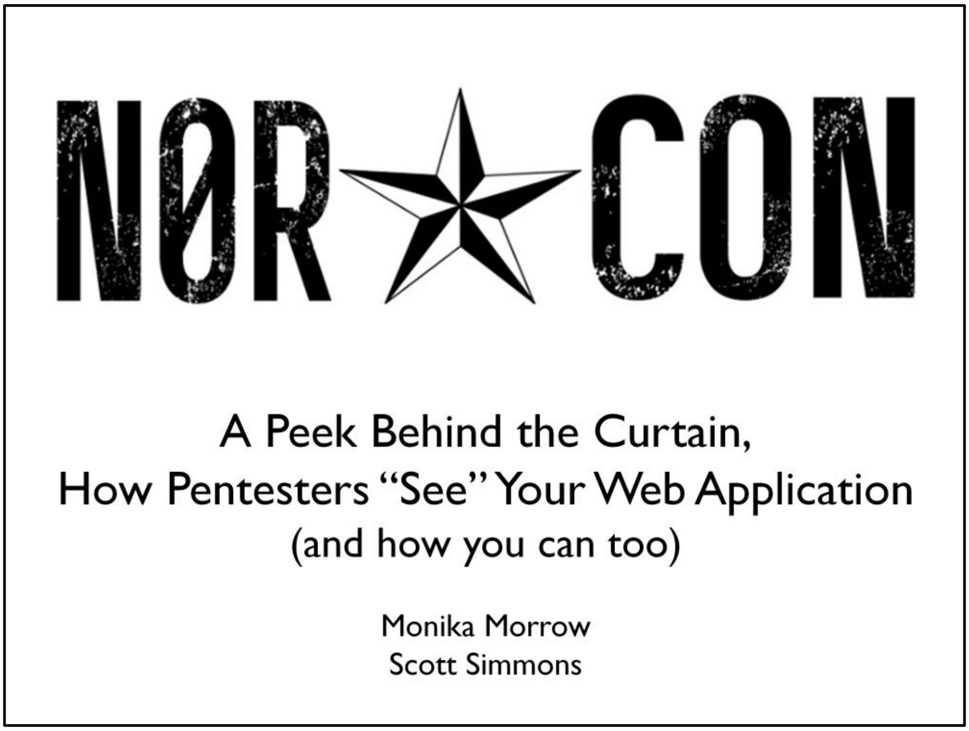
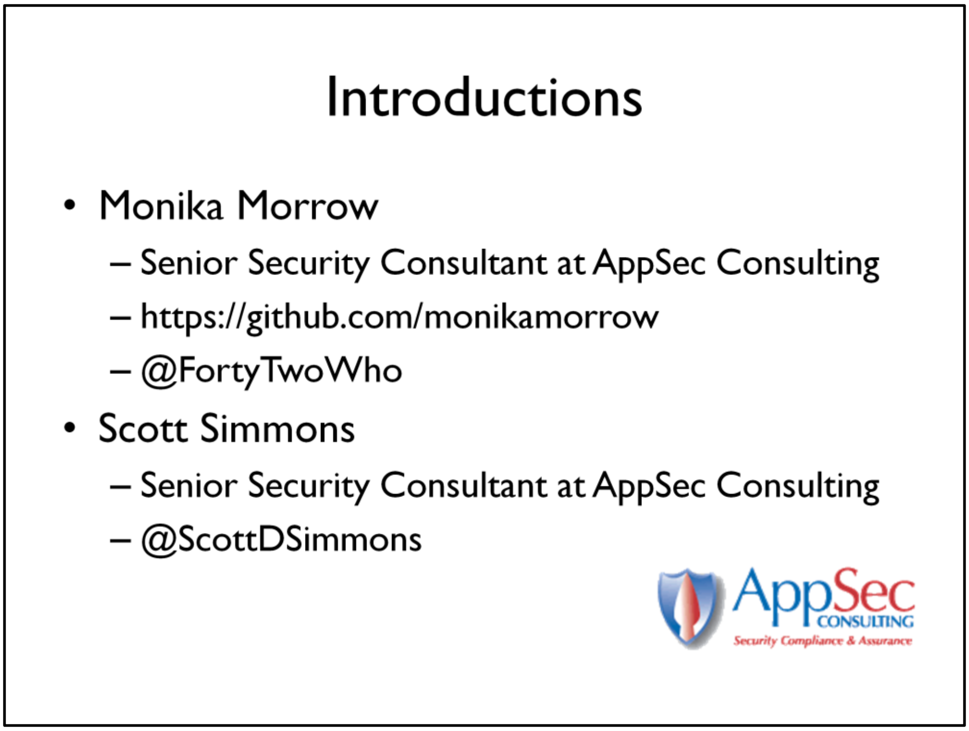


NØR★CON

A Peek Behind the Curtain, How Pentesters “See” Your Web Application (and how you can too)

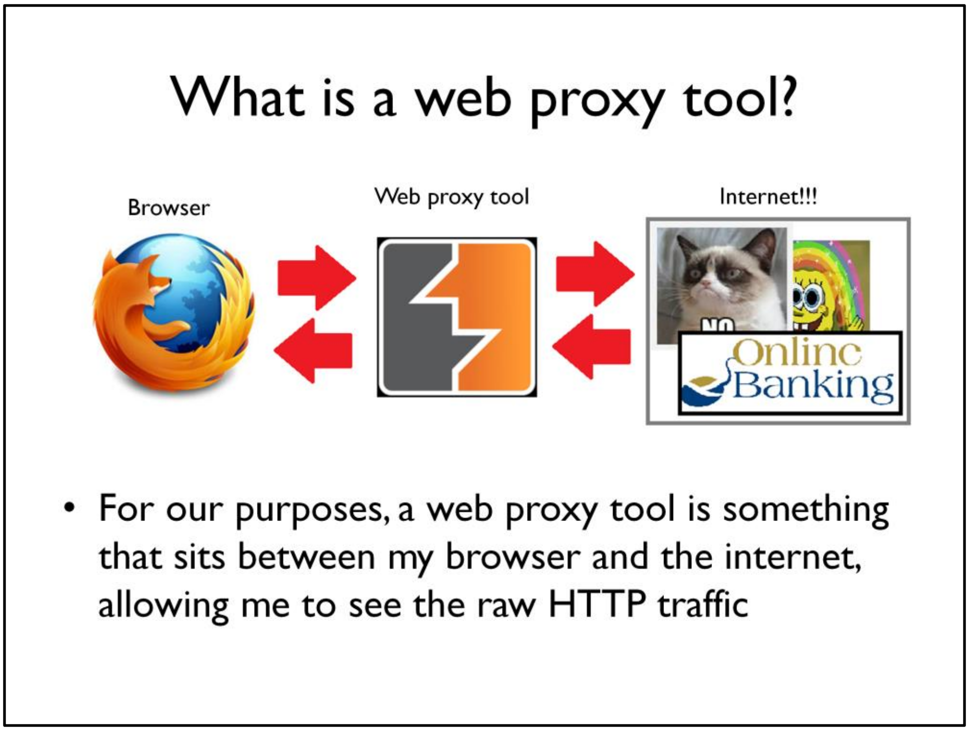
Monika Morrow
Scott Simmons



Introductions

- Monika Morrow
  - Senior Security Consultant at AppSec Consulting
  - https://github.com/monikamorrow
  - @FortyTwoWho
- Scott Simmons
  - Senior Security Consultant at AppSec Consulting
  - @ScottDSimmons

AppSec CONSULTING Security Compliance & Assurance



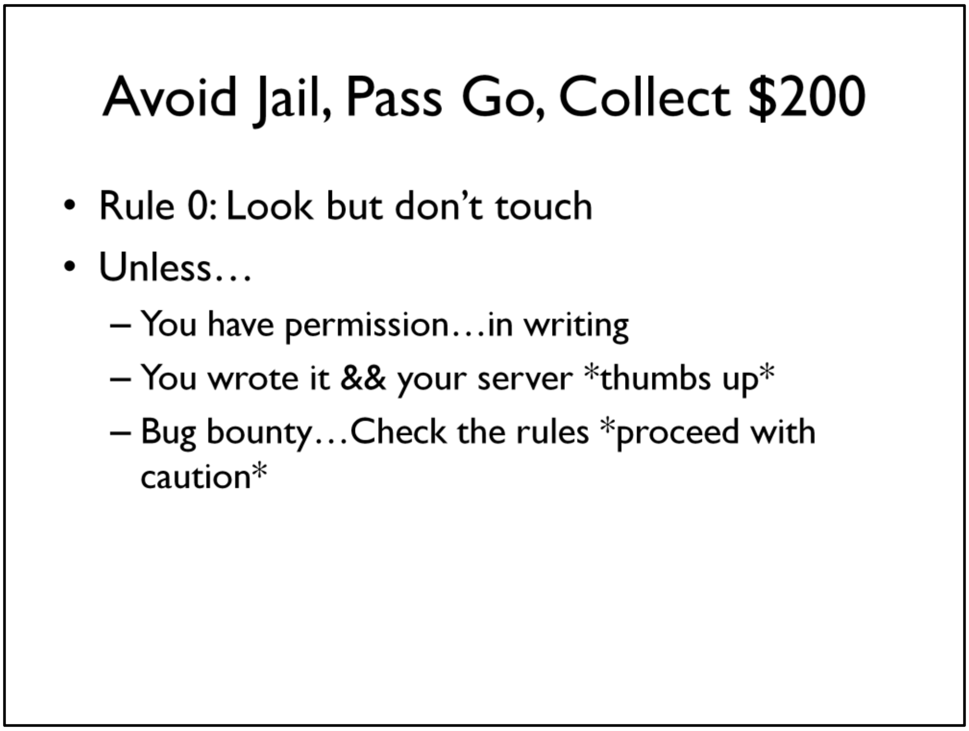
What is a web proxy tool?

Browser

Web proxy tool

Internet!!!

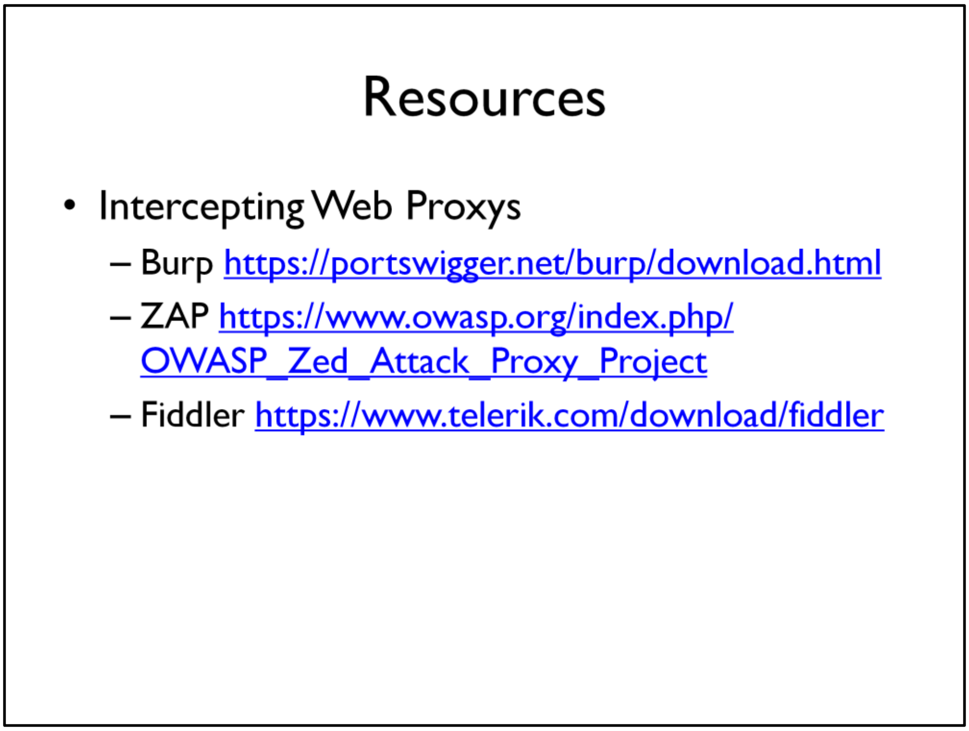
- For our purposes, a web proxy tool is something that sits between my browser and the internet, allowing me to see the raw HTTP traffic



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*

With great power….



Resources

- Intercepting Web 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

An intercepting web proxy allows you to view and modify all HTTP(S) traffic between a client and server by maintaining a man-in-the-middle position. The client makes a connection to the proxy (securely if required) and in turn the proxy makes a connection (securely if required) to the server.

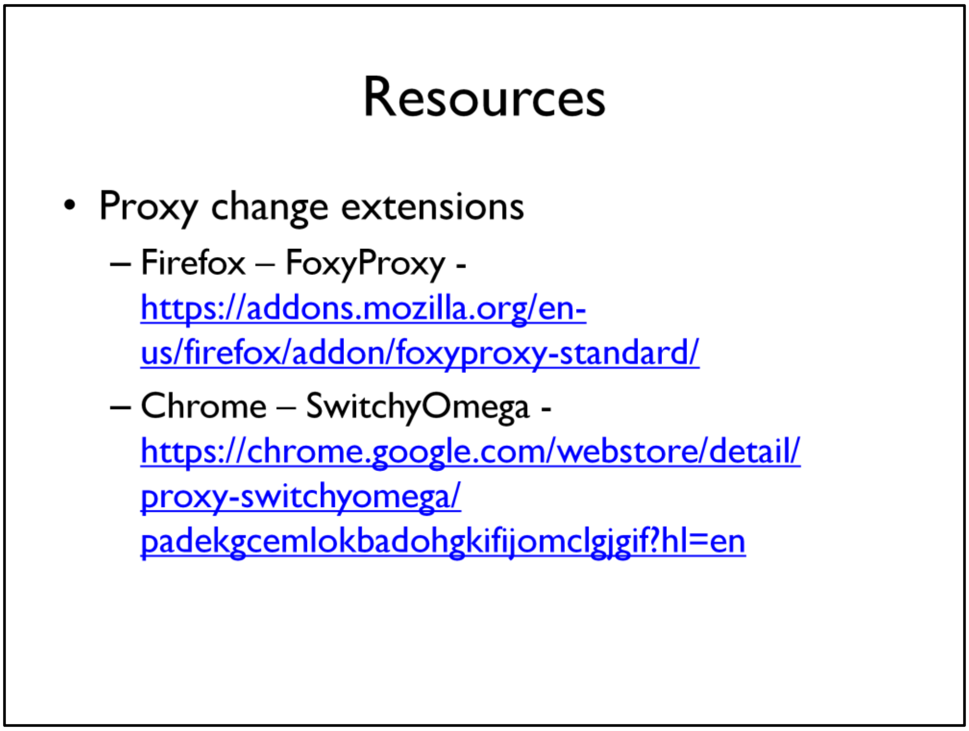
Link plaintext:
https://portswigger.net/burp/download.html
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
https://www.telerik.com/download/fiddler

Okay, Lets Do This Already

DEMO

Troy Hunt – Hack Yourself First
http://hackyourselffirst.troyhunt.com/

Troy Hunt – Hack Yourself First
Link plaintext:
http://hackyourselffirst.troyhunt.com/

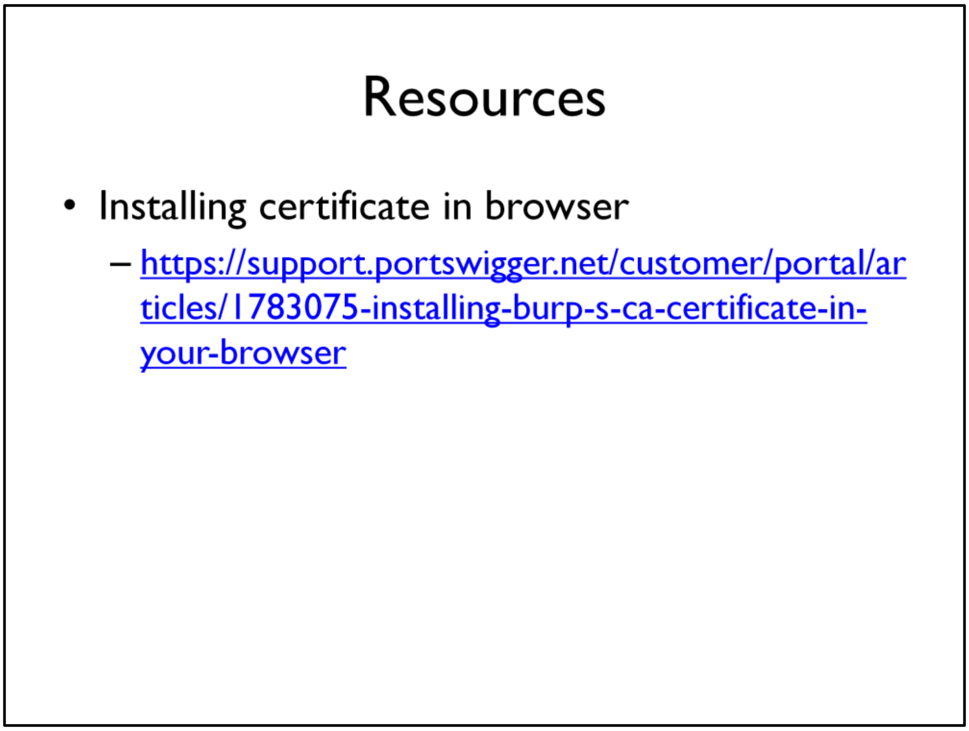


Resources

- 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

Firefox has its own proxy so it sends only browser traffic to the configured proxy. FoxyProxy makes it easier/faster to switch between configured proxys or no proxy. Chrome by default uses the system proxy so configuring Chrome to use a proxy sends all system HTTP(S)/Websocket traffic through the proxy. This can make it hard to isolate the traffic you want to examine. The SwitchyOmega extension for Chrome allows you to send only Chrome traffic to your web interception proxy and makes it easy to select a proxy or no proxy.

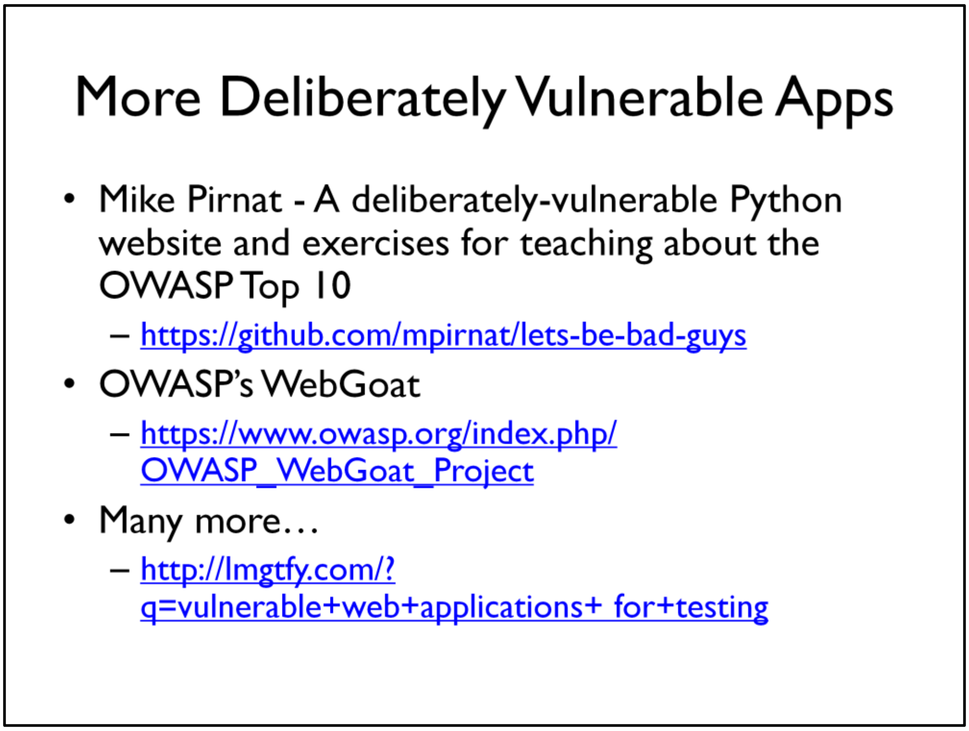
Link plaintext:
https://addons.mozilla.org/en-us/firefox/addon/foxyproxy-standard/
https://chrome.google.com/webstore/detail/proxy-switchyomega/padekgcemlokbadohgkifijomclgjgif?hl=en



Resources

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

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



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

Mike spoke at CodeMash (Thursday Jan 7, 2016), "Using Python to Get Out The Vote"
https://speakerdeck.com/mpirnat/using-python-to-get-out-the-vote
Also see:
https://speakerdeck.com/mpirnat/shiny-lets-be-bad-guys-exploiting-and-mitigating-the-top-10-web-app-vulnerabilities-2015-edition

Link plaintext:
https://github.com/mpirnat/lets-be-bad-guys
https://www.owasp.org/index.php/OWASP_WebGoat_Project
http://lmgtfy.com/?q=vulnerable+web+applications+for+testing

More?

- The Web Application Hackers Handbook
  http://mdsec.net/wahh/

Link plaintext:
http://mdsec.net/wahh/