Welcome to

# Webinar: Opdag sårbarheder – softwaresikkerhed og penetrationstest

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Codeberg https://codeberg.org/kramse/

webinar-sw-and-pentest.tex in the repo security-courses

# Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: xhek@kea.dk Mobile: +45 2026 6000

You are welcome to drop me an email

# Overview Diploma in IT-security

| OBLIGATORISKE MODULER | VALGFRIE MODULER | AFGANGSPROJEKT |
|---|---|---|
| NETVÆRKS- OG KOMMUNIKATIONS-SIKKERHED<br>10 ECTS | VALGFRI | AFGANGSPROJEKT |
| SOFTWARESIKKERHED<br>10 ECTS | | |
| VIDEREGÅENDE SIKKERHED I IT-GOVERNANCE (VIDEREGÅENDE SIKKERHEDSLEDELSE)<br>5 ECTS | –<br>Heraf mindst 10 ECTS fra Diplom i IT-sikkerhed<br>20 ECTS | 15 ECTS |

## Dit og virksomhedens udbytte

Du bliver en medarbejder, der i høj grad er i stand til at analysere, planlægge og vurdere it-sikkerhed i forbindelse med drift, kontrol og udvikling af it-systemer i både private og offentlige virksomheder. Dette på et strategisk, taktisk såvel som operativt niveau på en reflekterende og handlingsorienteret måde.

# Course Data: VF1 Softwaresikkerhed (10 ECTS)

- Slide shows - presentation – like this file and exercise booklet
- Books listed in the lecture plan and here – expect 1.000 - 1.500DKK
- Additional resources from the internet

Teaching dates - fall 2024 17:00 - 20:30 with Henrik Kramselund
29/8, 3/9, 10/9, 12/9, 17/9, 19/8, 24/9, 26/9, 1/10, 3/10, 8/10, 10/10, 22/10, 24/10

Exam: 5/11 2024

Photo by Pawel Janiak on Unsplash

# Course Description: VF1 Softwaresikkerhed (10 ECTS)

Indhold
Modulet fokuserer på sikkerhedsperspektivet i software, blandt andet programkvalitet og fejlhåndterings samt datahåndterings betydning for en software arkitekturs sårbarheder. Elementet introducerer også til forskellige designprincipper, herunder "security by design".

**Læringsmål**
Viden – Den studerende har viden om og forståelse for:

- Hvilken betydning programkvalitet har for it-sikkerhed ift.:
- Trusler mod software
- Kriterier for programkvalitet
- Fejlhåndtering i programmer
- Forståelse for security design principles, herunder:
- security by design

- privacy by design.

Færdigheder – Den studerende kan:

- Tage højde for sikkerhedsaspekter ved at:
- Programmere håndtering af forventede og uventede fejl
- Definere lovlige og ikke-lovlige input data, bl.a. til test
- Bruge et Application Programming Interface (API) og/eller standard biblioteker
- Opdage og forhindre sårbarheder i programkoder
- Sikkerhedsvurdere et givet software arkitektur.

Kompetencer – Den studerende kan:

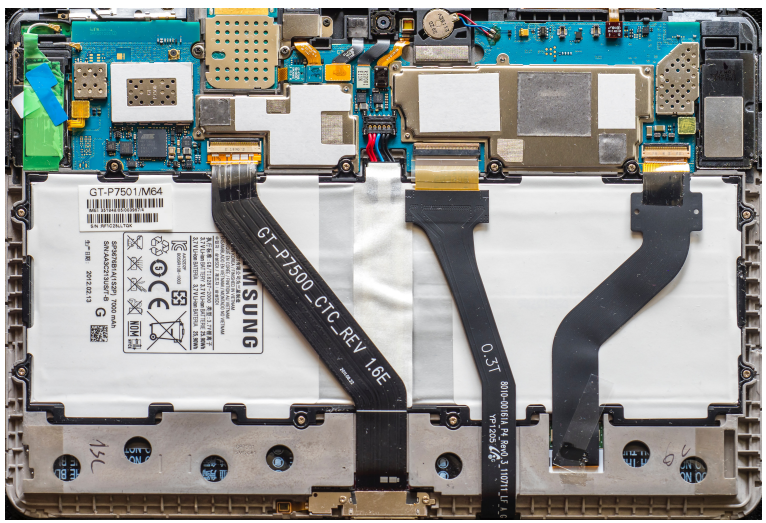
- Håndtere risikovurdering af programkode for sårbarheder.
- Håndtere udvalgte krypteringstiltag.

## Some keywords relating to this course

Buffer overflow Common Vulnerabilities and Exposures (CVE)
String handling Format String C code buffers shell code
Common Vulnerability Scoring System (CVSS) Unicode frameworks
Address space layout randomization (ASLR) libraries input validation
Common Weakness Enumeration (CWE) Stack protection
Static and dynamic application security testing
Software composition analysis fuzzing design and testing
Web Security and Defense secure software development

- Lots of new terms, technologies and tools

# What is Infrastructure – Software




- Enterprises today have a lot of computing systems supporting the business needs
- These are very diverse and often discrete systems

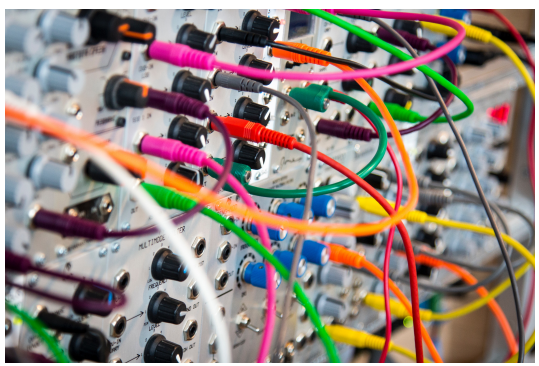
Photo by Alexander Schimmeck on Unsplash

# Business Challenges


- Accumulation of software
- Legacy systems
- Partners
- Various types of data
- Employee churn, replacement

Photo by Adam Bignell on Unsplash

# Software Challenges



- Complexity
- Various languages
- Various programming paradigms, client server, monolith, Model View Controller
- Conflicting data types and available structures
- Steam train vs electric train

Photo by John Barkiple on Unsplash

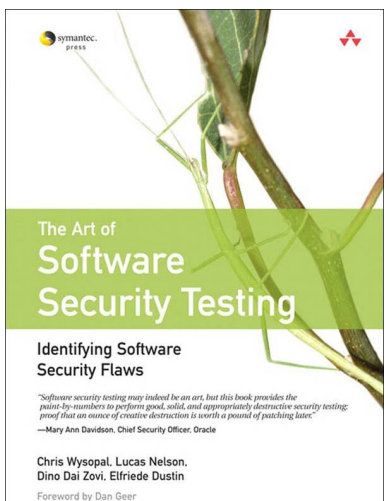
# Primary literature

Primary literature:

Free graphics by Lumen Design Studio

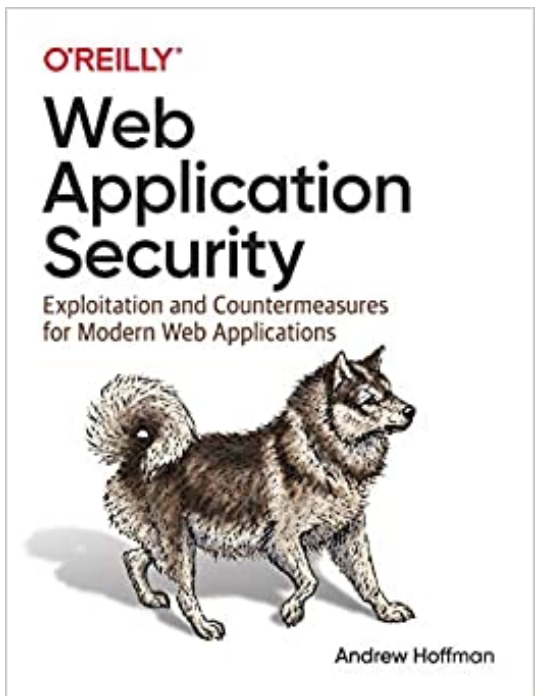
- *The Art of Software Security Testing Identifying Software Security Flaws*, Chris Wysopal, ISBN: 9780321304865, AoST or the Green Book
- *Web Application Security*, Andrew Hoffman, 2020, ISBN: 9781492053118 called WAS
- Pwning OWASP Juice Shop Official companion guide to the OWASP Juice Shop Can be found online for free, but recommend buying the PDF from https://leanpub.com/juice-shop - suggested price USD 5.99

# Book: The Art of Software Security Testing



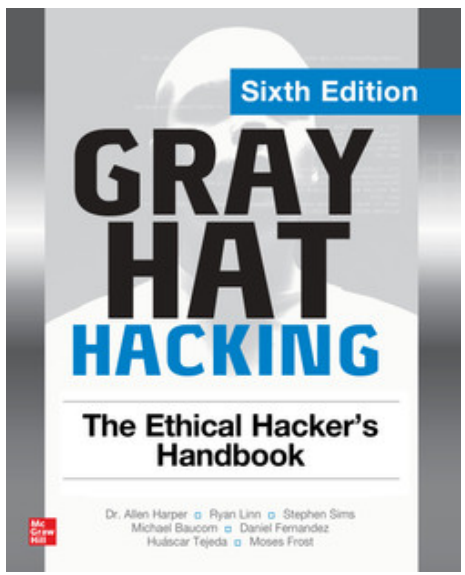

*The Art of Software Security Testing Identifying Software Security Flaws*
Chris Wysopal ISBN: 9780321304865, AoST or the Green Book

# Web Application Security




*Web Application Security*, Andrew Hoffman, 2020, ISBN: 9781492053118 called WAS

# Book: Gray Hat Hacking (Grayhat)

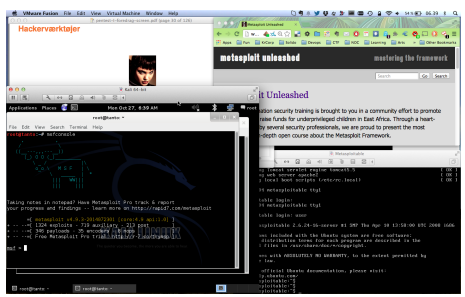



*Gray Hat Hacking: The Ethical Hacker's Handbook*, sixth edition by Allen Harper, Ryan Linn, Stephen Sims, Michael Baucom, Huascar Tejeda, Daniel Fernandez, Moses Frost, Published: March 2022, ISBN: 9781264268955

Note: has some programming introduction which are very useful. Also this book is used in the KEA Network Pentest course

# Exercises: Hackerlab Setup

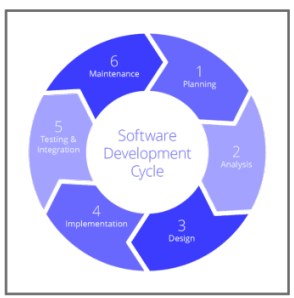
Exercise theme: Virtual Machines allows us play with tech




- Hardware: modern laptop CPU with virtualisation
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Linux server system: Debian amd64 64-bit https://www.debian.org/
- Setup instructions can be found at https://github.com/kramse/kramse-labs

It is enough if these VMs are pr team

# Systems Development Lifecycle (SDLC)



A typical SDLC representation

**The Systems Development Lifecycle (SDLC)** is often depicted as a 6 part cyclical process where every step builds on top of the previous ones. In a similar fashion, security can be embedded in a SDLC by building on top of previous steps with policies, controls, designs, implementations and tests making sure that the product only performs the functions it was designed to and nothing more.

However, modern Agile practitioners often find themselves at an impasse, there is a wealth of competing projects, standards and vendors who all claim to be the best solution in the field.

Source: picture and text from https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdlc/

# Hacking and Intrusion Kill Chains

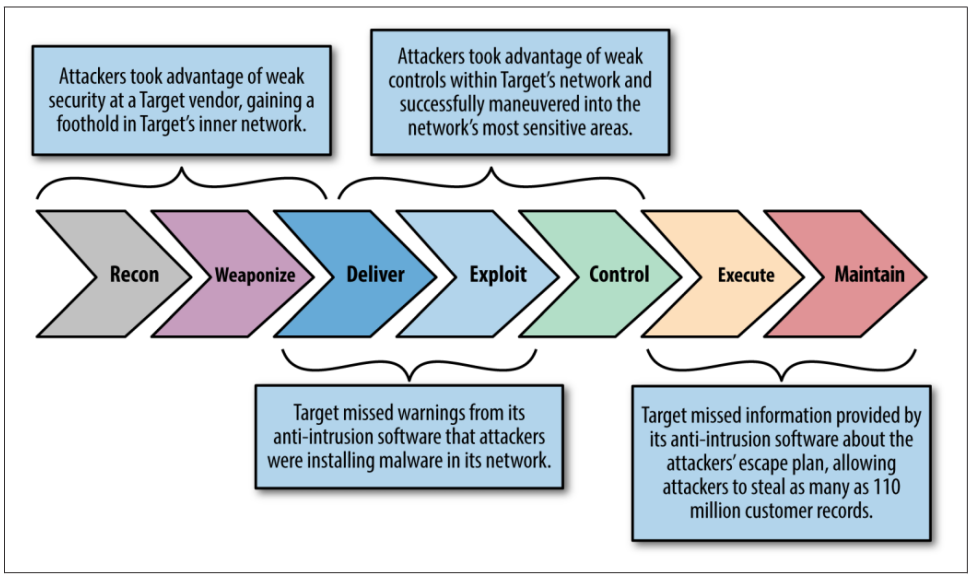



*Figure 7-1. The kill chain*

- See also *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corporation

  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

# OWASP Web Security Testing Guide

> The Web Security Testing Guide (WSTG) Project produces the premier cybersecurity testing resource for web application developers and security professionals.
>
> The WSTG is a comprehensive guide to testing the security of web applications and web services. Created by the collaborative efforts of cybersecurity professionals and dedicated volunteers, the WSTG provides a framework of best practices used by penetration testers and organizations all over the world.

Source: https://owasp.org/www-project-web-security-testing-guide/
and https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

- OWASP Web Security Testing Guide version 4.2 is a 465 page PDF!

# Course Data: Netværkspenetrationstest (5 ECTS)

- Slide shows - presentation – like this file and exercise booklet
- Books listed in the lecture plan and here – expect 1.000 - 1.500DKK
- Additional resources from the internet

Teaching dates - fall 2024 17:00 - 20:30 with Thomas Bach
4/9, 11/9, 25/9, 2/10, 9/10, 23/10, 30/10

Exam: 6/11 2024

Photo by Pawel Janiak on Unsplash

# Course Description: Netværkspenetrationstest (5 ECTS)

Den studerende lærer om hvordan en penetration test udføres, samt kan indhente oplysninger om de seneste sårbarheder, og kan benytte sig af de relevante værktøjer til dette formål.

Viden – Den studerende har viden om og forståelse for:

- Etiske samt kontraktuelle forhold omkring en penetrationstest.
- Standardiseringorganisationers og myndigheders krav til og om penetrationstesting

Færdigheder – Den studerende kan:

Tage højde for sikkerhedsaspekter ved at:

- Anvende relevante metoder ved udførsel af en penetrationstest
- Udarbejde en angrebsplan ud fra indsamlede oplysninger om et mål
- Finde sårbarheder i et givet system
- Dokumentere og rapportere fundne sårbarheder

Kompetencer – Den studerende kan:

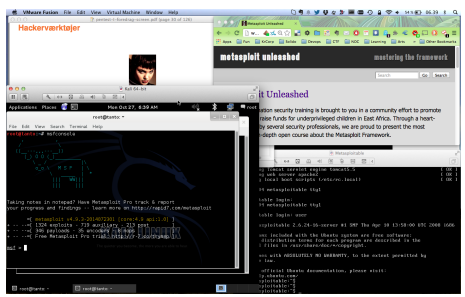
- Planlægge en penetration test, samt eksekvere den både ved brug af værktøjer og manuelt.

## Some keywords relating to this course

Buffer overflow Common Vulnerabilities and Exposures (CVE)
Format String C code buffers shell code
Pentest execution hacker tools discovery tools port scan
Exploits Metasploit Nmap OWASP Security Testing
Common Vulnerability Scoring System (CVSS) brute force
Address space layout randomization (ASLR) password attacks
Common Weakness Enumeration (CWE) Kali Linux
Web Hacking and Attack tools Burp Suite

- Lots of new terms, technologies and tools

# Demo: Hackerlab Setup




- Hardware: modern laptop CPU with virtualisation
  Dont forget to enable hardware virtualisation in the BIOS
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine amd64 64-bit https://www.kali.org/
- Linux server system: Debian amd64 64-bit https://www.debian.org/
- Setup instructions can be found at https://github.com/kramse/kramse-labs

# OWASP Juice Shop Project


We will also use the OWASP Juice Shop Tool Project as a running example. This is an application which is modern AND designed to have security flaws.

Read more about this project at: https://www.owasp.org/index.php/OWASP_Juice_Shop_Project
https://github.com/bkimminich/juice-shop

It is recommended to buy the Pwning OWASP Juice Shop Official companion guide to the OWASP Juice Shop from https://leanpub.com/juice-shop - suggested price USD 5.99

# Questions?

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

You are always welcome to send me questions later via email

Mobile: +45 2026 6000