Secure WEB Applications:
Best Practices for Protection and Development
Pontypridd, Wales, 2013

Hans-Joachim Hof
Klaus Köhler
Alexandru Soceanu
Munich University of Applied Sciences
Intensive Programme - Secure WEB Applications: Best Practices for Protection and Development

- **Funding:** Erasmus Intensive Programmes
- **Duration:** September 2011 – August 2013 (1. & 2. year) repeated 2014 if approved (3. year)
- **Website:** [http://web-security.metropolia.fi/teachers/](http://web-security.metropolia.fi/teachers/) for teachers

  - Munich University of Applied Sciences, Germany
  - Frederick University, Cyprus
  - University of Cantabria, Spain
  - Helsinki Metropolia University of Applied Sciences, Finland
  - University of Glamorgan, United Kingdom
  - University of Padova, Italy
Partner Universities

A: Munich
   IP 2012
B: Glamorgan
   Pontypridd
   IP 2013
C: Metropolia
   Helsinki
D: Cantabria
   Santander
   IP 2014
E: Frederick
   Nicosia
F: Padova
Objectives of the Programme

- To improve the quality and to increase the volume of student and teaching staff mobility throughout Europe, so as to contribute to the achievement by 2012 of at least 3 million individual participants in student mobility under the Erasmus programme and its predecessor programmes;
- To improve the quality and to increase the volume of multilateral cooperation between higher education institutions in Europe;
- To increase the degree of transparency and compatibility between higher education and advanced vocational education qualifications gained in Europe;
- To improve the quality and to increase the volume of cooperation between higher education institutions and enterprises;
- To facilitate the development of innovative practices in education and training at tertiary level, and their transfer, including from one participating country to others;
- To support the development of innovative ICT-based content, services, pedagogies and practice for lifelong learning.
Priorities of the Programme

- Focus on “IT-security”, a strategic area of the Information and Communication Technology (ICT).
- Increase the student and teaching staff mobility throughout Europe: 72 EU-students and 20 lecturers from 6 European universities.
- Reinforce the cooperation among universities and IT-security companies.
- Train students to cooperate in international teams and thus gain intercultural social competences.
Contributions to the Priorities

- Encourages students and teachers to work together with their counterparts from different European countries.
- Working in join workshops of students and teachers together will stimulate … a better compatibility and comparability of the systems of higher educations.
- The results of the intensive programme will be available online for all the members and selected partners.
- Online learning environment is used widely throughout the whole intensive programme both for course development and collaboration.
- The intensive programme is the most cost effective method for fostering student and staff mobility ….
- ... promotes … transparency of qualifications and competences and offers curriculum benchmarking for the participating universities.
Contributions to the Priorities (cont.)

- Students will become competent in the selecting of security technologies and methods … and apply these to the development of information systems and to service provisioning. …. 
- Documentation on the methods and techniques as regards methods for project management and information service provisioning, and techniques for information systems development per university including security aspects.
- Documentation on the test case presented as a solution to the cases
- A website containing information on security techniques per university. The developed course material is available online and is shared with by partners and offered to other institutions.
- Number of ECTS = 5. Each of the participating universities will give 5 ECTS point to each student that completes the IP. These points correspond to a workload of 140 hours.
Programme: The Birdseye View

1. Preparatory phase:
   - Application and Selection (November)
   - Recommended Reading (December)
   - Preliminary Exercises (via vhb, December)
   - Assignments of the Preliminary Exercises (February)

2. Course: Pontypridd April 7th – April 20th, 2013
   - Lectures
   - Labs
   - Presentations
   - Exam

3. Evaluation
Where is Pontypridd, Wales, Great Britain?
Programme of Lectures and Other Activities

1. Arrival. Travelling and accommodation arrangements in Cardiff
2. Introduction to IP; Industrial Speaker
   WEB-Application Attacks
3. cont.
4. cont.
5. Develop Secure Network Applications
6. Web Application Integration
7. Social Programme / Free Time
8. Social Programme / Free Time
9. Classical network access attacks
10. Protection of the Applications and of Network Access
11. Biometric protection, Security of e-Health applications
12. Cloud and virtualization Network Security Vulnerabilities
13. Context of IT- Security; Industrial Speaker;
    Exam; Labs and Contest Results.
14. Departure from Cardiff
Didactic Concept

- Bring together 72 students from 6 European countries
- Build 12 teams of 6 students from 6 European universities
- 2-4 professors from each of the 6 European universities teach the subjects they are specialised in

- Morning: lectures
- Afternoon: practical exercises, small projects in groups each team presents its results
- Evening: repetition and preparation for the next day
- Weekends: relax, social programme
Exam

- Preliminary assignment (at home universities): 30% of the grade
- Final exam at the end of the IP weeks (multiple choice): 40% of the grade
- Group assignments (active participation in the daily labs and presentations): 30% of the grade

- The final grade will be represented in percentage and not as a numeric grade.
- Each partner university will convert the percentage grade into their own numeric grade based on their own grading scale.
- The course is considered successfully completed if the student has achieved at least 50% in all of the 3 parts listed above.
Duties and Reward

Prerequisites

- At least basic knowledge in computer networks, IT-security, and software development of WEB applications, Java
- Ability to communicate verbally and to write effectively in English
- Open-minded for new experiences in an international setting
- Ready to work hard in a heterogeneous team

ECTS Recognition

- Course recognized as elective course with lab  
  *(FWP mit Praktikum)*

*Security and Privacy for Internet and Web 2.0*

with 5 ECTS credit points
Flights and Local Traffic

- **Flight tickets** (ordered & paid by students, 90% reimbursed later)
  - Su April 7  *Munich* → *London*  (arrive in London at about *3 p.m.*)
  - Sa April 20  *London* → *Munich*

- **Transfer** (coach or train)
  - Home ↔ Airport *Munich* (paid by students, 90% reimbursed later)
  - London ↔ Hostel in Cardiff
    by coach: organised and paid by project,
    or by train: paid by students, 90% reimbursed later

- **Local Traffic** (paid by students)
  - Cardiff ↔ Pontypridd (~ 6 €/day/student for local train or coach)
  - Free time in Cardiff

- **Limit**: 220 € for flight and transfer (~64€) ⇒ book early
Accommodation and Subsistence

- **Accommodation**
  Probably 2 simple Hotels in Cardiff (2 beds, en-suite, breakfast) in walking distance from train station

- **Subsistence**
  - 28.60 € / day paid by project, rest by students (max. 50 € for 2 weeks)
  - Lunch and dinner paid by students

- **Excursions, Social Programme**
  - 75 € paid by students

- **Hot Nights** in Cardiff (paid by students 😞)
Preparation for the IP

- Open Web Application Security Project
  https://www.owasp.org
- OWASP Top 10 Web Application Security Risks
- OWASP Appsec Tutorial Series on YouTube
  http://www.youtube.com/watch?v=CDbWvEwBBxo
- Hacking-Lab
  https://www.hacking-lab.com/
- OWASP ESAPI: web application security control library
  http://code.google.com/p/owasp-esapi-java/
- Google: Web Application Exploits and Defenses
  http://google-gruyere.appspot.com/
- Haking, IT Security Magazin
  http://de.hakin9.org/