CS 410/510: Web Security
Motivation

- Security issues are impacting the real world constantly
  - 2017 Wannacry Ransomware, Stuxnet, Snowden, F-35 fighter, Bangladesh heist, etc.
- Most new apps offered via web
  - Web as a “carrier” protocol for Internet apps
- Exploitation via the web now a common vector
  - SQL injection
  - Cross-site requests
  - Session hijacking
  - Click-jacking
This course

- A quick primer on the web and how it works
- A look at common classes of web vulnerabilities
- Hands-on practice exploiting web vulnerabilities
  - Exercises meant to demonstrate the overall class
  - Help train an adversarial mindset
- Prevention techniques
Based all on CTFs

- “Capture-the-Flag”
  - Sets of challenges used in security competitions
  - Understand and apply specific security concepts to find a hidden flag
  - Used to train a variety of skills (reverse-engineering, exploitation, cryptography etc.)
  - Focus on skill development
  - Puts valuable content in a fun format
- Many CTFs focused on web security due to its importance
- Why build a course on CTFs?
  - Extracurricular CTF not working
  - CTF for credit!
Attendance and participation

- Mandatory
  - Treat classes as practice (e.g. like in sports, music)
  - Attendance taken at the beginning of class
  - Absences impact grade directly
In-class labs and lab notebook

- Flipped Classroom Model Short Video Lectures reviewing an issue in Web Security (approx. 1 hour)
- In-class labs to demonstrate and exploit
  - Can optionally be done in pairs
    - Peer learning
    - Ensure progression
  - Write-ups for each level to be kept in a single lab notebook document turned in at the end of course
    - Grading rubric
      - Number of levels solved
      - Description of vulnerability
      - Description of technique, URL, or script used to exploit vulnerability
      - Description of prevention or other remediation to mitigate threat
- Will require some short Ruby programs
Homework and programs

- To be done individually
  - Homework CTF
    - [http://cs410.oregonctf.org](http://cs410.oregonctf.org)
    - Levels opened up (and closed) as we go along
  - Programming assignments
    - Python programs to programmatically attack web vulnerabilities
    - Assumes knowledge of Python or willingness to learn it on your own
Final project and group CTF

- Chosen from selected PentesterLab exercises
  - Turned in as a screencast walkthrough posted on course channel on MediaSpace (https://media.pdx.edu)
- Grading rubric
  - Exercise difficulty
  - Availability of prior walkthroughs
    - https://www.pentesterlab.com/badges/ctf
  - Clarity and completeness of walkthrough (including setup)
  - Analysis of vulnerability and description of prevention/remediation
- Final exam slot
  - Walkthrough of another group’s final project
Ethics

• You will learn techniques for compromising web systems
• Do *NOT* use them against any site outside of the course web sites unless given permission
• CTFs help you learn and practice security concepts in the form of fun-filled games (without breaking the law)
  • CFAA
Jeff Williams, Dave Wichers (2013)
  - Vulnerabilities ranked based on business risk (likelihood + impact)
Course logistics

- Course site (https://thefengs.com/wuchang/courses/cs410)
- Homework site (http://cs410.oregonctf.org)
- Program submission via D2L (https://d2l.pdx.edu)
- Final project submission via Media Space (https://media.pdx.edu)
- Course discussion on #cs410_510_summer2017 on Slack (https://pdx-CS.slack.com)
- Instructor contact @llawrens on pdx-cs Slack