DVA489 Web Security

CAMPUS AND DISTANCE, HT21

COURSE INFORMATION

DVA489 Web Security

- Welcome to DVA489 Web Security
  - Apologies for the belated start – it was sadly out of my hands
- 7.5 credit course running at 25%
  - Distinct distance flavor – with on campus support (provided covid-19 allows for it)
- Based around a number of web apps, where you
  - First build, then attack and finally protect

Course responsible and examiner

- Daniel Hedin
  - daniel.hedin@mdh.se
- Who am I?
  - Senior lecturer at MDH since 2014, visiting researcher at CTH
  - interest in programming languages and programming language techniques (analyses, compilers, formal languages, language semantics, …)
  - Recent research focus: information flow control for JavaScript
  - https://www.jsflow.net/

Distance and Campus

- DVA489 was originally only taught to industry
  - Essentially designed to be a self study course. Those part remain, but
- The intention was to add campus activities, such as
  - Supervision – individual and in groups, with the possibility to
  - Demonstrate – think of this as a less formal version of a lecture
- However, covid-19 currently prohibits campus activities
  - We will have to make do – initially we try booked supervision, and
  - If that is not enough, we will have to find other ways forward

Canvas and Zoom

- Canvas is the main source of information
  - Empty right now, but I will start publishing course content on Monday, September 13 (the latest)
  - Content will be posted gradually – I'm moving it from another way of hosting to Canvas and will revise the content before adding it
- Zoom will be used for supervision and other online activities
  - We use the same Zoom link for everything

Course Contents

- Part 1: Security Practice, Backend
  - Implementation and attacks with a focus on the web application backend
- Part 2: Security Practice, Frontend
  - Implementation and attacks with a focus on the web application frontend
- Part 3: Information Security
  - Taint Tracking and Information Flow Control

Course Contents – subject to revision

- Part 1: Security Practice, Backend
  - **My first web application: denial of service, reflected XSS**
  - My first authenticated web application: resource theft, password protection, session hijacking
  - My first social media web application: stored XSS, CSRF, Regular Expression DOS
  - My first multi-tiered web application: noSQL injection, Cookie integrity
- Part 2: Security Practice, Frontend
  - Under revision, but things like clickjacking, SOP, CORS, etc.

Will be made available on Monday, September 13

Examination

- 6 + 1 hand ins via Canvas
- 6 web applications plus attacks
  - Unpatched source
  - A description of the attacks in text – no demands on the quality of text as long as it can be understood
  - Patched source code
  - Video of you performing the attack
- 1 exercise on taint tracking and IFC (an attack game)

Supervision

- Via email – available to all
- Via Zoom – technically only for the Campus instance of the course
  - The distance instance contains too many participants, but
  - We will try things out to see how they work out

- Guaranteed time slots – Campus Course
  - Thursdays, 10.00 – 12.00 in blocks of 30 minutes, HT1 (first autumn period)
  - Wednesdays 13.00 – 15.00 in blocks of 30 minutes, HT2 (second autumn period)
  - Will be made available in the campus instance schedule

- Outside of this is subject to availability – do email me to set up a time slot (both instances)

Literature

- The course uses mostly free resources, but
  - Parts refer to the book ‘The Tangled Web’ by Michal Zalewski
  - It’s a good book, but a bit dated (2011)
  - It’s not mandatory to be able to pass the course

- If I come across something better (well, newer) I’ll let you know.

Development Platform

Unless explicitly told to, of course.

- Basis for all node.js, https://nodejs.org/en/
  - Do not use 3rd party npms – the intention is to get you hands dirty to appreciate the complexity and the why you should always use 3rd party, well-vetted libraries
  - Unless the 3rd party npms are flawed they will most likely block many of the attacks we want to perform
- Suggested editor
  - Visual Studio Code, or JetBrains WebStorm
  - or any other of your choice
- Windows, Mac OS or Linux should be fine
  - I use WSL1 under Windows 10 at the moment – transitioned from Mac for various reasons (WSL2 did have some DNS issues last I tried)

Questions?