Workshop & Convo: Web Application Pentesting

Seth Piercey
Focus: Why Web Apps?

- Many attack vectors
- Many users
- Easily accessible
- $$$ if you’re good at it
OWASP Top Ten

• **OWASP**: “The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.”
  - Great resource

• **Top Ten**: “The Ten Most Critical Web Application Security Risks”
  - Per year
WebGoat

• A vulnerable web app
• Follow Instructions at https://github.com/WebGoat/WebGoat
• When its running, go to http://localhost:8080/WebGoat/login
Proxies

- WebGoat > General > HTTP Proxies
- TL;DR
  Proxies sit between your computer and a server to allow you to analyze web traffic between the two machines
- We’re using Zed Attack Proxy (ZAP) as the proxy service, and FoxyProxy to turn it on/off
ZAP & FoxyProxy setup

- Start ZAP > “No, do not persist session”
  - Tools > Options
  - Select Local Proxy
  - Input 8090 for port
- FoxyProxy > Options
  - Add new proxy
  - IP: 127.0.0.1
    Port: 8090
- Test it out! You should see traffic on ZAP
WebGoat 8

• Some things to try:
  – Http Proxies
  – Authentication Bypasses
  – XSS
  – SQL Injection
  – Client Side
Getting a Job in Web App PT

- Know OWASP & OWASP Top Ten
- Understand differences between different attack subclasses, and when to use each
- Always improve your skills
  - CTFs (hackthebox, hacker101 ctf, WebGoat)
  - Studying latest and greatest
- Use your skills IRL