Seguridad de Recursos y Aplicaciones Web

1. Welcome

Contact Info

- Prof. Salvador Moreno Picot
  - Office: 2.3.24 at ETSE
  - Tutorial Time:
    - Mondays 14:30-17:30
  - E-mail: salvador.moreno@uv.es

Student Workload

- 3 ECTS
- Attendance workload (24-26 hours)
  - 13 hours – Lectures (6 sessions)
  - 11 hours – Labs (5 sessions)
  - 4 hours – Tutorial Activities
  - 0 hours – Exams
- Non-attendance workload (47-49 hours)
  - 34 hours – Individual Home works *
  - 2 hours – External Activities (1 Seminars)
  - 7-9 hours – Autonomous Work *
  - 6 hours – Preparing Lectures

Contents (30 hours)

- Unit 1. HTTP Security (S1,S2)
- Unit 2. Web Server Security (S3)
- Unit 3. Web Client Security (S4)
- Unit 4. Web Apps Security (S5, S6)
- Unit 5. Web Service Security (S7, S8)
- Unit 6. DB Security (S9)
- Unit 7. Cloud Computing Security (S10, S11)

Evaluation

- 10% -> Continuous Evaluation
  - Regular assistance to lectures (CE)
- 90 % -> Practical Exercises
  - 50% Final Practice (PE_FP) (25 hours)
  - 30% Exercises for all the Units (PE_UE) (9 hours)
  - 10% Problem Resolution (PE_PR) (5 hours)
- **Restrictions:**
  - Both Final Practice and Exercises must be approved to pass this subject

Contents (24-26 hours)

- Unit 1 & Unit 2. HTTP and Web Server Security (S1, S2,S3)
  - *HTTP Protocol
  - HTTP Authentication
    - Basic*, Digest, Client-Cert, eDNI, Form*, Token
  - Exercise 1 (2 hours)
  - Tomcat Authentication
  - User list back-ends
  - Understanding SSL in Tomcat
  - Exercise 2 (2 hour)

- Unit 3. Web Client Security (S4)
  - *Session Hijaking
  - * Cookies,
  - *Insecure Storage
  - * Same Original Policy
  - * Code Signature: Applet, JNLP
  - *Warning: Eval()
  - DOM/XML/JSON Injection
  - Silent Transaction Attack

- Unit 4. Web Apps Security (S5, S6)
  - Single Sing On solutions, Federated Authentication:
    - OpenID, SAML
  - Authorization: XACML, RBAC
  - Controller -> hidden page

- Unit 5. Web Service Security (S7, S8)
  - * SOAP
  - * XML-Encryption + XML-DS
  - * PKI, OCSP, CRL
  - XKMS

- Unit 6. DB Security (S9)
  - Validacion de la Entrada
  - Formularios Web
  - *SQL Injection
  - JDBC over SSL

- Unit 7. Cloud Computing Security (S10, S11)
  - Introduccion a Cloud Computing
  - Introduccion a Authentication en la Nube
  - Introduccion a Authorization en la Nube
  - Introduccion a Encriptacion en la Nube
  - Introduccion a Seguridad Perimetral en la Nube

- http://tomcat.apache.org/tomcat-5.5-doc/config/host.html#Single_Sign_On
- http://en.wikipedia.org/wiki/List_of_single_sign-on_implementations
- http://dacs.dss.ca/, http://www.josso.org/confluence/display/JOSSO1/JOSSO+-+Java+Open+Single+Sign-On+Project+Home