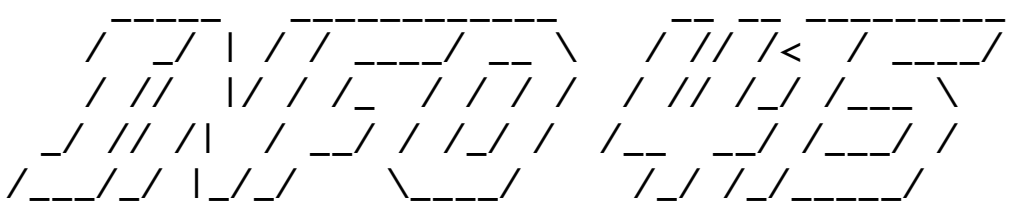


Web Application Security

Andrew McKenna

- @_amckenna

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™

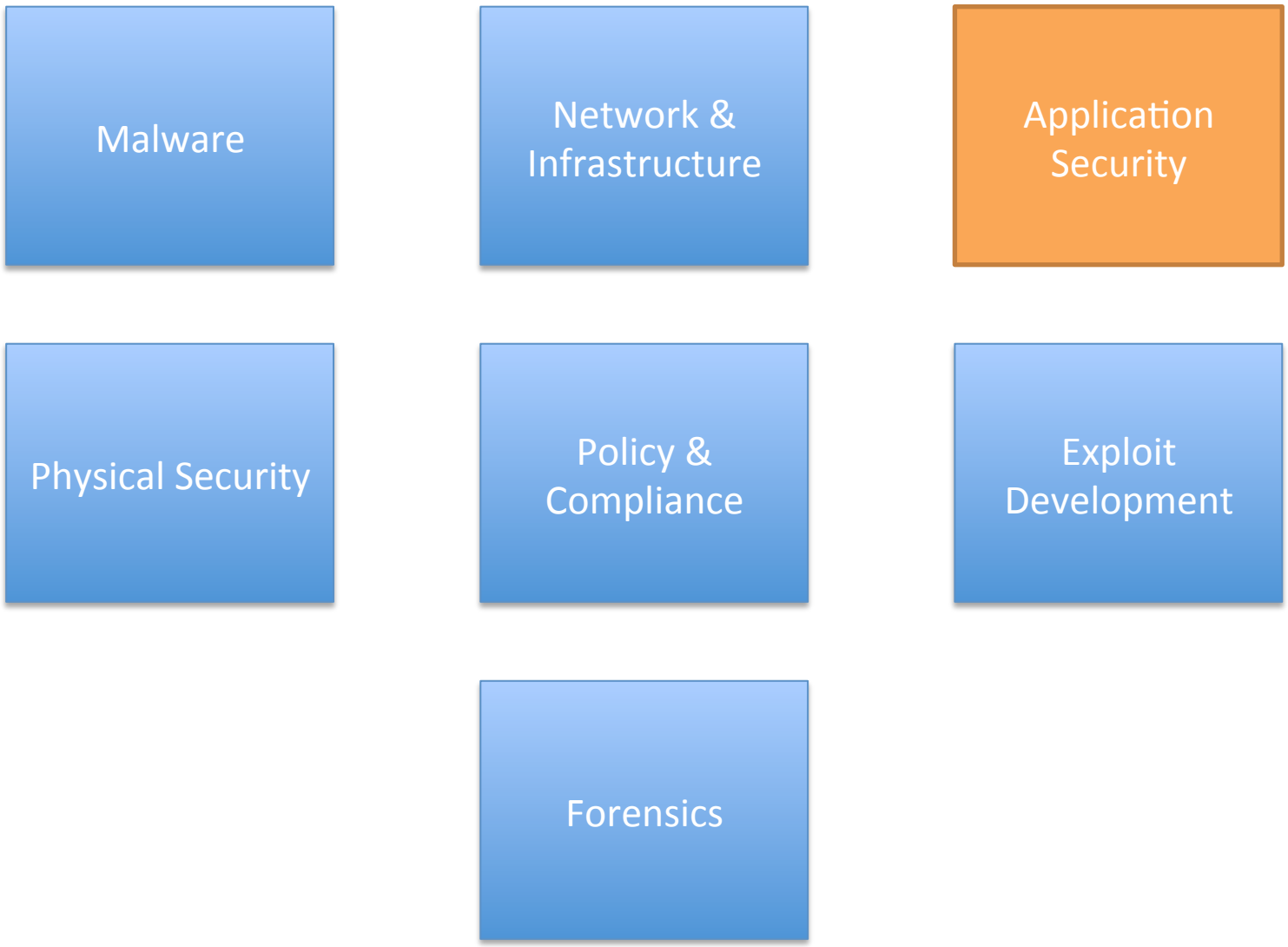
The Class

- Purpose is to both instruct and share knowledge
- We will actually be hacking
- Recent college grad, I remember how it goes
- If you have a large influx of projects or exams happening all at once, please let me know
- 4 late days to use how you want
- Late penalty: 10% daily, stops at 50% reduction
- Grading
  - midterm: 25%
  - final: 15%
  - hw: 60%
- 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

Bug Bounties

- https://bugcrowd.com/list-of-bug-bounty-programs
- https://hackerone.com
- Bonus points for successful bug
- 10% of your earnings

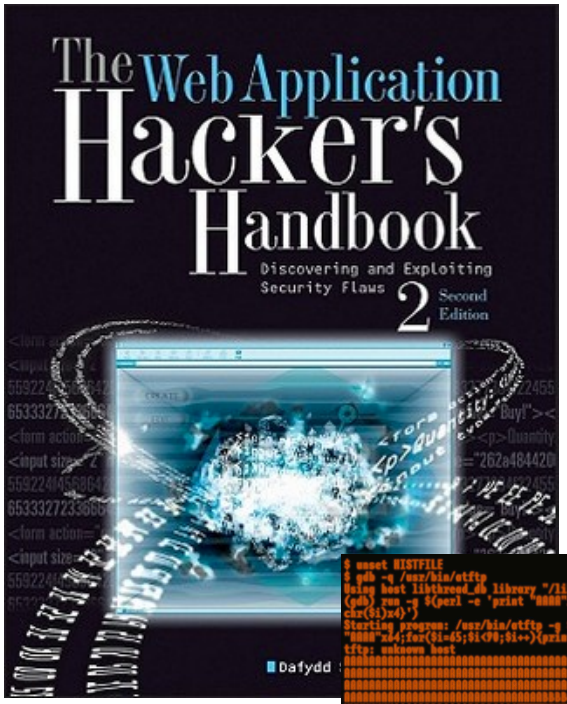
Responsible Disclosure

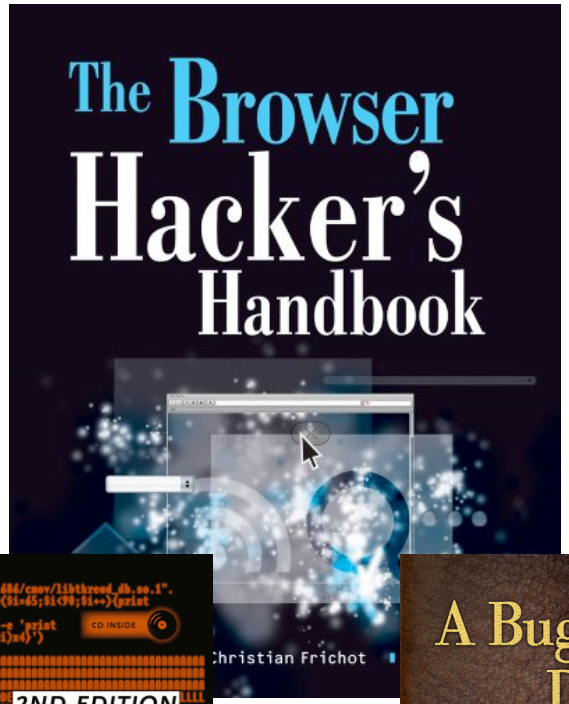
- Absolutely no full disclosure in this class
- Legal quicksand
- Be careful how you find and prove vulnerabilities

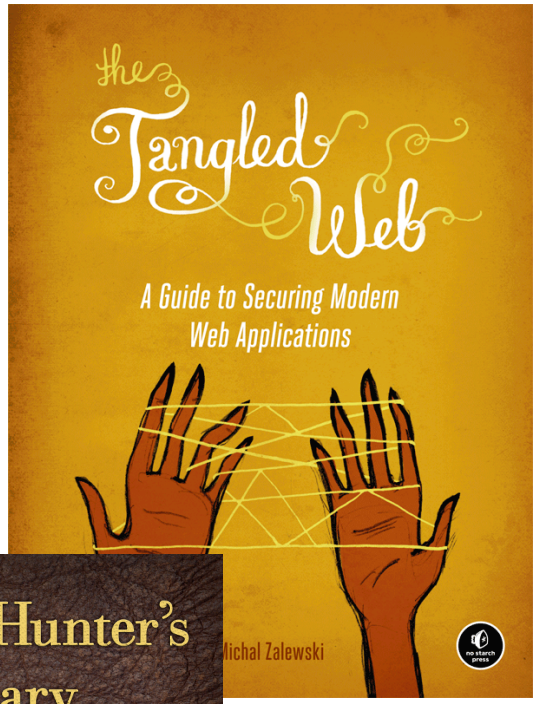
Tips & Tricks

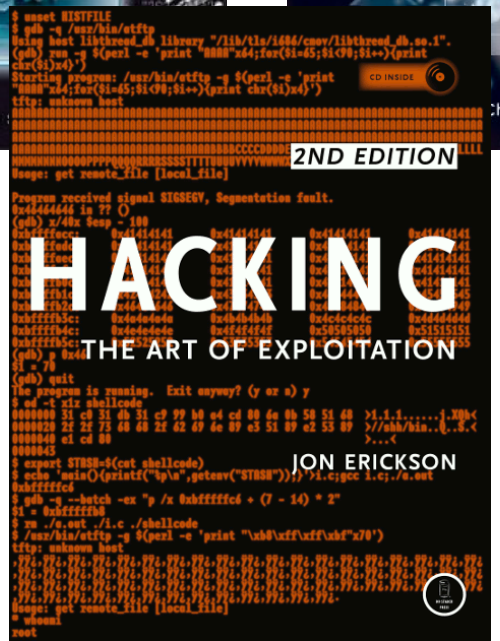
- Stay away from automated tools
- Keep your eyes open
- Send bad input
- Come up with favorite testing payloads
- Develop an "eye" for it

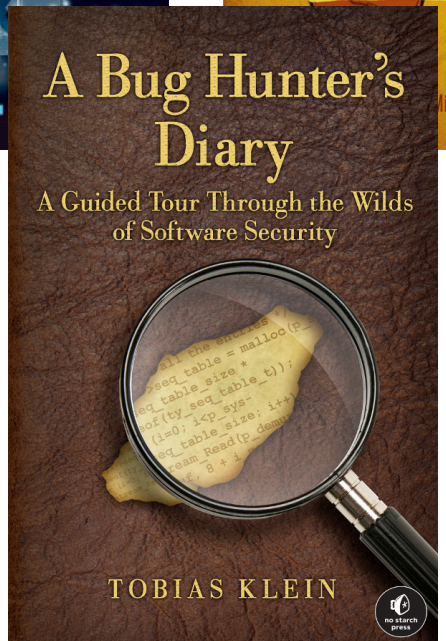
Books


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


The Browser
Hacker's
Handbook
Christian Frichot

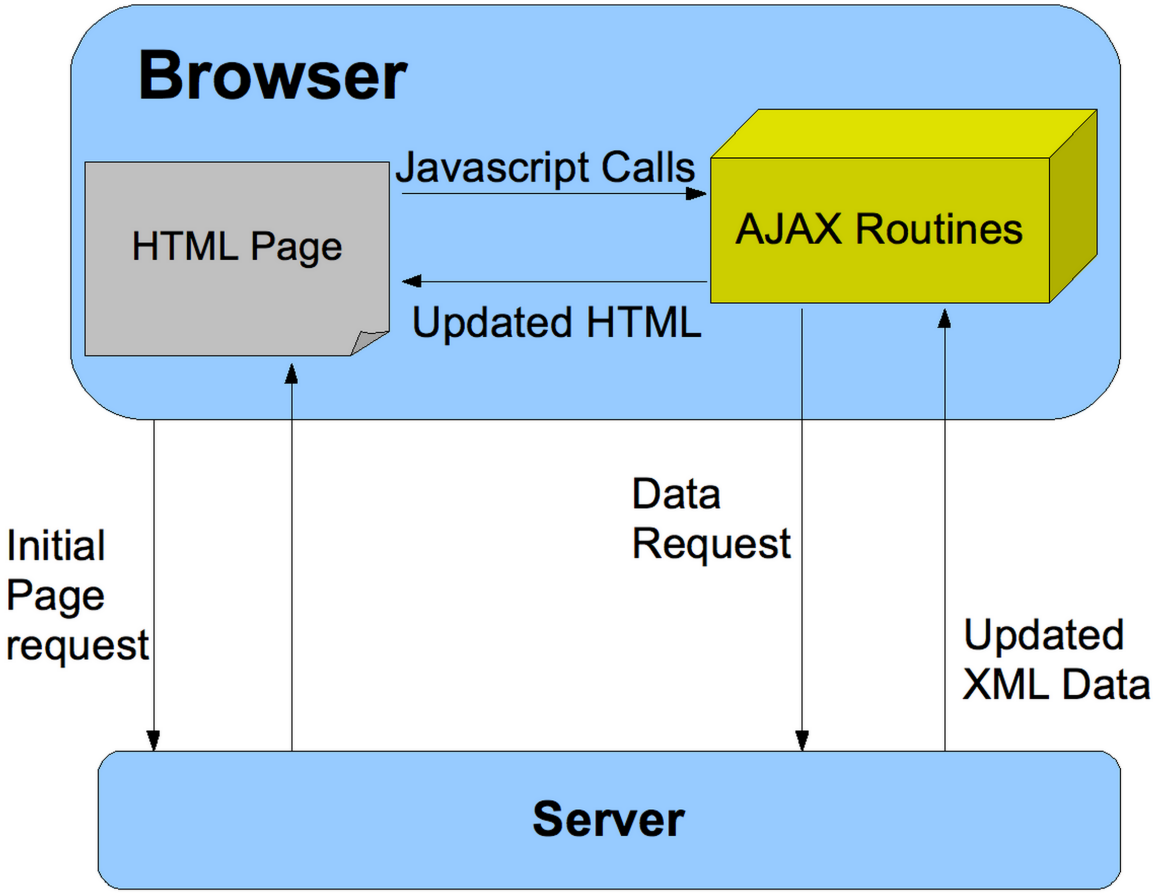

the
Tangled
Web
A Guide to Securing Modern
Web Applications
Michal Zalewski


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

Anatomy of a Web Application

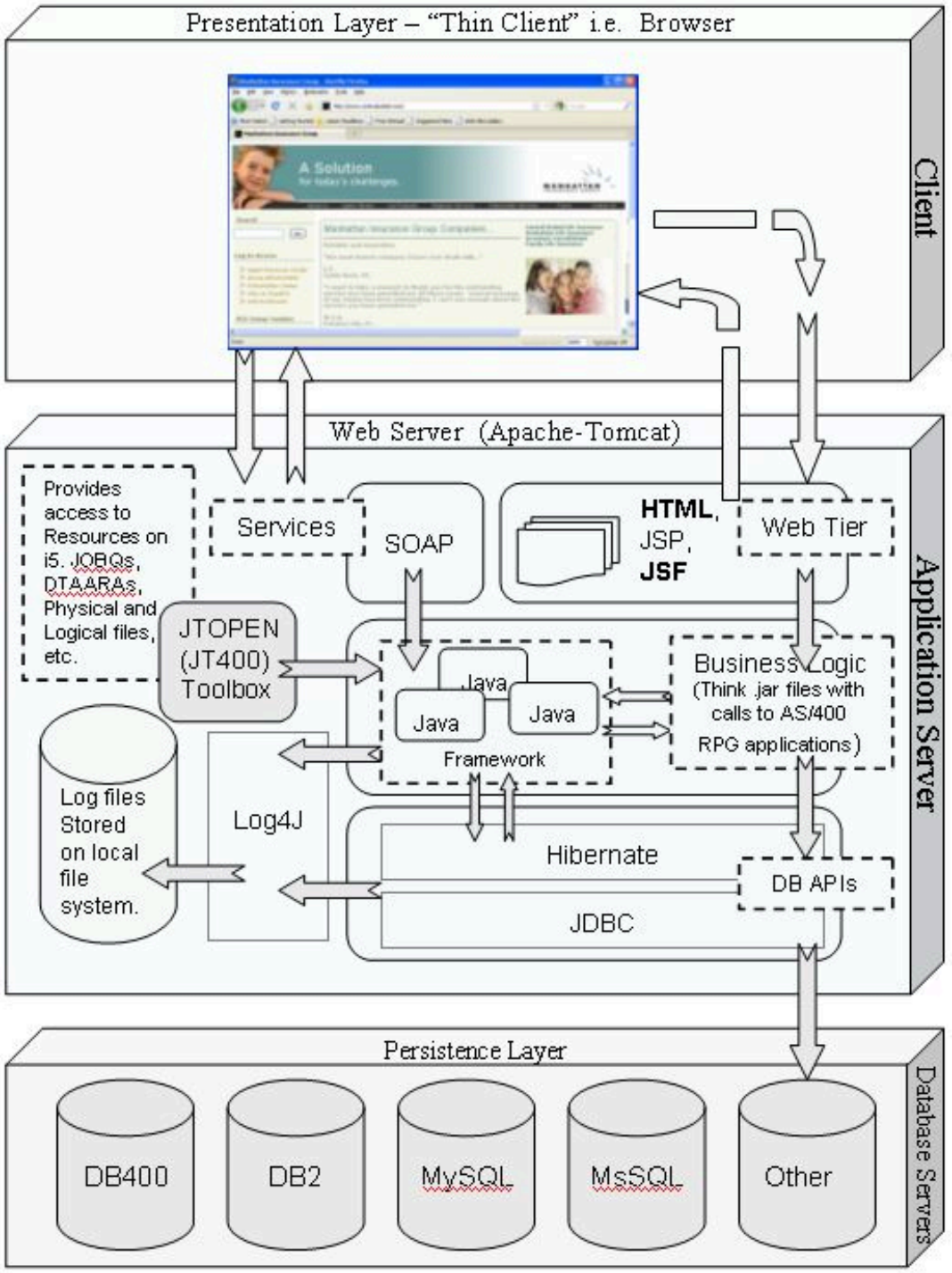
- Frontend
  - Content delivered to client
  - HTML, JavaScript, CSS
  - Ajax
- Middle layer
  - PHP, Python, RoR, Node, ASP.NET
  - Pages are dynamically generated
  - Requests parameters are parsed
- Database
  - MySQL, MSSQL, PostgreSQL, Sqlite
  - Direct queries or through ORM


Browser
HTML Page
Javascript Calls
AJAX Routines
Updated HTML
Initial
Page
request
Data
Request
Updated
XML Data
Server

Cookies

- Session management (usually)
- Storage (sometimes)
- Sent with every request
- Essentially an ID badge
- Show in Burp
- Demo session sidejacking

- Way more happening clientside
- Lots of Ajax
- Lots of moving parts
- Interfacing with host system more
- Increase reliance on 3rd party code



MVC Frameworks