OWASP
Open Web Application Security Project

ZAP, Burp, and Other Funny Noises

Paul Kern
December 13, 2018

INTERCEPTION PROXIES

The Lowdown

- Analyze, inject, modify web traffic
- Works with a browser
- Some are simple with limited function
- Some are multi-function and can scan
- Essential for pen-testers
- Incredibly useful for developers

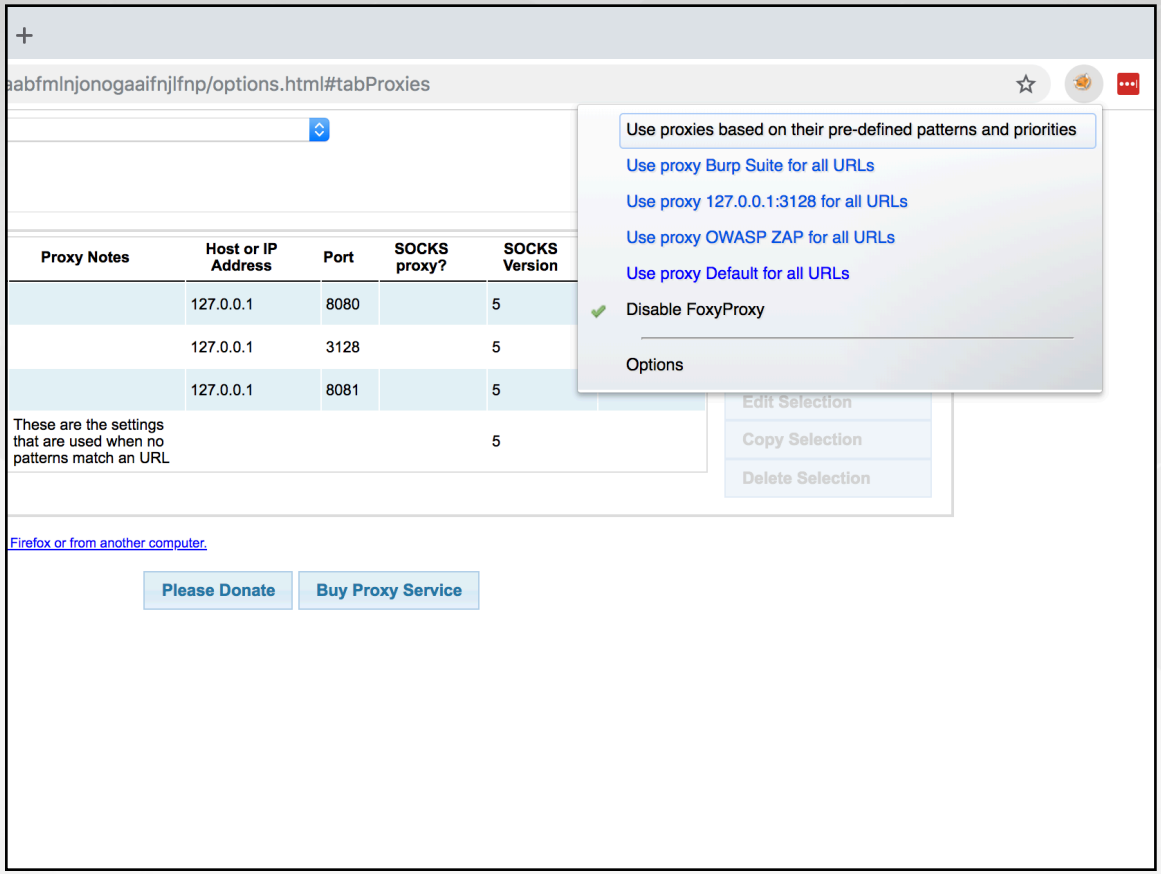
Santa says: "Only test sites for which you have permission!"

Popular Examples

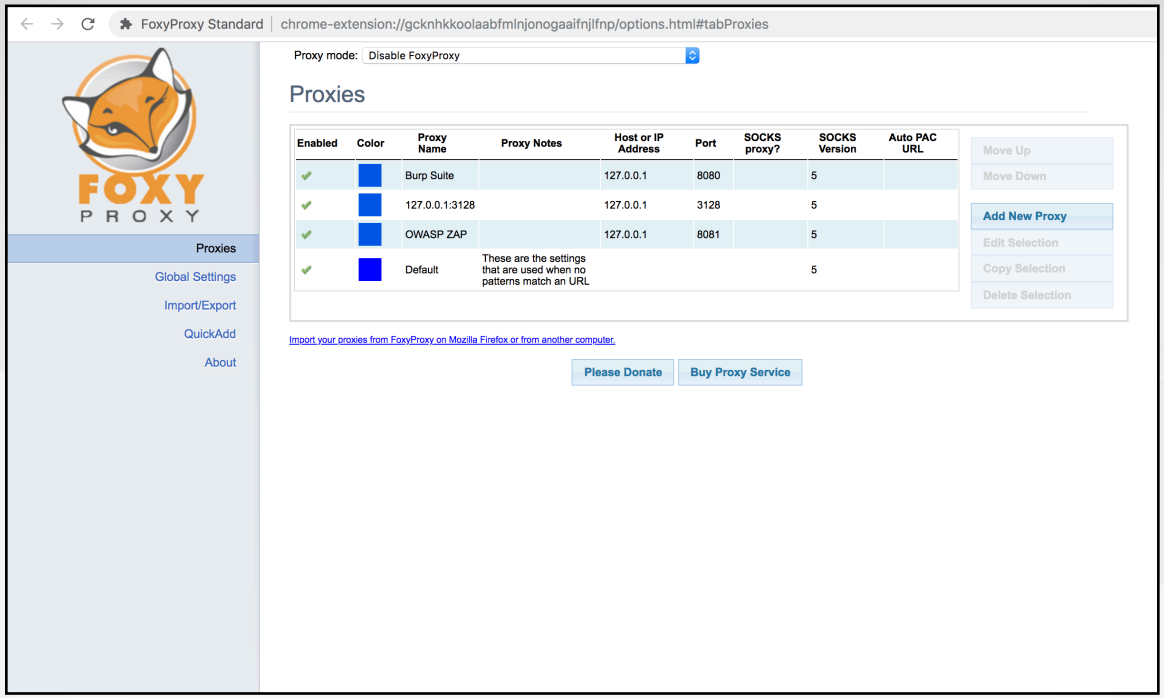
- OWASP Zed Attack Proxy (ZAP)
- Burp Suite
- Web Scarab, W3AF, MITMProxy, Fiddler
- Typically utilize local system/browser proxy settings
- Recommend a proxy switcher plugin
  - Foxy Proxy is my goto plugin
  - Works best in Chrome and Firefox

Proxy Switcher Plugin

- Browser plugin
- Quickly enable/disable/switch proxies
- Foxy Proxy and SwitchyOmega
- https://getfoxyproxy.org/downloads/
- https://chrome.google.com/webstore/detail/proxy-switchyomega/padekgcemlokbadohgkifijomclgjgif



Foxy Proxy Quick Change



Foxy Proxy Settings

OWASP ZAP

ZAP

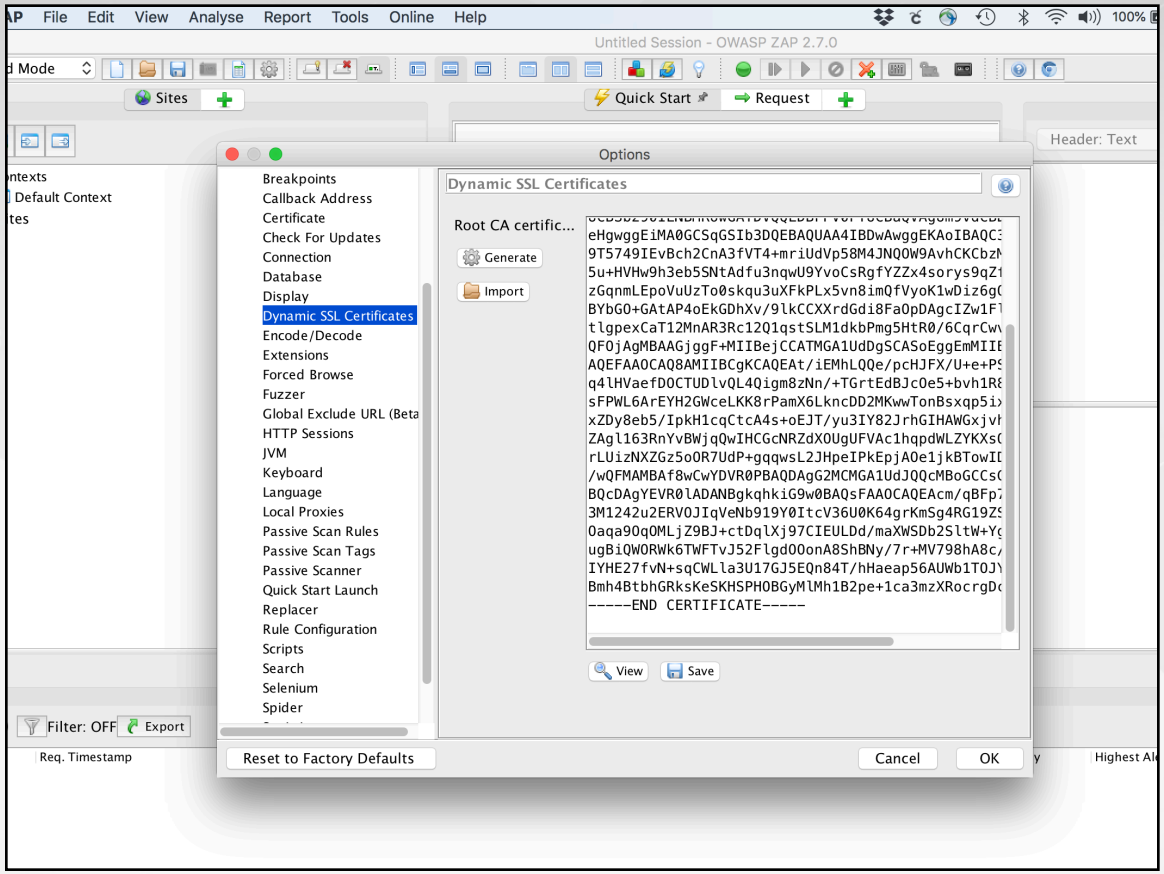
- Zed Attack Proxy
- Current version is 2.7.0
- Requires the Java Runtime Environment
- Useful for pen testers, developers, beginners
- Open Source (Free)
- Windows/Mac/Linux
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

ZAP Functionality

- Intercepting Proxy
- Traditional and AJAX Spiders
- Automated Scanner
- Passive Scanner
- Forced Browsing
- Fuzzer
- Supports Web Sockets
- REST based API
- More

ZAP Root CA Certificate

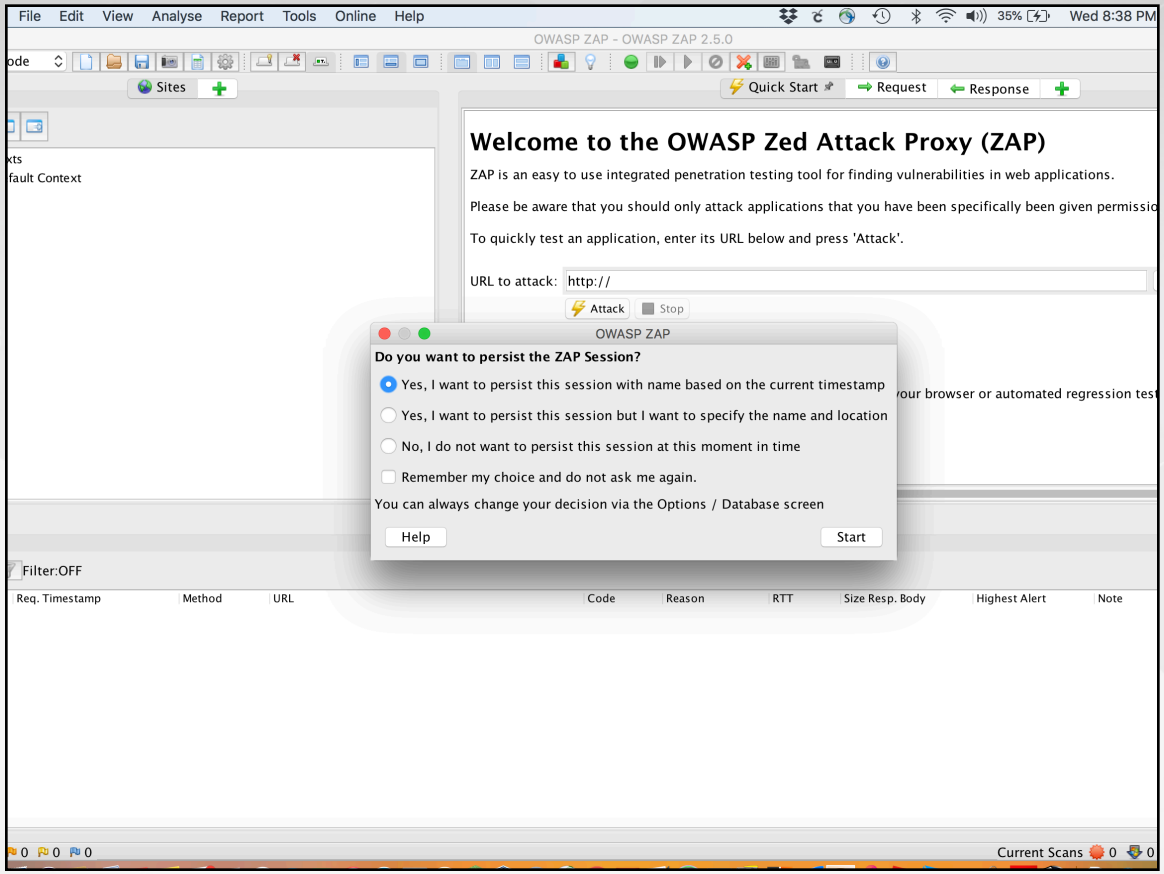
- First run will tell you to regenerate the root CA certificate
- Needed to prevent the browser from throwing SSL warnings
  - **Tools > Options > Dynamic SSL Certs**
  - Click ***Generate*** and then save the cert
  - Import the new cert to your browser
  - https://support.portswigger.net/customer/portal/articles/1783075-installing-burp-s-ca-certificate-in-your-browser



Generate CA Certificate

Session Persistance

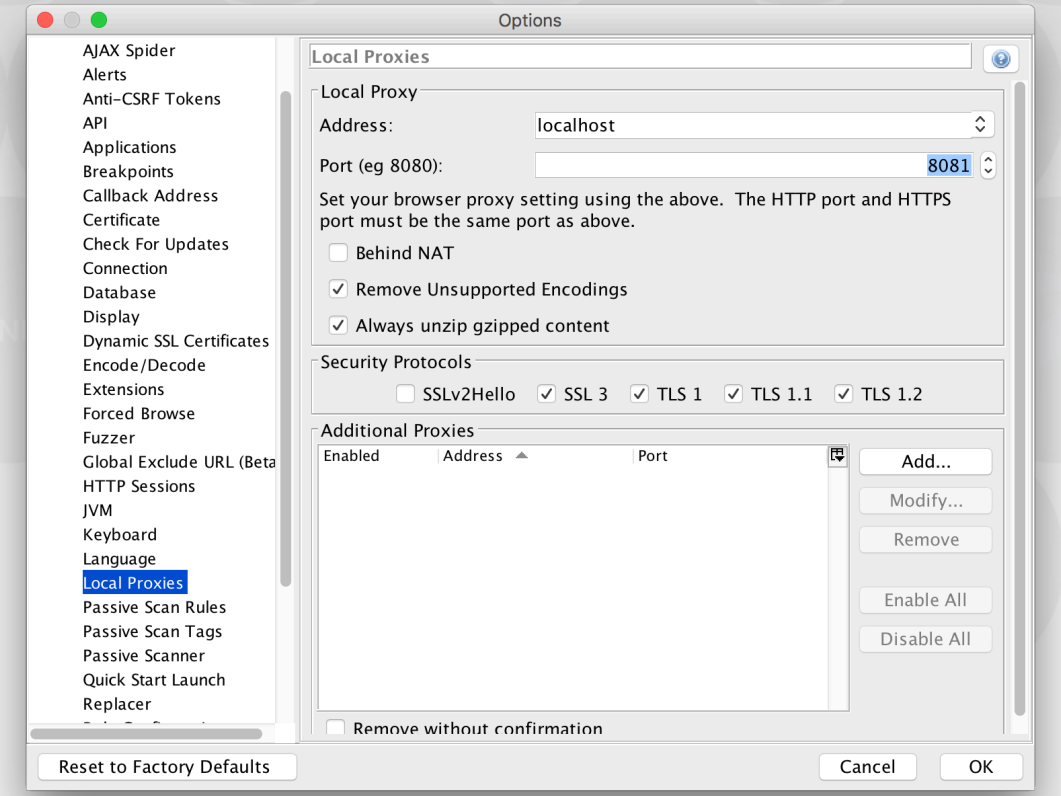
- Prompts you when ZAP starts
- Useful for long-term engagements
- Can decide not to store sessions
  - Data is lost when ZAP closes
- Popup can be disabled
  - **Options** > **Database** to re-enable



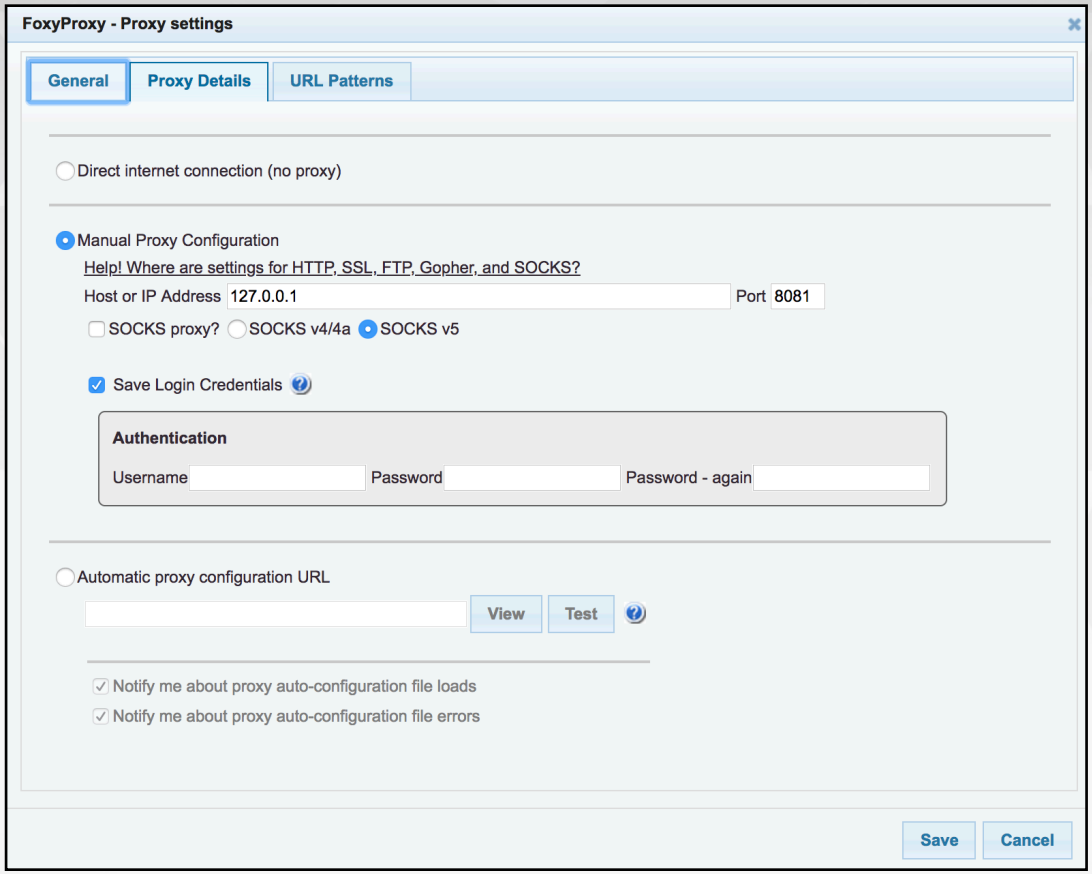
Session Persistance Prompt

Proxy Settings in ZAP

- **Zap > Preferences > Local Proxy**
- Default port is 8080 - I change it to 8081
- Go to Foxy Proxy and add ZAP



ZAP Proxy Settings



ZAP in Foxy Proxy

Manual Intercept with ZAP

- Open ZAP and enable it in your browser
- Browse to the web application location to be tested
- Find it in the history and then set a break point
- Browse to that same location
- A Break Point tab will be shown next to the Request and Response tabs.
- Modify the request and then click the ***Submit and Step to Next Request or Response*** button
- Let's try it.

Passive and Active Scanning with ZAP

- ZAP is also a Web application scanner
- A useful tool to have in the toolbox
- Can supplement other tools
- Possible alternative to commercial tools
- Can do passive and active scanning
- Crawling is also an option
- Let's check it out…

Learn More!

- https://chrisdecairos.ca/intercepting-traffic-with-zaproxy/
- http://sashimw.blogspot.com/2017/01/use-zap-tool-to-intercept-http-traffic.html
- https://blog.sodaksec.com/2018/12/owasp-zap-part-1-intercepting-traffic.html

BURP SUITE

About Burp Suite

- Developed and maintained by Portswigger
- https://portswigger.net/burp/
- Great documentation and tutorials
- Requires Java (sigh)
- Three versions
  - Community
  - Professional
  - Enterprise

Version Comparison

Community

- Free
- Essential Manual Tools
- Intruder Functionality is Time-Throttled

Professional

- $399/year
- Web App Scanner
- Essential Manual Tools
- Advanced Manual Tools

Enterprise

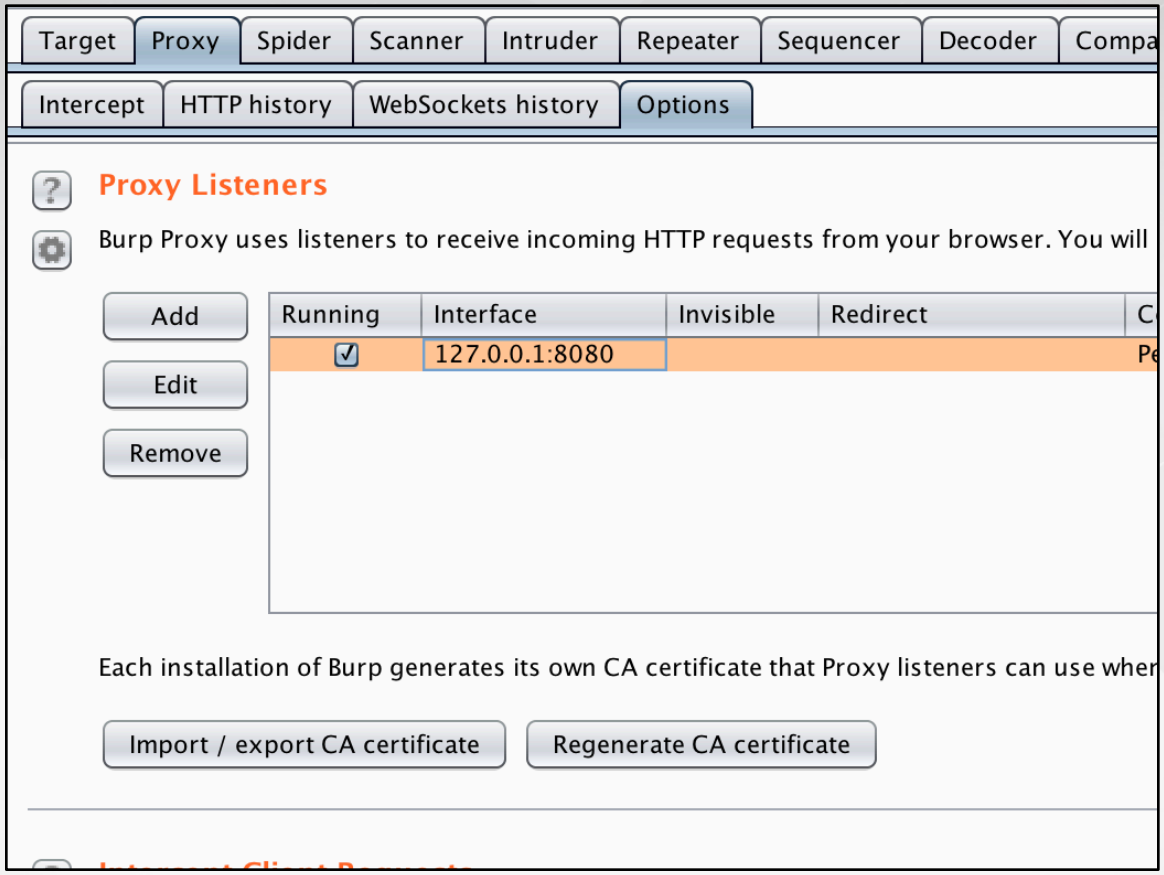
- $3,999/year
- Web App Scanner
- Scan Scheduler
- CI Integration
- Unlimited Scalability

Install Burp

- Need Java Runtime Environment
- Full install or run a stand-alone JAR
- https://portswigger.net/burp/

Burp Proxy Settings

- In Burp, go to the ***Proxy*** tab
- Choose the ***Options*** sub tab
- **127.0.0.1:8080** should already be listed
- Check that item if it isn't already
- 8080 is an arbitrary port - we will keep it
- Close the window to keep changes
- Add Burp to Foxy Proxy



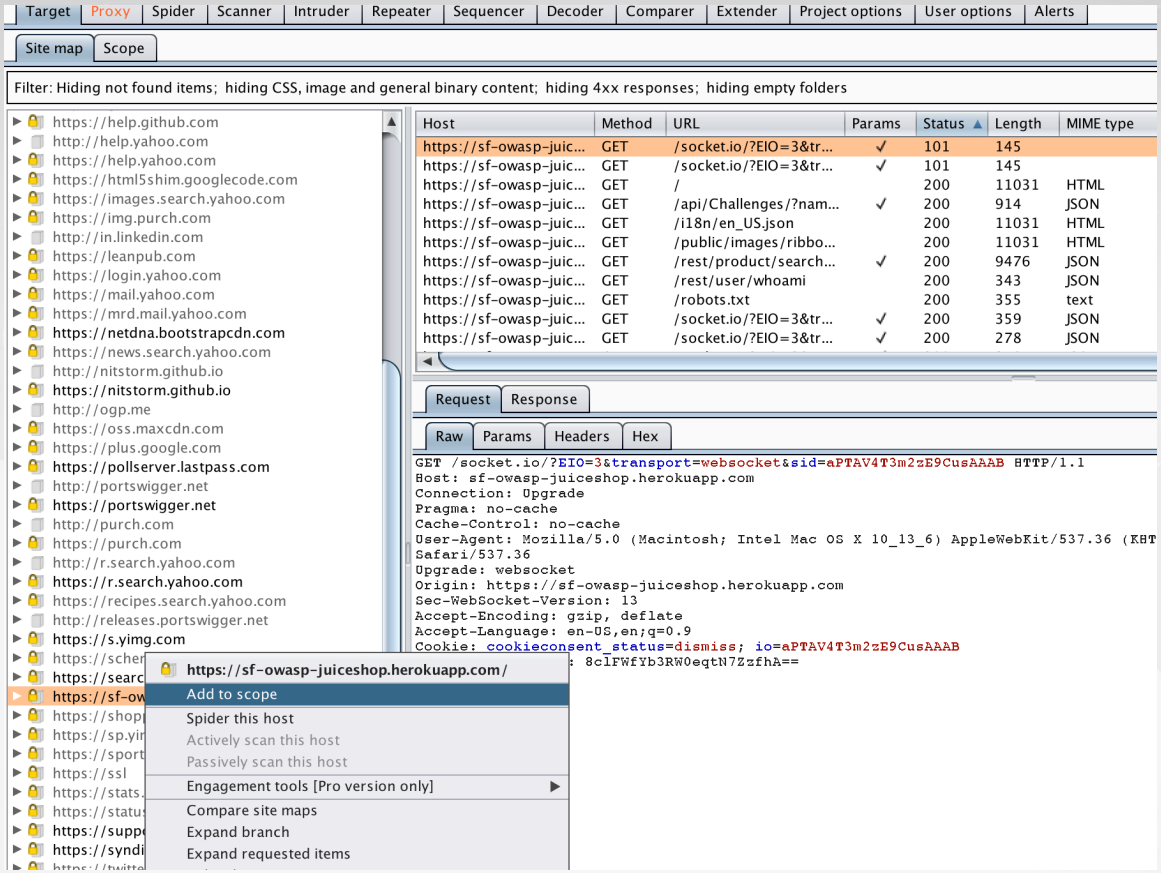
Burp Proxy Settings

Portswigger CA Certificate

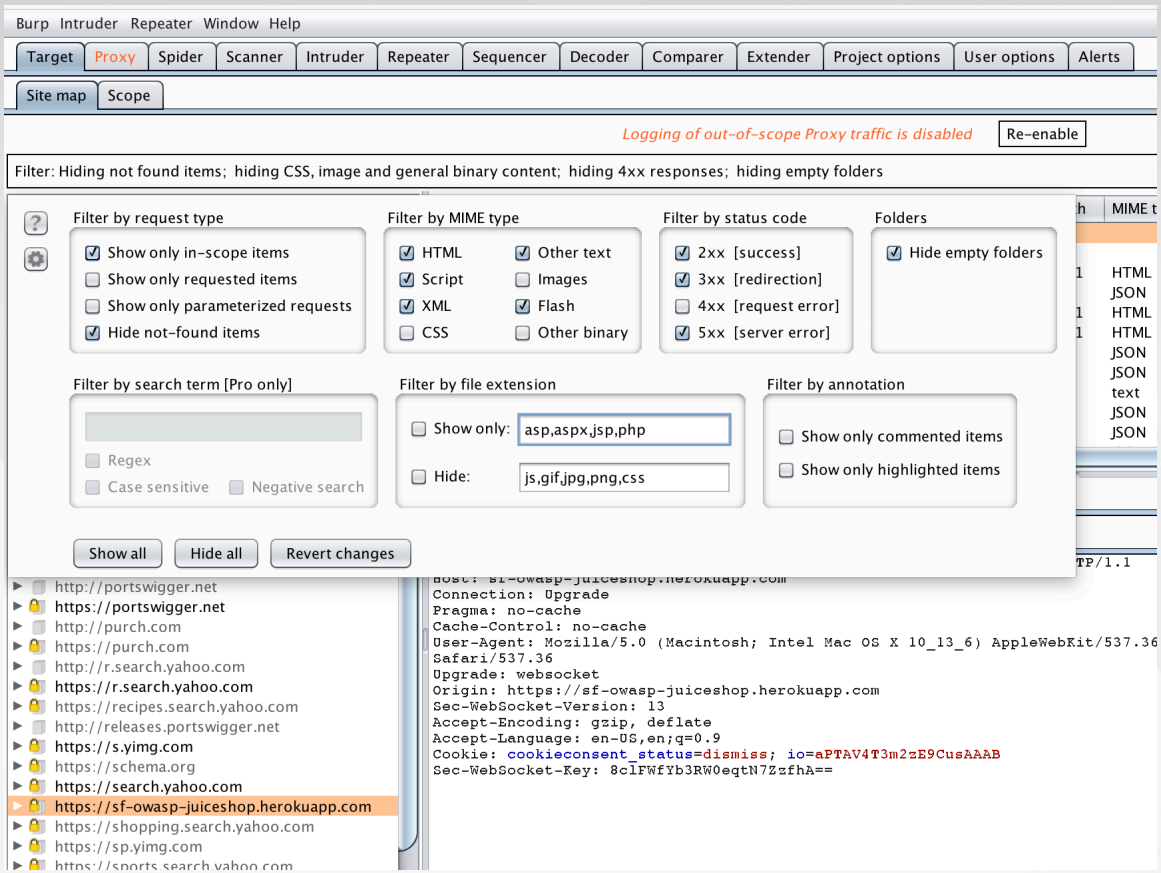
- Start Burp and Enable it in Foxy Proxy
- In the browser, go to https://burp
- Download the CA Certificate
- Import the certificate to your browser
- https://support.portswigger.net/customer/portal/articles/1783075-installing-burp-s-ca-certificate-in-your-browser

Target Tab

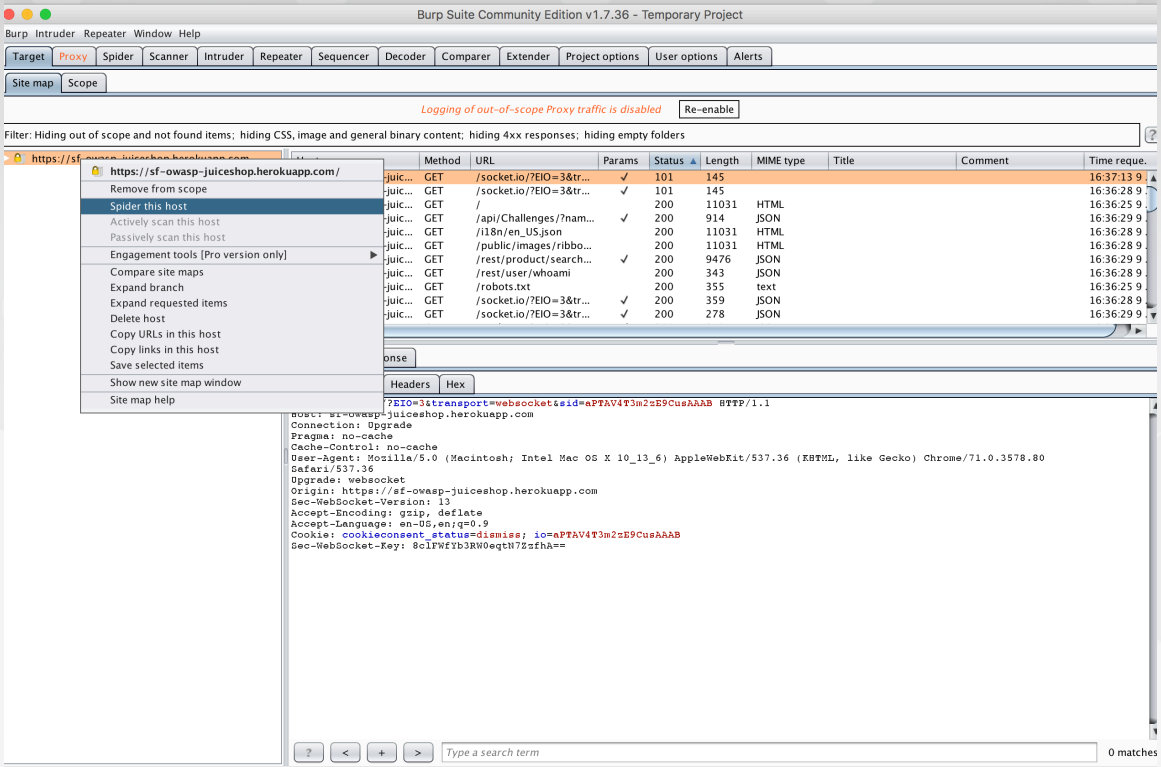
- Identified sites & spider results
- Connection history
- Requests and Responses
- Scope should be set here
- Good idea to crawl the site from here



Adding a URL to the Scope



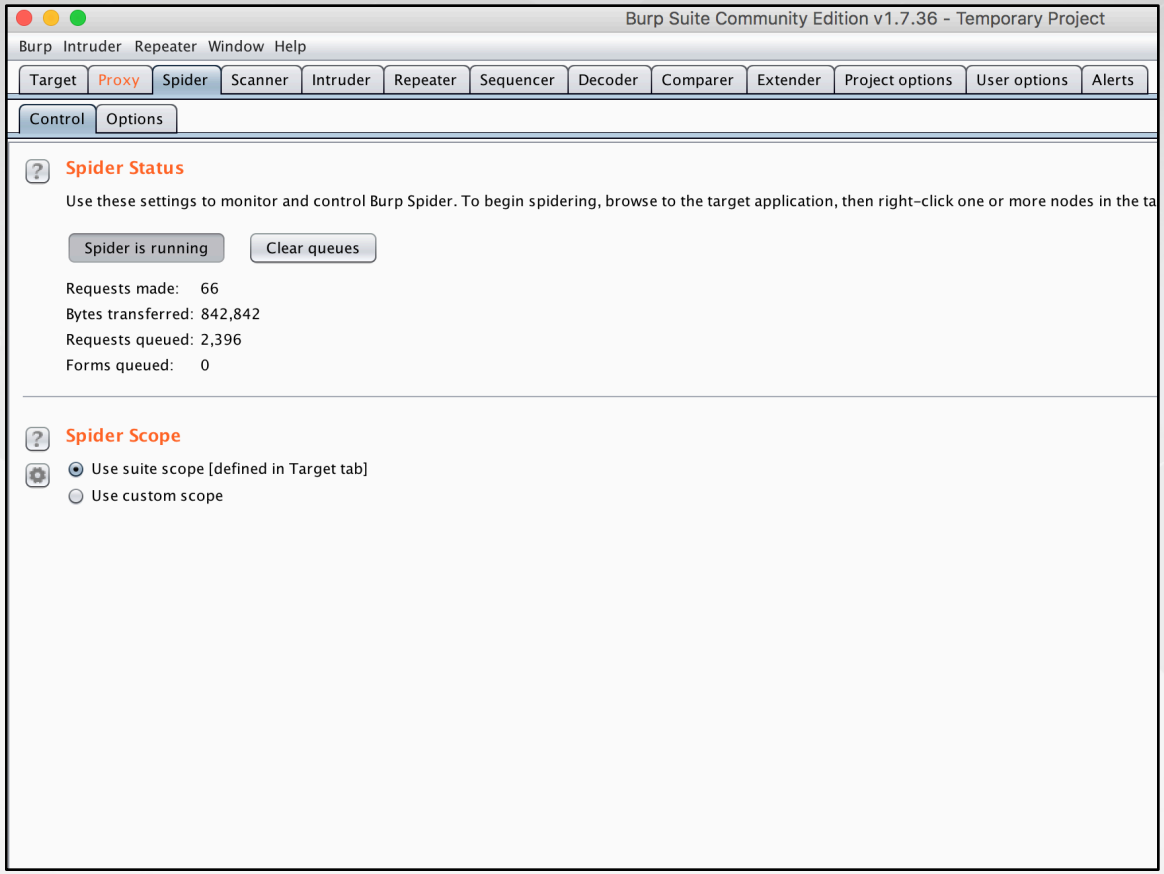
Filtering by Scope



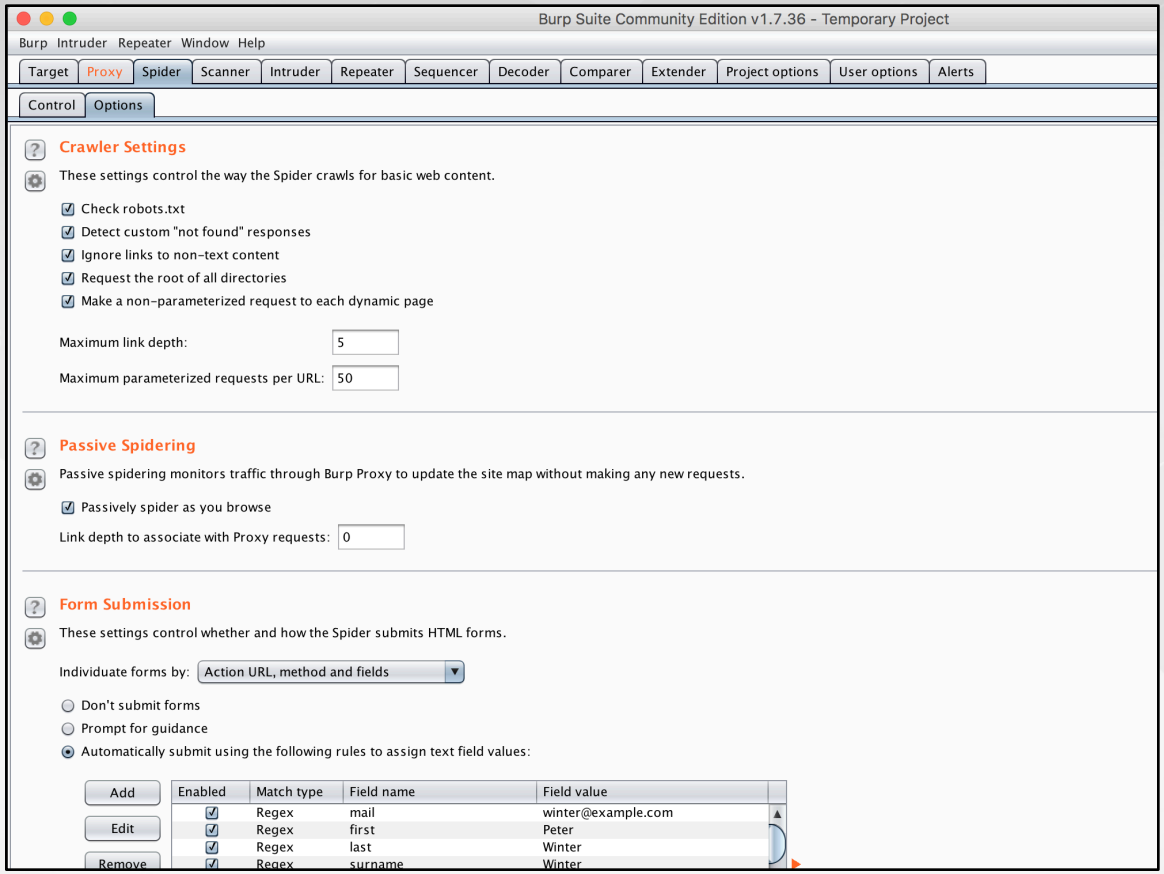
Spider the Site

Spider Tab

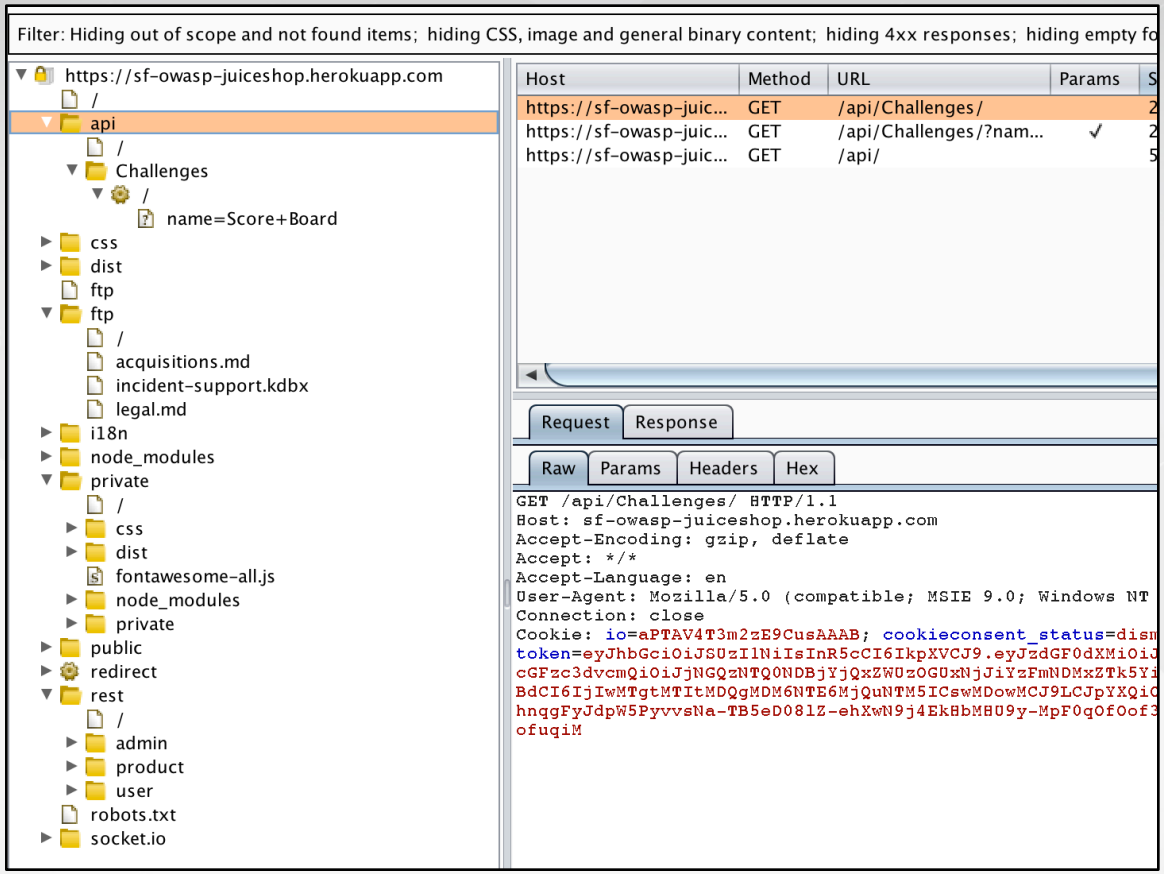
- Contains results from a spider operation
- Spider populates data in Target tab
- Helps identify the structure of the site
- Helps find low-hanging fruit
- Multiple options that can be configured


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Control Options
Spider Status
Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the ta
Spider is running
Clear queues
Requests made: 66
Bytes transferred: 842,842
Requests queued: 2,396
Forms queued: 0
Spider Scope
Use suite scope [defined in Target tab]
Use custom scope

Spider Tab



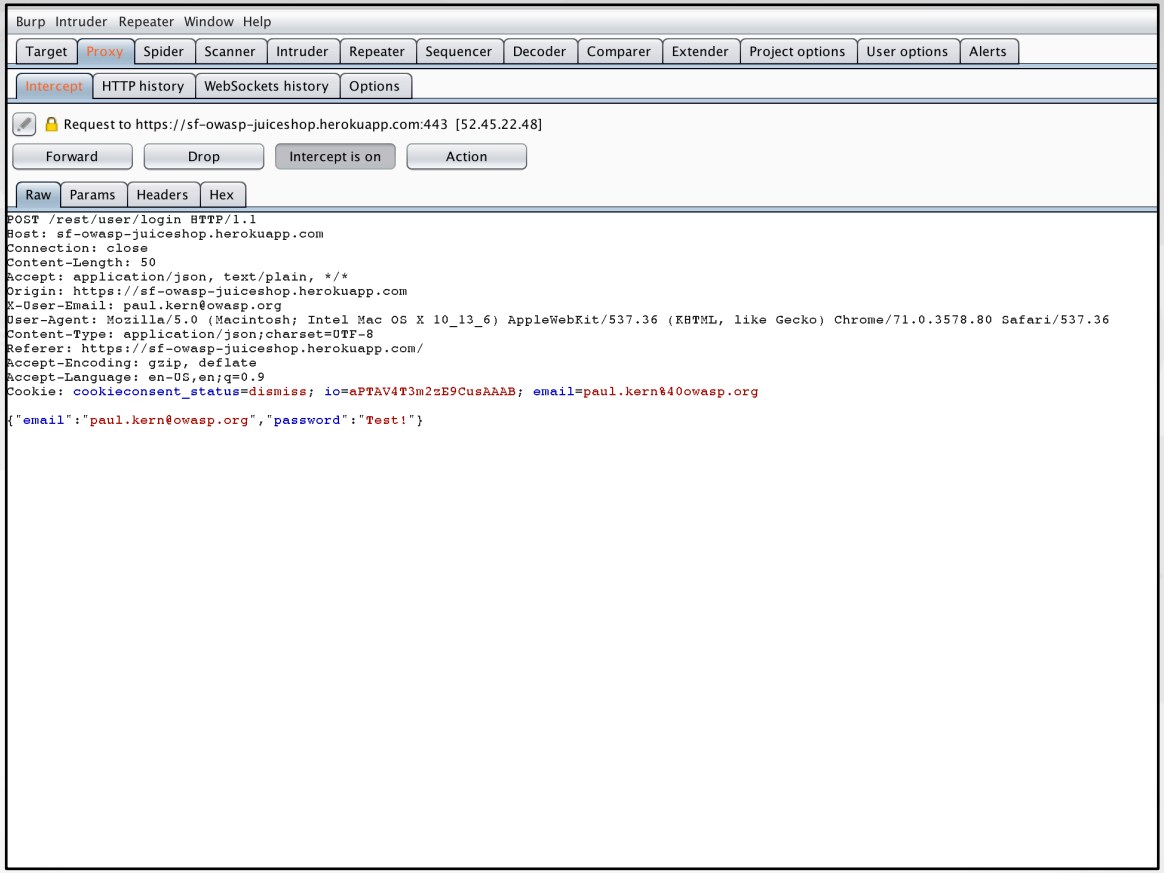
Spider Options



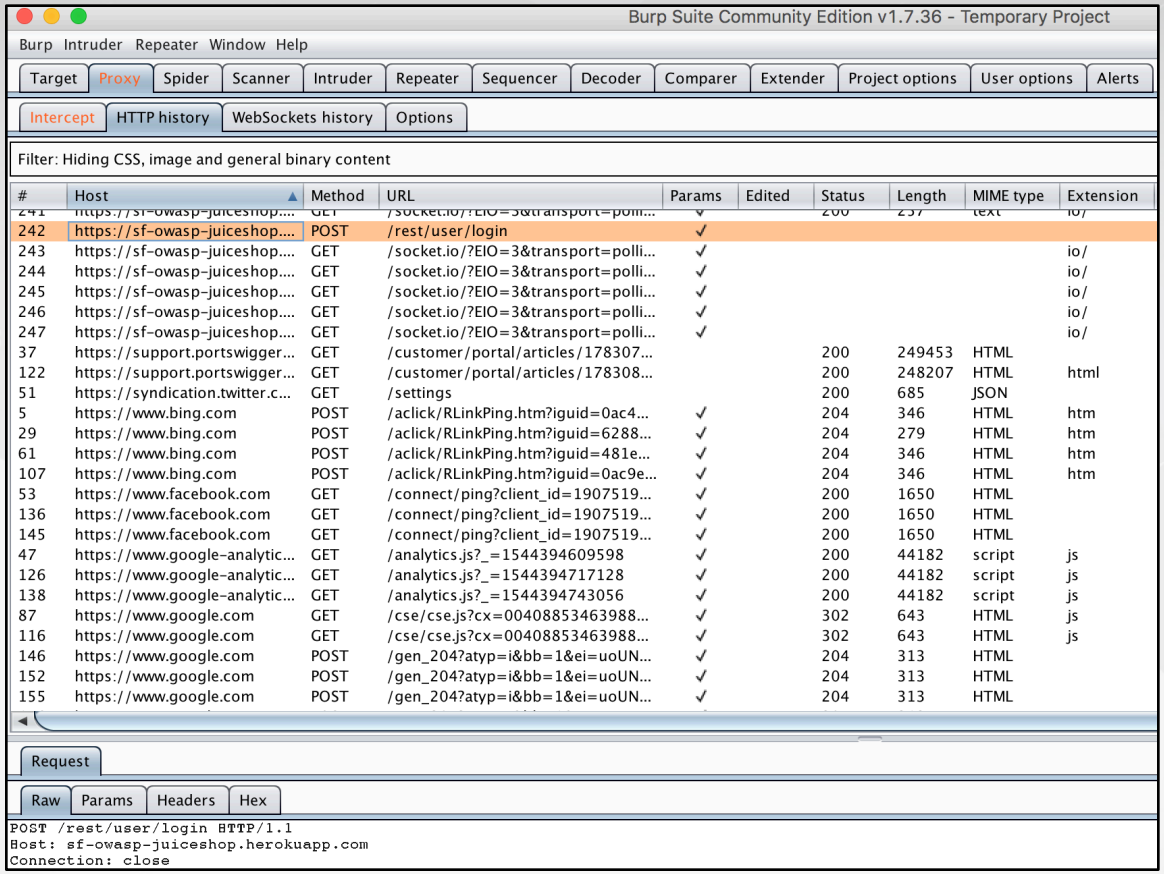
Target Information Populated by Spider

Proxy Tab/Manual Intercept

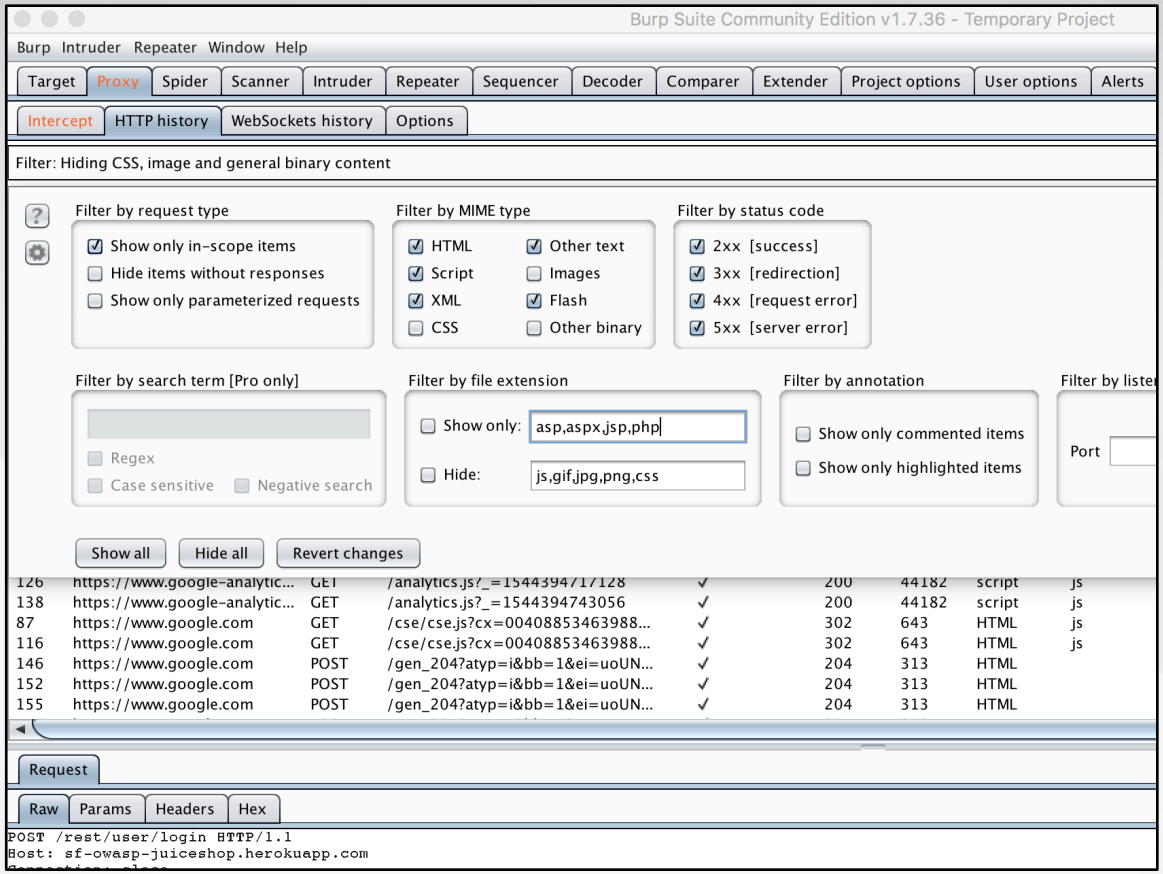
- The most basic function of the tool
- Manually intercept requests and responses
- Identify potential problems
- Proof of concept testing
- Quick examinations
- lots_of_time_spent_here = FALSE


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to https://sf-owasp-juiceshop.herokuapp.com:443 [52.45.22.48]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /rest/user/login HTTP/1.1
Host: sf-owasp-juiceshop.herokuapp.com
Connection: close
Content-Length: 50
Accept: application/json, text/plain, */*
Origin: https://sf-owasp-juiceshop.herokuapp.com
X-User-Email: paul.kern@owasp.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.80 Safari/537.36
Content-Type: application/json;charset=UTF-8
Referer: https://sf-owasp-juiceshop.herokuapp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: cookieconsent_status=dismiss; io=aPTAV4T3m2zE9CusAAAB; email=paul.kern%40owasp.org
{"email":"paul.kern@owasp.org","password":"Test!"}

Proxy Tab



Proxy History



Scope Filter

Manual Tools

Burp Posts
https://blog.sodaksec.com

Burp Repeater
https://portswigger.net/burp/documentation/desktop/tools/repeater/using

Burp Intruder
https://portswigger.net/burp/documentation/desktop/tools/intruder/getting-started

Burp Sequencer
https://portswigger.net/burp/documentation/desktop/tools/sequencer/getting-started

Burp Decoder
https://portswigger.net/burp/documentation/desktop/tools/decoder

Burp Comparer
https://portswigger.net/burp/documentation/desktop/tools/comparer

Burp and ZAP Together

- Burp and ZAP can be used together
- Can supplement Burp Community with ZAP scanning
- Can chain proxies
  - Can scan while using Burp Community
  - https://bit.ly/2PxDZGJ
  - https://bit.ly/2LcO8b2

Other Learning Opportunities

- Set up your own Juice Shop Instance
  - VM or the Cloud
  - Check cloud providers AUP
  - Heroku is pretty lenient
- SANS Holiday Hack Challenge
  - https://bit.ly/2ErtGTj
  - Educational, fun and free.

Questions?

- paul.kern@owasp.org
- https://blog.sodaksec.com
  - I have some tutorials on ZAP and Burp
  - Be gentle in the comments
  - If you find a mistake, let me know