Web Application Security

Syllabus 2014-15

1. The Owasp project

- introduction to web applications security
- threats and OWASP principles
- introduction to secure design

2. Web server

- introduction to a secure set-up of Apache
- firewalling a web server

3. Browser

- general concepts, functionalities, browsers war
- configuration (HTTP-cookies, contents, scripting, etc.)
- attack to browsers and users tracking/profiling (third party cookies, supercookies, XSS, CSFR, command injection)
- browser security (add-ons, plugins, same-origin policy etc.) and secure browsing

4. Privacy preserving

- attacks to privacy (spyware and backdoors, browser, email etc.)
- tracking techniques (HTTP-cookies, third party cookies, browser fingerprinting, CSP)
- advanced browser configuration
- anonymity and onion routing (Tor)

5. Internet E-Mail

- architecture and infrastructure, functions, agents and standards
- MIME and PGP
- phishing, spamming & spoofing, DKIM, SPF
- introduction to email forensics