Paweł Rajba
pawel@ii.uni.wroc.pl
http://kursy24.eu/

Application Security Outline

Outline

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

Outline

- Authentication & authorization
  - Solutions in .NET
  - Different types, e.g. challenge response, certificates
  - Role of Active Directory
  - Protocols NTLM & Kerberos
- Securing Web Services
  - WS-* specifications
  - A&A in different architectural styles
    - SOAP RPC, RESTful

Outline

- Security Architecture
  - Security components, access model (e.g. RBAC)
- Integration with external providers
  - Facebook, Google, Azure, SMS, Payment services
- Signing code, obfuscation & deobfuscation
  - Methods and tools
  - Benefits
- Database layer
  - Secure communication with a database
  - Security in a database server

Outline

- Mobile security
  - Security architecture
  - Security of data, communication, application itself
  - Considered platforms: Android, iOS (maybe)
- Infrastructure security
  - Application servers
  - Security zones
  - IDS, IPS, WAF software

Outline

- Security tests
  - Type of tests: black box, grey box, white box
  - Penetration tests, vulnerability assessments
  - Tools and possibilities
- Security in SDLC
  - The process, stages overview
  - Description of activities in early stages
    - Gathering requirements
    - Risk analysis
    - Threat modelling

Tools

- Fiddler
  - http://www.telerik.com/fiddler
- Web Scarab
  - https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- Postman – REST Client
  - http://www.getpostman.com/
- OWASP Mantra
  - http://www.getmantra.com/