## Principali informazioni sull'insegnamento

| | | |
|---|---|---|
| Denominazione dell'insegnamento | **Sicurezza nelle Applicazioni** | |
| Corso di studio | Laurea Magistrale in Sicurezza Informatica | |
| Anno Accademico | 2023/24 | |
| Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS) | | 9 CFU |
| Settore Scientifico Disciplinare | ING-INF/05 | |
| Lingua di erogazione | Italiano | |
| Anno di corso | Primo | |
| Periodo di erogazione | Primo 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/sicurezza-informatica/laurea-magistrale-in-informatica | |

## 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^ 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 | Paolo Mignone |
| Indirizzo mail | paolo.mignone@uniba.it |
| Telefono | 080 544 2283 |
| Sede | Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n. 571, 5^ piano. |
| Sede virtuale | Piattaforma ADA - https://elearning.uniba.it/ |

| | |
|---|---|
| Sito web del docente | http://www.di.uniba.it/~mignone/ |
| Ricevimento (giorni, orari e modalità, es. su appuntamento) | Venerdì 15:00 17:00 - Il ricevimento degli studenti può essere concordato via email |

| **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** | Programmazione in Java |
| **Contenuti di insegnamento (Programma)** | Ruolo e impatto della Cybersecurity (6 ore)<br>Infrastrutture e Centri: Internet Nazionale (10 ore)<br>Azioni abilitanti: (18 ore)<br>- analisi della sicurezza di applicazioni e servizi;<br>- analisi dei malware e banca dati nazionale delle minacce;<br>- anticipare la risposta ad attacchi cibernetici;<br>- anticipare la risposta ad attacchi sociali;<br>- anticipare la risposta ad attacchi fisici;<br>- analisi forense e conservazione delle prove;<br>- gestione del rischio a livello sistemico;<br>- difesa attiva.<br>Tecnologie abilitanti: (14 ore)<br>- architetture hardware<br>- crittografia<br>- i sistemi biometrici;<br>- blockchain e distributed ledger;<br>- tecnologie quantistiche;<br>- intelligenza artificiale.<br><br>Sicurezza delle applicazioni in Java (10 ore)<br>- Lifetime dei dati sensibili<br>- Lettura file<br>- Cookie<br>- Cross-site scripting (XSS)<br>- Sessione http<br>- https: SSL/TLS con Apache Tomcat<br>- Caricamento file con Apache Tika<br>- Sql injection<br>- Prepared statement via JDBC<br>- Gestione delle Password<br>- Classi mutabili<br>- Metodo clone<br>- Metodi ignorabili da codice non attendibile<br><br>Programmazione Difensiva (6 ore)<br>- Minimizzare lo scope delle variabili<br>- Ridurre l'accessibilità delle classi<br>- Feedback output dei metodi<br>- Identifica i file utilizzando più informazioni<br>- Thread-Safety |

| | |
|---|---|
| **Testi di riferimento** | Per la parte di teoria svolta durante le lezioni frontali:<br>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<br><br>Per la parte di esercitazione svolta durante il laboratorio:<br>F. Long, D. Mohindra, R.C. Seacord, D. F. Sutherland, D. Svoboda. Java Coding Guidelines. Addison-Wesley, 2014.<br>(disponibile in biblioteca e su piattaforma Ada)<br><br>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 dispense forniti dal docente durante lo svolgimento del corso. |

## Organizzazione della didattica

**Ore**

| Totali | Didattica frontale | Pratica (laboratorio e progetto) | Studio individuale |
|---|---|---|---|
| 225 ore | 48 ore | 65 ore | 112 ore |

**CFU/ETCS**

| | | | |
|---|---|---|---|
| 9 CFU | 6 CFU | 3 CFU | |

## Metodi didattici

Le 93 ore previste per l'insegnamento sono ripartite come segue:

- 48 ore di didattica frontale (in presenza);
- 15 ore di laboratorio (in presenza);
- 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.<br>○ 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**<br>○ 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.<br>○ L'autonomia di giudizio viene acquista attraverso lo studio e l'interpretazione critica di testi e programmi.<br>○ Il raggiungimento dell'adeguata autonomia è verificato attraverso delle esercitazioni, che si tengono durante il corso, e con l'esame finale di profitto.<br><br>**Abilità comunicative**<br>○ Gli studenti sono in grado di esporre le tematiche incluse nel programma del corso mediante il lessico specifico della disciplina.<br><br>**Capacità di apprendere in modo autonomo**<br>○ Gli studenti sono in grado di approfondire in autonomia le tematiche incluse nel programma del corso anche ricorrendo a risorse non direttamente coinvolte nella erogazione delle ore di lezione. |

| **Valutazione** | |
|---|---|
| **Modalità di verifica dell'apprendimento** | ○ Prova scritta sulla parte teorica.<br>○ Svolgimento di un progetto di realizzazione semplici applicazioni Java miranti a dimostrare le vulnerabilità e le varianti utili a migliorare la sicurezza. |
| Criteri di valutazione | **Conoscenza e capacità di comprensione:**<br>○ esposizione critica dei concetti appresi relativi agli ambiti progettuali strategici sulla sicurezza informatica.<br><br>**Conoscenza e capacità di comprensione applicate:**<br>○ competenze di programmazione sicura in Java, capacità di individuazione delle vulnerabilità nello sviluppo di semplici applicazioni software e capacità di correzione delle stesse<br><br>**Autonomia di giudizio:**<br>○ Capacità di svolgere semplici esercizi assegnati durante il corso delle lezioni<br><br>**Abilità comunicative:**<br>○ Uso del lessico specifico della disciplina informatica<br><br>**Capacità di apprendere:**<br>○ 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:<br><br>• https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea<br>• https://www.uniba.it/it/ricerca/dipartimenti/informatica |

- https://elearning.uniba.it/

I programmi degli insegnamenti sono disponibili qui:

- https://elearning.uniba.it/course/index.php?categoryid=288

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.uniba.it/

## Main information on the course

| | | |
|---|---|---|
| Course name | **Security in Applications** | |
| Degree | Master's Degree in Cybersecurity | |
| Academic year | 2023/24 | |
| European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU) | | 9 CFU<br>(each CFU corresponds to 25 hours (h) of student's time);<br>CFU are of type T1, T2 or T3<br>T1 = 8 h lecture + 17 h individual study<br>T2 = 15 h practice + 10 h individual study<br>T3 = 25 h individual study |
| Scientific Disciplinary Sector | ING-INF/05 | |
| Course language | Italian | |
| Academic year | First | |
| Delivery period | First semester, exact dates are specified in the program/regulations. | |
| Attendance requirement | It is highly recommended to attend classes | |
| Course of study's website | 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 | Paolo Mignone |
| Email | paolo.mignone@uniba.it |
| Phone | 080 544 2283 |
| Office | Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Room n. 571, 5th floor. |
| E-learning platform | Platform ADA - https://elearning.uniba.it/ |
| Teacher's homepage | http://www.di.uniba.it/~mignone/ |
| Office hours | Friday 15:00-17:00 - Student office hours can be scheduled via email |

## 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** | Java Programming |
| **Course program** | Role and Impact of Cybersecurity (6 hours)<br>Infrastructure and Centers: National Internet (10 hours)<br>Enabling Actions: (18 hours)<br>- Analysis of security for applications and services<br>- Analysis of malware and national threat database<br>- Anticipating responses to cyber attacks<br>- Anticipating responses to social attacks |

| | |
|---|---|
| | - Anticipating responses to physical attacks<br>- Forensic analysis and evidence preservation<br>- System-level risk management<br>- Active defense<br>Enabling Technologies: (14 hours)<br>- Hardware architectures<br>- Cryptography<br>- Biometric systems<br>- Blockchain and distributed ledger<br>- Quantum technologies<br>- Artificial intelligence<br><br>Security of Java Applications (10 hours)<br><br>- Lifetime of sensitive data<br>- File reading<br>- Cookies<br>- Cross-site scripting (XSS)<br>- HTTP session<br>- HTTPS: SSL/TLS with Apache Tomcat<br>- File uploading with Apache Tika<br>- SQL injection<br>- Prepared statement via JDBC<br>- Password management<br>- Mutable classes<br>- Clone method<br>- Ignorable methods for untrusted code<br>Defensive Programming (6 hours)<br>- Minimizing the scope of variables<br>- Reducing class accessibility<br>- Feedback output of methods<br>- File identification using multiple pieces of information<br>- Thread safety |
| **Books of reference** | For the theoretical part covered during the lectures:<br>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.<br><br>For the practical part covered during the lab:<br>F. Long, D. Mohindra, R.C. Seacord, D. F. Sutherland, D. Svoboda. "Java Coding Guidelines." Addison-Wesley, 2014.<br>(available in the library and on the Ada platform)<br><br>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?<br>and contact the library to arrange the loan. |
| **Notes to the books** | The reference texts are supported by scientific articles and handouts provided by the instructor during the course. |

## Organization of the didactic activities

| **Hours** | | | |
|---|---|---|---|
| Total | Lectures | Practice sessions | Individual study |
| 225 hours | 48 hours | 65 hours | 122 hours |
| **CFU/ETCS** | | | |
| 9 CFU | 6 CFU | 3 CFU | |

## Teaching methods

| | |
|---|---|
| | The 93 hours allocated for the teaching are distributed as follows:<br>- 48 hours of frontal teaching (in person);<br>- 15 hours of laboratory activities (in person);<br>- 50 hours of project activities (to be carried out individually).<br>The project, which implements the concepts learned during the laboratory activities, will be discussed during the exam session. |

| **Expected learning outcomes** | |
|---|---|
| **Knowledge and understanding** | ○ Acquisition of knowledge related to strategic project areas in cybersecurity.<br>○ 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** | *Making judgements*<br>○ 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.<br>○ Independent judgment is acquired through the study and critical interpretation of texts and programs.<br>○ The achievement of adequate autonomy is assessed through exercises held during the course and the final exam.<br><br>*Communication*<br>○ Students are able to present the topics included in the course curriculum using the specific vocabulary of the discipline.<br><br>*Learning skills*<br>○ 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.<br>○ Development of a project involving the creation of simple Java applications aimed at demonstrating vulnerabilities and useful variations to enhance security. |
| **Evaluation criteria** | **Knowledge and Understanding:**<br>○ Critical presentation of the concepts learned related to strategic project areas in cybersecurity.<br><br>**Applied Knowledge and Understanding:**<br>○ Secure programming skills in Java, ability to identify vulnerabilities in the development of simple software applications, and capacity to address and correct them.<br><br>**Autonomy of Judgment:**<br>○ Ability to carry out simple exercises assigned during the course lectures.<br><br>**Communication Skills:**<br>○ Use of specific vocabulary in the field of computer science.<br><br>**Ability to Learn:**<br>○ 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:<br><br>• https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea<br>• https://www.uniba.it/it/ricerca/dipartimenti/informatica<br>• https://elearning.uniba.it/<br><br>The course syllabi are available here:<br>• https://elearning.uniba.it/course/index.php?categoryid=288<br><br>The information that all students should know is detailed in the educational regulations and course handbooks available on the website:<br>• https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea<br><br>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.<br><br>_____<br><br>Link to the course on the department's ADA e-learning platform: https://elearning.uniba.it/ |