



OWASP

Open Web Application  
Security Project

# ZAP, Burp, and Other Funny Noises

Paul Kern  
December 13, 2018

CONNECT.

LEARN.

GROW.

# INTERCEPTION PROXIES



**OWASP**  
Open Web Application  
Security Project

# 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!”

GROW.



**OWASP**  
Open Web Application  
Security Project

# 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

Proxies

Global Settings

Import/Export

QuickAdd

About

Proxy mode: Disable FoxyProxy

### Proxies

Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL
✓	■	Burp Suite		127.0.0.1	8080		5	
✓	■	127.0.0.1:3128		127.0.0.1	3128		5	
✓	■	OWASP ZAP		127.0.0.1	8081		5	
✓	■	Default	These are the settings that are used when no patterns match an URL				5	

Move Up

Move Down

Add New Proxy

Edit Selection

Copy Selection

Delete Selection

[Import your proxies from FoxyProxy on Mozilla Firefox or from another computer.](#)

Please Donate

Buy Proxy Service

## Foxy Proxy Settings





CONNECT.

LEARN.

GROW.

# OWASP ZAP



**OWASP**  
Open Web Application  
Security Project

# 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](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)



# ZAP Functionality

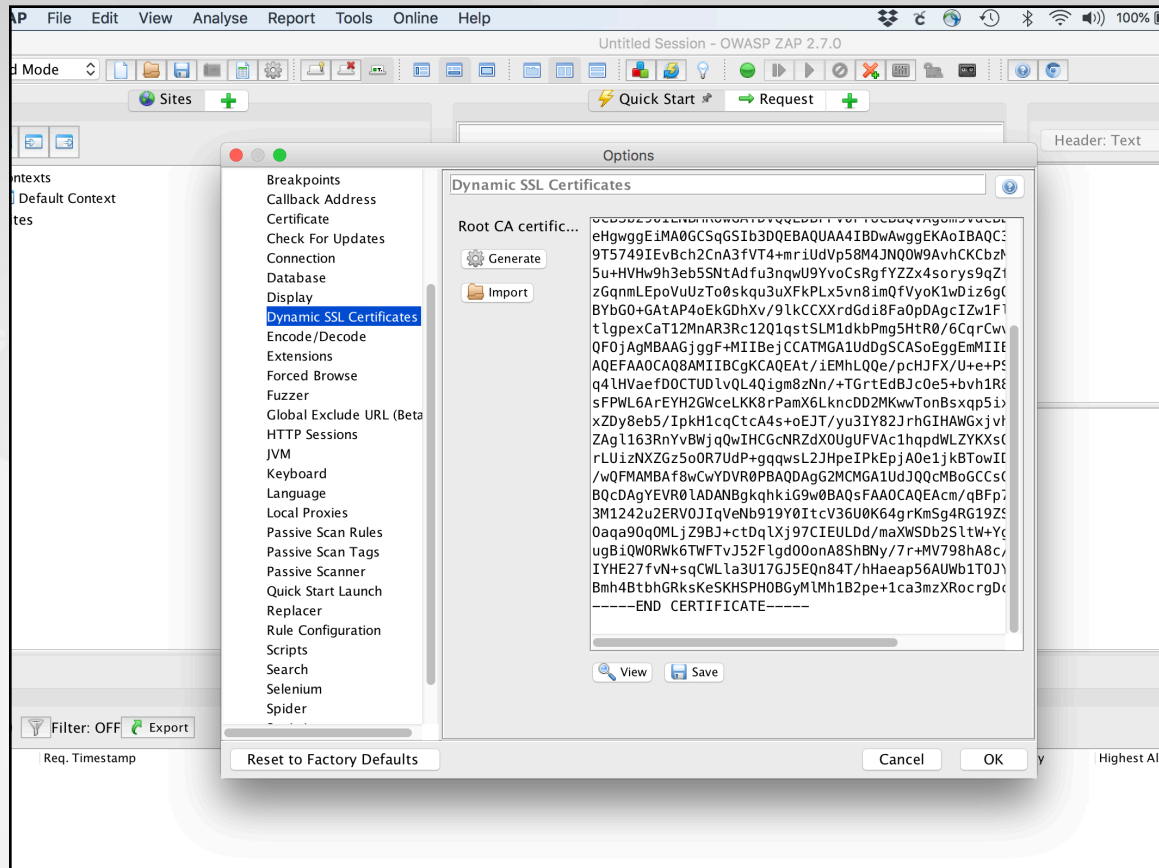
- Intercepting Proxy
- Traditional and AJAX Spiders
- Automated Scanner
- Passive Scanner
- Forced Browsing
- Fuzzer
- Supports Web Sockets
- REST based API
- More



# 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>





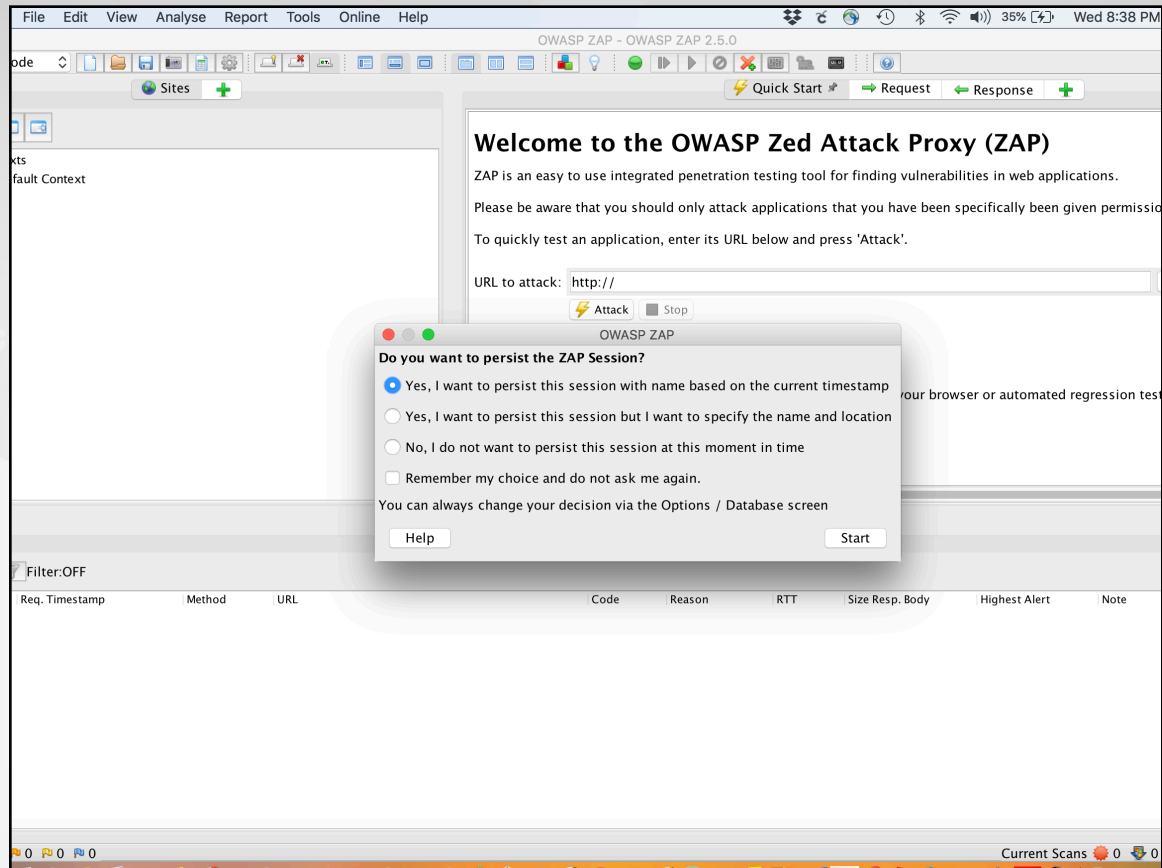
## Generate CA Certificate



# Session Persistence

- 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





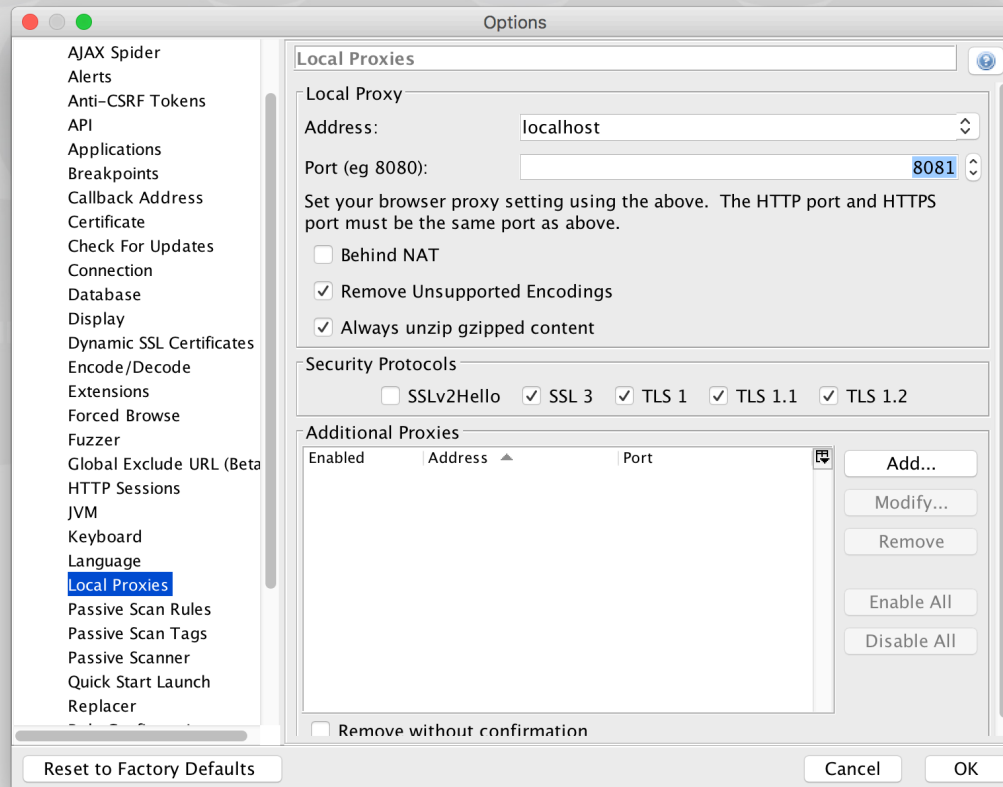
## Session Persistence Prompt

# 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



**FoxyProxy - Proxy settings**

**General** Proxy Details URL Patterns

☐ Direct internet connection (no proxy)

☒ Manual Proxy Configuration  
[Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?](#)

Host or IP Address  Port

☐ SOCKS proxy? ☐ SOCKS v4/4a ☒ SOCKS v5

☒ Save Login Credentials

**Authentication**

Username  Password  Password - again

☐ Automatic proxy configuration URL

☒ Notify me about proxy auto-configuration file loads

☒ Notify me about proxy auto-configuration file errors

## 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>



CONNECT.

LEARN.

GROW.

# BURP SUITE



**OWASP**  
Open Web Application  
Security Project

# 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

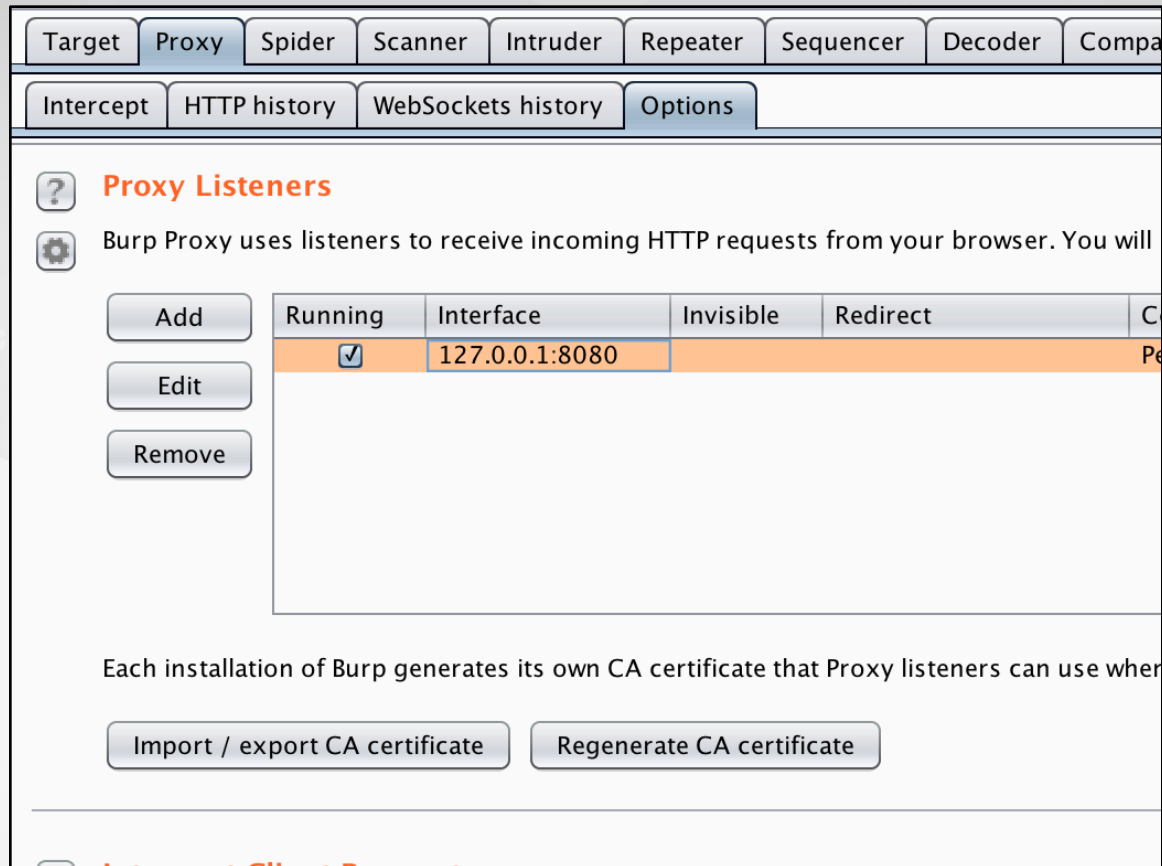
- Need Java Runtime Environment
- Full install or run a stand-alone JAR
- <https://portswigger.net/burp/>



# 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



Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type
https://sf-owasp-juic...	GET	/socket.io/?EIO=3&tr...	✓	101	145	
https://sf-owasp-juic...	GET	/socket.io/?EIO=3&tr...	✓	101	145	
https://sf-owasp-juic...	GET	/		200	11031	HTML
https://sf-owasp-juic...	GET	/api/Challenges/?nam...	✓	200	914	JSON
https://sf-owasp-juic...	GET	/i18n/en_US.json		200	11031	HTML
https://sf-owasp-juic...	GET	/public/images/ribbo...		200	11031	HTML
https://sf-owasp-juic...	GET	/rest/product/search...	✓	200	9476	JSON
https://sf-owasp-juic...	GET	/rest/user/whoami		200	343	JSON
https://sf-owasp-juic...	GET	/robots.txt		200	355	text
https://sf-owasp-juic...	GET	/socket.io/?EIO=3&tr...	✓	200	359	JSON
https://sf-owasp-juic...	GET	/socket.io/?EIO=3&tr...	✓	200	278	JSON

Request Response

Raw Params Headers Hex

```

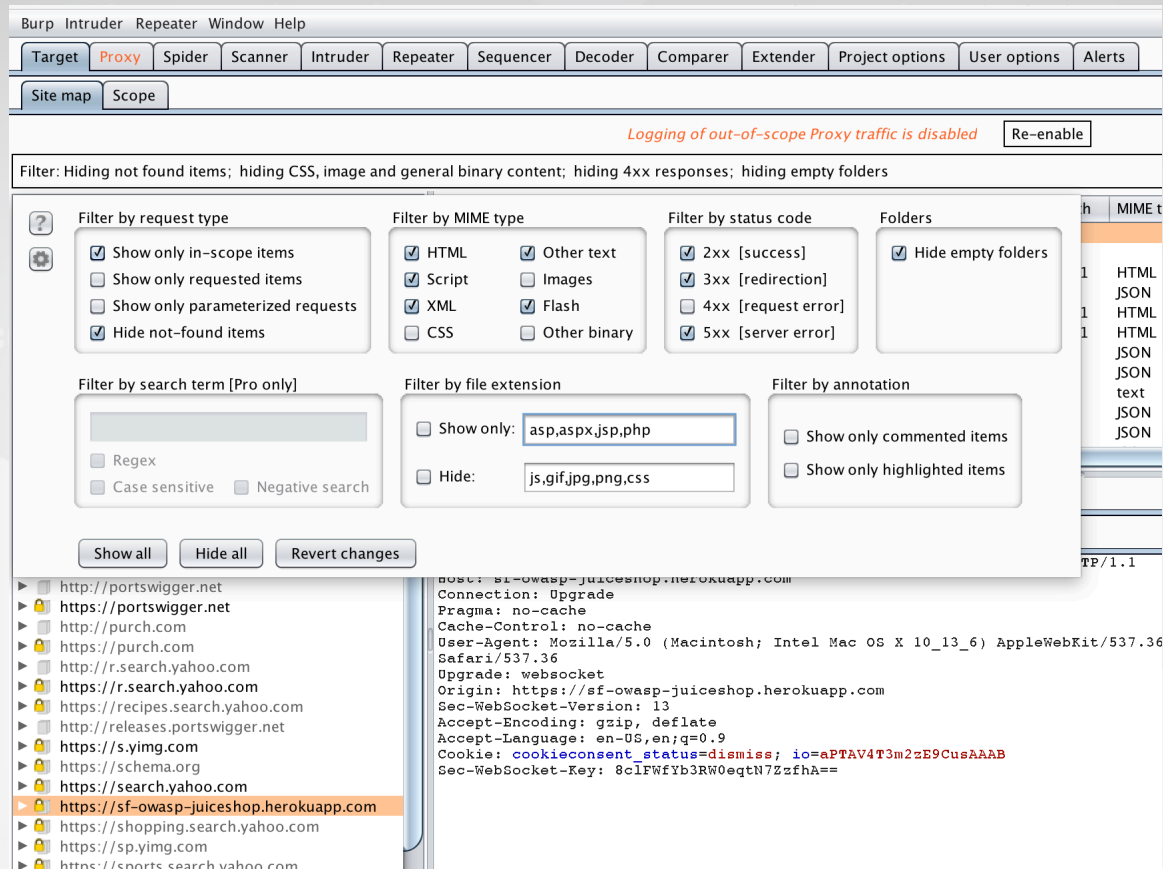
GET /socket.io/?EIO=3&transport=websocket&sid=aPTAV4T3m2zE9CusAAAB HTTP/1.1
Host: sf-owasp-juiceshop.herokuapp.com
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Upgrade: websocket
Origin: https://sf-owasp-juiceshop.herokuapp.com
Sec-WebSocket-Version: 13
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: cookieconsent_status=dismiss; io=aPTAV4T3m2zE9CusAAAB
      8c1FWfYb3RW0eqtN7Zzfha==
  
```

https://sf-owasp-juiceshop.herokuapp.com/

- Add to scope
- Spider this host
- Actively scan this host
- Passively scan this host
- Engagement tools [Pro version only]
- Compare site maps
- Expand branch
- Expand requested items

## Adding a URL to the Scope

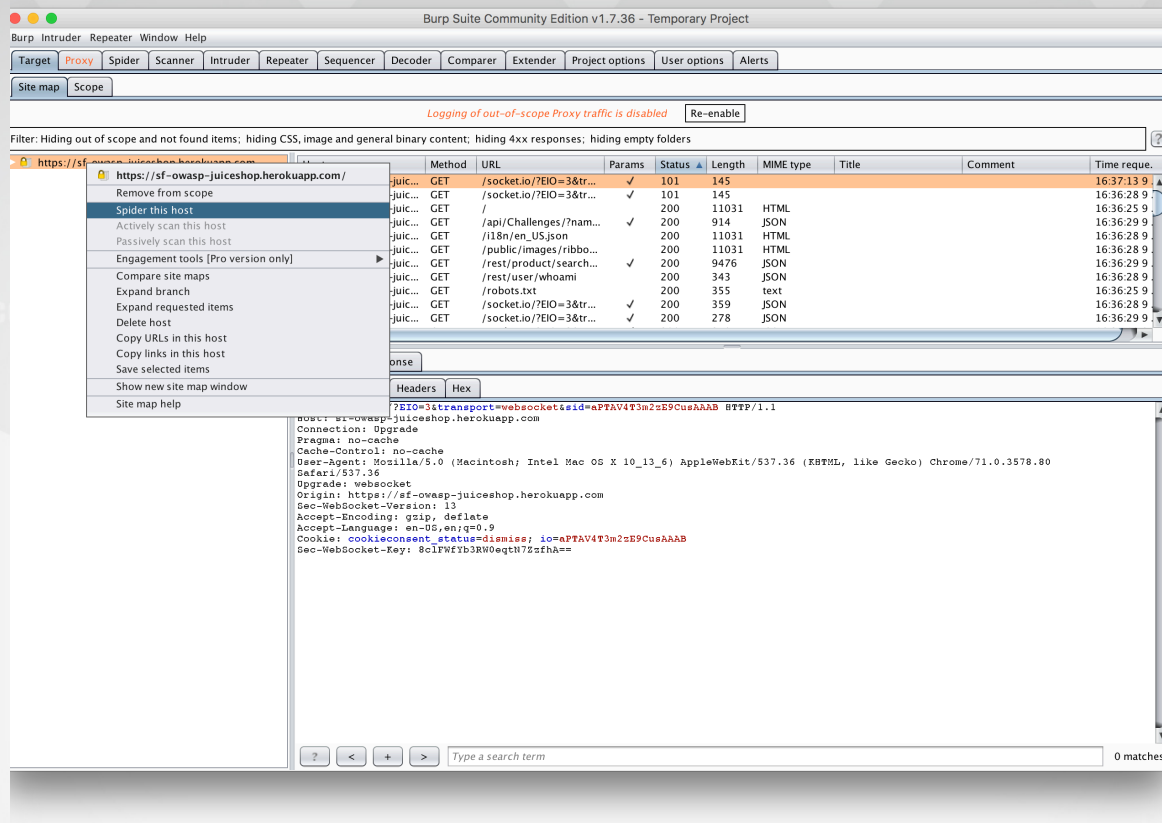




## Filtering by Scope







## Spider the Site



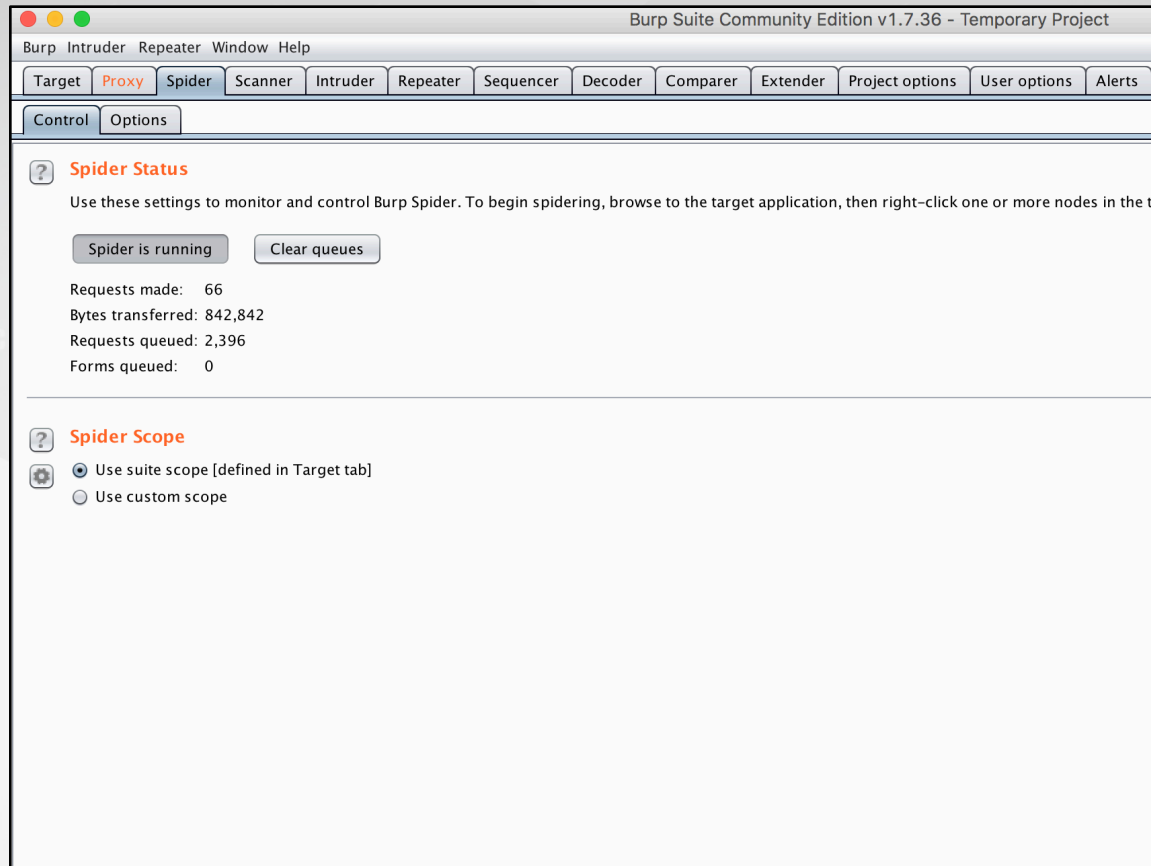
**OWASP**  
Open Web Application  
Security Project



# Spider Tab

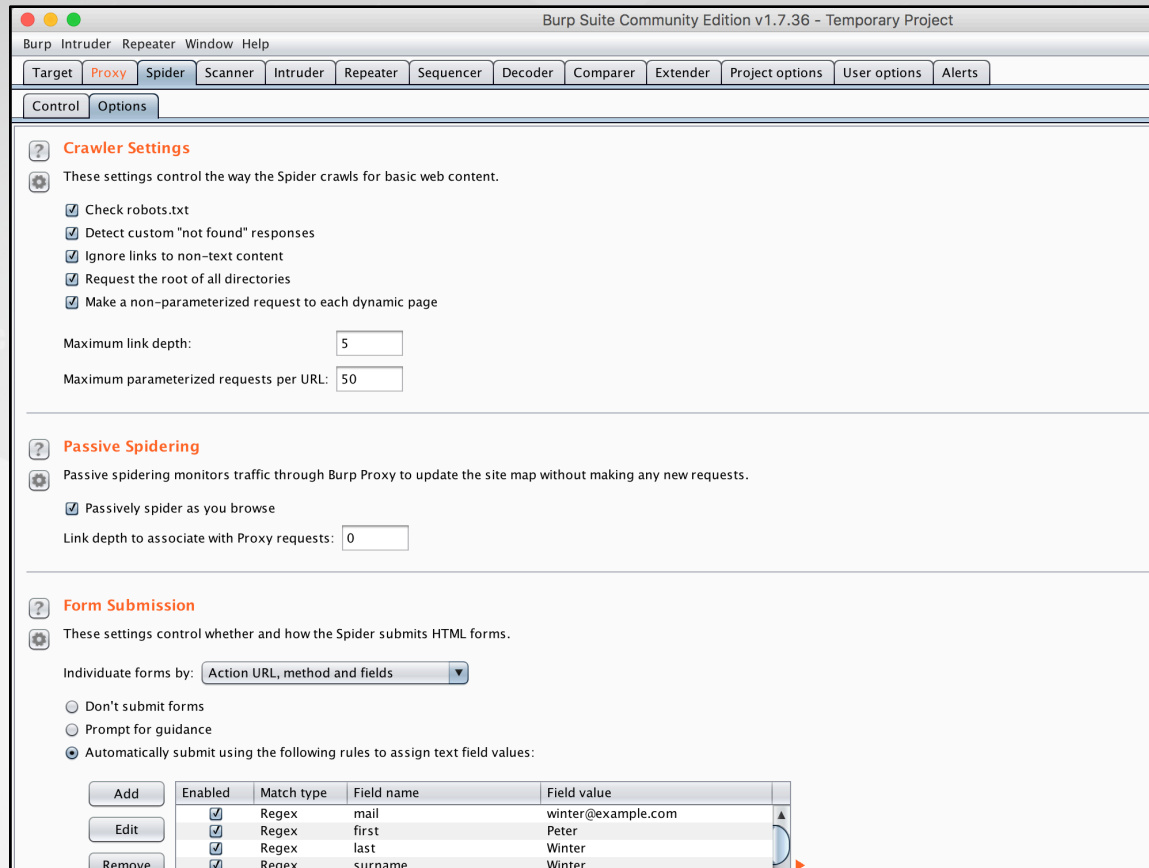
- Contains results from a spider operation
- Spider populates data in Target tab
- Helps identify the structure of the site
- Helps find low-hanging fruit
- Multiple options that can be configured





## Spider Tab





## Spider Options



Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty fo

- https://sf-owasp-juiceshop.herokuapp.com
  - /
  - api
    - /
    - Challenges
      - /
      - name=Score+Board
    - css
    - dist
    - ftp
      - /
      - acquisitions.md
      - incident-support.kdbx
      - legal.md
    - i18n
    - node\_modules
    - private
      - /
      - css
      - dist
      - fontawesome-all.js
      - node\_modules
      - private
      - public
      - redirect
      - rest
        - /
        - admin
        - product
        - user
      - robots.txt
      - socket.io

Host	Method	URL	Params	S
https://sf-owasp-juic...	GET	/api/Challenges/		2
https://sf-owasp-juic...	GET	/api/Challenges/?nam...	✓	2
https://sf-owasp-juic...	GET	/api/		5

Request

Response

Raw

Params

Headers

Hex

```

GET /api/Challenges/ HTTP/1.1
Host: sf-owasp-juiceshop.herokuapp.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
Connection: close
Cookie: io=aPTAV4T3m2zE9CusAAB; cookieconsent_status=dis
token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdGF0dXMiOiJ
cGFzc3dvcmQ0IjJjNGQzNTQ0NDJYjQxZWUzOGUzNjJiYzFmNDMxZTk5Yi
BdCI6IjIwMTgtMTItMDQgMDM6NTE6MjQuNTM5ICswMDowMCJ9LCJpYXQiOi
hnngFyJdpw5PyvvaNa-TB5eD081Z-ehXwN9j4Ek8bMBU9y-MpF0qOfOof3
ofuqiM

```

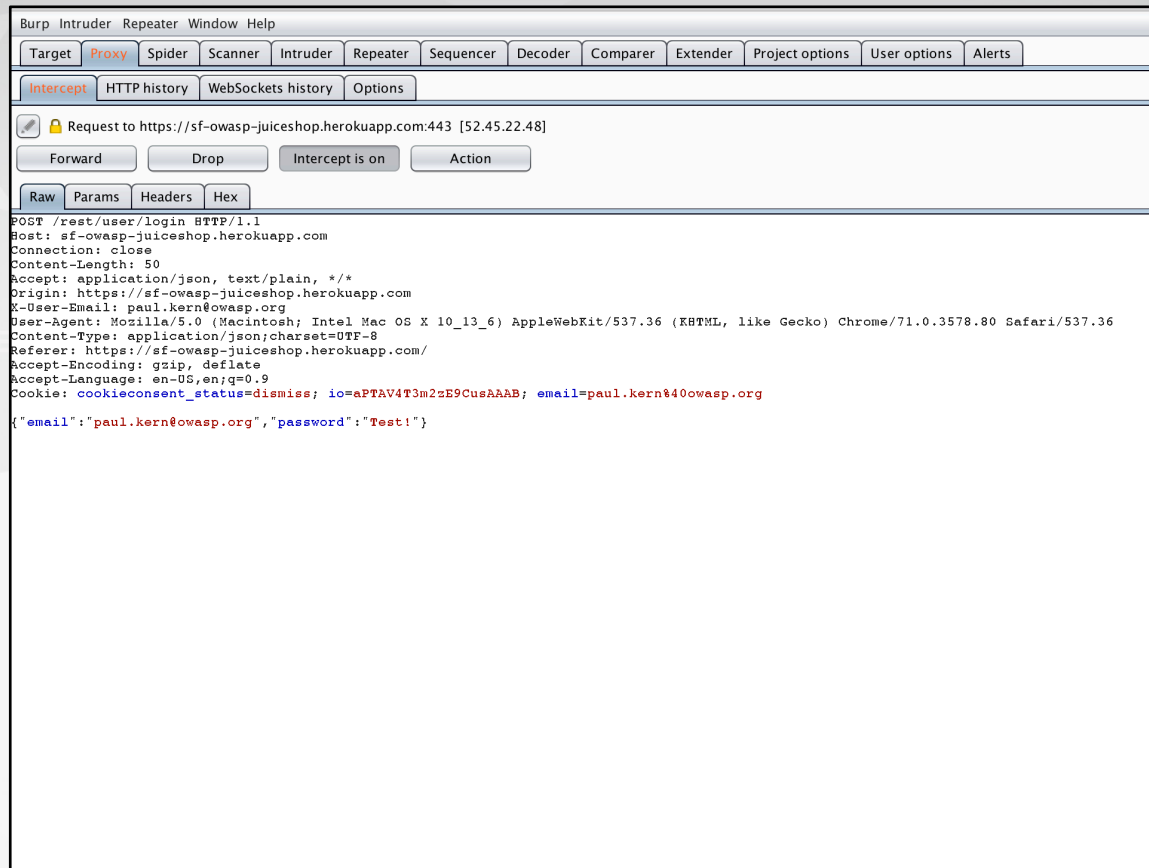
## Target Information Populated by Spider



# 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`





## Proxy Tab



**OWASP**  
Open Web Application  
Security Project

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  
 Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
242	https://sf-owasp-juiceshop....	POST	/rest/user/login	✓		200	237	text	io/
243	https://sf-owasp-juiceshop....	GET	/socket.io/?EIO=3&transport=polli...	✓					io/
244	https://sf-owasp-juiceshop....	GET	/socket.io/?EIO=3&transport=polli...	✓					io/
245	https://sf-owasp-juiceshop....	GET	/socket.io/?EIO=3&transport=polli...	✓					io/
246	https://sf-owasp-juiceshop....	GET	/socket.io/?EIO=3&transport=polli...	✓					io/
247	https://sf-owasp-juiceshop....	GET	/socket.io/?EIO=3&transport=polli...	✓					io/
37	https://support.portswigger...	GET	/customer/portal/articles/178307...			200	249453	HTML	
122	https://support.portswigger...	GET	/customer/portal/articles/178308...			200	248207	HTML	html
51	https://syndication.twitter.c...	GET	/settings			200	685	JSON	
5	https://www.bing.com	POST	/aclick/RLinkPing.htm?guid=0ac4...	✓		204	346	HTML	htm
29	https://www.bing.com	POST	/aclick/RLinkPing.htm?guid=6288...	✓		204	279	HTML	htm
61	https://www.bing.com	POST	/aclick/RLinkPing.htm?guid=481e...	✓		204	346	HTML	htm
107	https://www.bing.com	POST	/aclick/RLinkPing.htm?guid=0ac9e...	✓		204	346	HTML	htm
53	https://www.facebook.com	GET	/connect/ping?client_id=1907519...	✓		200	1650	HTML	
136	https://www.facebook.com	GET	/connect/ping?client_id=1907519...	✓		200	1650	HTML	
145	https://www.facebook.com	GET	/connect/ping?client_id=1907519...	✓		200	1650	HTML	
47	https://www.google-analytic...	GET	/analytics.js?_=1544394609598	✓		200	44182	script	js
126	https://www.google-analytic...	GET	/analytics.js?_=1544394717128	✓		200	44182	script	js
138	https://www.google-analytic...	GET	/analytics.js?_=1544394743056	✓		200	44182	script	js
87	https://www.google.com	GET	/cse/cse.js?cx=00408853463988...	✓		302	643	HTML	js
116	https://www.google.com	GET	/cse/cse.js?cx=00408853463988...	✓		302	643	HTML	js
146	https://www.google.com	POST	/gen_204?atyp=i&bb=1&ei=uoUN...	✓		204	313	HTML	
152	https://www.google.com	POST	/gen_204?atyp=i&bb=1&ei=uoUN...	✓		204	313	HTML	
155	https://www.google.com	POST	/gen_204?atyp=i&bb=1&ei=uoUN...	✓		204	313	HTML	

Request

Raw Params Headers Hex

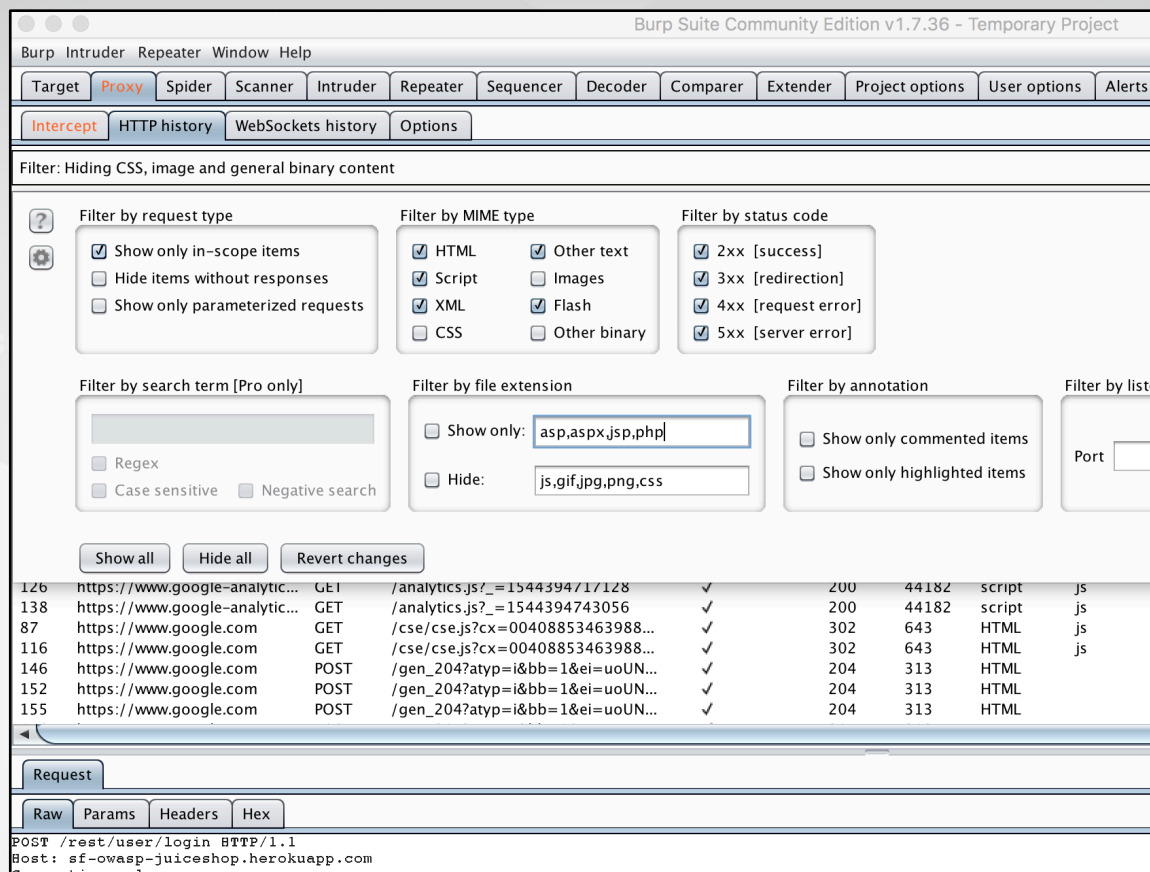
```

POST /rest/user/login HTTP/1.1
Host: sf-owasp-juiceshop.herokuapp.com
Connection: close
  
```

## Proxy History



**OWASP**  
 Open Web Application  
 Security Project



## 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/2Lc08b2>



# 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](mailto: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

