A Peek Behind the Curtain How Pentesters "See" Your Web Application

(and how you can too)

Who Am I?

- Recovering developer
  - Not originally web! C, C++
- Web Application Security Consultant
  AppSec Consulting
  - AKA Pentester

- Occasional Twitter user
  - @fortytwowho

Dispelling Myths & Gaining Visibility

- I validated that field on the client, the user can’t modify that
- Client side obfuscation protects me from XYZ
- When security through obscurity…isn’t

Avoid Jail, Pass Go, Collect $200

- Rule 0: Look but don’t touch
- Unless…
  - You have permission…in writing
  - You wrote it && your server *thumbs up*
  - Bug bounty…Check the rules *proceed with caution*

Resources

- Proxys
  - Burp https://portswigger.net/burp/download.html
  - ZAP https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
  - Fiddler https://www.telerik.com/download/fiddler

Resources

- Proxy change extensions
  - Firefox – FoxyProxy - https://addons.mozilla.org/en-us/firefox/addon/foxyproxy-standard/
  - Chrome – SwitchyOmega - https://chrome.google.com/webstore/detail/proxy-switchyomega/padekgcemlokbadohgkifijomclgjgif?hl=en

Resources

- Installing certificate in browser
  - https://support.portswigger.net/customer/portal/articles/1783075-installing-burp-s-ca-certificate-in-your-browser

Okay, Lets Do This Already

DEMO

More Deliberately Vulnerable Apps

- Mike Pirnat - A deliberately-vulnerable Python website and exercises for teaching about the OWASP Top 10
  - https://github.com/mpirnat/lets-be-bad-guys
- OWASP's WebGoat
  - https://www.owasp.org/index.php/OWASP_WebGoat_Project
- Many more…
  - http://lmgtfy.com/?q=vulnerable+web+applications+for+testing