



Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	Sicurezza nelle Applicazioni	
Corso di studio	Laurea Magistrale in Sicurezza Informatica	
Anno Accademico	2024/25	
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	9 CFU	
Settore Scientifico Disciplinare	IINF-05/A - Sistemi di elaborazione delle informazioni	
Lingua di erogazione	Italiano	
Anno di corso	Primo	
Periodo di erogazione	1 ^a semestre, le date esatte sono riportate nel manifesto/regolamento	
Obbligo di frequenza	No, ma la frequenza è fortemente raccomandata	
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea	

Docente/i	
Nome e cognome	Donato Malerba
Indirizzo mail	donato.malerba@uniba.it
Telefono	080 5443269
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n.508, 5 ^a piano.
Sede virtuale	Piattaforma ADA - https://elearning.uniba.it/
Sito web del docente	https://www.uniba.it/it/docenti/malerba-donato
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Mercoledì 11.00-13.00 o su appuntamento

Nome e cognome	Pasquale Ardimento
Indirizzo mail	donato.malerba@uniba.it
Telefono	
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n.569, 5 ^a piano.



Sede virtuale	Piattaforma ADA - https://elearning.uniba.it/
Sito web del docente	https://www.uniba.it/it/docenti/ardimento-pasquale
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Mercoledì 14:30 – 15:30, o in altro giorno previo appuntamento per e-mail

Syllabus	
Obiettivi formativi	Acquisizione di adeguate conoscenze relative a ambiti progettuali strategici sulla sicurezza informatica. Comprensione delle criticità nello sviluppo di applicazioni software. Acquisizione di competenza nello sviluppo di applicazioni sicure in linguaggio Java.
Prerequisiti	Conoscenze richieste per l'accesso al corso di laurea Magistrale.
Contenuti di insegnamento (Programma)	Ruolo e impatto della Cybersecurity (6 ore) Infrastrutture e Centri: Internet Nazionale (10 ore) Azioni abilitanti: (18 ore) - analisi della sicurezza di applicazioni e servizi; - analisi dei malware e banca dati nazionale delle minacce; - anticipare la risposta ad attacchi cibernetici; - anticipare la risposta ad attacchi sociali; - anticipare la risposta ad attacchi fisici; - analisi forense e conservazione delle prove; - gestione del rischio a livello sistemico; - difesa attiva. Tecnologie abilitanti: (14 ore) - architetture hardware - crittografia - i sistemi biometrici; - blockchain e distributed ledger; - tecnologie quantistiche; - intelligenza artificiale. Sicurezza delle applicazioni in Java (10 ore) - Lifetime dei dati sensibili - Lettura file - Cookie - Cross-site scripting (XSS) - Sessione http - https: SSL/TLS con Apache Tomcat - Caricamento file con Apache Tika - Sql injection - Prepared statement via JDBC - Gestione delle Password - Classi mutabili - Metodo clone - Metodi ignorabili da codice non attendibile Programmazione Difensiva (6 ore) - Minimizzare lo scope delle variabili - Ridurre l'accessibilità delle classi - Feedback output dei metodi - Identifica i file utilizzando più informazioni - Thread-Safety



Testi di riferimento	Per la parte di teoria svolta durante le lezioni frontali: R. Baldoni, R. De Nicola, P. Prinetto. Il futuro della cybersecurity in Italia: Ambiti progettuali strategici. Consorzio Interuniversitario Nazionale per l'Informatica. 2018 (disponibile online) - Cap. 1-4 Per la parte di esercitazione svolta durante il laboratorio: F. Long, D. Mohindra, R.C. Seacord, D. F. Sutherland, D. Svoboda. Java Coding Guidelines. Addison-Wesley, 2014. (disponibile in biblioteca e su piattaforma Ada) 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 supportati da articoli scientifici e materiale fornito dal docente durante lo svolgimento del corso.				
Organizzazione della didattica					
Ore					
Totali	Didattica frontale	Laboratorio/esercitazione	Progetto	Studio individuale	
225 ore	48 ore	15 ore	50 ore	112 ore	
CFU/ETCS					
9 CFU	6 CFU	1 CFU	2 CFU		

Metodi didattici					
	Le 63 ore di didattica frontale sono ripartite come segue: - 48 ore di teoria (in presenza); - 15 ore di laboratorio (in presenza). Alle 112 ore studio individuale si aggiungono 50 ore di attività di progetto (da svolgersi individualmente). Il progetto, che istanzia i concetti visti durante le attività di laboratorio, è discusso in sede di esame di appello.				

Risultati di apprendimento previsti					
Conoscenza e capacità di comprensione	○ Acquisizione di conoscenze relative a ambiti progettuali strategici sulla sicurezza informatica. ○ Comprensione delle criticità nello sviluppo di applicazioni software.				



Conoscenza e capacità di comprensione applicate	○ Capacità di progetto e realizzazione di semplici applicazioni sicure in linguaggio Java.
Competenze trasversali	Autonomia di giudizio ○ Gli studenti sono in grado di apprezzare le criticità di programmi scritti in Java e di operare le necessarie modifiche al fine di rispondere alle linee guida per lo sviluppo di applicazioni sicure in Java. ○ L'autonomia di giudizio viene acquisita attraverso lo studio e l'interpretazione critica di testi e programmi. ○ Il raggiungimento dell'adeguata autonomia è verificato attraverso delle esercitazioni, che si tengono durante il corso, e con l'esame finale di profitto. Abilità comunicative ○ Gli studenti sono in grado di esporre le tematiche incluse nel programma del corso mediante il lessico specifico della disciplina. Capacità di apprendere in modo autonomo ○ Gli studenti sono in grado di approfondire in autonomia le tematiche incluse nel programma del corso anche ricorrendo a risorse (articoli su temi di sicurezza informatica e/o strumenti di analisi e programmazione) non direttamente utilizzate nelle ore di lezione/laboratorio.

Valutazione	
Modalità di verifica dell'apprendimento	○ Prova scritta sulla parte teorica. ○ Discussione orale di un progetto di realizzazione di semplici applicazioni Java miranti a dimostrare le vulnerabilità e le varianti utili a migliorare la sicurezza. La prova scritta e la discussione orale sono indipendenti. La votazione finale è in trentesimi. Ad essa contribuiscono il voto della prova scritta e la valutazione del progetto discusso. Sono previste due prove parziali, una a metà corso e una a fine corso, che nell'insieme sostituiscono la prova scritta sulla parte teorica. Le prove parziali sono mantenute per il solo anno accademico in cui sono state sostenute. Durante la prova scritta non è ammesso l'uso di testi e appunti, né l'accesso a web, mentre nella discussione del progetto è possibile utilizzare il proprio PC dove sono installati gli ambienti utilizzati per la realizzazione del progetto.
Criteri di valutazione	Conoscenza e capacità di comprensione: ○ esposizione critica dei concetti appresi relativi agli ambiti progettuali strategici sulla sicurezza informatica. Conoscenza e capacità di comprensione applicate: ○ competenze di programmazione sicura in Java, capacità di individuazione delle vulnerabilità nello sviluppo di semplici applicazioni software e capacità di correzione delle stesse Autonomia di giudizio: ○ capacità di svolgere semplici esercizi assegnati durante il corso delle lezioni teorico/pratiche Abilità comunicative:



	○ uso del lessico specifico della disciplina informatica Capacità di apprendere: ○ sviluppo di argomenti su sicurezza nelle applicazioni non direttamente trattati nel corso ma assegnati dal docente
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	Il voto finale sarà attribuito sulla base della valutazione comparativa di tutti i criteri di valutazione sopra citati
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 • https://www.uniba.it/it/ricerca/dipartimenti/informatica • https://elearning.uniba.it/ I programmi di tutti gli insegnamenti sono disponibili al seguente link: • https://elearning.uniba.it/course/index.php?categoryid=455 Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei regolamenti didattici dei Corsi di Studi disponibili nel sito: • https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/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 ADA: • https://elearning.uniba.it/course/index.php?categoryid=455



Main information on the course

Course name	Security in Applications	
Degree	Master's Degree in Cybersecurity	
Academic year	2024/25	
European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU)	9 CFU (each CFU corresponds to 25 hours (h) of student's time); CFU are of type T1, T2 or T3 T1 = 8 h lecture + 17 h individual study T2 = 15 h practice + 10 h individual study T3 = 25 h individual study	
Settore Scientifico Disciplinare		
Course language	Italian	
Course year	First	
Course period	First Semester - exact dates can be found in the didactic regulations	
Course attendance requirement	None, but it is highly recommended to attend classes	
Website of the Degree	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica	

Teacher(s)

Name and Surname	Donato Malerba
email	donato.malerba@uniba.it
phone	080 5443269
office	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Room n.508, 5th floor.
e-learning platform	Platform ADA - https://elearning.uniba.it/
Teacher's homepage	https://www.uniba.it/it/docenti/malerba-donato
Office hours	Wednesday 11:00-13:00 or on appointment

Name and Surname	Pasquale Ardimento
email	pasquale.ardimento@uniba.it
phone	
office	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Room n.569, 5th floor.
e-learning platform	Platform ADA - https://elearning.uniba.it/
Teacher's homepage	https://www.uniba.it/it/docenti/ardimento-pasquale
Office hours	Wednesday 14:30 – 15:30 or on e-mail appointment

Syllabus

Course goals	Acquisition of adequate knowledge related to strategic project areas in cybersecurity. Understanding the criticalities in the development of software applications. Gaining expertise in the development of secure applications in Java programming language.
Prerequisites/requirements	Knowledge required for admission to the Master's degree program.
Course program	Role and Impact of Cybersecurity (6 hours) Infrastructure and Centers: National Internet (10 hours) Enabling Actions: (18 hours)



	- Analysis of security for applications and services - Analysis of malware and national threat database - Anticipating responses to cyber attacks - Anticipating responses to social attacks - Anticipating responses to physical attacks - Forensic analysis and evidence preservation - System-level risk management - Active defense Enabling Technologies: (14 hours) - Hardware architectures - Cryptography - Biometric systems - Blockchain and distributed ledger - Quantum technologies - Artificial intelligence Security of Java Applications (10 hours) - Lifetime of sensitive data - File reading - Cookies - Cross-site scripting (XSS) - HTTP session - HTTPS: SSL/TLS with Apache Tomcat - File uploading with Apache Tika - SQL injection - Prepared statement via JDBC - Password management - Mutable classes - Clone method - Ignorable methods for untrusted code Defensive Programming (6 hours) - Minimizing the scope of variables - Reducing class accessibility - Feedback output of methods - File identification using multiple pieces of information - Thread safety
Books of reference	For the theoretical part covered during the lectures: R. Baldoni, R. De Nicola, P. Prinetto. "The Future of Cybersecurity in Italy: Strategic Project Areas." Consorzio Interuniversitario Nazionale per l'Informatica. 2018 (available online) - Chapters 1-4. For the practical part covered during the lab: F. Long, D. Mohindra, R.C. Seacord, D. F. Sutherland, D. Svoboda. "Java Coding Guidelines." Addison-Wesley, 2014. (available in the library and on the Ada platform) Students who wish to can borrow the texts from the Library. It may be advisable to check their availability through the University Library System at https://opac.uniba.it/easyweb/w8018/index.php? and contact the library to arrange the loan.
Notes to the books	The reference texts are supported by scientific articles and slides provided by the teachers during the course.
Organization of the didactic activities	



Hours				
Total	Lectures	Practice sessions	Project work	Individual study
225 hours	48 hours	15 hours	50 hours	122 hours
CFU/ETCS				
9 CFU	6 CFU	1 CFU	2 CFU	

Teaching methods	
	The 63 hours of classes are divided as follows: - 48 hours of theory (in-person); - 15 hours of laboratory work (in-person). In addition to the 112 hours of individual study, there are 50 hours of project activities (to be completed individually). The project, which applies the concepts covered during the practice sessions, is discussed during the exam session.

Expected learning outcomes	
Knowledge and understanding	○ Acquisition of knowledge related to strategic project areas in cybersecurity. ○ Understanding the criticalities in the development of software applications.
Applying knowledge and understanding	○ Ability to design and develop simple secure applications in Java programming language.
Other skills	<i>Making judgements</i> ○ Students will be able to identify the critical aspects of Java programs and make the necessary modifications to comply with the guidelines for secure application development in Java. ○ Independent judgment is acquired through the study and critical interpretation of texts and programs. ○ The achievement of adequate autonomy is assessed through exercises held during the course and the final exam. <i>Communication</i> ○ Students are able to present the topics included in the course curriculum using the specific vocabulary of the discipline. <i>Learning skills</i> ○ Students are able to independently delve into the topics covered in the course curriculum, even using resources not directly involved in the delivery of lecture hours.

Assessment	
Assessment methods	○ Written examination on the theoretical part. ○ Development of a project involving the creation of simple Java applications aimed at demonstrating vulnerabilities and useful variations to enhance security. The written exam and the oral discussion are independent of each other. The final grade is out of thirty. It is determined by the score of the written exam and the evaluation of the project discussed.



	Two partial exams are scheduled, one halfway through the course and one at the end, which together replace the written exam on the theoretical part. The partial exams are valid only for the academic year in which they are taken. During the written exam, the use of textbooks, notes, or web access is not allowed. However, during the project discussion, it is permitted to use your own PC with the environments used for the project installed.
Evaluation criteria	Knowledge and Understanding: ○ Critical presentation of the concepts learned related to strategic project areas in cybersecurity. Applied Knowledge and Understanding: ○ Secure programming skills in Java, ability to identify vulnerabilities in the development of simple software applications, and capacity to address and correct them. Autonomy of Judgment: ○ Ability to carry out simple exercises assigned during the course lectures. Communication Skills: ○ Use of specific vocabulary in the field of computer science. Ability to Learn: ○ Development of topics on application security not directly covered in the course but assigned by the instructor.
Measurements and final grade	The final grade will be awarded based on the comparative evaluation of all the assessment criteria mentioned above.
Further information	It is recommended that students rely exclusively on information and communications provided on the official websites of the Department of Computer Science or on social groups only if they are established and managed solely by the instructors of the respective courses: ● 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.uniba.it/ The course syllabi are available here: ● https://elearning.uniba.it/course/index.php?categoryid=455 The information that all students should know is detailed in the educational regulations and course handbooks available on the website: ● https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea Students are advised to be cautious regarding information and materials circulating on unofficial websites or social groups, as they can often be unreliable, incorrect, or incomplete. For any doubts, students should arrange a meeting with the instructor following the specified office hours. Link to the course on the department's ADA e-learning platform: ● https://elearning.uniba.it/course/index.php?categoryid=455