Course description

Security in web development is designed to give the students an idea of some of the challenges that web developers face when implementing web applications. It also gives some suggestions on how to handle these challenges, and what to be especially aware of.

Learning Goals

- Understand basic web application security concepts
- Understand how hackers exploit web applications
- Understand the principle of layered security
- Spot potential security flaws in web applications
- Use best practice on some web security challenges

Content

- Hacking in general
  - History, cases, vulnerability info etc
- Basic Applied Cryptography
  - Symmetric and asymmetric encryption
  - TLS (create certificate and install it on server)
  - Hashing and salting
- Security principles, least privilege etc.
- Security touchpoints

Content

- Attack patterns
  - SQL injection, XSS, XXE, XSRF, Client side manipulation, Session hijacking, DoS, DDoS
- Linux security
  - Basic CLI (folders, privileges), basic firewall (iptables/ufw), basic servers (SSH, Apache, MySQL, Nginx)
  - Server security settings (Apache, PHP)

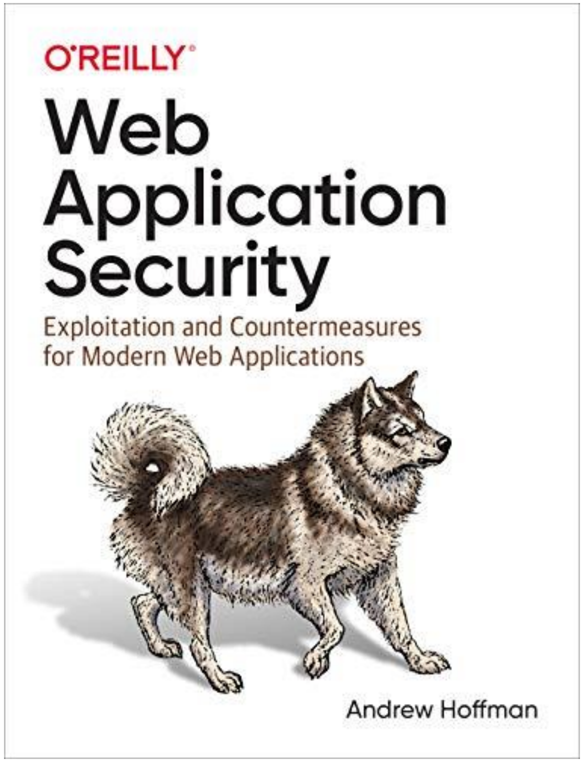
Exam Project

- You will work in groups
- Build a simple and secure web application, using the “security toolbox” you have obtained.
- Deploy it on a live environment
- Penetration test the other groups web applications

Literature

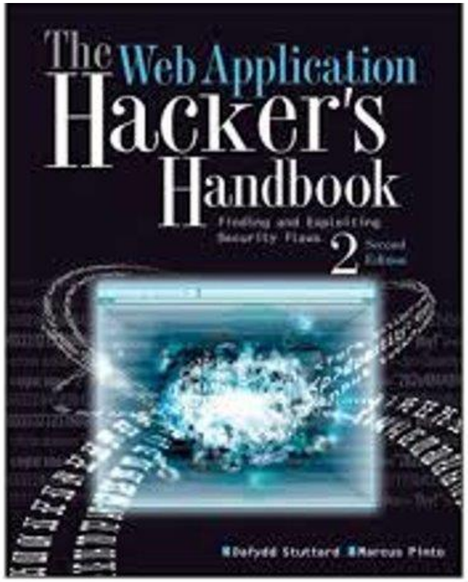
Primary book

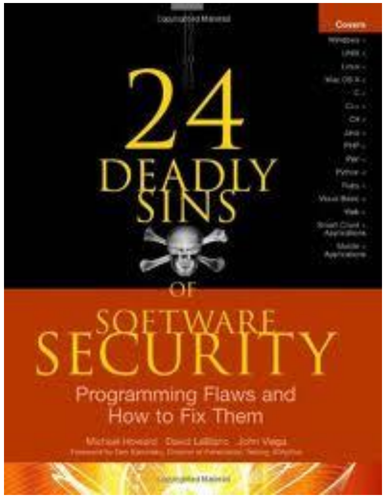
- Web Application Security, Andrew Hoffman, 2020, ISBN: 9781492053118


O'REILLY
Web Application Security
Exploitation and Countermeasures for Modern Web Applications
Andrew Hoffman

More literature

Other books of interest (Not mandatory)
The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (second edition)
Dafydd Stuttard and Marcus Pinto Wiley 2011


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard Marcus Pinto


Covers
24 DEADLY SINS OF SOFTWARE SECURITY
Programming Flaws and How to Fix Them
Michael Howard David LeBlanc John Viega