
    - Time Based
    - Union Based

	▪ Stacked Based ▪ inline Based ○ Cross-Site Scripting (XSS) ▪ Reflected ▪ Stored ▪ DOM ○ Cross-Site Request Forgery (CSFR) ○ Brute Force - Application Security Challenges - Secure Software Development Life Cycle (SSDLC) - Responsive Security Environment - Application Security Tools **Caso di studio (ore 2 + 3 esercitazione)** - Introduzione caso di studio - Esempi e best practices - Progettazione caso di studio
Testi di riferimento	• Omar Santos, Joseph Muniz, Stefano De Crescenzo, "CCNA Cyber Ops SECFND 210-250", Cisco Systems; Har/Psc edizione (3 aprile 2017) Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.
Note ai testi di riferimento	I testi di riferimento sono integrati con slide, dispense del docente e altro materiale didattico messi a disposizione degli studenti sulla piattaforma di e-learning usata dal CdS.

Organizzazione della didattica

Ore

Totali	Didattica frontale	Pratica (laboratorio, progetto, esercitazione, altro)	Studio individuale
225 ore	56 ore	15 + 25 ore di laboratorio ed esercitazioni guidate	129 ore

CFU/ETCS

9 CFU	7 CFU	1 + 1P CFU	

Metodi didattici

	Lezioni frontali con l'ausilio di slide che riportano esempi per illustrare gli argomenti trattati. Esercitazioni pratiche sull'utilizzo dei vari principi e tecniche presentate a lezione attraverso esercizi da svolgere singolarmente. Un progetto da svolgere preferibilmente in gruppo utilizzando Fortify SCA quale strumento di Static Code Analysis. Utilizzo della piattaforma di e-learning del Dipartimento di Informatica per la distribuzione del materiale e per le interazioni tra docenti e studenti durante e dopo il corso.

Risultati di apprendimento previsti	
Conoscenza e capacità di comprensione	• Il principale risultato di apprendimento atteso è la conoscenza relativa a processi, metodi e tecniche per l'analisi e la modellazione di minacce cyber e di integrare in tutte le fasi del ciclo di vita del software requisiti di sicurezza e privacy. • Lo studente acquisisce tale conoscenza sia attraverso le lezioni frontali e la partecipazione a seminari tematici erogati durante il corso, sia attraverso esercitazioni che gli consente di mettere in pratica e verificare quanto appreso, acquisendo così consapevolezza della capacità di comprensione e di come migliorare l'applicazione delle tecniche apprese.
Conoscenza e capacità di comprensione applicate	• Per consentire allo studente di applicare le conoscenze per l'identificazione e la gestione delle vulnerabilità, si svolgono in aula sia esercitazioni individuali che collettive. • Allo studente è richiesto di sviluppare un progetto, nel quale è necessario applicare alcune delle tecniche presentate in aula, dopo aver selezionato quelle più appropriate per il caso specifico. Questo progetto contribuisce alla valutazione finale dello studente e quindi al voto finale d'esame.
Competenze trasversali	**Autonomia di giudizio** • Acquisire una significativa autonomia nel valutare i pericoli inerenti alle minacce cyber di sistemi informatici. • Acquisire la capacità di lavorare in team per lo sviluppo si sistemi sicuri e orientati alla privacy. Le esercitazioni che si svolgono durante il corso contribuiscono al raggiungimento di tali competenze grazie anche alla discussione di tali scelte con il docente. • L'autonomia di giudizio è parte della valutazione finale dello studente e tiene conto delle discussioni avvenute durante le lezioni, delle esercitazioni e della presentazione del progetto. **Abilità comunicative** • Illustrare in modo chiaro ed efficace le conoscenze apprese, presentare casi applicativi ed esempi illustrativi. • La presentazione e discussione del progetto sviluppato in gruppo è parte della prova orale d'esame e consente allo studente di mostrare le proprie abilità comunicative. **Capacità di apprendere in modo autonomo** • Per stimolare la capacità di apprendere in modo autonomo, allo studente è richiesto di approfondire specifici argomenti oppure è invitato a partecipare a seminari tenuti da altri docenti, interni o in visita al dipartimento, sui quali lo studente deve poi presentare durante le lezioni, e riportare in sede d'esame.

Valutazione	
Modalità di verifica dell'apprendimento	La verifica dei risultati formativi raggiunti avviene durante l'esame finale, che prevede:

<table>
<tr><td></td><td>
Un colloquio orale in cui si presenta e si discute il progetto sviluppato in gruppo e si verificano le competenze acquisite durante il corso e le capacità espositive dello studente.
Per gli studenti frequentanti sono previste le seguenti facilitazioni:
Bonus punteggio a valere sulla valutazione del progetto per gli studenti che svolgono positivamente le esercitazioni sul progetto/caso di studio.
</td></tr>
<tr><td>Criteri di valutazione</td><td>

Conoscenza e capacità di comprensione
Lo studente dovrà essere in grado di effettuare opportune scelte per individuare, elaborare e organizzare informazioni appropriate per soluzioni di problemi connessi alle minacce di sicurezza informatica.
Conoscenza e capacità di comprensione applicate
Si valuta la presentazione del progetto per verificare le competenze acquisite dallo studente e la sua capacità di sintesi nonché la chiarezza di esposizione, la capacità di fare confronti significativi tra metodologie, tecniche e tecnologie diverse adottate e riportare un proprio giudizio critico.
Autonomia di giudizio
Lo studente dovrà essere in grado di applicare opportune soluzioni per la gestione dei problemi connessi alle minacce di sicurezza informatica.
Si valuta la presentazione del progetto per verificare le competenze acquisite dallo studente e la sua capacità di sintesi nonché la chiarezza di esposizione, la capacità di fare confronti significativi tra metodologie, tecniche e tecnologie diverse adottate e riportare un proprio giudizio critico.
Abilità comunicative
Lo studente dovrà essere in grado di produrre una documentazione chiara e contenente le informazioni necessarie per le minacce di sicurezza e il contesto identificato.
Capacità di apprendere
Lo studente dovrà essere in grado di applicare e tradurre autonomamente le tecniche apprese per lo sviluppo sicuro di sistemi e che integrino le normative vigenti per la protezione della privacy.

</td></tr>
<tr><td>Criteri di misurazione dell'apprendimento e di attribuzione del voto finale</td><td>
<table>
<tr><th>Voto</th><th>Descrittori</th></tr>
<tr><td>< 18 insufficiente</td><td>Conoscenze frammentarie e superficiali dei contenuti, errori nell’applicare i concetti, descrizione carente.</td></tr>
<tr><td>18 - 20</td><td>Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell’applicazione di concetti teorici.</td></tr>
<tr><td>21 - 23</td><td>Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice.</td></tr>
<tr><td>24 - 25</td><td>Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato.</td></tr>
<tr><td>26 - 27</td><td>Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta.</td></tr>
<tr><td>28 - 29</td><td>Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta.</td></tr>
</table>
</td></tr>
</table>

	30 30 e lode	Conoscenze dei contenuti molto ampie, complete ed approfondite, capacità ben consolidata di applicare i contenuti, ottima capacità di analisi, di sintesi e di collegamenti interdisciplinari, padronanza di descrizione.
Altro	Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti: • https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea • https://www.uniba.it/it/ricerca/dipartimenti/informatica • https://elearning.di.uniba.it/ I programmi degli insegnamenti sono disponibili qui: • https://programmi.di.uniba.it/ Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito: • https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento. ——————— Link al corso sulla piattaforma e-learning del dipartimento ADA: https://elearning.di.uniba.it/	