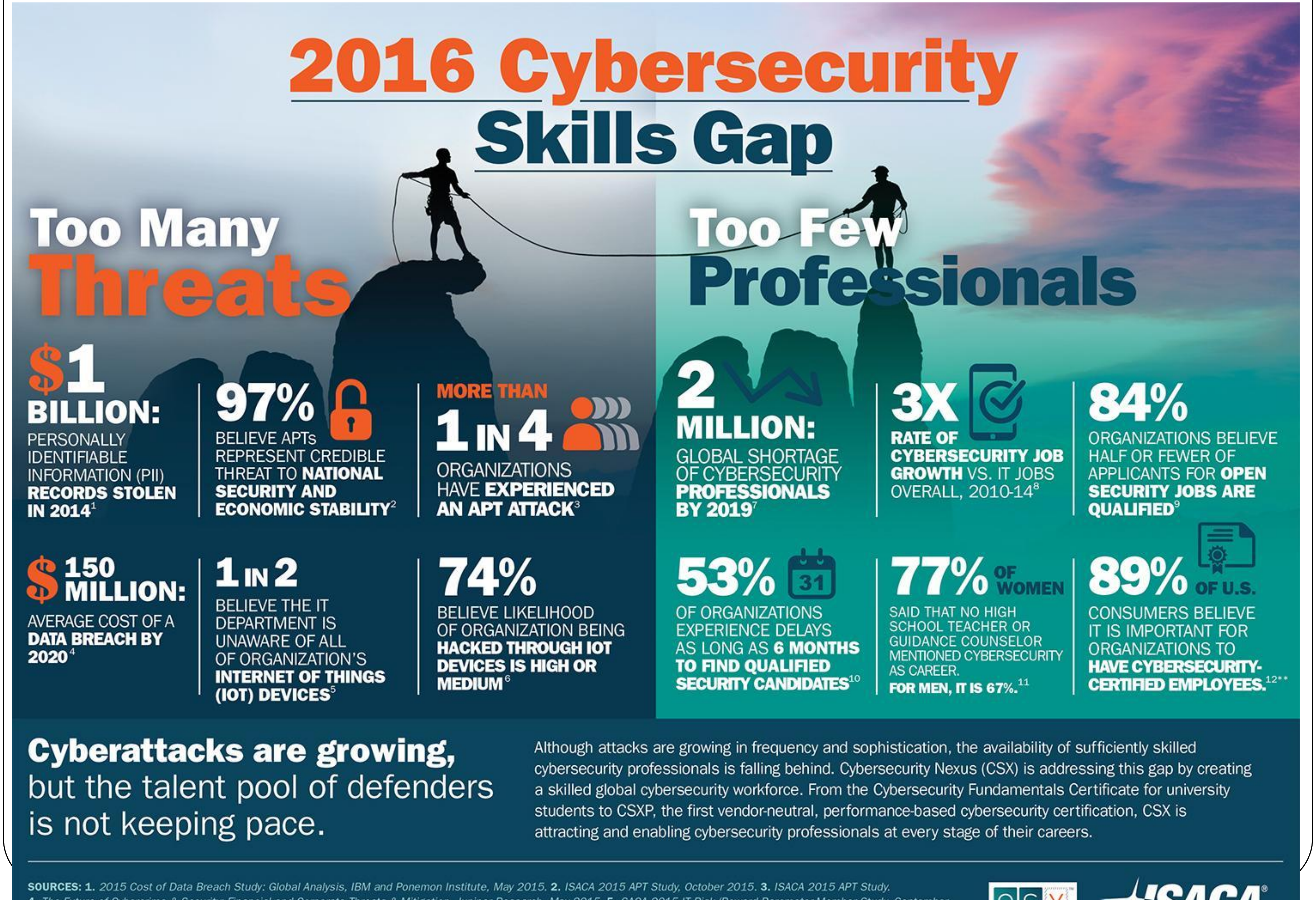
CS 410/510:
Web Security

Motivation

- Security issues are having a real impact
  - 2016 election
  - Stuxnet
  - Snowden
  - F-35 fighter
  - Bangladesh heist

Problem



2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

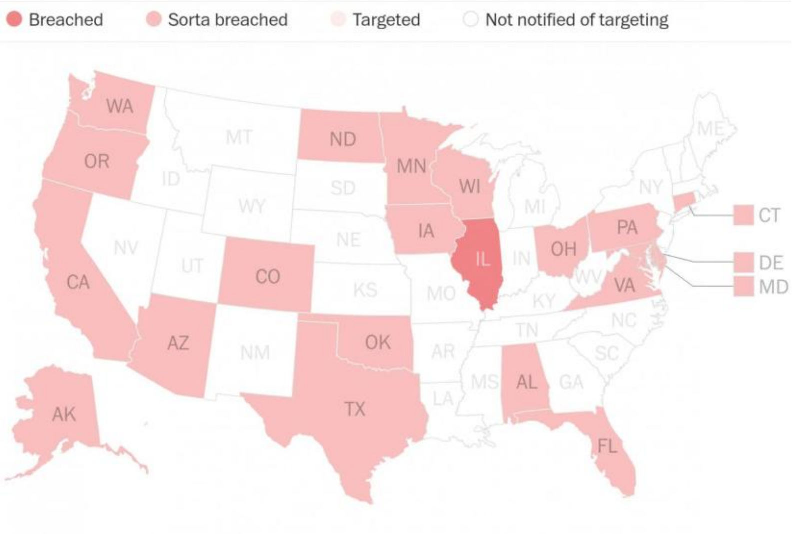
Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, October 2015.* **3.** *ISACA 2015 APT Study.* **4.** *The Future of Cybercrime & Security Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *ISACA 2015 IT Risk/Reward Barometer Member Study, September*

Example: Russian 2016 election hacking

- Influence election via fake news and exposing secrets
- Destroy confidence in the US election system
  - Slow down voting systems used in strategic local election offices
  - Compromise machines used to count votes and register voters
  - https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

States notified by DHS of Russian hacking attempts



Source: News reports and public statements

THE FIX

Future elections

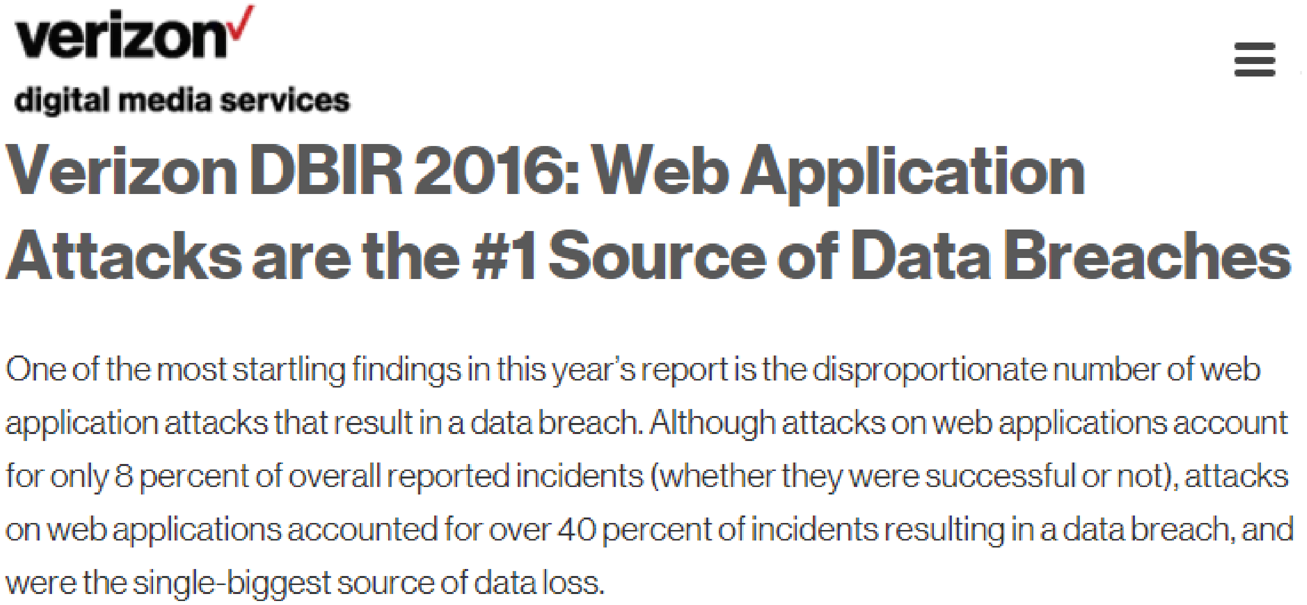
- What should we focus on for 2018?
- Election systems only considered critical infrastructure recently
- Gen. John Allen
  - https://www.lawfareblog.com/lawfare-podcast-brookings-panel-cybersecurity-us-elections

    "As a guy who has spent a lot of time overseas dealing with threats to America, I now recognize at the speed of light, the very heartland of America is under threat today. The enemy has moved beyond my reach. The first line of defense of American democracy and the last line of defense are in our states and counties."

Why web security?

- 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

Why web security?



verizon

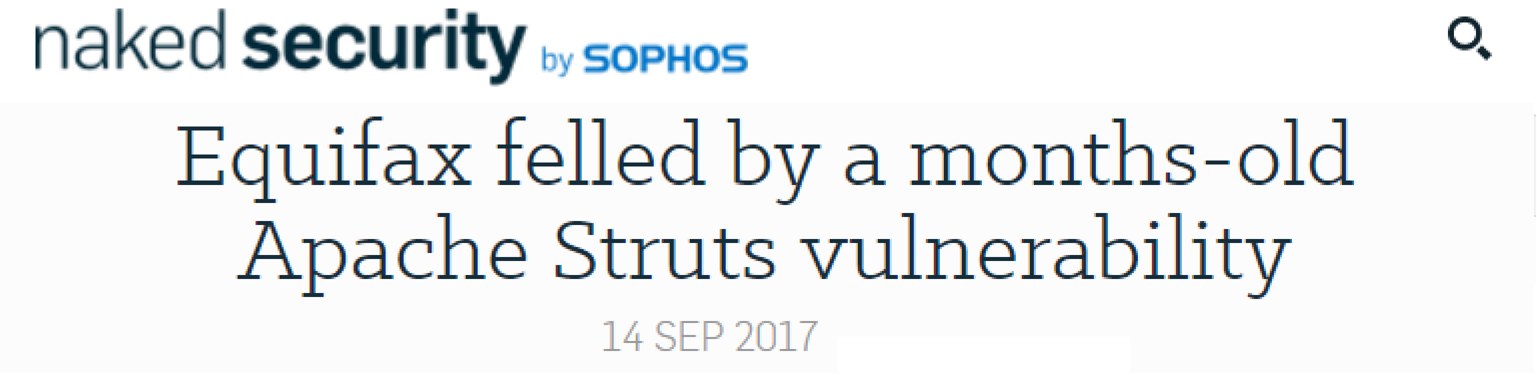
digital media services

Verizon DBIR 2016: Web Application Attacks are the #1 Source of Data Breaches

One of the most startling findings in this year's report is the disproportionate number of web application attacks that result in a data breach. Although attacks on web applications account for only 8 percent of overall reported incidents (whether they were successful or not), attacks on web applications accounted for over 40 percent of incidents resulting in a data breach, and were the single-biggest source of data loss.

https://www.owasp.org/index.php/OWASP_Portland_2017_Training_Day
https://www.eventbrite.com/e/portland-owasp-training-day-2017-tickets-37297273148
https://bsidespdx.org/

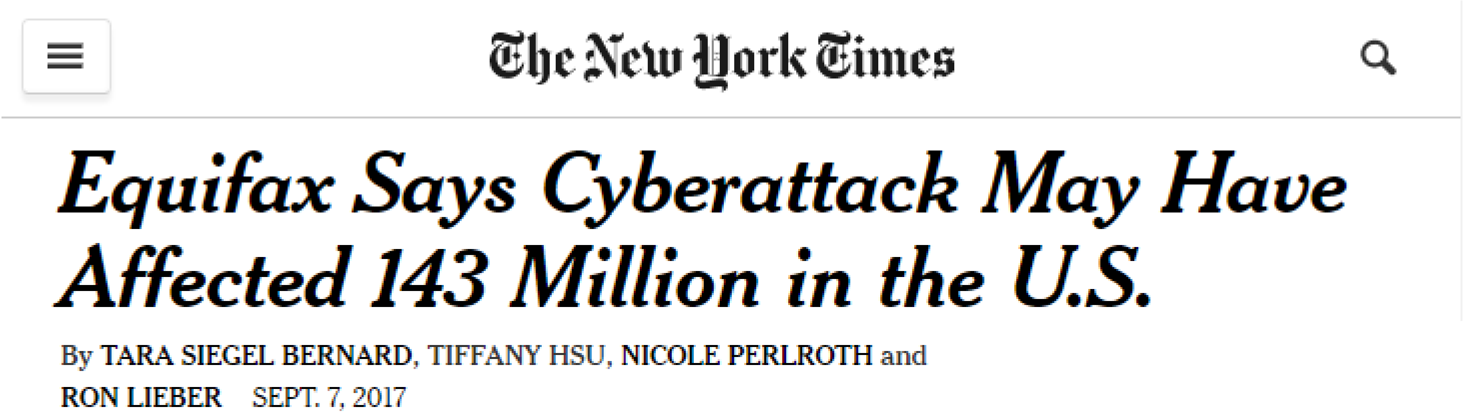
Example: Equifax identity dump



naked security by SOPHOS

Equifax felled by a months-old Apache Struts vulnerability

14 SEP 2017



The New York Times

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By TARA SIEGEL BERNARD, TIFFANY HSU, NICOLE PERLROTH and RON LIEBER SEPT. 7, 2017

- A problem you can help fix (after this class)

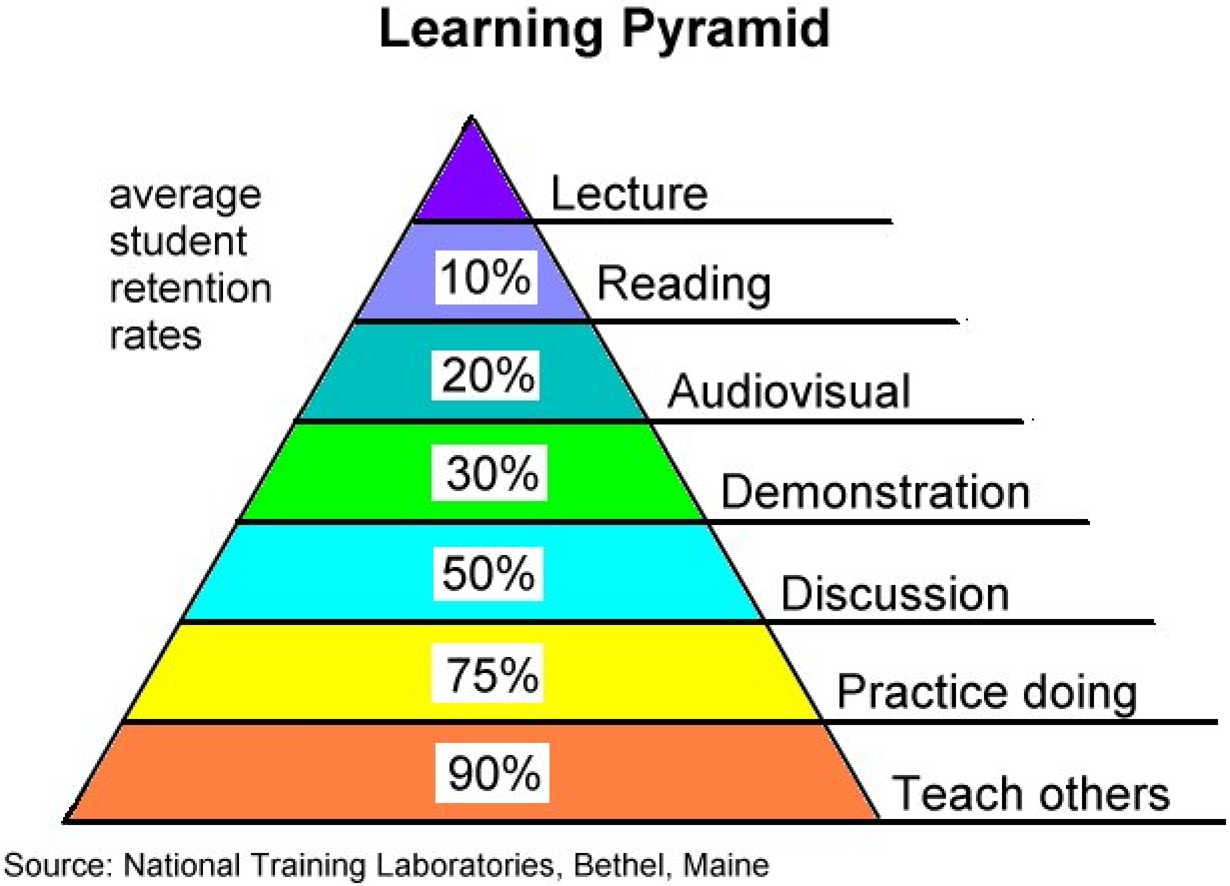
This course

- 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 to demonstrate the overall vulnerability class
  - Help train an adversarial mindset
- Prevention techniques

- Will hopefully be useful at some point in your career

Format

- Lectures followed by labs and homework



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!

In-class labs and lab notebook

- Short lectures reviewing an issue in web security
- 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
  - 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
  - Suggested book: Lubanovic, "Introducing Python"

Final project

- Can optionally be done in pairs
- 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
  - 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

Attendance and participation

- Attendance graded
  - Treat classes as practice (e.g. like in sports, music)
- Special days
  - OWASP workshop
    - https://www.eventbrite.com/e/portland-owasp-training-day-2017-tickets-37297273148
    - You may make-up absences by attending one
    - Turn in your badge for credit
  - Bsides PDX
    - Class exchange for Wednesday, Nov 22nd
    - Attend at least one session on Friday Oct. 20 or Saturday Oct. 21 to replace this class
    - Registration is free at https://bsidespdx.org
    - Turn in your badge for credit

Schedule and Grading

- See web site

Course logistics

- Course site (https://thefengs.com/wuchang/courses/cs410)
  - Schedule
  - Grading
  - Content links
- 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_websecurity on Slack (https://pdx-cs.slack.com)
- Instructor contact @wuchang on pdx-cs Slack
- In-class questions and feedback (anonymous)
  - https://sayat.me/wu4f

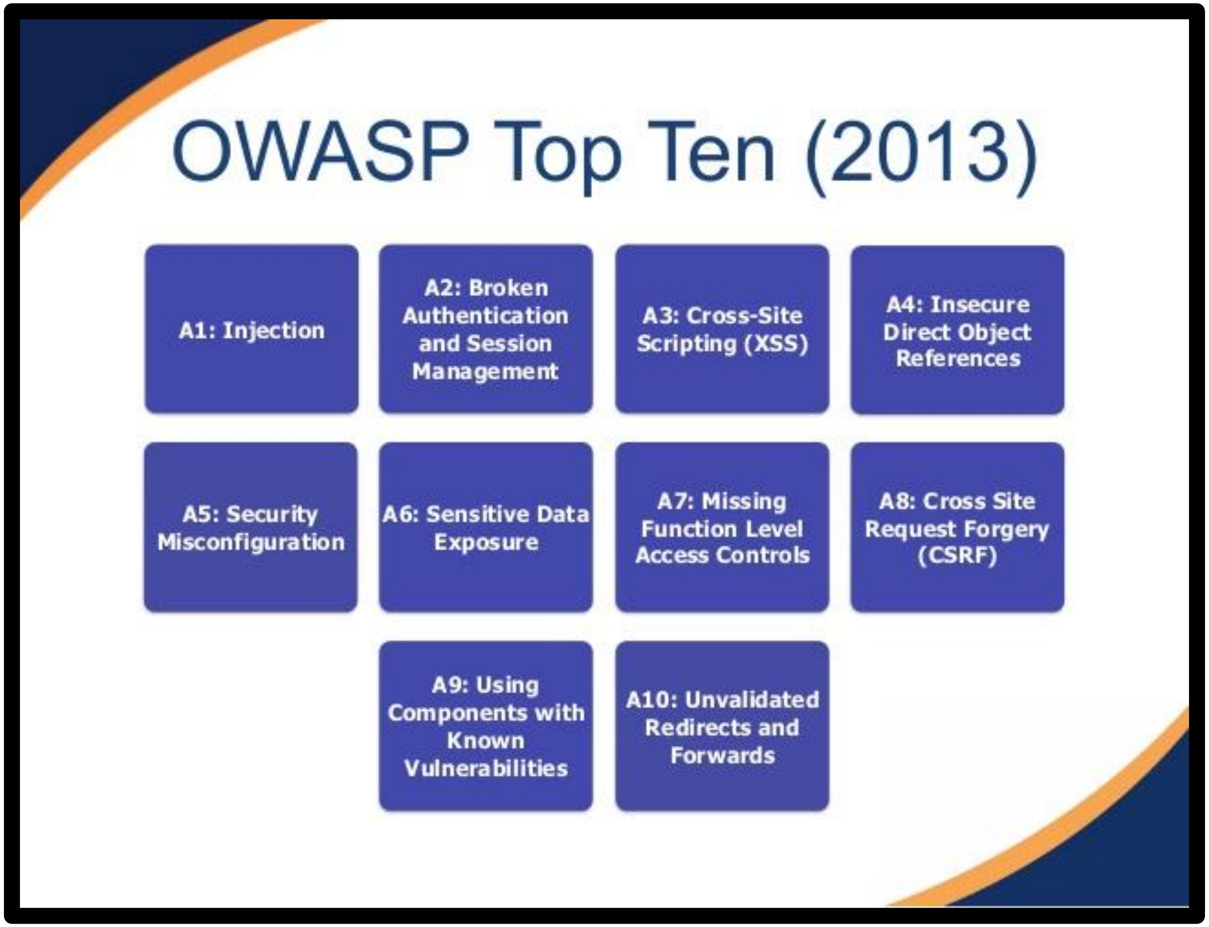
Ethics

- You will learn techniques and tools for compromising web systems
- Do *NOT* use them against any site outside of the course web sites unless given permission
- CTFs and private instances help you learn and practice security concepts (without breaking the law)
    - CFAA

Extra

Preview

- Jeff Williams, Dave Wichers (2013)
  - Vulnerabilities ranked based on business risk (likelihood + impact)



OWASP Top Ten (2013)

- A1: Injection
- A2: Broken Authentication and Session Management
- A3: Cross-Site Scripting (XSS)
- A4: Insecure Direct Object References
- A5: Security Misconfiguration
- A6: Sensitive Data Exposure
- A7: Missing Function Level Access Controls
- A8: Cross Site Request Forgery (CSRF)
- A9: Using Components with Known Vulnerabilities
- A10: Unvalidated Redirects and Forwards