SYLLABUS

1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master
1.6 Program of study / Qualification	Cybersecurity Engineering
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	Web Security			Subject code	**8.00**
2.2 Course responsible / lecturer	Assoc.prof.dr.eng. Teodor-Traian ȘTEFĂNUȚ - teodor.stefanut@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Assoc.prof.dr.eng.Teodor-Traian ȘTEFĂNUȚ - teodor.stefanut@cs.utcluj.ro				
2.4 Year of study	I	2.5 Semester	2	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DA
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DI

3. Estimated total time

3.1 Number of hours per week	3	of which:	Course	2	Seminars	0	Laboratory	1	Project	0
3.2 Number of hours per semester	42	of which:	Course	28	Seminars	0	Laboratory	14	Project	0
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										16
(b) Supplementary study in the library, online and in the field										16
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										49
(d) Tutoring										0
(e) Exams and tests										2
(f) Other activities:										0
3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))										83
3.5 Total hours per semester (3.2+3.4)										125
3.6 Number of credit points										5

4. Pre-requisites (where appropriate)

4.1 Curriculum	Security issues at the source code level
4.2 Competence	Web programming, Databases, Computer networks

5. Requirements (where appropriate)

5.1. For the course	blackboard, beamer, computers, internet connection
5.2. For the applications	blackboard, beamer, computers, internet connection

6. Specific competence

6.1 Professional competences	implement ICT risk management develop information security strategy perform ICT security testing execute ICT audits develop contingency plans for emergencies manage system security implement ICT recovery system manage IT security compliances identify ICT security risks define security policies perform risk analysis educate on data confidentiality provide ICT consulting advice perform data analysis establish an ICT security prevention plan implement ICT security policies ensure compliance with legal requirements ensure information privacy monitor developments in field of expertise keep up with the latest information systems solutions
6.2 Cross competences	The graduate • develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded

7. Expected Learning Outcomes

Knowledge	The student has knowledge of: • web application security threats • ICT security standards • cyber attack counter-measures • information security strategy • safety engineering • security engineering • software anomalies • ICT encryption • ICT safety • cloud technologies • ethical hacking principles • organisational resilience • ICT network security risks • database development tools • system backup best practices • ICT infrastructure • ICT security legislation • cloud monitoring and reporting • cloud security and compliance • GDPR • attack vectors

Skills	The student is able to: • analyse ICT systems • define security policies • define technical requirements • execute software tests • identify ICT security risks • identify ICT system weaknesses • perform ICT security testing • perform risk analysis • provide ICT consulting advice • report test findings • address problems critically • implement cloud security and compliance • manage cloud data and storage • manage databases • manage keys for data protection • perform backups • protect personal data and privacy • cope with stress • ensure information security
Responsibilities and autonomy	The student has the ability to work independently in order to: • develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	Understanding of common vulnerabilities of Web applications and how they can be leveraged with malicious intentions. Learn best practice techniques for secure Web applications development, deployment, and configuration.
8.2 Specific objectives	1. Understand how Web applications work 2. Develop abilities for identifying vulnerabilities in the implementation of Web applications 3. Learn techniques to leverage vulnerabilities of Web applications (XSS, SQL injection, etc.) 4. Develop necessary skills to write secure code for Web applications 5. Learn how to correctly configure Web applications, from security perspective

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
Overview of Web technologies (1): general concepts (client/server, web 2.0, DOM, etc.), architecture of a web application (frontend/middleware/backend)	2	Blackboard illustrations and explanations,	
Overview of Web technologies (2): protocols (ISO-OSI, HTTP, FTO, TCP, SOAP etc.) and programming/description languages (HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)	2		
Web Security (1): authentication (identity), authorization, encryption, and applicable legislation	2		
Web Security (2): confidentiality, integrity and availability, network level (firewall, IPS)	2		
Servers' security (1): vulnerabilities and attacks (OWASP, SQL injection / session hijacking / SSL / direct objects referencing / etc.)	2		
Servers' security (2): availability assurance ((D)DoS attacks) and correct configuration	2		

		beamer presentations, discussions, short challenges	
Clients' security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking	2		
Clients' security (2): configuration, sandboxing, user scripting, malware/spyware	2		
Web cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SSL, HTTPS, etc.)	2		
Proactive security measures: detecting intrusions in Web applications, security incidents management, honeytokens	2		
Security on Web 2.0: AJAX paradigm, cloud computing, etc.	2		
Secure Web programming (1): input validation, sanitizing error messages, identity, access control, sessions management	2		
Secure Web programming (2): management of sensitive personal/financial data, best practices in secure programming of Web applications	2		
Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students	2		

Bibliography:

- 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)
- Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
- Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)
- The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
- Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)
- Online articles and web sites

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Implementation of a minimal Web application (frontend/middleware/backend)	1	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	
Study of network packages in Web protocols, implementation / configuration of a firewall	1		
Forensics of Web attacks: OWASP, session related vulnerabilities, SQL injection	1		
Forensics of Web attacks: XSS, CSRF, direct unsecured references, SSL	1		
Analysis and exploitation of vulnerabilities in Web browsers: JavaScript, path traversal, browsers' plugins (Unity, Java, etc.)	1		
Secure programming: input validation, error messages sanitization, sensitive data management, best practices in Web security	1		
Use of validation instruments for websites: fuzzers and vulnerabilities scanners	1		

Bibliography

- 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)
- Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
- Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)
- The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
- Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)
- Online articles and web sites

[*] *Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

Achieved through periodic discussions with the representatives of significant employers, mainly companies that have projects in information security.
Web security disciplines are present in many similar master programs in computers and information security, like:

- XACS241 - Web Security 2.0 (Stanford) – http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=1284858
- 06-20009 Network Security (University of Birmingham) – http://www.cs.bham.ac.uk/internal/modules/2010/20009/
- Internet and Security (Nottingham University) – http://targetpostgrad.com/course/31312-internet-and-security
- Master of Science in Cybersecurity (University of Maryland) – http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity.cfm
- Applied Cyber Security (MIT) – http://web.mit.edu/professional/short-programs/courses/applied_cyber_security.html

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to address and solve problems specific to Web security Attendance, active participation to the activities during lectures	Written exam and/or multiple-choice questions and/or oral presentation and/or research presentation on topics from discipline. Examination will be face-to-face or online.	40%
		Exercises on identification and exploitation of specific vulnerabilities of web applications, organized during lectures	20%
Laboratory	Ability to solve problems that are specific to Web security Attendance, active participation to the activities during classes	Completion of practical activities, on-time submission of homework and/or solving specific problems in a practical exam. Multiple-choice exam for testing knowledge of important concepts in Web security, on paper or electronic support, organized face-to-face or online.	40%

Minimum standard of performance:

Course. Attendance to **minimum 50%** of lecture to be admitted to the final exam. Solving the exercises from the lectures and submitting solution on time. These exercises cannot be recovered. Capability of defining and explaining basic concepts of Web applications' security (SQL injection, XSS, CSRF, etc.) and of identifying the main risks involved in data management and public Web applications.

Laboratory. Attendance to **100%** of classes (1 class can be recovered during the semester and a second one during the re-examination interval) to be admitted to the final exam. Activity from the laboratory classes is validated only after all the required exercises from each class are solved and submitted to the teacher. The submission deadline is three weeks from the laboratory class and they cannot be recovered later. The ability to identify basic/most common vulnerabilities (SQL injection, CSS, CSRF, configuration, etc.) in source code. The ability to write secure code for small Web applications.
Final grade for discipline: 40% laboratory + 40% final exam + 20% lectures exercises
Acceptance to final exam: minimum **50%** attendance to lectures, **100%** attendance to laboratory classes, **≥ 5** laboratory grade
Graduate requirements: ≥ 5 final exam

Date of filling in: 01.09.2025	**Responsible**	**Title First name Last name**	**Signature**
	Course	Assoc.prof.dr.eng. Teodor-Traian ȘTEFĂNUȚ	
	Applications	Assoc.prof.dr.eng. Teodor-Traian ȘTEFĂNUȚ	

Date of approval in the department 17.09.2025	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council 19.09.2025	Dean, Prof.dr.eng. Vlad Mureșan