```
   _____   ____________     __ __ _________
  /  _/ | / / ____/ __ \   / // /<  / ____/
  / //  |/ / /_  / / / /  / // /_/ /___ \
 _/ // /|  / __/ / /_/ /  /__  __/ /___/ /
/___/_/ |_/_/    \____/     /_/ /_/_____/
```

Web Application Security

Andrew McKenna

Information School
UNIVERSITY of WASHINGTON

BOEING

Security Innovation®
THE SOFTWARE SECURITY COMPANY

No one knows everything. Myself included.

I will be working full time.

WHEN IN DOUBT..

Google™

(c) happii.tumblr.com

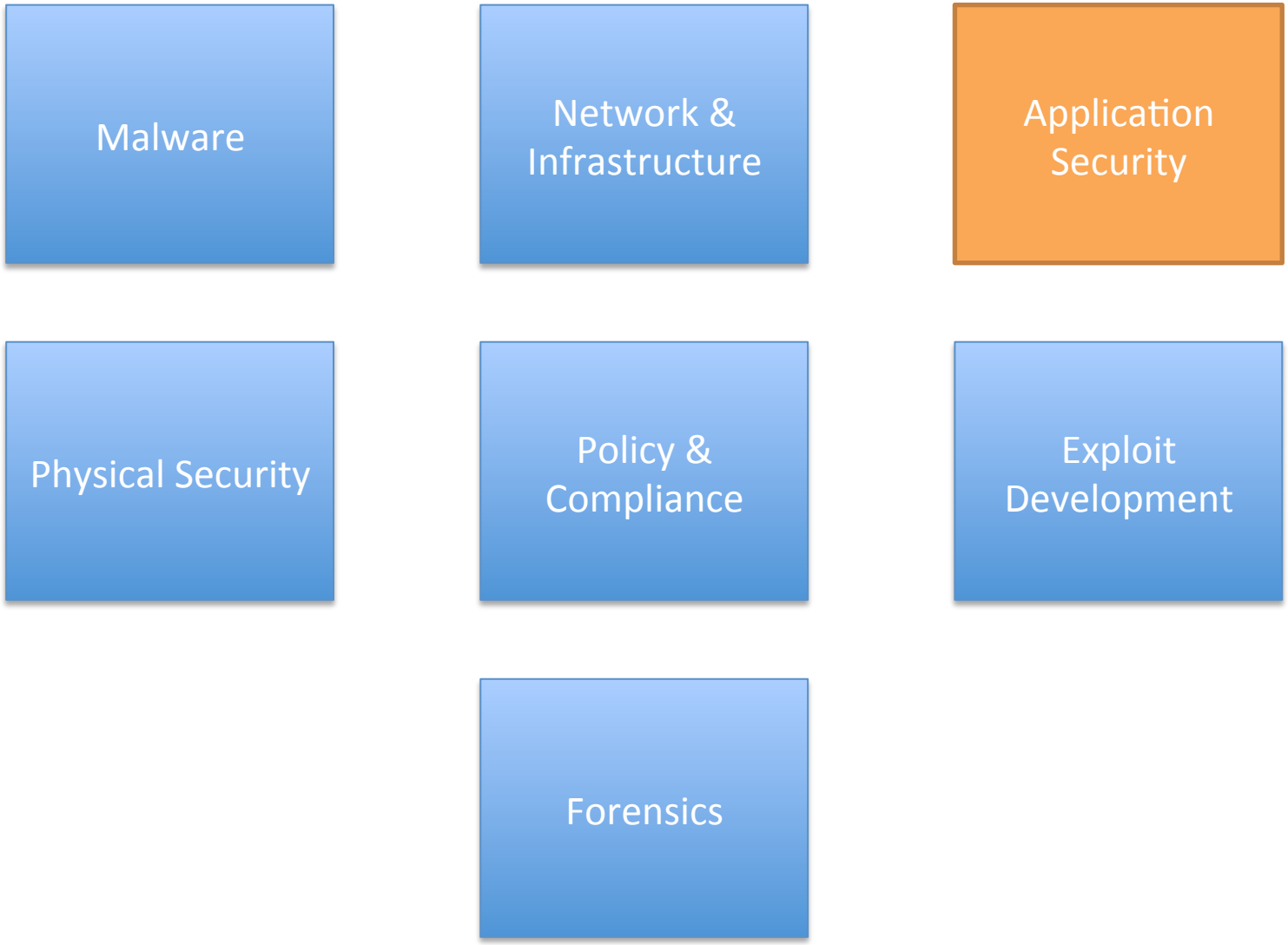
The Class

- Purpose is to both instruct and share knowledge
- We will actually be hacking
- If you have a large influx of projects or exams happening all at once, please let me know
- Late penalty: 10% daily, stops at 50% reduction
- Grading
  - final: 20%
  - hw: 80%
- Criticism is welcome!
- Ask me about unrelated security topics

Github

- We will use github for class materials
- File issues, enhancements, questions
- Use github to build and display your work
- Catalyst to turn in work
- Demo

Where Web Application Security Fits



Sources of Security News & Learning

- Honestly: twitter
- https://reddit.com/netsec
- https://news.ycombinator.com/
- http://www.securitytube.net/
- http://opensecuritytraining.info/Training.html
- https://www.youtube.com/user/DEFCONConference/videos
- https://recon.cx/2014/archive.html
- https://www.alchemistowl.org/pocorgtfo/
- http://magazine.hitb.org/hitb-magazine.html

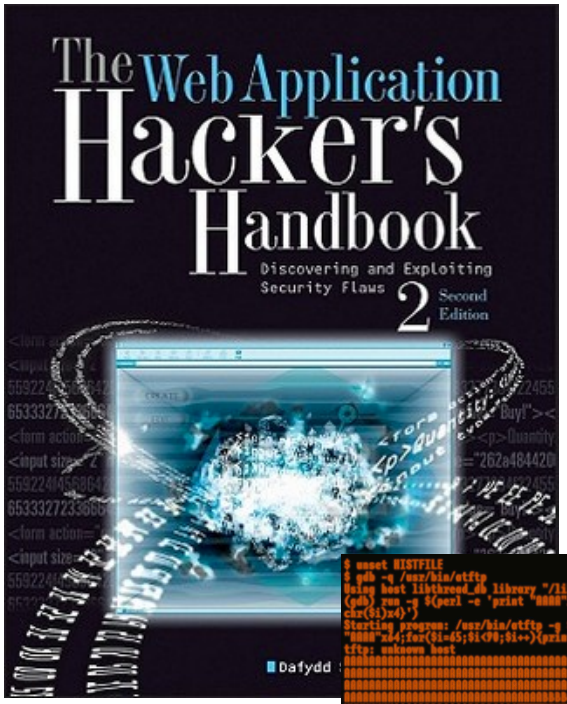
Responsible Disclosure

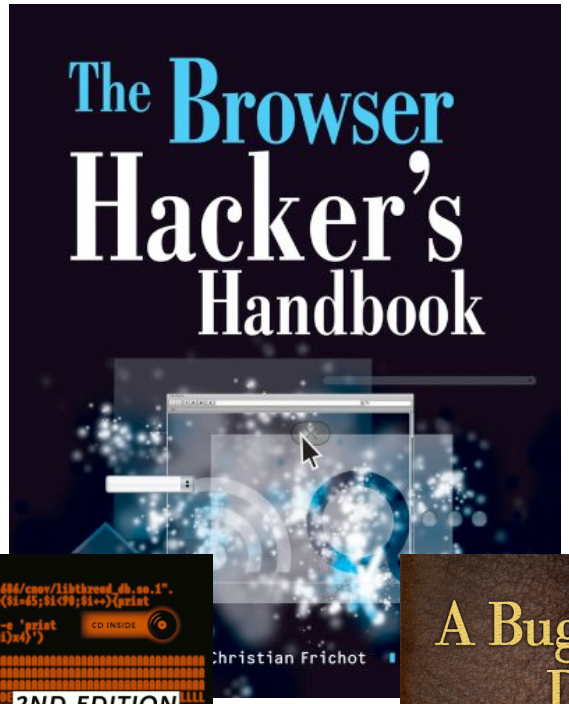
- Absolutely no full disclosure in this class
- Legal quicksand
- Be careful how you find and prove vulnerabilities

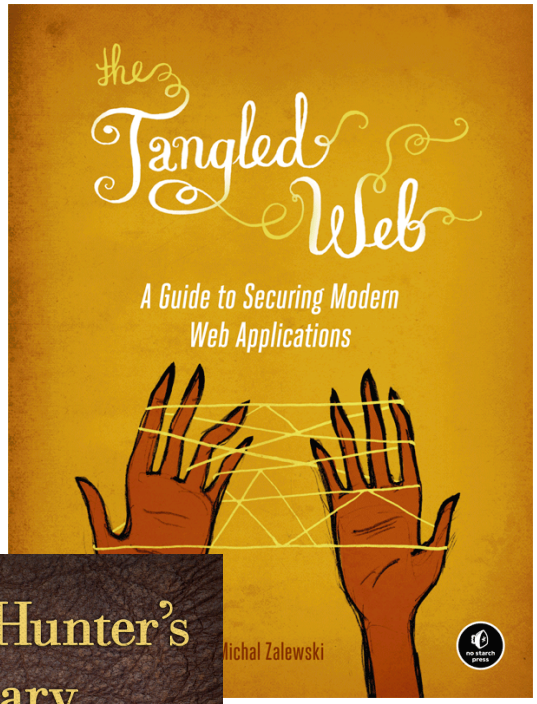
Tips & Tricks

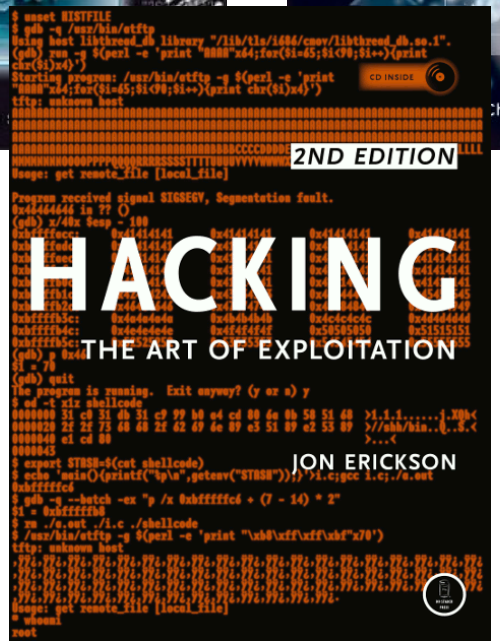
- Stay away from automated tools
- Keep your eyes open
- Send bad input
- Come up with favorite testing payloads
- Develop an "eye" for it

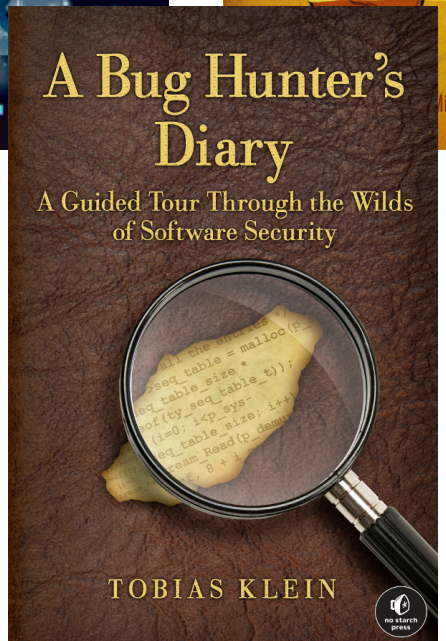
Books


The Web Application
Hacker's
Handbook
Discovering and Exploiting
Security Flaws
2 Second Edition
Dafydd


The Browser
Hacker's
Handbook
Christian Frichot


the Tangled Web
A Guide to Securing Modern
Web Applications
Michal Zalewski


2ND EDITION
HACKING
THE ART OF EXPLOITATION
JON ERICKSON


A Bug Hunter's
Diary
A Guided Tour Through the Wilds
of Software Security
TOBIAS KLEIN