Web Application Security

Jason Ko

Agenda

- Problem statement
- What have I been doing all week?
- The Lernaean Challenge?
- Impact on Stakeholders
- Remediation
- SDLC and Prevention

What the heck is wrong?

- Businesses need web applications as a platform to stay competitive
- Most web applications are preeeetty bad security wise
- What happens if someone does a hacky hack hack?
- Very bad things depending on the application

What have I actually been doing all week?

- Good question.

The Lernaean Challenge

Also known as how to try SQL Injection for 20 minutes before Larry asks if you've tried googling the challenge name for hints and you do and then you find out you have to use hydra and then you cry but then you suck it up because there is no time for crying in this subject.

What is Lernaean?

- Web challenge on HackTheBox
- Involves using Hydra, a brute force password cracker
- I cracked the thing and entered the password and hey presto
- Using curl to get the response page to get the flag
- Or alternatively actually remembering how to use Burp Suite properly to get you the flag

Impact on Stakeholders

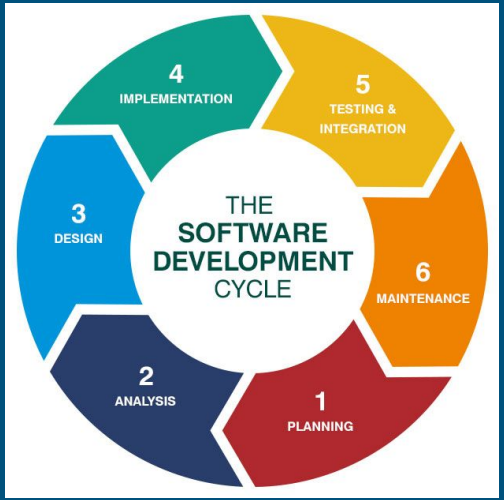
- It’s pretty bad
  - Gaining administrator access on anything is pretty bad
- Financial and Reputation loss
  - I mean look at RSA Security after 2011

Remediation

- Remediation Pro Tip:
  - Actually secure your internal system before you do a public service announcement
- Remediation is half public relations and half technical recovery
- Be transparent, but not so transparent you get hacked again
  - That’s pretty bad

Prevention and the SDLC

- “IDS and IPS has never been useful for anything” - Robert Mitchell
- Software Development Life Cycle
  - Only useful if you develop with security in mind at EVERY step of the cycle
  - No point only thinking about security at the testing stage and finding out everything is insecure



Thank