



<https://twitter.com/portlandowasp>



meetup

<https://www.meetup.com/OWASP-Portland-Chapter/>



<https://www.linkedin.com/groups/4223013/>

Pacific NW Software Quality Conference

Achieving higher quality software through knowledge exchange

PNSQC Conference Kickoff event, 2020 Vision: Lighting the Torch

January 23, 2020, 6-8 PM

Cvent, 308 Southwest 2nd Avenue #200, Portland, OR

Come and listen to futuristic lightening talks on software quality. Better yet give a 10 minute talk on the future of AppSec.

For more information visit:

<https://www.pnsqc.org/2020-vision-lighting-the-torch/>

So You Want to Teach Security?

Bully for You!



John L. Whiteman



*Opinions expressed are
solely my own and do not
express the views or
opinions of my employer
or anyone else for that
matter.*

Some Titles That Didn't Make It

Learn Test Automation Security

How to Use Doan's Backache Kidney Pills to Get Me Shaved



About Me - John L. Whiteman



Experience spans two centuries

Product Security @ Intel

PT Instructor @ UP

U.S. Navy Sonar Instructor

Worked in Radio News

Literally grew up in a bakery



<https://linkedin.com/in/johnlwhiteman>

Today in Security News



❖ [HackerOne](#) got hacked! [Cookie leak](#) allowed researcher to access other customer vulnerability reports.

- Got paid [\\$20K](#) for it



- What if HackerOne didn't pay?
 - Called police instead, broke the rules
- What are your thoughts?

Why Today in Security News?

- Every lecture is a performance
 - It's the class monologue
- Topics can be anything:
 - To reinforce lessons
 - Promote upcoming security events
- Puts a new shine on an old lecture



Today's Objectives



Start Here

- ✓ Can you teach?
- ✓ Teaching in academia
- ✓ Teaching in the workplace
- ✓ Why soft skills are so darn hard
- ✓ Questions and Answers

Let Me Ask You This



Have you ever taken a class by a teacher who couldn't teach but was a subject matter expert?

Can You Teach?

- Start with knowing what you're talking about
- But that's not what we're talking about
- Not all people can teach (as is)
- But most can learn to teach



Can You Teach?



- Anyone see Eva Galperin's [keynote](#) @ BSides PDX 2019?
- Poor teaching skills can be a matter of life and death
- [Security Education Companion](#) focuses on training the vulnerable
 - Stalker victims, journalists, activists, ...
- Who is training the trainers?

Here's What Scares Them

- Global gap of nearly 3.5 million cybersecurity jobs by 2021



Here's What Scares Me

- Gajillion lines of code being checked into GitHub everyday
- Newly minted CS graduates who never learned about secure coding
- Who's making the problems? The security people?





Romanaggi Hall



Teaching Security in Academia

University of Portland (UP)

Spring 2019

(Thank You, OWASP)

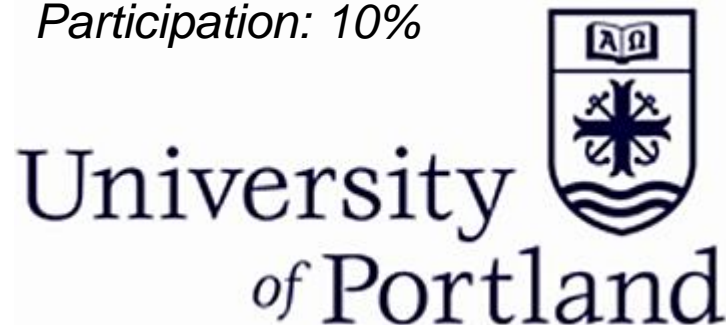


- I'm not a professor, not a doctor
 - But I do perform surgeries
- I'm not an educator
 - But I love to teach
- What I say is not the only way
 - Yours might be a better way

UP Syllabus

- 26 lectures (~85 mins each), 17 domains
- 10 weekly homework assignments
- 31 in-class labs and exercises
- 4 take-home labs
- 4 extra-credit
- 7 demos
- Midterm
- Final

Homework: 50%
Midterm: 20%
Final: 20%
Participation: 10%



NEW

Date	Lecture Topic	Reading	Assignments	Deliverables
1/15/2019	Introduction to Cybersecurity	Ch 1		
1/17/2019	Legal and Ethical Issues	Ch 19	HW 1	
1/22/2019	Identity, Authentication and Authorization I	Ch 3		
1/24/2019	Identity, Authentication and Authorization II	Ch 3	HW 2	HW 1
1/29/2019	Access Control and Auditing	Ch 3		
1/31/2019	Cryptography I	Ch 2, 20	HW 3	HW 2
2/5/2019	Cryptography II	Ch 2, 20, 21		
2/7/2019	Cryptography III	Ch 2, 20, 21	HW 4	HW 3
2/12/2019	Cryptography IV	Ch 2, 20, 21		
2/14/2019	Database and Cloud Security	Ch 5	HW 5	HW 4
2/19/2019	Network and Wireless Security I	Ch 22, 23, 24		
2/21/2019	Network and Wireless Security II / Midterm Review	Ch 22, 23, 24	HW 6	HW 5
2/26/2019	MIDTERM EXAM			

2/28/2019	OS Security, Virtualization and Containers	Ch 12, *25, *26		HW 6
3/5/2019	Spring Vacation (No Classes)			
3/7/2019				
3/12/2019	Malware, Threats and Attacks	Ch 6		
3/14/2019	Hardware Security, Secure Software Development Lifecycle	Ch 27	HW 7	
3/19/2019	Secure Coding I	Ch 10, 11		
3/21/2019	Secure Coding II	Ch 10, 11		HW 7
3/26/2019	Web Security I	TBD		
3/28/2019	Web Security II		HW 8	HW 7
4/2/2019	Security Assessment and Testing I	TBD		
4/4/2019	Security Assessment and Testing II		HW 9	HW 8
4/9/2019	Firewalls / IDS / IPS	Ch 9		
4/11/2019	Incident Response, Recovery and Forensics	TBD	HW 10	
4/16/2019	Security Risk Management, Personnel and Physical Security, Reverse Engineering w/Ghidra	Ch 14, 16		HW 9
4/18/2019	Easter Break (No Classes)			
4/23/2019	Emerging Technologies			HW 10
4/25/2019	Open Topics / Final Review			
4/30/2019	FINAL EXAM			

The Lecture Sandwich Analogy

Objectives

Homework (Review)

Security News

Slides

Labs & Exercises

Demos

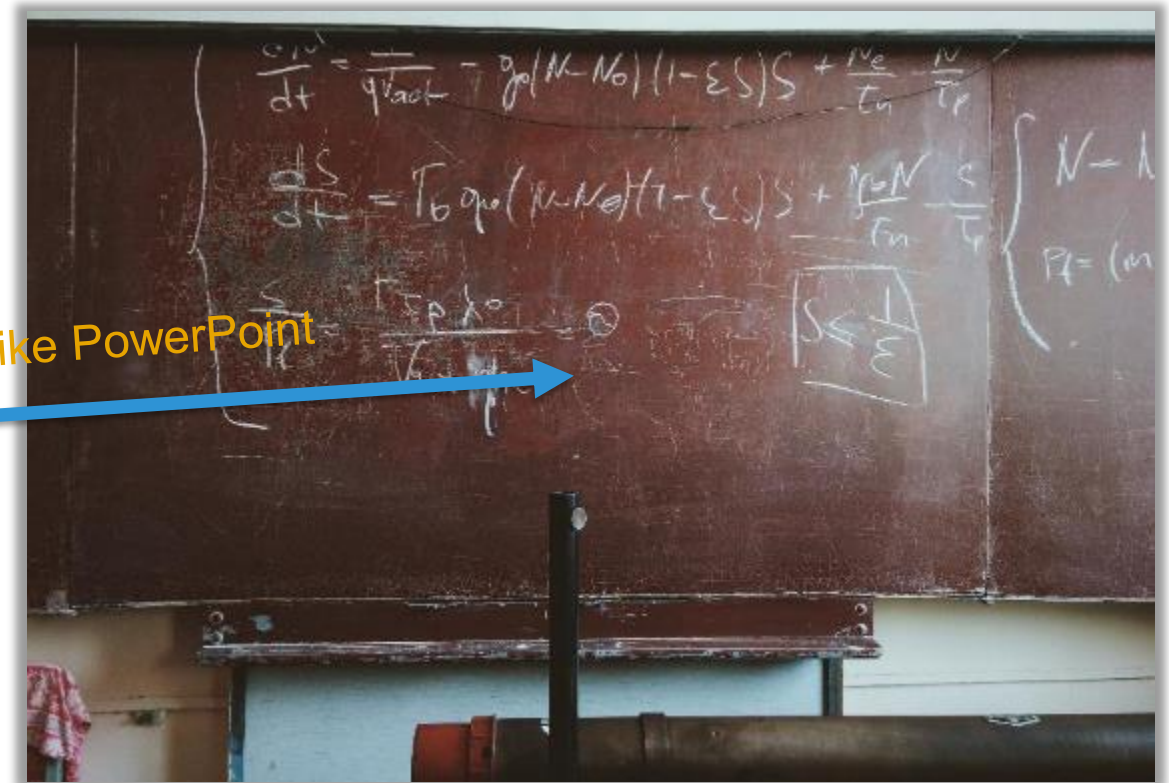


What's Next

Slides

- PowerPoint has no name in ancient cultures
- Guilty of PowerPoint by death
- Some other options:
 - Use blackboard
 - Do exercises
 - Run demos
 - Discuss

Nicely Orange, like PowerPoint



Homework and Take-home Labs

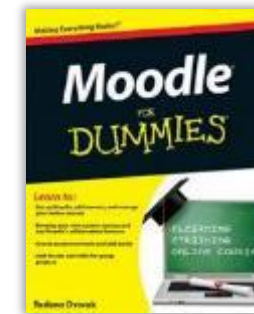
Weekly Online Assignments (Moodle)

Take-Home Labs

- Diffie-Hellman Key Exchange (C)
- Containers & Security
- Hacking & Hardening Websites
- Whitelisting, Scanning & Threat Modeling

Extra Credit

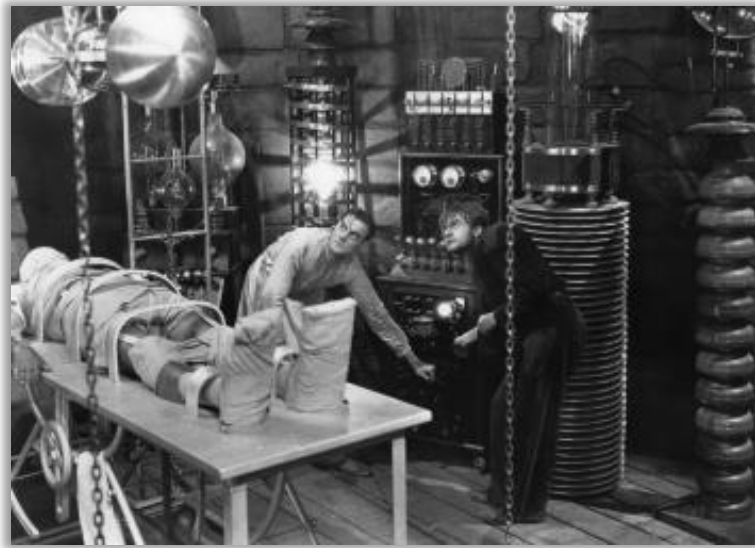
- Early Lab Setup for Ubuntu / Kali / Metasploitable
- Vigenère Cipher
- Steganography (Audio)
- Fuzzing (AFL)




Labs/Extra Credit Not Stored in GitHub

In-Class Lab Options

- Local VMs (kind of suck)
 - Need a powerful computer
 - Inconsistent install issues



Always Run Labs in a Sandbox

- Network VMs (IT kind of sucks)
 - And rightfully so 
 - *Students with Fuzzers* (scary)



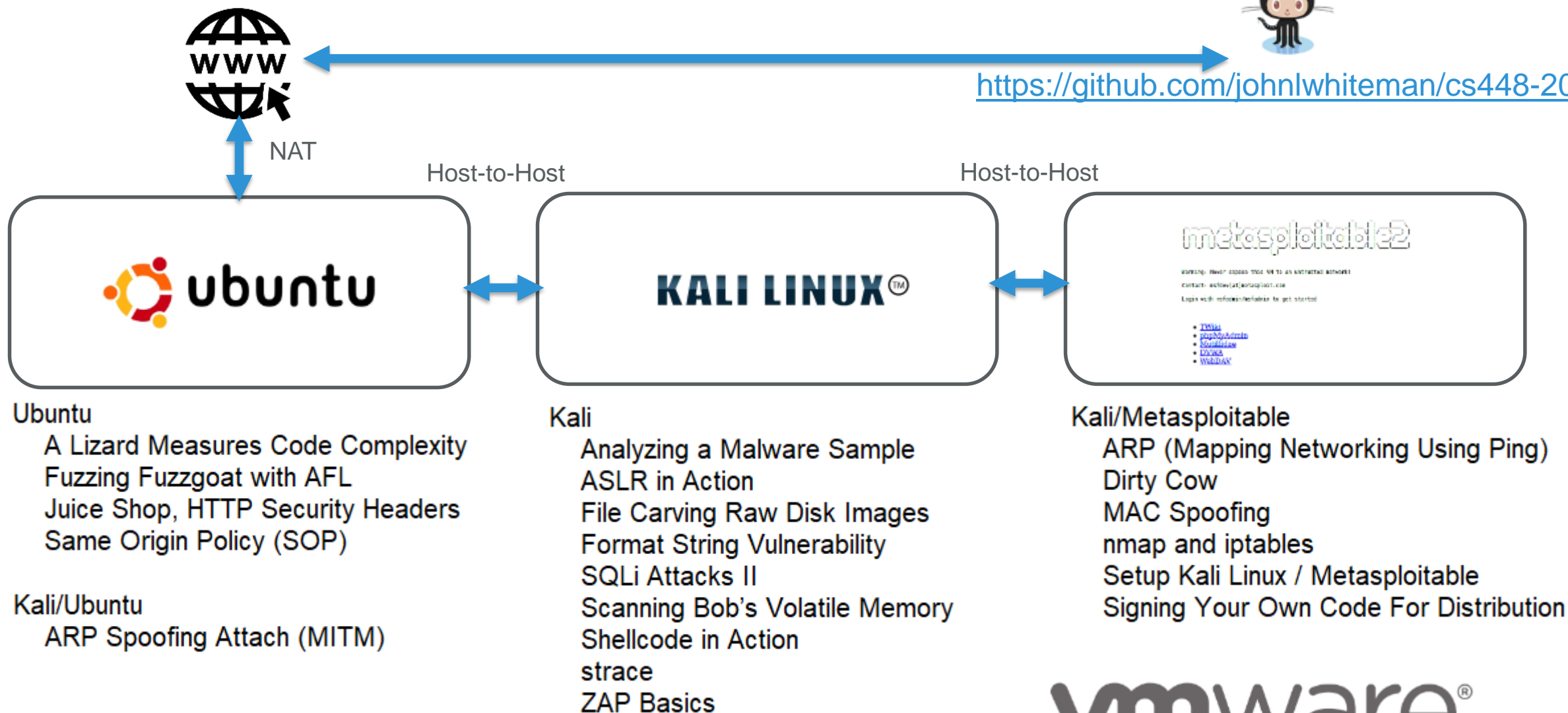
- Cloud (most preferred)
 - Cheap, consistent and automatable



In-Class Labs and Exercises (3 Local VMs)



<https://github.com/johnlwhiteman/cs448-2019>



In-Class Labs and Exercises (Other)

AlienVault

Manual Code Reviews

Naïve Stack Buffer Overflow

Not-So-Naïve Stack Buffer Overflow

Run a JavaScript TPM HW Simulator

Search for CVEs

Search for CWEs

SQLi Attacks I

Tabletop Exercises

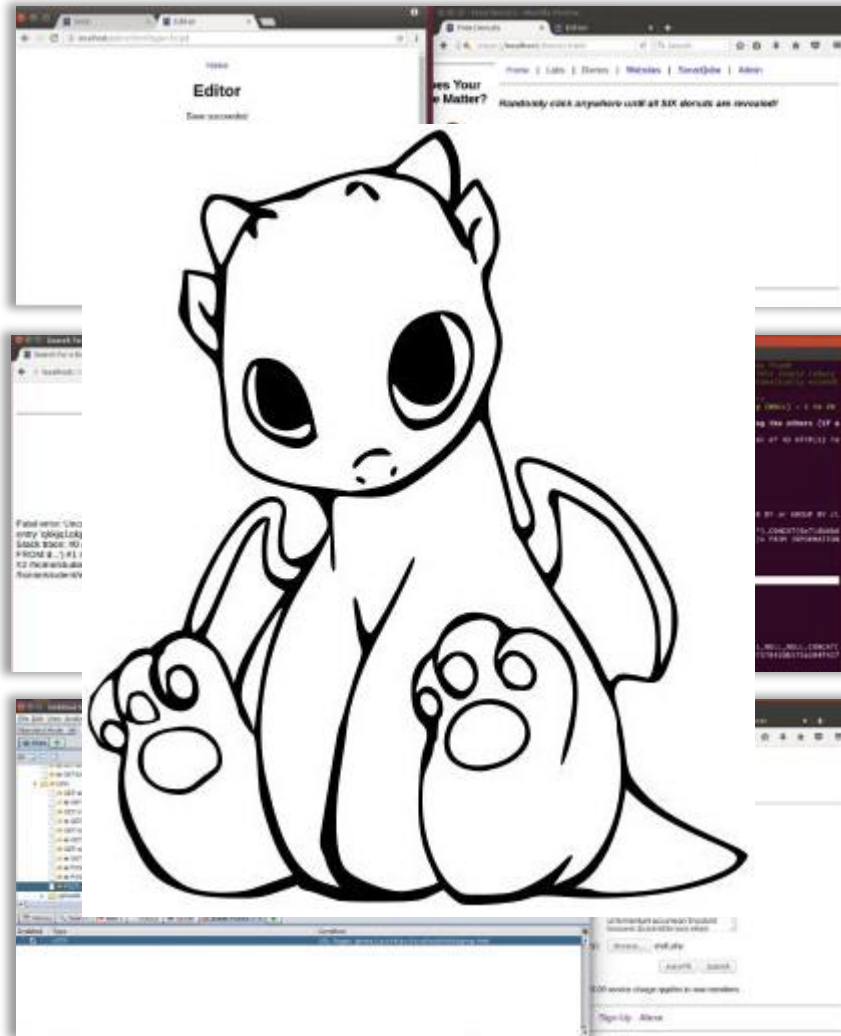
Threat Model a Body Vitals Devices

Threat Model Diagramming

自動販売機



Demos



- Live Demos
 - OWASP Threat Dragon
 - ARP Spoofing (MITM)
 - SonarQube and OWASP Dep Check
- Video Demos (Thank you, OHSU)
 - Preventing Clickjacking Attacks
 - SQLi Attacks Using Automation
 - Using ZAP to Scan and Attack



If you can, consider creating online content first for profit: Cybrary, Pluralsight, ...

Three Questions to Ask on the First Day of Class



A New Demographic for Me

- 1) Who are you?
 - Never remember names
- 2) What do you want to be when you grow up?
 - Security or not? (< 20%)
- 3) What do you hope to get out of the class?
 - Didn't know yet
 - But that's why they're there

A word cloud shaped like a heart, containing various terms related to online learning and student experiences. The words are arranged in a circular pattern, with the most prominent words in the center and smaller words towards the edges. The colors of the words vary, including shades of blue, green, yellow, orange, and red.

Key words visible in the cloud include:

- students
- activities
- really
- good
- lot
- interesting
- learning
- lecture
- fantastic
- questions
- paying
- instructor
- understandable
- cybersecurity
- network
- resource
- lab's
- field
- time
- topics
- like
- think
- make
- provide
- learn
- able
- professors
- school
- please
- useful
- better
- frustrating
- constraints
- without
- make
- think
- VMs
- student
- willing
- though
- get
- stuff
- general
- examples
- slides
- pretty
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
- refused
- helped
- just
- seemed
- cool
- much
- word
- work
- needed
- multiple
- paying
- present
- participation
- understandable
- concepts
- powerpoint
- anonymous
- great
- job
- professor
- things
- discuss
- explaining
- made
- spaces
- felt
- nice
- can
- use
- one
- much
- small
- attention
- responsive
- helpful
-

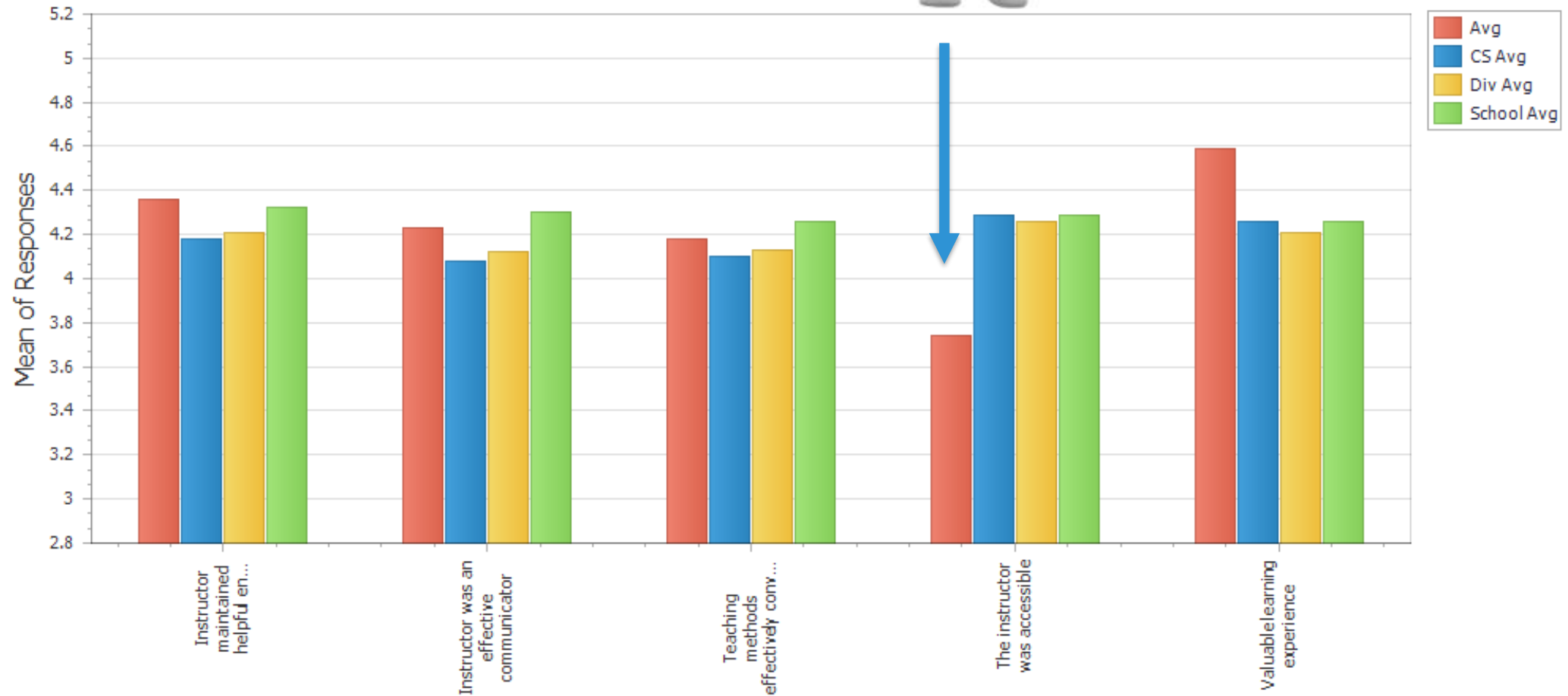
- Instructor maintained helpful environment
- Instructor was an effective communicator
- Teaching methods effectively conveyed content
- The instructor was accessible
- Valuable learning experience

Results as Word Cloud

How Did We Fare?



Question Averages



No Office Hours

- Dedicated time (Yes)
- Dedicated place (No)
- Students want both
 - How about workplace too?
- Students want privacy
 - Speaking of privacy



Family Education Rights and Privacy Act (FERPA)

Read it.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the Department of Education.

(FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the Department of Education.



<https://www.ferpa.gov/>

This Photo by Unknown Author is licensed under CC BY-NC-ND



Spring 2020

*Network VMs
Containers
Office Hours
NCL*



Identity, Authentication & Authorization

Cloud Security

Containers and Virtualization

Cryptography I

Cryptography II

Cryptography III

Cryptography IV

Emerging Technologies

Forensics

Introduction to Cybersecurity

IT Security

Legal and Ethical Issues

Malware

Network Security I

Network Security II

OS Security

Penetration Testing I

Penetration Testing II

Reverse Engineering

Threat Modeling

Secure Coding I

Secure Coding II

Web Security I

Web Security II

TBD

TBD

Integrate *National Cyber League*



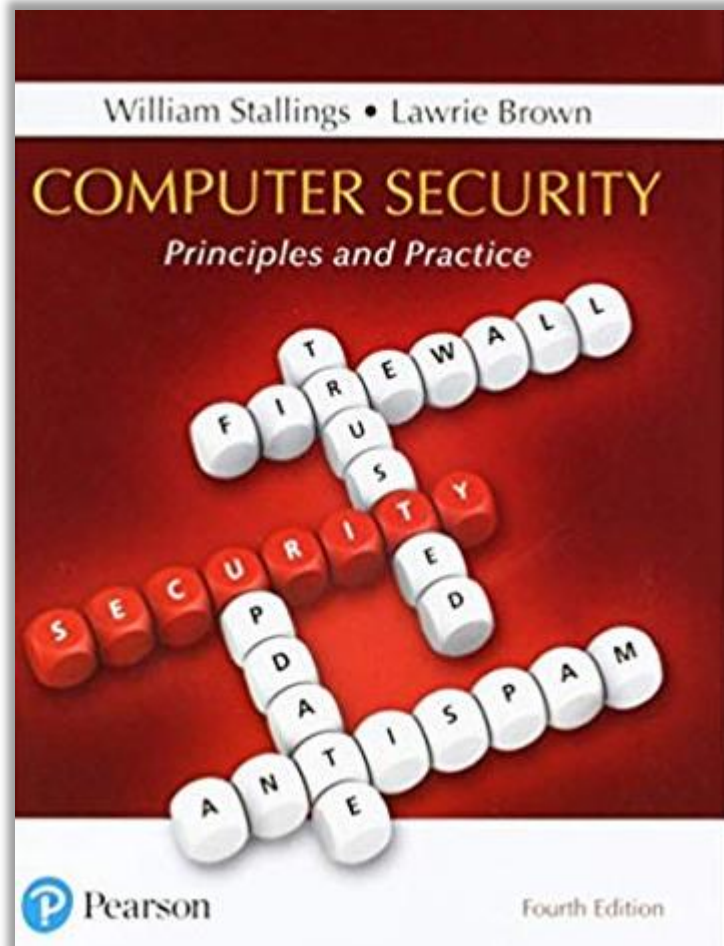
- Biannual ethical hacking competition for schools
 - Leaderboards, tutorials, live coaching calls ...
- OSINT, scanning & enumeration, exploitation, password cracking, traffic & log analysis, wireless security, cryptography, web app sec
- Students can download scouting report
 - Evidence for potential employers



\$35 included as class fee

<https://www.nationalcyberleague.org/>

Obsolete the Security Textbook



- Too expensive, hard to keep up-to-date (\$122)
 - Security is moving at the speed of light
- Maybe an online book subscription service
 - O'Reilly's Safari is \$39 a month (unlimited)
 - Lynda.com (LINKEDIN)
- Negative is that you never own the books

Reflections - A Germantown Road Experience

- Hard but rewarding
- Students respectful, polite and hardworking
- Proud of them



Even though most won't pursue a career in security, they're the next generation of architects, developers and security teachers



*That's great, Professor Johnny,
but what about teaching security
at the workplace?*

You Have Some Options

- Most applies as before except maybe the teacher?
 - ☑ Hire a third party vendor
 - ☑ Find something off-the-shelf
 - ☑ Leverage online classes
 - ☑ Do it yourself
- Any combination of the first three is great
 - Sometimes that's not possible



Possible Scenario

- Let's say you have products that make web applications
- Code scanners find numerous security vulnerabilities
- Products are proprietary and data confidential
- Decide to build a secure coding class
- But you have reservations ...



Two Kinds of Students at the Workplace

Those who want to hear what you say ...



... and those who don't!

Who Are These Folks?

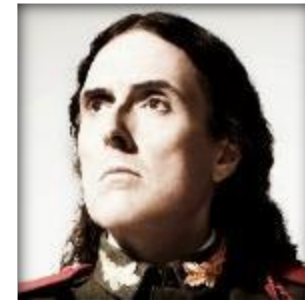
- Usually people not in security
- Maybe developers, program managers, ...
- Security gets in the way of the schedule
- Spend more energy complaining than complying



TOUGH FOR THE TEACHER

It's Like Trying to Explain the Dangers of ...

- Not wearing seatbelts
- Smoking cigarettes
- Diving naked in a pool of double-edged razor blades



Sir Weir Al

Some people are just willing to take the risk

How to Overcome?

Policy is the stick

**"Speak softly
and carry
a big stick."**

Theodore Roosevelt



- For us it starts with ...
 - Patience
 - Persuasion
 - Perseverance
- And if all else fails ...

You can build it, but without policy, they won't come.



Case Study: Secure Coding Class



- Student registers for an available session
- Gets a welcome e-mail with a link to a questionnaire
- Completes the class and a final exam
- Gets a thank you e-mail with a link to a post-class survey
- Gets credit in the system (S-SDL ... make it mandatory)

Case Study: Secure Coding Class



- How do you support multiple languages?
- Containerize your syllabus (labs)
 - Create a Dockerfile unique to each language
- Use pre-survey questionnaire to help

ColdFusion

- CF 2016
- Security Scanner

.NET

- Windows
- Roslyn

JavaScript

- NodeJS
- NodeJSScan

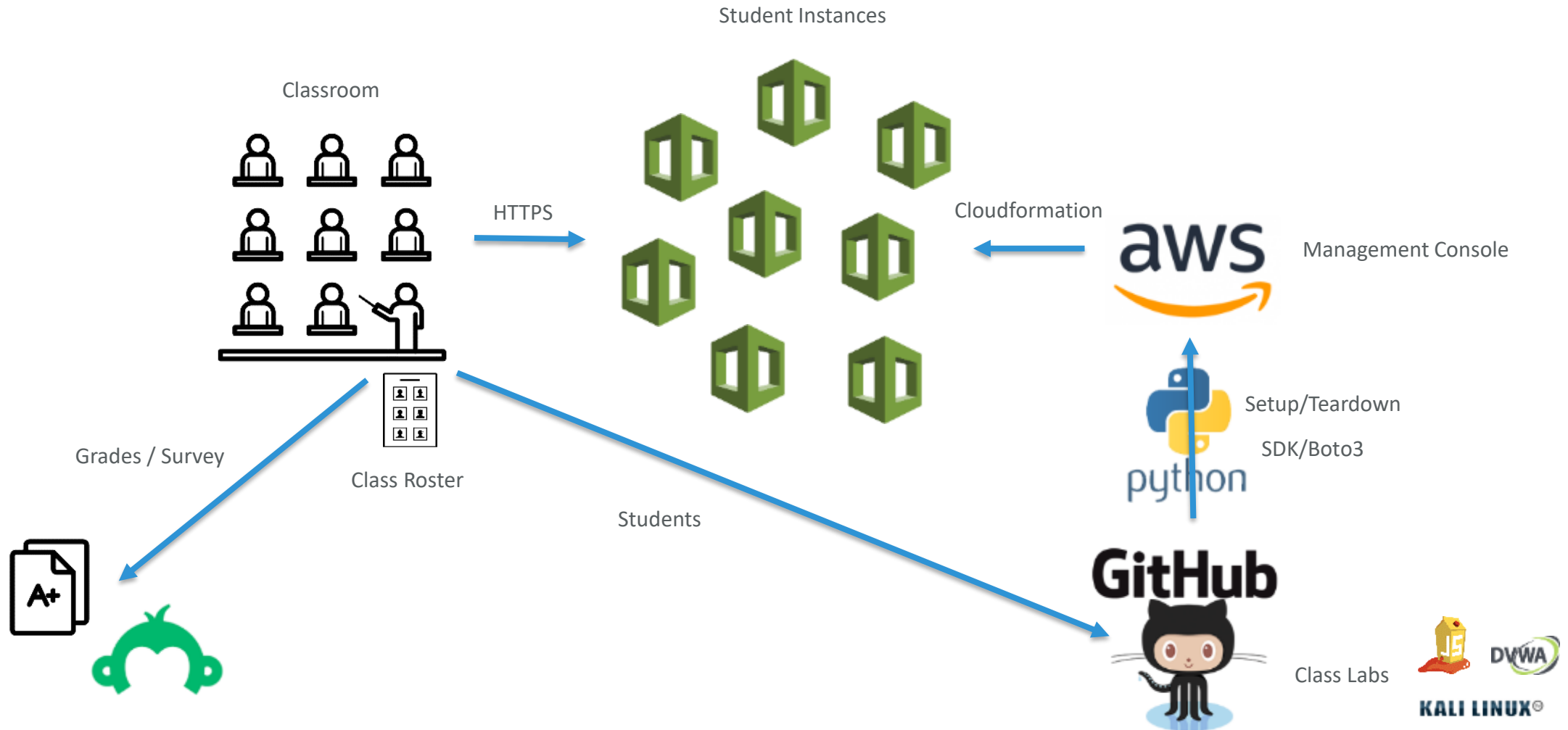
PHP

- 7.0
- RIPS

Java

- SE/EE
- SonarQube

Case Study: Secure Coding Class



Case Study: Secure Coding Class



What Differentiates Workplace from Academia

In the workplace, the content is focused on the product

In academia, the product is the student

Why are Soft Skills So Hard?



The Art of the Critique



Bob

- Slow down
- Engage in eye contact
- Move about
- **Just be yourself**



You

- Speed up -
- Creepy -
- U Tweeking? -

Just be yourself -



Alice

It can take years of practice to just be yourself.

Critiquing is Hard



- Take it with a grain of salt
- Self record and critique yourself often
 - What you hear in your head is different
- Get a fellow trainer to critique you
 - Make it a requirement in you training program
- Attend Toastmasters if you need help

Here's My Most Memorable Critiques

Don't finger comb your hair (fixed itself)



It's "Thailand", not "Thigh Land" (on air)

You sound better with the microphone off (huh?)



Distracting Mannerism Can Really Hurt

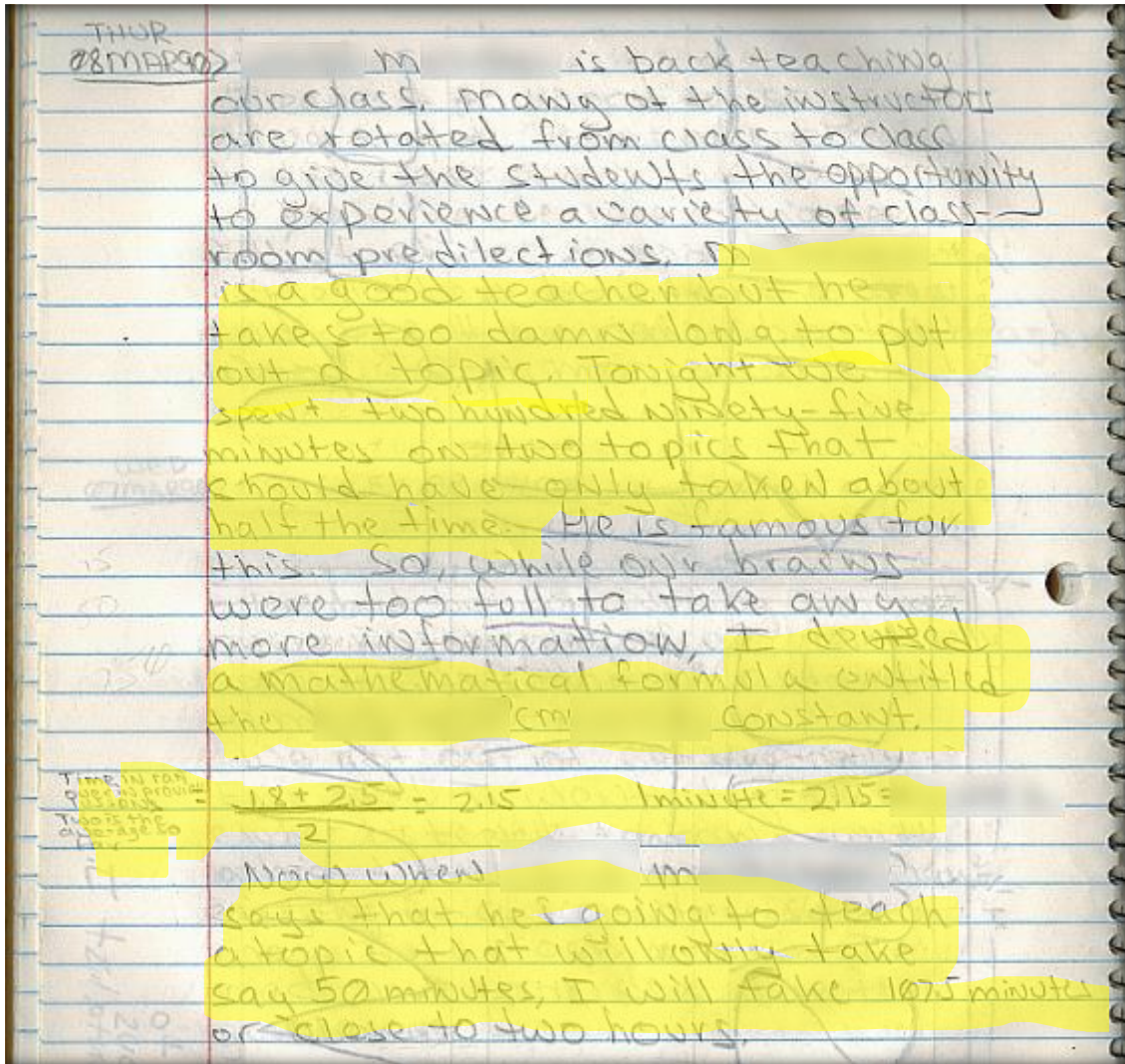
spitting
poor eye contact
lack confidence
too casual
under enunciating
standing in place too long
too much back and forth
jingling keys
talking with back to students

rocking back and forth
playing with chalk
too emotional
no emotion
skinning a live cat
running off the mouth
lack of facial expressions
bad timing
chewing toenails

whistling
smacking lips
crutch words
creepy staring
hands in pocket
clicking pen
checking out
turning ring
shotgunning
texting
data dumping
voice fry
ending all sentences like a question
clearing throat too much
speaking before thinking
drumming fingers

ums and ahs

An Example of an Extreme Mannerism: The Melcher Constant



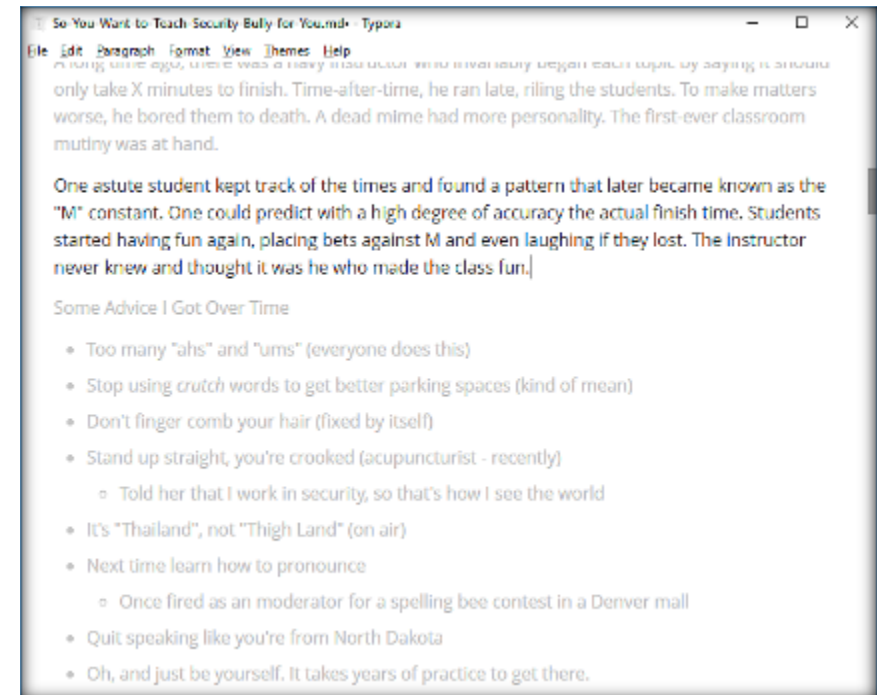
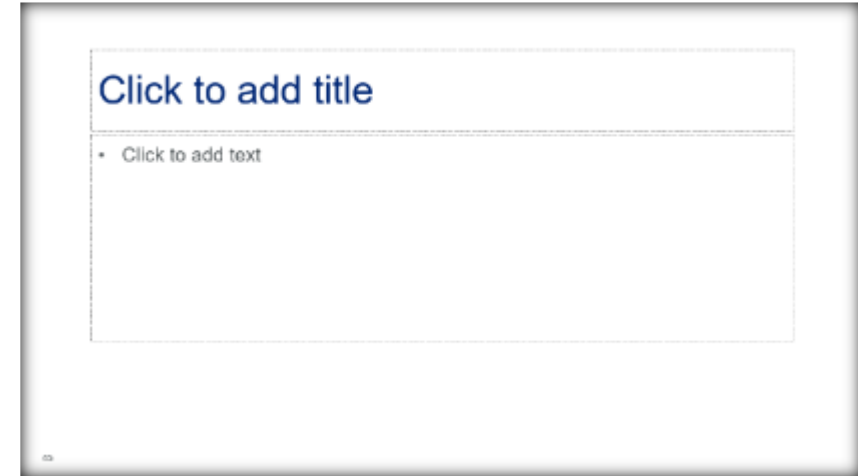
- Instructor who never finished a topic on time as promised. Always late.
- First classroom mutiny ever?
 - Students angry ... hard to study
- Yours truly discovered this pattern:

$$X = \{x_0, x_1, \dots, x_n\}$$

$$M = \mu_x = \frac{1}{n} \sum_{i=1}^n X_i = 2.15$$

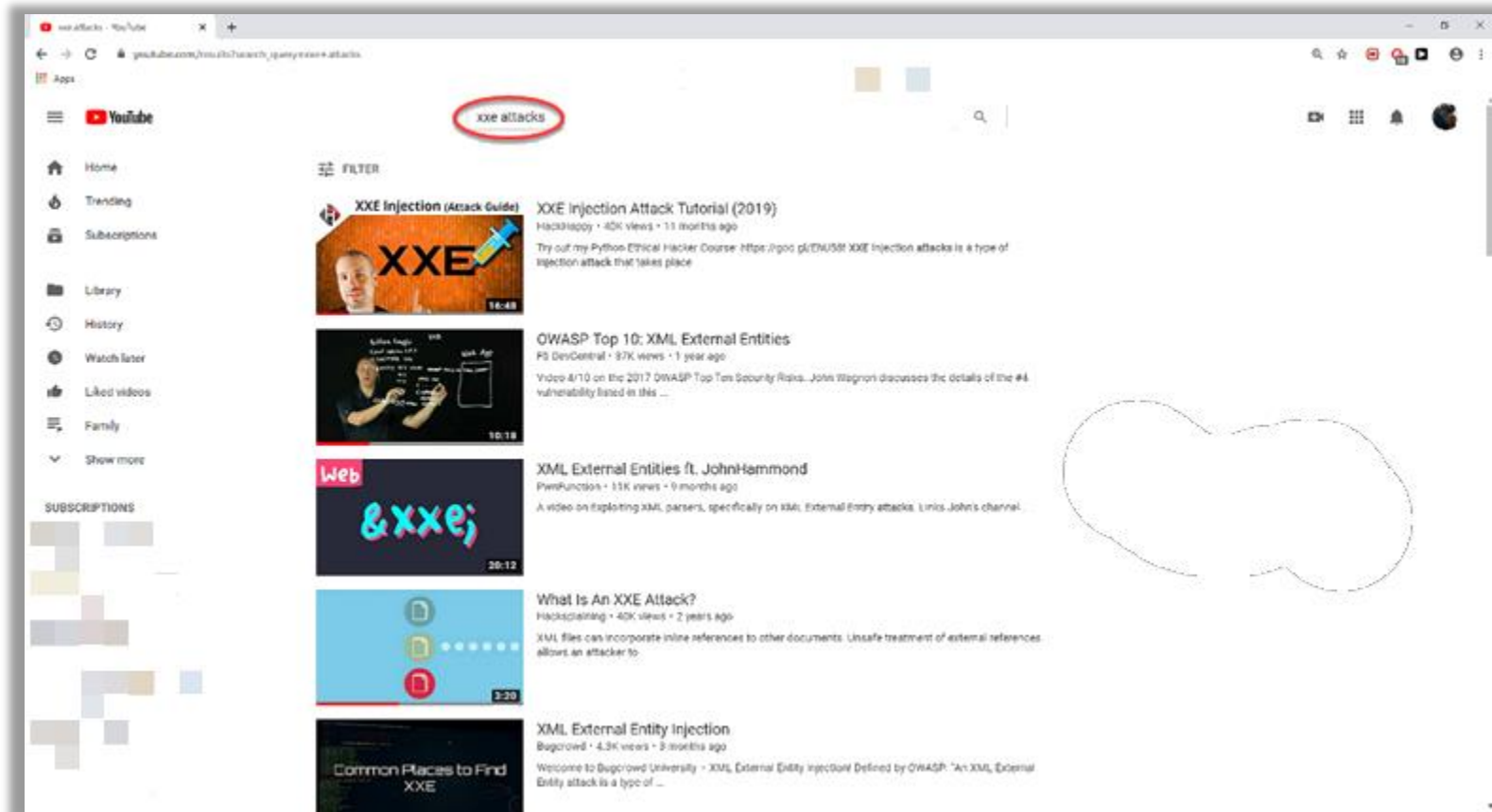
Why Start with Markdown?

- PowerPoint is a zoning law nightmare
 - Obstructs streams of conscience
- Start with a minimalist markdown editor
 - Typora, disable grammar checker
- Always be curriculuming (ABC)
 - Take good notes ... then derive
 - Easy to convert to other formats



Minimize the Rat Holes

Extensions to block out YouTube distractions (DF Tube Chrome)



Know the Space Before You Teach (Recon)

- OSINT is a good start (Google)
- Capacity, space to move, sound, ...
- Projector, desks, tables, outlets, ...
- Come early to do dry run



[Autodesk Blogs](#)

Use the Space: The White Turtle



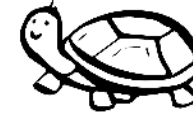
University of Portland Classroom



Cisco Router

Any concerns? 

Use the Space: The White Turtle



- White turtle became an early, constant reminder for security best practices
- Later adopted as a visual aid for a lecture on using codes for security
- Navajo used it in WW2. Bob and Alice used it in Spring 2019.



NAVAJO CODES NAME OF SHIPS		
SHIPS	TOH-DINEH-IH	SEA FORCE
BATTLESHIP	LO-TSO	WHALE
AIRCRAFT	TSIDI-MOFFA-YE-HI	BIRD CARRIER
SUBMARINE	BESH-LO	IRON FISH
MINE SWEEPER	CHA	BEAVER
DESTROYER	CA-LO	SHARK
TRANSPORT	DINEH-NAY-YE-HI	MAN CARRIER
CRUISER	LO-TSO-YAZZIE	SMALL WHALE
MOSQUITO BOAT	TSE-E	MOSQUITO

Use the Space: The White Turtle

The Scenario



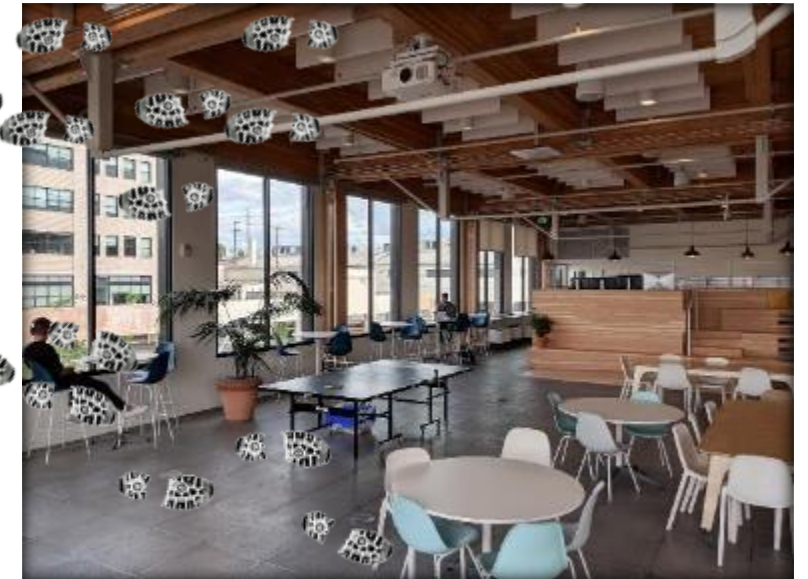
- Alice and Bob are students with an evil plan to steal passwords
- They use codes to conceal their plot from the others in the room
- "White turtle" is the router, "turtleneck" is a network capture device
- Alice says, "When does the white turtle get its turtleneck?"
- Bob answers, "Tonight, after the exam!"
- It almost worked but the turtle ratted them out
- Now Alice and Bob are wearing matching "turtle suits" in prison



Expect Failure: Adapt and Overcome



- ✓ Move about the audience
- ✓ Never turn your back on the audience
- ✓ Make the PowerPoint transitions seamless



Questions and Answers

Thank you!