Web Exploitation

News since last meeting

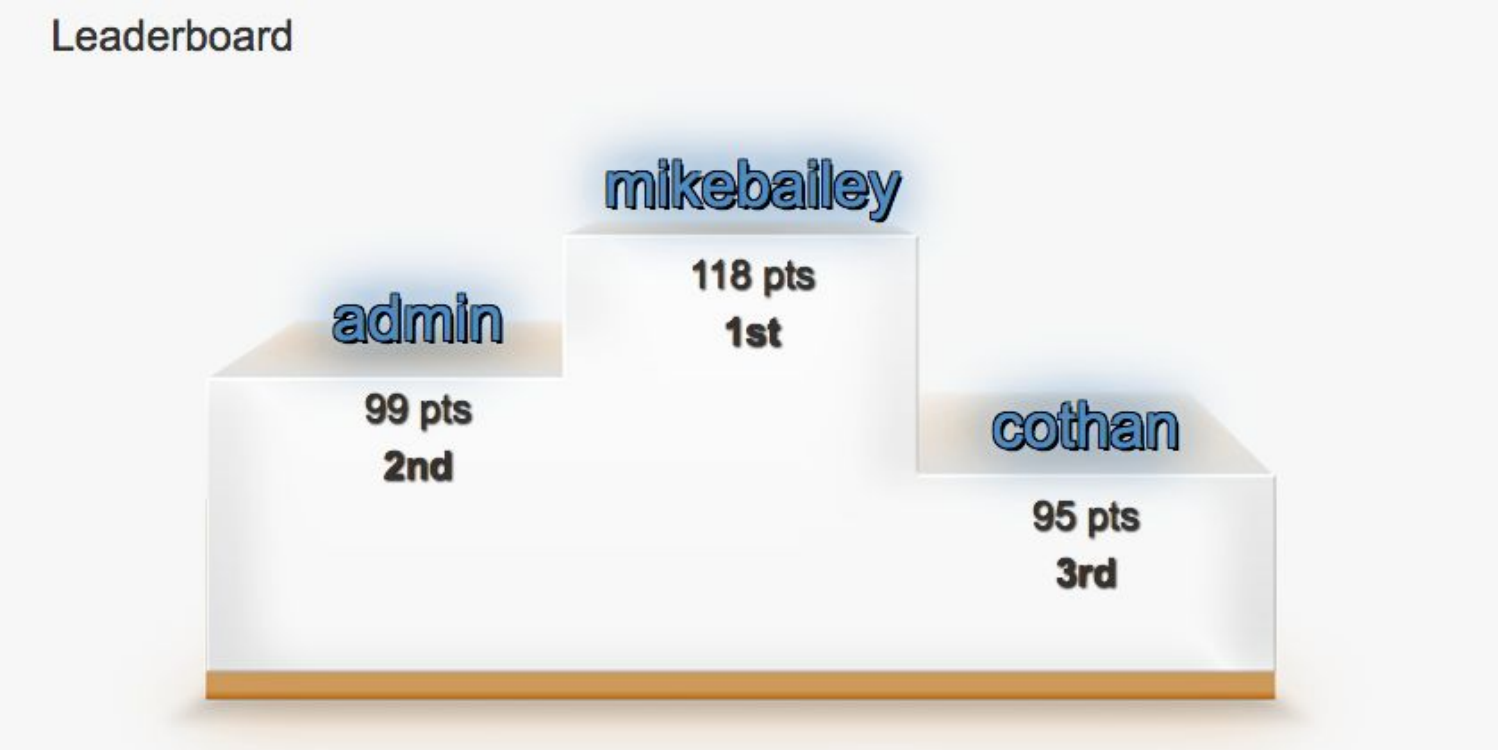
- Equifax hack
  - Credit reporting agency
  - 143 million people's PII was stolen
  - People filed a ton of class action lawsuits

- Virginia Election board to decertify eVoting machines that do not provide receipts
  - Every voting machine at DEFCON was hacked

- MongoDB ransomware attacks
  - 26,000 MongoDB servers attacked
  - Cause: ~~people using default admin creds~~ stupid people

Recent CTFs

- Booz Allen Hamilton CTF
  - 50 people registered
  - Michael Bailey got 1st
  - Paul Benoit got 2nd



Upcoming CTFs & Events

- Mitre CTF
  - September 15 3pm to September 16, 3pm
  - Online
- CSAW CTF Qualification Round
  - September 15 12pm to September 17, 12pm
  - Online
  - Finals at NYU November 9-11

Things to Look At in Web

- Right click, view page source
  - Could also use right click, Inspect element
- Login boxes
- Browser Development Tools
- Cookies
  - Chrome - EditThisCookie
  - Firefox - Cookies Manager+
- URL crawling

Command Injection

- User inputs command that runs on server
  - Input in URL, in Login box, in a form that the user fills out, etc.
  - Probably linux commands
  - “;” vs “&&”

- Code injection
  - Like command injection but with code (PHP, JavaScript)

Cross-Site Scripting (XSS)

- Kind of like code injection except malicious code (usually JavaScript) is executed client-side and not server-side

Types of XSS

- Reflective XSS
  - Usually means JavaScript in URL
  - Chrome and FF try to stop this
  - Not persistent because it's all in one HTTP request and response
- Stored XSS
  - Persistent because stored in text on page (like in a comment)
- Self XSS
  - U R dumb
  - Someone social engineered you into opening browser dev tools and running it on yourself

Preventing XSS

- Filter HTML, PHP, JavaScript
  - How?

- <> ( ) { } [ ] " ' ; / \
  - Escape the above characters

Cookies

- Store info on user session
  - It's the way site's "remember" you
- In real life, attackers try to steal yours
- In competition, you're the attacker.
  - May have to modify the value of your own cookie
  - Or create cookie

SQL Injection

- Structured Query Language
  - Used for accessing databases
- Normal User Login
  - User enters creds
  - Generates a query to database
  - If user and password in database, logs in
- SQL Injection Login
  - User generates own query
  - Could be used to view, change, delete, or steal data from database
  - Unauthorized log in

SQL Injection Example

- pass
- SELECT * FROM users WHERE name='admin' and password='pass'

- ' or '1'='1
- SELECT * FROM users WHERE name='admin' and password='' or '1'='1

- In competition, done almost exclusively in login boxes
- In real world, can be executed in URL

Preventing SQL Injection

- Sanitize database inputs
  - Use escape strings
- Limit length of login input
- Don’t store passwords in plaintext
  - Hash them and SALT THE HASHES

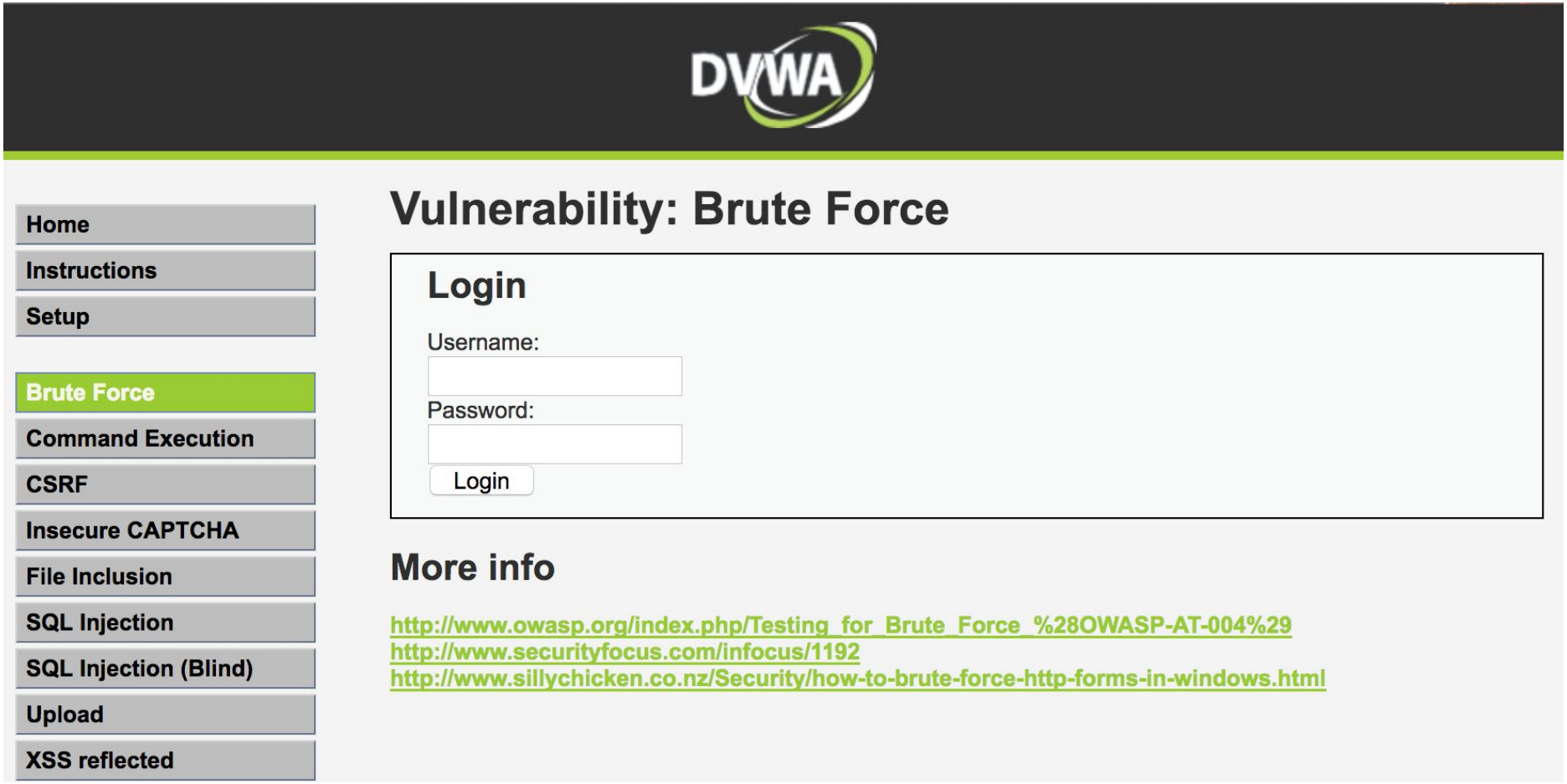
Further Resources

- OWASP Top 10
  - Open Web Application Security Project
  - go.gmu.edu/owasp

- Hack This Site
  - Web Exploitation Challenges
  - go.gmu.edu/hackthissite

Damn Vulnerable Web App

- go.gmu.edu/damn
  - Web Exploitation Challenges



Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™