INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA ACADÉMICA

DIRECCIÓN DE EDUCACIÓN SUPERIOR

SYNTHESIZED SCHOOL PROGRAM

ACADEMIC UNIT: Escuela Superior de Cómputo

ACADEMIC PROGRAM: Ingeniería en Sistemas Computacionales.

LEARNING UNIT: Web Security **LEVEL:** III

AIM OF THE LEARNING UNIT:
The student develops secure web applications, through the detection of vulnerabilities, the application of defense mechanisms and protection techniques against common threats.

CONTENTS:

I. Input-based attacks.
II. Injection attacks.
III. Cross-site scripting.
IV. Authentication.

TEACHING PRINCIPLES:
The teacher will apply a Projects-Based learning process, through inductive and heuristic methods using analysis techniques, technical data, charts, cooperative presentation, exercise-solving and the production of the learning evidences. Moreover, an autonomous learning will be encouraged by the development of a final project.

EVALUATION AND PASSING REQUIREMENTS:
The program will evaluate the students in a continuous formative and summative way, which will lead into the completion of proyect portfolio. Some other assessing methods will be used, such as revisions, practical´s, class participation, exercises, learning evidences and a final project.

Other means to pass this Unit of Learning:

- Evaluation of acknowledges previously acquired, with base in the issues defined by the academy.
- Official recognition by either another IPN Academic Unit of the IPN or by a national or international external academic institution besides IPN.

REFERENCES:

- Clarke J. (2009). *SQL injection attacks and defense*. E.U.A.: Ed. Syngress. ISBN-13: 978-1597494243.
- Cross, M. (2007). *Developer's guide to web application security*. E.U.A.: Ed. Syngress. ISBN-13: 978-1597490610.
- Hope, P. Walther B. (2008). *Web security testing cookbook:Systematic tecniques to find problems fast.* E.U.A.: Ed. O'Reilly Media. ISBN-13: 978-0596514839.
- Scambray, J. Shema, M. (2003). *Hackers de sitios web*. España: Ed. McGrawHill. ISBN-13: 9788448133788.
- Stuttard, D. Pinto, M. (2007). *The web application hacker's handbook:Discovering and exploiting security flaws*. E.U.A.: Ed. Wiley. ISBN-13 978-0470170779.

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA ACADÉMICA

DIRECCIÓN DE EDUCACIÓN SUPERIOR

ACADEMIC UNIT: Escuela Superior de Cómputo.
ACADEMIC PROGRAM: Ingeniería en Sistemas Computacionales
LATERAL OUTPUT: Analista Programador de Sistemas de Información.
FORMATION AREA: Professional.
MODALITY: Presence.

LEARNING UNIT: Web security.
TYPE OF LEARNING UNIT: Theorical - Practical, Optative.
VALIDITY: August, 2011
LEVEL: lll.
CREDITS: 7.5 Tepic, 4.39 SATCA

ACADEMIC AIM

Furthermore, this program allows to develop abilities to identify the most common attacks against web applications and also to design and implement secure web applications. Moreover, it allows acquiring some other abilities like creative and strategic thought, assertive communication, collaborative work, student's participation.

This unit has the units Network applications, Web technologies and Database management as antecedents. The consequent units are Terminal Work I and II.

AIM OF THE LEARNING UNIT:

The student develops secure web applications, through the detection of vulnerabilities, the application of defense mechanisms and protection techniques against common threats.

CREDITS HOURS

THEORETICAL CREDITS / WEEK: 3.0

PRACTICAL CREDITS / WEEK: 1.5

THEORETICAL HOURS /SEMESTER: 54

PRACTICAL HOURS / SEMESTER: 27

AUTONOMOUS LEARNING HOURS: 54

CREDITS HOURS / SEMESTER: 81

LEARNING UNIT DESIGNED BY:
Academia de Ingeniería de Software.

REVISED BY:
Dr. Flavio Arturo Sánchez Garfias.
Subdirección Académica

APPROVED BY:
Ing. Apolinar Francisco Cruz Lázaro.
Presidente del CTCE

AUTHORIZED BY: Comisión de Programas Académicos del Consejo General Consultivo del IPN

Ing. Rodrigo de Jesús Serrano Domínguez
Secretario Técnico de la Comisión de Programas Académicos

THEMATIC UNIT: I **TITLE:** Input-based attacks

UNIT OF COMPETENCE

The student analyzes web application inputs through the use of tecniques to detect security vulnerabilites.

No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
1.1	Web security threats.	0.5		0.5		2B, 4B,5B,3C
1.2	Detection of security vulnerabilities	1.5	1.5	3.0	3.0	
1.2.1	Web testing proxies					
1.2.2	Vulnerabilitiy Scanners					
1.2.3	Web application security testing.					
1.3	Prevention.	1.5		4.0		
1.3.1	Prevention rules					
1.3.2	Access control					
	Subtotals:	3.5	1.5	7.5	3.0	

TEACHING PRINCIPLES

This Thematic Unit must begin with a framing of the course and the formation of teams. Will be Projects-Based learning strategy, through inductive method, with the techniques of elaboration of charts, technical data and exercise-solving, exhibition in team, practical and production of learning evidence and the accomplishment of a project proposal.

LEARNING EVALUATION

Diagnostic test

Project Portfolio:

Proposal of project	20%
Charts	5%
Report of Practicals	20%
Self-Evaluation Rubric	5%
Cooperative Evaluation Rubrics	5%
Written Learning Evidence	45%

THEMATIC UNIT: II **TITLE:** Injection attacks

UNIT OF COMPETENCE

The student designs protection schemes for databases associated to web applications, through defense mechanisms and data encryption.

No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
2.1 2.1.1 2.2 2.3 2.3.1 2.3.2 2.3.3	Characteristics of an injection attack Risk in using an interpreter Types of injection Mechanisms of protection Defense in depth Encryption Secure key management	0.5 0.5 5.5	0.5 1.5	0.5 0.5 8.0	1.0 6.0	2B,4B,1C
	Subtotals:	6.5	2.0	9.0	7.0	

TEACHING PRINCIPLES

Will be projects-Based learning strategy, trough heuristic method, with the techniques of charts, exercise-solving, cooperative presentation, advance of the project, practical and the production of the learning evidences.

LEARNING EVALUATION

Portfolio of Evidences:

Charts	10%
Report of Practicals	20%
Advance of the Project	20%
Self-Evaluation Rubric	5%
Cooperative Evaluation Rubric	5%
Written Learning Evidence	40%

THEMATIC UNIT: IV **TITLE:** Cross-site scripting

UNIT OF COMPETENCE

The student examines input of web applications, using code review techniques and prevention mechanisms.

No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
3.1 3.1.1 3.1.2 3.2 3.2.1 3.2.2 3.2.3	Description of XSS attack. Untrusted data Types of XSS. Defense mechanisms Escaping Prevention of XSS attacks Code review techniques	1.5 4.0	0.5 0.5	3.0 6.0	2.5 2.5	1B,3B,4B
	Subtotals:	5.5	1.0	9.0	5.0	

TEACHING PRINCIPLES

Will be projects-Based learning strategy, trough inductive and heuristic methods, with the techniques of elaboration of exercise-solving, cooperative presentation, practical and learning evidence, the production of the learning evidences and advance of the project.

LEARNING EVALUATION

Project Portfolio:

Charts	5%
Development of complementary themes	20%
Report of Practicals	20%
Advance of the Project	20%
Self-Evaluation Rubric	5%
Cooperative Evaluation Rubric	5%
Written Learning Evidence of Learning	25%

THEMATIC UNIT: IV **TITLE:** Authentication

UNIT OF COMPETENCE

The student manages properly the authentication mechanisms for web applications, through secure criteria for authentication.

No.	CONTENTS	Teacher led-instruction HOURS		Autonomous Learning HOURS		REFERENCES KEY
		T	P	T	P	
4.1	Authentication attacks	2.0	0.5	2.0	1.0	2B,3B,4B,5B,3C
4.1.1	Bad passwords					
4.2	Secure mechanisms of authentication.	1.5		1.5	3.0	
4.2.1	Securing passwords					
4.2.2	CAPTCHAs					
4.3	SSL	0.5		1.5		
4.4	Session management	0.5	0.5	1.0	2.5	
4.5	Web application firewalls	1.5		1.0		
4.5.1	Configuration					
	Subtotals:	6.0	1.0	7.0	6.5	

TEACHING PRINCIPLES

Will be projects-Based learning strategy, trough inductive and heuristic methods, with the techniques of cooperative presentation, practical, the production of the learning evidences and the presentation of the final project.

LEARNING EVALUATION

Project Portfolio:

Charts	5%
Technical data	5%
Cooperative Presentation	10%
Report of Practicals	20%
Final Project	40%
Self-Evaluation Rubric	5%
Cooperative Evaluation Rubric	5%
Written learning Evidence	10%

RECORD OF PRACTICALS

No.	NAME OF THE PRACTICAL	THEMATIC UNITS	DURATION	ACCOMPLISHMENT LOCATION
1.	Detection of vulnerabilities.	I	1.5	Computer Labs.
2.	Using a testing proxy.	I	1.5	
3.	Evaluating an application web using a scanner.	I	1.5	
4.	Injection attacks.	II	1.5	
5.	Applying defense mechanisms against injection attacks.	II	3.0	
6.	Encrypting sensitive data.	II	3.0	
7.	Secure key management.	II	1.5	
8.	XSS attack.	III	3.0	
9.	Code review of a web application.	III	3.0	
10.	Breaking passwords.	IV	1.5	
11.	Securing passwords	IV	3.0	
12.	Configuration of web application firewall	IV	3.0	
		TOTAL OF HOURS	27.0	

EVALUATION AND PASSING REQUIREMENTS:

The practicals are considered mandatory to pass this learning unit.
The practical worth 20% in each thematic unit.

PERIOD	UNIT	EVALUATION TERMS
1 2 3	I II III IV	Continuous evaluation 55% and written learning evidence 45% Continuous evaluation 60% and written learning evidence 40% Continuous evaluation 75% and written learning evidence 25% Continuous evaluation 90% and written learning evidence 10% The learning unit I is 20% worth of the final score The learning unit II is 20% worth of the final score The learning unit I is 20% worth of the final score The learning unit I is 40% worth of the final score Other means to pass this Learning Unit: • Evaluation of acknowledges previously acquired, with base in the issues defined by the academy. • Official recognition by either another IPN Academic Unit of the IPN or by a national or international external academic institution besides IPN. If accredited by Special Assessment or a certificate of proficiency, it will be based on guidelines established by the academy on a previous meeting for this purpose.

KEY	B	C	REFERENCES
1		X	Clarke J. (2009). *SQL injection attacks and defense*. E.U.A.: Ed. Syngress. ISBN-13: 978-1597494243.
2	X		Cross, M. (2007). *Developer's guide to web application security*. E.U.A.: Ed. Syngress. ISBN-13: 978-1597490610.
3		X	Hope, P. Walther B. (2008). *Web security testing cookbook:Systematic tecniques to find problems fast.* E.U.A.: Ed. O'Reilly Media. ISBN-13: 978-0596514839.
4	X		Scambray, J. Shema, M. (2003). *Hackers de sitios web*. España: Ed. McGrawHill. ISBN-13: 9788448133788.
5	X		Stuttard, D. Pinto, M. (2007). *The web application hacker's handbook:Discovering and exploiting security flaws*. E.U.A.: Ed. Wiley. ISBN-13 978-0470170779.

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA ACADÉMICA

DIRECCIÓN DE EDUCACIÓN SUPERIOR

TEACHER EDUCATIONAL PROFILE PER LEARNING UNIT

1. GENERAL INFORMATION

ACADEMIC UNIT: Escuela Superior de Cómputo.

ACADEMIC PROGRAM: Ingeniería en Sistemas Computacionales. **LEVEL** III

FORMATION AREA:

Institutional	Basic Scientific	Professional	Terminal and Integration
		■	

ACADEMY: Ingeniería de Software. **LEARNING UNIT:** Web security

SPECIALTY AND ACADEMIC REQUIRED LEVEL: Masters Degree or Doctor in Computer Science.

2. AIM OF THE LEARNING UNIT :
The student develops secure web applications, through the detection of vulnerabilities, the application of defense mechanisms and protection techniques against common threats.

3. PROFESSOR EDUCATIONAL PROFILE:

KNOWLEDGE	PROFESSIONAL EXPERIENCE	ABILITIES	APTITUDES
• Web technologies. • Netwok security. • Web security. • Database management. • Cryptography • Knowledge of the Institutional Educational Model. • English.	• A year in voice and web technologies, network security and cryptography • Actual in educational as facilitator of the knowledge of two years • A year experience in the Institutional Educational Model.	• Analysis and synthesis. • Problems resolution. • Cooperative. • Leadership. • Applications of Institutional Educational Model. • Decision making.	• Responsible. • Tolerant. • Honest. • Respectful. • Collaborative. • Participative. • Interested to learning. • Assertive.

DESIGNED BY	REVISED BY	AUTHORIZED BY
M. en C. Sandra Díaz Santiago COORDINATING PROFESOR	Dr. Flavio Arturo Sánchez Garfias Subdirector Académico	Ing. Apolinar Francisco Cruz Lázaro Director
M. en C. Axel Ernesto Moreno Cervantes. M. en C. Eduardo Rodríguez Aldana. M. en C. Gilberto Sánchez Quintanilla. COLLABORATING PROFESSORS		

Date: 2011