



## Subject Definition document

Subject: Data and Application Security

Subject code: IWB404

### Summary:

The subject approaches the information security subject from application level point of view focusing on the fact that security as the chain is strong as its weakest part.

The nature and diversity and non-standard verbose development methods and techniques used by developers makes application layer one of the most vulnerable targets of attacks.



Main focus of the subject is to give the student an overview about the most common attacks that might affect the web applications trying emphasize the mindset and the process normally used by attackers and commonly used tools to execute those attacks.

The content provides detailed examples to enable student get a full understanding to theory and application.

Additionally, the subject explains briefly the most known effective methods to develop secure applications.

### Outcomes:

	Learning outcomes	Sessions	Assignment	Final Exam
LO1	Understand the application layer security concept and its importance	S1 S2		
LO2	Understand the attack process and attacker mindset	S3 S4 S5		
LO3	Examine the main types of attacks against application, understand related vulnerabilities and requirements and how those attacks are applied along with the used tools	S6 S7-S8 S9-S10		

<b>LO4</b>	Examine some of the main secure application development methodologies	S11 S12		
------------	---	------------	---	---

### Contents:

- Contents represented in the pdf file based on the Book (Web Application security the fast guide Edition 1- 2017 by Dr.Sami khiami)
- Tools and references provided by the tutor as supplementary materials.

### Assessment Criteria and outcomes coverage:

Learning Outcomes	Assessment Criteria and outcomes coverage
<b>LO1</b>	<ol style="list-style-type: none"> <li>1. Define information security and describe layered security model and the role of each layer</li> <li>2. Describe different web technologies used in application layer</li> </ol>
<b>LO2</b>	<ol style="list-style-type: none"> <li>1. Summarize different attack process steps, distinguish various activities applied at each step and explain related tasks</li> <li>2. Explain how different types of attackers thinks and main attackers motives</li> </ol>
<b>LO3</b>	<ol style="list-style-type: none"> <li>1. Explain different types of attacks</li> <li>2. Use the tools effectively to regenerate the attack execution of some of covered attacks</li> </ol>
<b>LO4</b>	<ol style="list-style-type: none"> <li>1. Compare main secure application development methodology</li> </ol>

### Proof generation:

Students of this subject are requested to generate a set of proofs to demonstrate a comprehensive coverage of all learning outcomes. Requested proofs are:

#### Assignment (25%):

In this assignment the main focus is on:

- scenario and assess the students' ability to understand, analyze and detect potential vulnerabilities, map it to related attack.
- Generate a draft document showing an understanding of main secure application development methodologies.

#### Exam (75%):

This proof covers most of the learning objectives with focus on knowledge and comprehension aspects.

## Links:

This subject mainly connected to web application development subject and software and web engineering related subjects as it has main web application focus and includes a set of web development methodologies.

## Resources

- Main subject content on Moodle ( pdf)
- Web application security the fast guide – Book by Dr.Sami khiami 1<sup>st</sup> edition 2017 and book slides.
- related Tools resources
- synchronous and recorded sessions

## Virtual sessions:

Session will be covering the subject using two different approaches:

- discussion to encourage and guide student to develop a full understanding of different concepts
- The practical illustration for some of the main attack scenarios and used tools.

## Suggested Readings:

1. AKAMAI. (2014). *A Guide to multilayer web security*.
2. Bryan Sullivan, V. L. (2012). MC Graw Hill.
3. Chandra, P. *Software Assurance maturity model*.
4. Christian S. Föttinger, W. Z. *Understanding a hacker's mind –A psychological insight into the hijacking of identities*.
5. Dafydd Stuttard, M. P. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second Edition*. 2011: Wiley.
6. Gary McGraw, P. S. *BSIMM7*.
7. JOEL SCAMBRAY, V. L. (2011). *Hacking exposed web application*. MC Graw Hill.
8. Mark Curphey, J. S. (2003). *Improving Web Application Security: Threats and Countermeasures*.
9. OWASP. (2013). *OWASP top 10*.
10. Roger Meyer, C. C. (2008). *Detecting attacks on web application from log files*.
11. sheama, M. (2011). *Web application security for dummies*. Wiley.
12. Tom Brennan, J. J. (2015). *Top 10 Considerations For Incident Response*.
13. Xue, X. L. (2013). *A Survey on Web Application Security*.