## **SYLLABUS**

## 1. Data about the program of study

1.1	Institution	Technical University of Cluj-Napoca
1.2	Faculty	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 of Science
1.6	Program of study / Qualification	Cybersecurity Engineering / Master
1.7	Form of education	Full time
1.8	Subject code	8.

## 2. Data about the subject

2.1	Subject name				Web Security		
2.2	Course responsible/lecturer				Conf.dr.ing. Teodor ȘTEFĂNUȚ - <u>teodor.stefanut@cs.utcluj.ro</u>		
2.3	.3 Teachers in charge of seminars Conf.dr.				Conf.dr.ing. Teodor \$TEFĂNUȚ - teodor.stefanut@cs.utcluj.ro		
2.4 Year of study I 2.5 Semester 2		2	2.6 Type of assessment (E - exam, C - colloquium, V - verification)	E			
2.7 Subject category		Formative category: DA – a		DA –	advanced, DS – speciality, DC – complementary	DA	
		Optionality: DI – imposed, I		osed,	DO – optional (alternative), DF – optional (free choice)	DI	

## 3. Estimated total time

3.1 Number of hours per week	3	of which	3.2 Course	2	3.3 Seminar	0	3.3 Laboratory	1	3.3 Proje	t 0
3.4 Total hours in the curriculum	42	of which	3.5 Course	28	3.6 Seminar	0	3.6 Laboratory	14	3.6 Proje	t 0
3.7 Individual study:										
(a) Manual, lecture material a	nd not	es, bibliogr	aphy							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				
3.8 Total hours of individual study (sum (3.7(a)3.7(f))) 83										
3.9 Total hours per semester (3.4+3.8) 125										
3.10 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
5.2	For the applications	blackboard, beamer, computers

## 6. Specific competences

Professional	C1. Identify and understand the security issues specific to the different contexts of computing
competences	system usage. Appropriately apply the basic elements of security management and methods
·	of evaluation and management of information security risks.
	• C1.1. Knowledge of advanced theoretical and practical terminology, concepts, and
	principles specific to cybersecurity field. Knowledge of concepts about cybersecurity risk
	evaluation, and management.
	C1.2. Understanding cybersecurity risks specific to new situations and their relationship     with provide the experienced situations and ricks. Be able to predict possible threat scenarios
	With previously experienced situations and risks. Be able to predict possible timeat scenarios when using cybersecurity solutions in new fields or situations
	<ul> <li>C1.2 Canability to identify and model new types of cybersecurity risks affecting and users.</li> </ul>
	computing systems and software applications and identify and evaluate possible solutions
	against such risks.
	• <b>C1.4.</b> Capability to identify and assess the limitations of existing cybersecurity solutions and
	their security risks, relative to well-known classifications.
	• C1.5. Capability to develop new theoretical models and methods to analyze and assess the
	cybersecurity properties and effectiveness of existing solutions.
	C3. Analyze and evaluate the security characteristics of computing system. Identify the
	misconfigurations and software vulnerabilities.
	• C3.1. Theoretical and practical knowledge of different cases of computing system
	misconfiguration and misusage that expose them to cybersecurity attacks, and of different
	types of software vulnerabilities and possible cybersecurity attacks.
	• <b>C3.2.</b> Be able to analyze and understand new kinds of software and communication
	protocols, in order to identify new possible cybersecurity interacts, vulnerabilities, and risks. Be able to use commonly used databases of reported vulnerabilities and attacks in the
	nrocess of assessing the cybersecurity of a new computing system.
	• C3.3. Capability to make cybersecurity assessments and identify possible attack surface of
	unknown computing systems, networks, or software applications.
	• <b>C3.4.</b> Capability to identify and assess theoretical and practical limitations of existing
	automatic vulnerability detection tools and propose possible combinations of such tools for
	improved results, where and if possible.
	• C3.5. Capability to propose new vulnerability identification, analysis, and classification,
	methods. Capability to propose solutions against exploitation techniques of such
	vulnerabilities.
	C4. Design and develop highly secure software, security solutions and tools.
	• <b>C4.1.</b> Knowledge of basic concepts and principles of secure software development and
	evaluation. Knowledge of common types of security software and cools. Knowledge of
	frameworks needed to develop effective security solutions
	• <b>C4.3</b> Capability to develop complex secure software, complying with recommended good
	practices of built-in security and secure coding. Capability to develop software tools used
	for cybersecurity pentesting and assessment.
	• C4.4. Capability to assess complex software projects and identify their cybersecurity
	vulnerabilities and flaws, regarding their design, implementation, or testing, and propose
	improved development methods from the cybersecurity perspective.
Cross	N/A
competences	

# 7. Discipline objectives (as results from the *key competences gained*)

7.1	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.			
7.2	Specific objectives	<ol> <li>Understand how Web applications work</li> <li>Develop abilities for identifying vulnerabilities in the implementation of Web applications</li> <li>Learn techniques to leverage vulnerabilities of Web applications (XSS, SQL injection, etc.)</li> <li>Develop necessary skills to write secure code for Web applications</li> </ol>			

5. Learn how to correctly configure Web applications, from security perspective	-		
		5.	Learn how to correctly configure Web applications, from security perspective

## 8. Contents

B1.1 Eccurre (synabus)       hours       reaching methods       Notes         Overview of Web technologies (1): general concepts       (client/server, web 2.0, DOM, etc.), architecture of a web       2         application (frontend/middleware/backend)       2         Overview of Web technologies (2): protocols (ISO-OSI, HTTP,       2         FTO, TCP, SOAP etc.) and programming/description languages       2         (ITML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)       2         Web Security (1): authentication (identity), authorization, encryption, and applicable legislation       2         Injection / session hijacking / SSL / direct objects referencing /       2         etc.)       Blackboard         Servers' security (1): common vulnerabilities (browsers, plugins, cookies, DSL), clickjacking       2         Clients' security (2): configuration, sandboxing, user scripting, cookies, DSL), clickjacking       2         Clients' security (1): comfiguration, sandboxing, user scripting, cookies, DSL), clickjacking       2         Proactive security modents management, honeytokens       2         applications, security noticels (SSL, HTTPS, etc.)       2         Proactive security modents management of sensitive       2         Secure Web programming (1): input validation, santizing error messages, identity, access control, sessions management       2         Security on Web 2.0: ALX paradigm, cloud co		Number of	Ta a abin a na ath a da	Natas			
Overview of Web technologies (1): general concepts (client/server, web 2.0, DOM, etc.), architecture of a web application (frontend/middleware/backend)     2       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, entwork level (firewall, IPS)     2       Servers' security (2): availability assurance (IDDoS attacks) and correct configuration     2       Blackboard     Blackboard       Clients' security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking     2       Proactity (2): configuration, sandboxing, user scripting, cookies, DNS), clickjacking     2       Proactive security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking     2       Proactive security (1): configuration, sandboxing, user scripting, applications, security incidents management, honeytokens     2       Security on Web 2.0: ALX paradigm, cloud computing, etc.     2       Security web 2.0: ALX paradigm, cloud computing, etc.     2       Secure Web programming (1): input validation, sanitizing error messages, identity, access control, sessions management Secure Web programming (2): management of sensitive personal/financial data, best practices in secure programming of 2     2       Bibliography     1     24 Decady Sins of Software Security (Howard, Michael –	8.1. Lecture (syllabus)	hours	reaching methods	Notes			
(client/server, web 2.0, DOM, etc.), architecture of a web       2         application (frontend/middleware/backend)       2         Overview of Web technologies (2): protocols (ISO-OSI, HTTP,       7         FTO, TCP, SOAP etc.) and programming/description languages       2         (HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)       2         Web Security (1): authentication (identity), authorization,       2         encryption, and applicable legislation       2         Servers' security (2): confidentiality, integrity and availability,       2         etc.)       Blackboard         Servers' security (2): availability assurance (ID)DoS attacks) and       2         correct configuration, sandboxing, user scripting,       2         maiware/spyware       2         Web cryptography: general aspects, public/private keys,       2         certify on Web 2:0: AIAX paradigm, cloud computing, etc.       2         Securet Veb programming (1): input validation, sanitizing error       2         messages, identity, access control, sessions management       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Synthetic overview of entire course, highlight of important       2         Secure Web programming (2): management of se	Overview of Web technologies (1): general concepts						
application (frontend/middleware/backend)         Overview of Web technologies (2): protocols (ISO-OSI, HTTP, FTO, TCP, SOAP etc.) and programming/description languages       2         (HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)       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 (2): vulnerabilities and attacks (OWASP, SQL injection / session hijacking / SSL / direct objects referencing / etc.)       2         Servers' security (2): configuration, sandboxing, user scripting, cookies, DNS), clickjacking       2       Blackboard         Clients' security (2): configuration, sandboxing, user scripting, malware/Spyware       2       clisus science, short challenges         Veb cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SSL, HTTPS, etc.)       2       clisus science, short challenges         Security Ow Web 2:0: AJAA paradigm, cloud computing, etc.       2       2       clisus science, splitic/private keys, certificates, message integrity, protocols (SSL, HTTPS, etc.)       2         Secure Web programming (1): input validation, sanitizing error messages, identity, access control, seesions management secure Web programming (2): management of sensitive personal/financial data, best practices in secure programming of 2       2         Web applications       2       contusion, discuss subjects chosen by students	lient/server, web 2.0, DOM, etc.), architecture of a web 2						
Overview of Web technologies (2): protocols (ISO-OSI, HTTP,       PTO, TCP, SOAP etc.) and programming/description languages       2         (HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)       Web Security (1): authentication (identify), authorization,       2         Web Security (1): authentication (identify), authorization,       2       2         Interval       2       Blackboard         Inetwork level (firewall, IPS)       2         Servers' security (1): vulnerabilities and attacks (OWASP, SQL       2         injection / session hijacking / SSL / direct objects referencing /       2         detc.)       Blackboard         Servers' security (2): availability assurance (ID)DoS attacks) and       2         correct configuration       2         Clients' security (2): comfiguration, sandboxing, user scripting,       2         malware/spyware       2         Web cryptography: general aspects, public/private keys,       2         certificates, message integrity, protocols (SSL, HTTPS, etc.)       2         Proactive security measures: dietecting intrusions in Web       2         applications, security unicidents management of sensitive       2         personal/financial data, best practices in secure programming of       2         Security on Web 2:: AUAX paradigm, cloud computing, etc.       2         Security oreview	application (frontend/middleware/backend)						
FTO, TCP, SOAP etc.) and programming/description languages       2         (HTML, CSS, SVG, JS, XNL, 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 (2): availability assurance (ID)DoS attacks) and correct configuration       2         etc.)       Blackboard         Servers' security (2): availability assurance (ID)DoS attacks) and correct configuration, sandboxing, user scripting, cookies, DNS), clickjacking       2         Clients' security (1): configuration, sandboxing, user scripting, cookies, DNS), clickjacking       2         Web cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SL, HTTPS, etc.)       2         Proactive security measures: detecting intrusions in Web applications, security, incidents management, honeytokens       2         Secure Web programming (1): input validation, sanitizing error messages, identity, access control, sessions management       2         Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2         Bibliography       2.02 AlAX paradigm, clow acometry, access of abplication Security Flaws (Stuttard, Dafydd – 2011 – WCBraw-Hill)         Web applications       2.02 AlAX paradigm, clow acometry, access and applicability of application (Gambray, u	Overview of Web technologies (2): protocols (ISO-OSI, HTTP,						
(HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)         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 (2): uninerabilities and attacks (OWASP, SQL injection / session hijacking / SSL / direct objects referencing / etc.)       2         Servers' security (2): availability assurance (ID)DoS attacks) and correct configuration       2         Clients' security (2): configuration, sandboxing, user scripting, cookies, DNS, lickipacking       2         Clients' security (2): configuration, sandboxing, user scripting, cookies, DNS, lickipacking       2         Proactive security measures: detecting intrusions in Web applications, security incidents management, honeytokens       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 Ueb applications       2         Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2         Bibliography 1. 24 Deadly Isin of Software Security (Howard, Michael – 2010 – McGraw-Hill)       4         2. Web Proprication Hacker's Handbook: Finding and Exploiting Security Flaws (Stutterd, Dafydd – 2011 – Wiley) (2nd ed)       1         3. Hacking Exposed: Web	FTO, TCP, SOAP etc.) and programming/description languages	2					
Web Security (1): authentication (identity), authorization,       2         encryption, and applicable legislation       2         Web Security (2): confidentiality, integrity and availability,       2         Servers' security (1): uulnerabilities and attacks (OWASP, SQL       2         injection / session hijacking / SSL / direct objects referencing /       2         etc.)       Blackboard         Servers' security (2): availability assurance (ID)DoS attacks) and       2         correct configuration       2         correct configuration       2         correct configuration, sandboxing, user scripting,       2         malware/spyware       2         Web cryptography: general aspects, public/private keys,       2         certificates, message integrity, protocols (SSL, HTTPS, etc.)       2         Proactive security incidents management, honeytokens       2         Secure Web programming (1): input validation, sanitizing error       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Web Applications       Secure Web programming (2): management of sensitive       2         Synthetic overview of entire course, highlight of important       2       2         conclusions, discuss subjects chosen by students<	(HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)						
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 (ID)DoS attacks) and correct configuration       2         Servers' security (2): availability assurance (ID)DoS attacks) and correct configuration       2         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         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 2       2         Web applications       2         Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2         Bibliography       1       4 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)	Web Security (1): authentication (identity), authorization,		-				
Web Security (2): confidentiality, integrity and availability,       2         Servers' security (1): vulnerabilities and attacks (OWASP, SQL       2         injection / session hijacking / SSL / direct objects referencing /       2         Blackboard       illustrations and         Servers' security (2): availability assurance (ID)DoS attacks) and       2         correct configuration       2         Clients' security (1): common vulnerabilities (browsers, plugins,       2         cookies, DNS), clickjacking       2         Clients' security (2): configuration, sandboxing, user scripting,       2         malware/spyware       2         Web cryptography: general aspects, public/private keys,       2         certificates, message integrity, protocols (SSL, HTTPS, etc.)       2         Proactive security measures: detecting intrusions in Web       2         applications, security incidents management, honeytokens       2         Secure Web programming (1): input validation, sanitizing error       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2	encryption, and applicable legislation	2					
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       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 incidents management, honeytokens     2       Secure Web programming (1): input validation, sanitizing error sessages, identify, 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     2     2010 – McGraw-Hill)       2.     Web Application Restrict 's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)       3.     Hacking and Penetration Testing with kili Linux (Muniz, Joseph – 2013 – Packt Publishing)       3.     Hacking and Penetration Testing with kili Linux (Muniz, Joseph – 2013 – Packt Publishing)       3.     Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill)       4.     The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed) </td <td>Web Security (2): confidentiality, integrity and availability,</td> <td></td> <td>-</td> <td></td>	Web Security (2): confidentiality, integrity and availability,		-				
Servers' security (1): vulnerabilities and attacks (OWASP, SQL injection / session hijacking / SSL / direct objects referencing / etc.)       2         Blackboard       Blackboard         Servers' security (2): availability assurance ((D)DoS attacks) and correct configuration       2         Clients' security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking       2         Clients' security (1): 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         Secure Web programming (1): input validation, sanitizing error 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       2       42 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2.       Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         3.       Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill)         3.       Hacking and Penetration Testing Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygre	network level (firewall, IPS)	2					
injection / session hijacking / SSL / direct objects referencing /       2       Blackboard         iturt       Servers' security (2): availability assurance ((D)DoS attacks) and       2       Blackboard         correct configuration       2       Blackboard       explanations,         Clients' security (1): common vulnerabilities (browsers, plugins,       2       beamer       presentations,         Clients' security (2): configuration, sandboxing, user scripting,       2       cities (configuration, security (2): configuration, sandboxing, user scripting,       2         malware/spyware       2       discussions, short       challenges         Web cryptography: general aspects, public/private keys,       2       2         Proactive security incidents management, honeytokens       2       2         Secure Web programming (1): input validation, sanitizing error       2       2         Secure Web programming (2): management of sensitive       2       2         personal/financial data, best practices in secure programming of       2       2         Synthetic overview of entire course, highlight of important       2       2         conclusions, discuss subjects chosen by students       2       2         Bibliography       1       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         1       24 Deadl	Servers' security (1): vulnerabilities and attacks (OWASP, SQL						
etc.)       Blackboard         Servers' security (2): availability assurance ((D)DoS attacks) and correct configuration       2       illustrations and explanations,         Clients' security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking       2       beamer         Clients' security (2): configuration, sandboxing, user scripting, malware/spyware       2       discussions, short challenges         Web cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SSL, HTTPS, etc.)       2       discussions, short challenges         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       2         Bibliography Meth Application (Scambray, Joel – 2010 – McGraw-Hill)       3       4       4         Number of Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)       5       5         1       The Basics of Hacking and Penetration Testing, Second Edition: Ethical	injection / session hijacking / SSL / direct objects referencing /	2					
Servers' security (2): availability assurance ((D)DoS attacks) and correct configuration       2       illustrations and explanations, beamer presentations,         Clients' security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking       2       illustrations and explanations,         Clients' security (2): configuration, sandboxing, user scripting, malware/spyware       2       discussions, short challenges         Web cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SL, HTTPS, etc.)       2         Proactive security incidents management, honeytokens       2         Security on Web 2.0: AIAX 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       2       2         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill)       2         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)       3         5. Web Application Hacker's Handbook: Finding and Exploiting: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)	etc.)		Blackboard				
correct configuration       2       explanations, beamer         Clients' security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking       2       beamer         Clients' security (2): configuration, sandboxing, user scripting, malware/spyware       2       discussions, short challenges         Web cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SSL, HTTPS, etc.)       2       discussions, short challenges         Proactive security measures: detecting intrusions in Web applications, security incidents management, honeytokens       2       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 2       2         Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2         Bibliography       1       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2.       Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Suttard, Dafydd – 2011 – Wiley) (2nd ed)         3.       Hacking Exposed: Web Application (Scambray, Joel – 2008 – O'Reilly Media)       Conline articles and web sites         8.       Seminar / Laboratory / Project       Number of hours       Teaching methods       Notes	Servers' security (2): availability assurance ((D)DoS attacks) and		illustrations and				
Clients' security (1): common vulnerabilities (browsers, plugins, cookies, DNS), clickjacking       2       beamer presentations, discussions, short challenges         Clients' security (2): configuration, sandboxing, user scripting, malware/spyware       2       discussions, short challenges         Web cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SSL, HTTPS, etc.)       2       discussions, short challenges         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 2       2         Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2       Secure Web Application         1.       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)       2       Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         3.       Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)       1       2011 – Wiley) (2nd ed)         5.       Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)       7       Teaching methods         6.       Web Security Testing Cookbook (Hope, Paco – 200	correct configuration	2	explanations.				
cookies, DNS), clickjacking     2     presentations,       Clients' security (2): configuration, sandboxing, user scripting, malware/spyware     2     discussions, short challenges       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       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     1     24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)       2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)     3       3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill)     2014 – Wiley) (2nd ed)       4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)     5       5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)     6	Clients' security (1): common vulnerabilities (browsers, plugins,		beamer				
Clients' security (2): configuration, sandboxing, user scripting, malware/spyware       2       discussions, short challenges         Web cryptography: general aspects, public/private keys, certificates, message integrity, protocols (SL, 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       1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)       2         2. Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)       3. Hacking Exposed: Web Application Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)       7. Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours       Teaching methods       Notes	cookies, DNS), clickjacking	2	presentations.				
malware/spyware       2       challenges         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 2       2         Web applications       2         Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2         Bibliography       1       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)       3.         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill)       23 dealy         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)       5.         5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)       6.         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)       7.       Te	Clients' security (2): configuration, sandboxing, user scripting,		discussions, short				
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 2       2         Web applications       2         Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2         Bibliography       2       2         .       2       Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         .       Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill)         2.       Web Yenetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3.       Hacking Exposed: Web Application Scambray, Joel – 2010 – McGraw-Hill)         2.       Wiley (2nd ed)         5.       The Web Application Alcker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         6.       Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7.       Online articles and	malware/spyware	2	challenges				
certificates, message integrity, protocols (SSL, HTTPS, etc.)       2         Proactive security measures: detecting intrusions in Web       2         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       2         messages, identity, access control, sessions management       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2         Bibliography       1       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Application Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)       3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)       5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)       7. Online articles and web sites         7. Onli	Web cryptography: general aspects, public/private keys,	2					
Proactive security measures: detecting intrusions in Web       2         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       2         messages, identity, access control, sessions management       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2         Bibliography       1       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         .       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         .       Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3.       Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4.       The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5.       The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6.       Web Security Testing Cookbook (	certificates, message integrity, protocols (SSL, HTTPS, etc.)	2					
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       2         messages, identity, access control, sessions management       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2         Bibliography       1         1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)       7. Online articles and web sites         7. Online articles and web sites       Number of hours       Teaching methods       Notes	Proactive security measures: detecting intrusions in Web	2					
Security on Web 2.0: AJAX paradigm, cloud computing, etc.       2         Secure Web programming (1): input validation, sanitizing error       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2         Bibliography       2         1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)       2         Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)       3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)       5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)       7. Online articles and web sites         7. Online articles and web sites       Number of hours       Teaching methods       Notes	applications, security incidents management, honeytokens	2					
Secure Web programming (1): input validation, sanitizing error       2         messages, identity, access control, sessions management       2         Secure Web programming (2): management of sensitive       2         personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2         Bibliography       1       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2.       Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3.       Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4.       The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5.       The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6.       Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7.       Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         Implementation of a minimal Web application       1	Security on Web 2.0: AJAX paradigm, cloud computing, etc.	2					
messages, identity, access control, sessions management       2         Secure Web programming (2): management of sensitive       personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2         Bibliography       2         1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7. Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         Implementation of a minimal Web application       1	Secure Web programming (1): input validation, sanitizing error	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       2         1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7. Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         1       Implementation of a minimal Web application	messages, identity, access control, sessions management	2					
personal/financial data, best practices in secure programming of       2         Web applications       2         Synthetic overview of entire course, highlight of important       2         conclusions, discuss subjects chosen by students       2         Bibliography       2         1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7. Online articles and web sites         8.2. Seminar / Laboratory / Project         Number of hours       Teaching methods         Notes	Secure Web programming (2): management of sensitive						
Web applications	personal/financial data, best practices in secure programming of	2					
Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students       2         Bibliography       1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7. Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         Implementation of a minimal Web application       1	Web applications						
conclusions, discuss subjects chosen by students       2         Bibliography       1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7. Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         Implementation of a minimal Web application       1	Synthetic overview of entire course, highlight of important	n					
Bibliography         1.       24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)         2.       Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)         3.       Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)         4.       The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)         5.       The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6.       Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7.       Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         Implementation of a minimal Web application       1	conclusions, discuss subjects chosen by students	2					
<ol> <li>24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)</li> <li>Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)</li> <li>Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)</li> <li>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)</li> <li>The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)</li> <li>Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)</li> <li>Online articles and web sites</li> </ol> 8.2. Seminar / Laboratory / Project           Number of hours         Teaching methods         Notes	Bibliography		·				
<ol> <li>Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)</li> <li>Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)</li> <li>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)</li> <li>The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)</li> <li>Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)</li> <li>Online articles and web sites</li> </ol> 8.2. Seminar / Laboratory / Project           Implementation of a minimal Web application         1	1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 -	- McGraw-Hill	)				
<ol> <li>Hacking Exposed: Web Application (scambray, Joel – 2010 – McGraw-Hill) (Srd ed)</li> <li>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)</li> <li>The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)</li> <li>Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)</li> <li>Online articles and web sites</li> </ol> 8.2. Seminar / Laboratory / Project           Implementation of a minimal Web application         1	2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)						
Wiley) (2nd ed)         5.       The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)         6.       Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7.       Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         Implementation of a minimal Web application       1	<ol> <li>наскіпу Exposed: web Application (scambray, joei – 2010 – McGraw-Hill) (3rd ed)</li> <li>The Web Application Hacker's Handbook; Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 –</li> </ol>						
<ul> <li>5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)</li> <li>6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)</li> <li>7. Online articles and web sites</li> <li>8.2. Seminar / Laboratory / Project</li> <li>Implementation of a minimal Web application</li> </ul>	Wiley) (2nd ed)						
Easy (Engebretson, Patrick – 2013 – Sygress)         6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7. Online articles and web sites         8.2. Seminar / Laboratory / Project         Implementation of a minimal Web application         1	5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made						
b.       Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)         7.       Online articles and web sites         8.2. Seminar / Laboratory / Project       Number of hours         Implementation of a minimal Web application       1	Easy (Engebretson, Patrick – 2013 – Sygress)						
8.2. Seminar / Laboratory / Project     Number of hours     Teaching methods     Notes	<ol> <li>Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)</li> <li>Online articles and web sites</li> </ol>						
8.2. Seminar / Laboratory / Project     Teaching methods     Notes       Implementation of a minimal Web application     1     1	7. Online articles and web sites	Number of					
Implementation of a minimal Web application 1	8.2. Seminar / Laboratory / Project	hours	Teaching methods	Notes			
	Implementation of a minimal Web application	1					

(frontend/middleware/backend)	
Study of network packages in Web protocols, implementation /	1
configuration of a firewall	T
Forensics of Web attacks: OWASP, session related	1
vulnerabilities, SQL injection	T
Forensics of Web attacks: XSS, CSRF, direct unsecured	1
references, SSL	Ť
Analysis and exploitation of vulnerabilities in Web browsers:	1
JavaScript, path traversal, browsers' plugins (Unity, Java, etc.)	Ŧ
Secure programming: input validation, error messages	
sanitization, sensitive data management, best practices in Web	1
security	
Use of validation instruments for websites: fuzzers and	1
vulnerabilities scanners	

#### Bibliography

- 1. 24 Deadly Sins of Software Security (Howard, Michael 2010 McGraw-Hill)
- 2. Web Penetration Testing with Kali Linux (Muniz, Joseph 2013 Packt Publishing)
- 3. 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)
- 5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy (Engebretson, Patrick 2013 Sygress)
- 6. Web Security Testing Cookbook (Hope, Paco 2008 O'Reilly Media)
- 7. Online articles and web sites

# 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-andsecurity
- Master of Science in Cybersecurity (University of Maryland) http://www.umuc.edu/academicprograms/masters-degrees/cybersecurity.cfm
- Applied Cyber Security (MIT) http://web.mit.edu/professional/shortprograms/courses/applied\_cyber\_security.html

### 10. Evaluation

Activity type	10.1 Assessment criteria	10.2 Assessment methods	10.3 Weight in the final grade
10.4 Course	Ability to address and solve problems specific to Web security Attendance, active participation to the activities	Written exam and/or multiple- choice questions and/or oral presentation and/or research presentation on topics from discipline. Examination will be face-	40%

	during lectures	to-face or online.	
		Exercises on identification and	
		exploitation of specific	20%
		vulnerabilities of web applications,	2076
		organized during lectures	
		Completion of practical activities,	
	Ability to solve problems that are specific to Web security Attendance, active participation to the activities	and/or solving specific problems in	
		a practical exam. Multiple-choice	
10.5 Laboratory		exam for testing knowledge of	40%
		important concepts in Web	
		security, on paper or electronic	
	uuning classes	support, organized face-to-face or	
		online.	

#### Minimum standard of performance

*Lecture.* Attendance to **minimum 50%** of lecture in order 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.

*Lab.* Attendance to **100%** of classes (1 class can be recovered during the semester and a second one during the reexamination interval) in order 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:		Title Surname Name	Signature
	Lecturer	Conf.dr.ing. Teodor ŞTEFĂNUȚ	
	Teachers in charge of application	Conf.dr.ing. Teodor ŞTEFĂNUȚ	

Date of approval in the department 20.02.2024

Head of department Prof.dr.ing. Rodica Potolea

Date of approval in the faculty 22.02.2024

Dean Prof.dr.ing. Mihaela Dinsoreanu