# COURSE SYLLABUS

*Academic year 2025 - 2026*

## 1. Programme Information

| | |
|---|---|
| 1.1. Higher education institution | Lucian Blaga University of Sibiu |
| 1.2. Faculty | Faculty of Science |
| 1.3. Department | Mathematics and Informatics |
| 1.4. Field of study | Informatics |
| 1.5. Level of study[1] | Master |
| 1.6. Programme of study/qualification | Cybersecurity |

## 2. Course Information

| | | | | | |
|---|---|---|---|---|---|
| 2.1. Name of course | Web Applications Security | | | Code | FSTI.MAI.CS.M.SO.4.1020.E-7.2 |
| 2.2. Course coordinator | Associate professor PhD. Florin Sofonea | | | | |
| 2.3. Seminar/laboratory coordinator | Associate professor PhD. Florin Sofonea | | | | |
| 2.4. Year of study[2] | 2 | 2.5. Semester[3] | 2 | 2.6. Evaluation form[4] | E |
| 2.7. Course type[5] | R | 2.8. The formative category of the course[6] | | | S |

## 3. Estimated Total Time

| 3.1. Course Extension within the Curriculum – Number of Hours per Week | | | | |
|---|---|---|---|---|
| 3.1.a. Lecture | 3.1.b. Seminar | 3.1.c. Laboratory | 3.1.d. Project | Total |
| 1 | | 2 | | **3** |
| 3.2. Course Extension within the Curriculum – Total Number of Hours within the Curriculum | | | | |
| 3.2.a. Lecture | 3.2.b. Seminar | 3.2.c. Laboratory | 3.2.d. Project | Total[7] |
| 12 | | 24 | | **36** |

| **Time Distribution for Individual Study**[8] | **Hours** |
|---|---|
| Learning by using course materials, references and personal notes | 33 |
| Additional learning by using library facilities, electronic databases and on-site information | 28 |
| Preparing seminars / laboratories, homework, portfolios and essays | 56 |
| Tutorial activities[9] | 14 |
| Exams[10] | 2 |
| **3.3. Total Individual Study Hours[11] *(NOSI$_{sem}$)*** | **133** |
| **3.4. Total Hours in the Curriculum (*NOAD$_{sem}$*)** | **42** |
| **3.5. Total Hours per Semester[12] (*NOAD$_{sem}$ + NOSI$_{sem}$*)** | **175** |
| **3.6. No. of Hours / ECTS** | **25** |
| **3.7. Number of credits[13]** | **7** |

**4. Prerequisites (if needed)**

| | |
|---|---|
| 4.1. Courses that must be successfully completed first (from the curriculum)[14] | - |
| 4.2. Competencies | - |

**5. Conditions** (where applicable)

| | |
|---|---|
| 5.1. For course/lectures[15] | Classroom, equipped with blackboard, computer, video projector and software |
| 5.2. For practical activities (lab/sem/pr/app) [16] | Laboratory room equipped with computers |

**6. Learning Outcomes [17]**

| Number of credits assigned to the discipline: 7 | | | | |
|---|---|---|---|---|
| Learning outcomes | | | | Credit distribution by learning outcomes |
| Nr. crt. | Knowledge | Skills | Responsibility and autonomy | |
| LO 1 | The student explains the fundamental concepts of web application security, the principles of security by default, and risk analysis techniques. | The student applies safety assessment methods and performs threat and risk analyses for web applications. | The student demonstrates responsibility in documenting assessments and adopts ethical conduct. | 1 |
| LO 2 | The student describes major client-side vulnerabilities (XSS, clickjacking, HTML5) and defense mechanisms. | The student detects and implements prevention measures for these vulnerabilities in modern web applications. | The student assumes responsibility for protecting users and complies with legal and ethical principles. | 1.5 |
| LO 3 | The student understands server-side attacks (SQL injection, file upload, session management, access control). | The student implements defense measures in web applications and correctly configures servers and databases. | The student shows autonomy in selecting technical solutions and adopts professional best practices. | 1.5 |
| LO 4 | The student explains security aspects of web frameworks and PHP applications. | The student configures secure development environments and applies SDL and Agile SDL mechanisms. | The student assumes responsibility for secure application development and adopts a long-term vision. | 1.5 |
| LO 5 | The student describes incident response processes, business continuity, and communication in web application security. | The student applies incident response procedures and prepares clear reports for both technical and non-technical stakeholders. | The student demonstrates high responsibility in incident management and adopts professional conduct. | 1.5 |

**7. Course objectives** (resulted from developed competencies)

| | |
|---|---|
| 7.1. Main course objective | Learn a comprehensive understanding of web application security principles, techniques, and best practices, and to equip them with the knowledge and skills needed to identify, assess, and mitigate security risks in web applications. |
| 7.2. Specific course objectives | Understand how to conduct security testing of web applications, including vulnerability scanning, penetration testing, and code review. Understand how to conduct incident |

| | |
|---|---|
| | response and management in the context of web application security, including how to detect and respond to security incidents |

## 8. Content

| 8.1. Lectures[18] | Teaching methods[19] | Hours |
|---|---|---|
| Introduction in Information Security – how to implement a safety assessment, threat analysis, risk analysis, principles of security by default, data and code separation | Lecture, use of video projector, discussions with students | 1 |
| Safety on the Client Side – Sandbox browser, Malicious URL intercept, Rapid development of browser security | Lecture, use of video projector, discussions with students | 1 |
| Cross-Site scripting attack – Types of XSS, XSS Phishing, Construction of a XSS Attack, JavaScript Development Frameworks and XSS, XSS Defense | Lecture, use of video projector, discussions with students | 1 |
| Clickjacking – Introduction about clickjacking, image covering attacks, drag hijacking and data theft, clickjacking on mobile devices (Tapjacking), defense against clickjacking | Lecture, use of video projector, discussions with students | 1 |
| HTML5 Securities – New tags for XSS, Iframe Sandbox, HTML5 Canvas, Browser Web Storage | Lecture, use of video projector, discussions with students | 1 |
| Application Security on the Server side – Injection attacks, database attacking techniques, properly defending against SQL injection, Other Injection Attacks, File upload vulnerability, authentication and session management, access control | Lecture, use of video projector, discussions with students | 1 |
| Web Framework Security – MVC Framework security, Template engines and XSS, Web Frameworks, Application layer denial of service attacks (DDoS) | Lecture, use of video projector, discussions with students | 1 |
| PHP Security – File inclusion vulnerability, variable coverage vulnerability, code execution vulnerability, file writing code execution, securing a PHP environment, web server configuration security | Lecture, use of video projector, discussions with students | 1 |
| Security of an Internet Business – Security products, Security requirements for internet products, business logic security, phishing, user privacy protection, Security development lifecycle, Agile SDL (Security Development Lifecycle), Security Operations | Lecture, use of video projector, discussions with students | 2 |
| Incident response and management (Security incident response procedures, Forensic investigations and incident reporting, Business continuity and disaster recovery planning) | Lecture, use of video projector, discussions with students | 1 |
| Communicating about web application security (Effective communication with technical and non-technical stakeholders, Presentations and reports on web application security topics, Ethical and legal considerations in security reporting) | Lecture, use of video projector, discussions with students | 1 |
| | **Total lecture hours:** | **12** |

| 8.2. Practical activities (8.2.a. Seminar[20]/ 8.2.b. Laboratory[21]/ 8.2.c. Project[22]) | Teaching methods | Hours |
|---|---|---|
| Vulnerability assessment and testing: perform a vulnerability assessment, using tools to identify common web application security vulnerabilities, such as SQL injection, | Use of video projector, discussions with students | 6 |
| Vulnerability assessment and testing: perform a vulnerability assessment, using tools to identify common web application security vulnerabilities, such as cross-site scripting, and cross-site request forgery | Use of video projector, discussions with students | 4 |
| Vulnerability assessment and testing: perform a vulnerability assessment using Vulrnerable by design applications like Metasploitable, OWASP Mutillidae | Use of video projector, discussions with students | 6 |
| Incident response: Simulated security incident involving a web application, and asked to respond to the incident by identifying the root cause, containing the incident, and developing a remediation plan. | Use of video projector, discussions with students | 4 |

| | | |
|---|---|---|
| Compliance and regulation: OWASP Top Ten and GDPR, analyze a web application for compliance with the standards and regulations, as well as to suggest remediation measures. | Use of video projector, discussions with students | 4 |
| | **Total seminar/laboratory hours:** | 24 |

## 9. Bibliography

| | |
|---|---|
| 9.1. Recommended Bibliography | 1. OWASP TOP 10 - https://owasp.org/www-project-top-ten/<br>2. OWASP ZAP – Zed Attack Proxy - https://www.zaproxy.org/docs/<br>3. OWASP Juice Shop - https://owasp.org/www-project-juice-shop/<br>4. OWASP Vulnerable Web Applications Directory - https://github.com/koenbuyens/Vulnerable-OAuth-2.0-Applications |
| 9.2. Additional Bibliography | 1. A curated list of Web Security materials and resources - https://github.com/qazbnm456/awesome-web-security |

## 10. Conjunction of the discipline's content with the expectations of the epistemic community, professional associations and significant employers of the specific study program[23]

It is done through regular contacts with the representatives of the companies. Web application security topic is actual and is of great interest in existing software companies on the local, national and global market.

## 11. Evaluation

| Activity Type | 11.1 Evaluation Criteria | 11.2 Evaluation Methods | | 11.3 Percentage in the Final Grade | Obs.[24] |
|---|---|---|---|---|---|
| 11.4a Exam / Colloquy | • Theoretical and practical knowledge acquired (quantity, correctness, accuracy) | Tests during the semester[25]: | % | 50% (minimum 5) | CEF |
| | | Homework: | % | | |
| | | Other activities[26]: | % | | |
| | | Final evaluation: | 50% | | |
| 11.4b Seminar | • Frequency/relevance of participation or responses | Evidence of participation, portfolio of papers (reports, scientific summaries) | | 5% (minimum 5) | nCPE |
| 11.4c Laboratory | • Knowledge of the equipment, how to use specific tools; evaluation of tools, processing and interpretation of results | • Written questionnaire<br>• Oral response<br>• Laboratory notebook, experimental works, reports, etc.<br>• Practical demonstration | | 5% (minimum 5) | nCPE |
| 11.4d Project | • The quality of the project, the correctness of the project documentation, the appropriate justification of the chosen solutions | • Self-evaluation, project presentation<br>• Critical evaluation of a project | | 40% (minimum 5) | nCPE |
| 11.5 Minimum performance standard[27]<br>To pass the exam, the candidate must have a basic knowledge of the web application security topic and how to identify possible threads. | | | | | |

***The Course Syllabus will encompass components adapted to persons with special educational needs (SEN – people with disabilities and people with high potential), depending on their type and degree, at the level of all curricular elements (skills, objectives, contents, teaching methods, alternative assessment), in order to ensure fair opportunities in the academic training of all students, paying close attention to individual learning needs.***

Filling Date: |_1_|_5_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

Department Acceptance Date: |_3_|_0_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

| | **Academic Rank, Title, First Name, Last Name** | **Signature** |
|---|---|---|
| **Course Teacher** | Associate professor PhD. Florin Sofonea | |
| **Study Program Coordinator** | Associated Professor PhD. Nicolae Constantinescu | |
| **Department Head** | Professor PhD. Mugur Acu | |

[1] *Bachelor / Master*
[2] *1-4 for bachelor, 1-2 for master*
[3] *1-8 for bachelor, 1-3 for master*
[4] *Exam, colloquium or VP A/R - from the curriculum*
[5] *Course type: R = Compulsory course; E = Elective course; O = Optional course*
[6] *Formative category: S = Specialty; F = Fundamental; C = Complementary; I = Fully assisted; P = Partially assisted; N = Unassisted*
[7] *Equal to 14 weeks x number of hours from point 3.1 (similar to 3.2.a.b.c.)*
[8] *The following lines refer to individual study; the total is completed at point 3.37.*
[9] *Between 7 and 14 hours*
[10] *Between 2 and 6 hours*
[11] *The sum of the values from the previous lines, which refer to individual study.*
[12] *The sum (3.5.) between the number of hours of direct teaching activity (NOAD) and the number of hours of individual study (NOSI) must be equal to the number of credits assigned to the discipline (point 3.7) x no. hours per credit (3.6.)*
[13] *The credit number is computed according to the following formula, being rounded to whole neighbouring values (either by subtraction or addition*

$$No.credits = \frac{NOCpSpD \times C_C + NOApSpD \times C_A}{TOCpSdP \times C_C + TOApSdP \times C_A} \times 30\ credits$$

Where:

- NOCpSpD = Number of lecture hours / week / discipline for which the credits are calculated
- NOApSpD = Number of application hours (sem./lab./pro.) / week / discipline for which the credits are calculated
- TOCpSdP = Total number of course hours / week in the Curriculum
- TOApSdP = Total number of application hours (sem./lab./pro.) / week in the Curriculum
- $C_C$/$C_A$ = Course coefficients / applications calculated according to the table

| **Coefficients** | **Course** | **Applications (S/L/P)** |
|---|---|---|
| Bachelor | 2 | 1 |
| Master | 2,5 | 1,5 |
| Bachelor - foreign language | 2,5 | 1,25 |

[14] *The courses that should have been previously completed or equivalent will be mentioned*
[15] *Board, video projector, flipchart, specific teaching materials, online platforms, etc.*
[16] *Computing technology, software packages, experimental stands, online platforms, etc.*
[17] *Competences from the Grids related to the description of the study program, adapted to the specifics of the discipline*
[18] *Chapter and paragraph titles*
[19] *Exposition, lecture, board presentation of the studied topic, use of video projector, discussions with students (for each chapter, if applicable)*
[20] *Discussions, debates, presentations and/or analyses of papers, solving exercises and problems*
[21] *Practical demonstration, exercise, experiment*
[22] *Case study, demonstration, exercise, error analysis, etc.*
[23] *The relationship with other disciplines, the usefulness of the discipline on the labour market*
[24] *CPE – Conditions Exam Participation; nCPE – Does Not Condition Exam Participation; CEF - Conditions Final Evaluation; N/A – not applicable*
[25] *The number of tests and the weeks in which they will be taken will be specified*
[26] *Scientific circles, professional competitions, etc.*
[27] *The minimum performance standard in the competence grid of the study program is customized to the specifics of the discipline, if applicable*