Stanford

CS 253 Web Security

Fall 2019

This course is a comprehensive overview of web security. The goal is to build an understanding of the most common web attacks and their countermeasures. Given the pervasive insecurity of the modern web landscape, there is a pressing need for programmers and system designers improve their understanding of web security issues.

We'll be covering the fundamentals as well as the state-of-the-art in web security.

Topics include: Principles of web security, attacks and countermeasures, the browser security model, web app vulnerabilities, injection, denial-of-service, TLS attacks, privacy, fingerprinting, same-origin policy, cross site scripting, authentication, JavaScript security, emerging threats, defense-in-depth, and techniques for writing secure code. Course projects include writing security exploits, defending insecure web apps, and implementing emerging web standards.

Meeting time and place

Tuesdays and Thursdays, 1:30 PM - 2:50 PM in classroom 380-380Y

Course Staff

Instructor

Feross Aboukhadijeh (feross@cs.stanford.edu)

Teaching Assistant

Esther Goldstein (egolds@stanford.edu)

Office Hours

- Feross: Thursday 3-5pm, Gates 323
- Esther: Monday 3-5pm, Wednesday 3-5pm, Huang Basement

Course Policies

Communication

We will primarily use Piazza for sending out course announcements and answering questions. Please make sure to sign up.

We use Gradescope for assignment submissions. Enroll with the code 97BGZB .

To submit anonymous feedback to us at any point during the quarter, you may use this form.

Prerequisites

CS 142, or an equivalent amount of web development experience, is a prerequisite. You should also be curious about web security and excited to learn clever attacks, defenses, and techniques for writing secure code.

An introductory security course, such as CS 155, is not a formal prerequisite. The material in this course is focused specifically on the web, while CS 155 covers security more broadly.

Attendence

Attendance at lectures is mandatory. Do not enroll in this course if you are taking another course that meets at the same time.

Grading

- Assignments (75%)
- Final Exam (25%)

Each assignment is worth 15%. There is no midterm.

Final Exam

- Tuesday, December 10, 3:30pm - 6:30pm in 200-305

Previous Final Exams

- Final Exam 2019 (Solutions)
- More Sample Final Exam Questions (Solutions)

Collaboration Policy

You may discuss the assignments with other students and you may work together to come up with solutions to the problems. If you do so, you must list the name of your collaborators in the submission. Each student must write up their solutions independently.

Late Submissions

You get three “late days” in total during the quarter. You may use a late day to submit an assignment after the deadline. You can use at most three late days for any single assignment, and you may only use late days in one-day increments (no partial late days).

If you submit an assignment more than 72 hours after the deadline, or if you submit an assignment late after running out of late days, you will receive **no credit** for the submission. Please submit your assignments on time and save your late days for extraordinary situations.

If you have questions about these policies, please ask us.

Schedule

Sep 24: What is Web Security? HTML & JavaScript Review

- Slides
- Video
- Reading
  - Inside look at modern web browser (part 1)
  - Inside look at modern web browser (part 2)
  - Inside look at modern web browser (part 3)
  - A Re-Introduction to JavaScript

Sep 26: HTTP, Cookies, Sessions

- Slides
- Video
- Reading
  - An overview of HTTP
  - HTTP Cookies
  - Skim: HTTP headers

Oct 01: Session Attacks

- Slides
- Video
- Reading
  - SameSite Cookies Explained
  - Incrementally Better Cookies
  - CSRF Is Dead

Oct 03: Cross-Site Request Forgery, Same Origin Policy

- Slides

- Video
- Reading
  - Same Origin policy
  - Cross-Site Request Forgery Prevention

Oct 08: Exceptions to the Same Origin Policy, Cross-Site Script Inclusion

- Slides
- Video

Oct 10: Cross-Site Scripting (XSS)

- Slides
- Video
- Reading
  - Cross Site Scripting Prevention Cheat Sheet
  - XSS Filter Evasion Cheat Sheet

Oct 15: Cross-Site Scripting Defenses

- Slides
- Video
- Reading
  - Reining in the Web with Content Security Policy
  - CSP is Dead: Long Live CSP
  - Trusted Types
  - Sanitising HTML: the DOM clobbering issue

Oct 17: Fingerprinting and Privacy on the Web

- **Guest Lecture by Pete Snyder (Brave Software)**
- Slides
- Video
- Reading
  - Online tracking: A 1-million-site measurement and analysis
  - Most websites don't need to vibrate: A cost-benefit approach to improving browser security
  - Browser Fingerprinting: An Introduction and the Challenges Ahead
  - WebKit Ad Click Attribution
  - Protecting Browser State from Web Privacy Attacks
  - Skim: WebKit Tracking Prevention Policy

Oct 22: Denial-of-service, Phishing, Side Channels

- Slides
- Video
- Reading
  - Alice in Warningland: A Large-Scale Field Study of Browser Security
  - Clickjacking
  - Cross-Origin JavaScript Capability Leaks: Detection, Exploitation, and Defense

Oct 24: Code Injection

- Slides
- Video
- Reading
  - None

Oct 29: Transport Layer Security

- Slides
- Video
- Reading
  - Looking back at the Snowden revelations
  - HTTPS encryption on the web

Oct 31: HTTPS in the Real World: A Spooky Tale

- **Guest Lecture by Emily Stark & Chris Palmer (Google Chrome)**
- Slides
- Video
- Reading
  - DigiNotar on Wikipedia
  - About Public Key Pinning
  - What Is HPKP For?
  - Rolling out Public Key Pinning with HPKP Reporting

Nov 05: Authentication

- Slides
- Video
- Reading
  - Authentication Cheat Sheet

Nov 07: WebAuthn - The future of user authentication on the web 👆

- **Guest Lecture by Lucas Garron (GitHub)**
- Slides
- Video
- Reading
  - Guide to Web Authentication

Nov 12: No class

Nov 14: Managing security concerns in a large Open Source project

- **Guest Lecture by Myles Borins (Node.js technical steering committee, Google)**
- Slides
- Video
- Reading
  - Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript
  - A Roadmap for Node.js Security

Nov 19: Server security, Safe coding practices

- Slides
- Video
- Reading
  - Exploiting Buffer

Nov 21: Local HTTP server security

- Slides
- Video
- Reading
  - None

Dec 03: DNS rebinding attacks

- Slides
- Video
- Reading
  - Millions of Streaming Devices Are Vulnerable to a Retro Web Attack

- Protecting Browsers from DNS Rebinding Attacks

Dec 05: Browser architecture, Writing secure code

- Slides
- Video
- Reading
  - The Security Architecture of the Chromium Browser
  - Cross-Origin Read Blocking (CORB) primer
  - Skim: Cross-Origin Read Blocking (CORB) explainer
  - Backdooring Your JavaScript Using Minifier Bugs
  - I'm harvesting credit card numbers and passwords from your site. Here's how.
  - Major sites running unauthenticated JavaScript on their payment pages

Assignments

Assignment 0 - Web Programming Adventure 🚀

- Assigned: Tuesday, September 24
- Due: Friday, October 4 at 5:00pm

Assignment 1 - Journey to the Dark Side 🎡

- Assigned: Tuesday, October 8
- Due: Friday, October 18 at 5:00pm

Assignment 2 - Oh What a Tangled Web We Weave 🕸

- Assigned: Saturday, October 26
- Due: Thursday, November 7 at 11:59pm

Assignment 3 - See Piazza

- Assigned: Tuesday, November 12
- Due: Friday, November 22 at 5:00pm

Assignment 4 - See Piazza

- Assigned: Mon, November 25
- Due: Friday, December 6 at 5:00pm

Website design by Feross Aboukhadijeh.