

Paweł Rajba

pawel@cs.uni.wroc.pl

<http://itcourses.eu/>

Application Security Outline

Outline

- Introduction into topic
 - Information security basics
 - Cryptography in .NET
- OWASP Top 10, CWE Top 25
 - Review
 - Samples
- Certificates
 - SSL, PKI, CA
 - Qualified signatures, role of the National Certificate Center (NCC)
 - Use cases and software

Outline

- Identity and Access Management
 - Terminology, concepts, challenges
 - Different types, e.g. challenge response, certificates
 - Role of Active Directory
 - Protocols NTLM & Kerberos
 - More complex scenarios
 - Securing Web Services (RPC, REST) including WS-* specs
 - Identity Federation and authorization delegation
 - OAuth2, OpenID Connect, SAML2 and XACML
 - Integration with other services, e.g. FB, Google...

Outline

- Database layer
 - Secure communication with a database
 - Security in a database server (demo on SQL Server)
- Client-centric applications
 - Review of main types (SPA, desktop, mobile)
 - Review of challenges including offline mode
 - Signing code, obfuscation & deobfuscation
- Infrastructure Security
 - Review of main security components (FW, IDS/IPS, WAF,..)
 - Application Servers
 - Monitoring, SIEM function

Outline

- Security Architecture
 - Requirements and why are they important?
 - Review of security principles from different orgs.
 - Defence in depth in details
 - Architecture layers and the traceability
 - Risk-based approach
- Threat modeling
 - The process and the goals
 - STRIDE method and tools support
 - Risk assessment and methodologies
 - DREAD, CVSS, etc.

Outline

- Security tests
 - Type of tests: black box, grey box, white box
 - Penetration tests, vulnerability assessments
 - Tools and possibilities
 - Market standards, e.g. ASVS
 - Ethical hacking introduction
- Security Development Lifecycle (SDLC)
 - The process, stages overview
 - Market standards, e.g. Microsoft SDL, OpenSAMM
 - Documentation