Performing a Professional Web Application Penetration Test

Scott Miller
Security Consultant
Synopsys Software Integrity Group

Who is Scott?

- Security Consultant at Synopsys SIG
- Studied Computer Science at the University of Florida
- Vice President of the UF Student InfoSec Team
- Interned at Symantec in Mountain View, CA
- Diversity and inclusion
- I love fun, miniature things, and adventures (outside especially)
- White water kayaking is one of my favorite things

Why be a pen tester?

- Fun
- Money
- Fame
- Freedom
- Learning

Basic steps in a pen test

1. Scope the application
2. Create a threat model
3. Identify primary business operations
4. Destroy the app
5. Report your tales of destruction

Creating a Threat Model

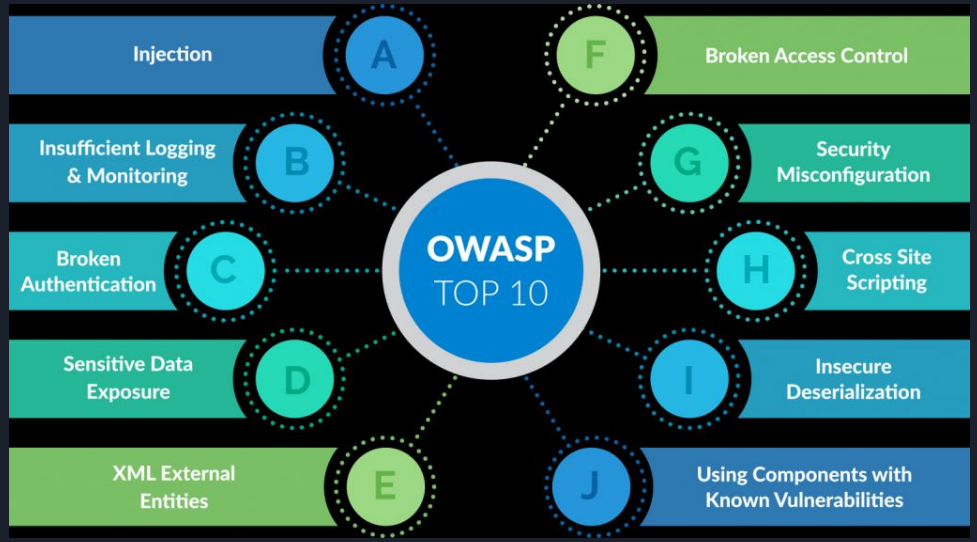
Assets	Threats	Attack Vectors	Controls	Priority
credentials	Leaked creds	Social engineering	Staff training	
Payment info	Unauthorized access	Injection - sql	Prepared statements Input validation	
Personal order info	‘’	Malicious file upload	Verifying file integrity Antivirus	
Personal info	‘’			

Identify Important Business Workflows

1. Login workflow
2. Order juice
3. Track an order
4. Send a complaint
5. File upload

Next Steps

1. Automated scan + triage
2. Checklist
3. Manual testing by priority



Resources

- https://github.com/juliocesarfort/public-pentesting-reports
- https://www.owasp.org/index.php/OWASP_Juice_Shop_Project
- https://www.owasp.org/
- https://synopsys.com/careers
  - Security Services Intern
  - Security Services Associate Consultant

Contact me!

- scott.miller@synopsys.com
- https://linkedin.com/in/scottalanmiller9
- Find me at a conference
- Find me using OSINT

QUESTIONS?