



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!”



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



OWASP
Open Web Application
Security Project

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>



aabfmlnjonogaaifnjlfpn/options.html#tabProxies

Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version
	127.0.0.1	8080		5
	127.0.0.1	3128		5
	127.0.0.1	8081		5

These are the settings that are used when no patterns match an URL

5

Firefox or from another computer.

Please Donate Buy Proxy Service

Use proxies based on their pre-defined patterns and priorities
Use proxy Burp Suite for all URLs
Use proxy 127.0.0.1:3128 for all URLs
Use proxy OWASP ZAP for all URLs
Use proxy Default for all URLs
Disable FoxyProxy

Options

Edit Selection
Copy Selection
Delete Selection

Foxy Proxy Quick Change



The screenshot shows the 'Proxies' section of the FoxyProxy Standard extension settings. The left sidebar has links for Global Settings, Import/Export, QuickAdd, and About. The main area displays a table of proxies:

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

On the right, there are buttons for Move Up, Move Down, Add New Proxy, Edit Selection, Copy Selection, and Delete Selection. Below the table is a note about importing proxies from Mozilla Firefox. At the bottom are 'Please Donate' and 'Buy Proxy Service' buttons.

Foxy Proxy Settings



OWASP
Open Web Application
Security Project

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



ZAP Functionality

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



OWASP
Open Web Application
Security Project

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>



The screenshot shows the OWASP ZAP 2.7.0 interface with the 'Dynamic SSL Certificates' options dialog open. The dialog contains fields for 'Root CA certificate' (with 'Generate' and 'Import' buttons) and a large text area for the 'Dynamic SSL Certificates' content. The content area displays a certificate template with placeholder values like 'eHgwggEiMA0GCSqSjB3DQEBAQUAA4IBDwAwggEKAoIBAQC...' and ends with '-----END CERTIFICATE-----'. At the bottom of the dialog are 'View' and 'Save' buttons.

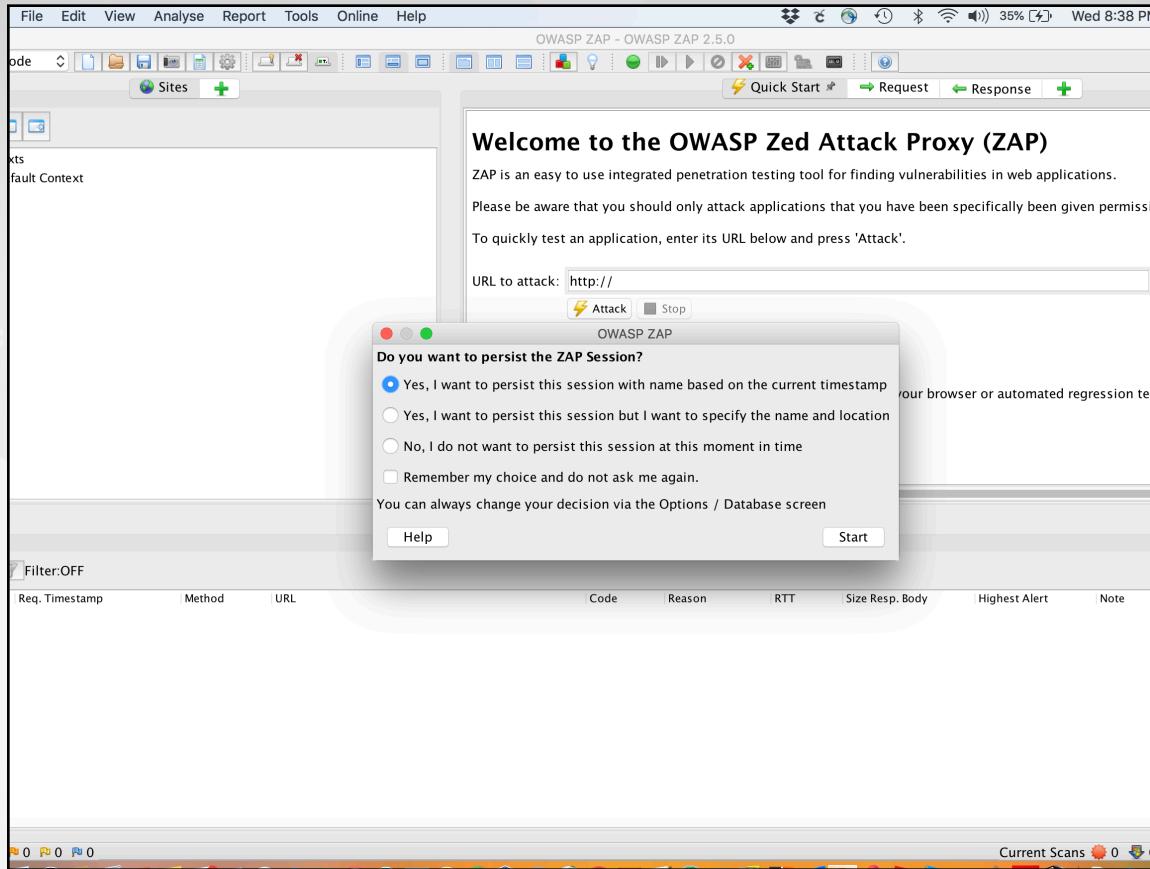
Generate CA Certificate



OWASP
Open Web Application
Security Project

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



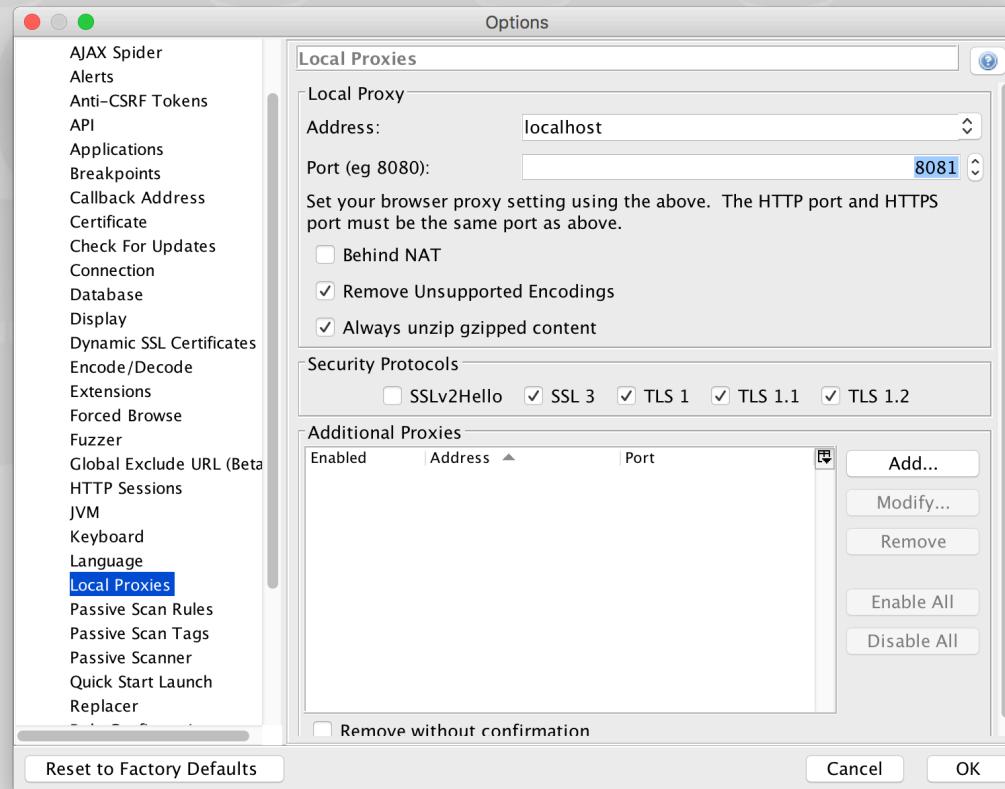
OWASP
Open Web Application
Security Project

Proxy Settings in ZAP

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



OWASP
Open Web Application
Security Project



ZAP Proxy Settings



OWASP
Open Web Application
Security Project

FoxyProxy - Proxy settings

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
 [View](#) [Test](#) [?](#)

Notify me about proxy auto-configuration file loads
 Notify me about proxy auto-configuration file errors

[Save](#) [Cancel](#)

ZAP in Foxy Proxy



OWASP
Open Web Application
Security Project

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...



OWASP
Open Web Application
Security Project

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>



OWASP
Open Web Application
Security Project

CONNECT.

LEARN.

GROW.

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



OWASP
Open Web Application
Security Project

Install Burp

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



OWASP
Open Web Application
Security Project

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



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the top navigation bar, the 'Proxy' tab is highlighted in blue. Below the tabs, there are four sub-navigation buttons: 'Intercept', 'HTTP history', 'WebSockets history', and 'Options'. The main content area is titled 'Proxy Listeners'. It contains a table with one row, showing a single listener configuration. The table has columns for 'Running' (with a checked checkbox), 'Interface' (containing '127.0.0.1:8080'), 'Invisible' (unchecked), and 'Redirect' (unchecked). To the left of the table are three buttons: 'Add', 'Edit', and 'Remove'. Below the table, a note states: 'Each installation of Burp generates its own CA certificate that Proxy listeners can use when intercepting traffic'. At the bottom of this section are two buttons: 'Import / export CA certificate' and 'Regenerate CA certificate'. The status bar at the bottom of the window shows the URL 'http://127.0.0.1:8080'.

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
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



Burp Intruder Repeater Window Help

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

Site map Scope

Logging of out-of-scope Proxy traffic is disabled Re-enable

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

Filter by request type

- Show only in-scope items
- Show only requested items
- Show only parameterized requests
- Hide not-found items

Filter by MIME type

- HTML
- Script
- XML
- CSS
- Other text
- Images
- Flash
- Other binary

Filter by status code

- 2xx [success]
- 3xx [redirection]
- 4xx [request error]
- 5xx [server error]

Folders

- Hide empty folders

Filter by search term [Pro only]

- Regex
- Case sensitive
- Negative search

Filter by file extension

- Show only: asp,aspx,jsp,php
- Hide: js,gif,jpg,png,css

Filter by annotation

- Show only commented items
- Show only highlighted items

Show all Hide all Revert changes

▶ <http://portswigger.net>

▶ <https://portswigger.net>

▶ <http://purch.com>

▶ <https://purch.com>

▶ <http://r.search.yahoo.com>

▶ <https://r.search.yahoo.com>

▶ <https://recipes.search.yahoo.com>

▶ <http://releases.portswigger.net>

▶ <https://syimg.com>

▶ <https://schema.org>

▶ <https://search.yahoo.com>

▶ <https://sf-owasp-juiceshop.herokuapp.com>

▶ <https://shopping.search.yahoo.com>

▶ <https://sp.yimg.com>

▶ <https://sports.search.yahoo.com>

▶ <https://sf-owasp-juiceshop.herokuapp.com>

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 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
Sec-WebSocket-Key: 8c1FWFyB3RW0eqtN7zzfha==

Filtering by Scope



OWASP
Open Web Application
Security Project

Burp Suite Community Edition v1.7.36 - Temporary Project

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

Site map Scope Logging of out-of-scope Proxy traffic is disabled Re-enable

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

	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requ.
https://sf-owasp-juiceshop.herokuapp.com/	GET	/socket.io/?EIO=3&tr...	✓	101	145				16:37:13 9 ▲
Remove from scope	GET	/socket.io/?EIO=3&tr...	✓	101	145				16:36:28 9 ▾
Spider this host	GET	/		200	11031	HTML			16:36:25 9 ▾
Actively scan this host	GET	/api/Challenges/?nam...	✓	200	914	JSON			16:36:29 9 ▾
Passively scan this host	GET	/i18n/en_US.json		200	11031	HTML			16:36:28 9 ▾
Engagement tools [Pro version only]	GET	/public/images/ribbon...		200	11031	HTML			16:36:28 9 ▾
Compare site maps	GET	/rest/product/search...	✓	200	9476	JSON			16:36:29 9 ▾
Expand branch	GET	/rest/user/whoami		200	343	JSON			16:36:28 9 ▾
Expand requested items	GET	/robots.txt		200	355	text			16:36:25 9 ▾
Delete host	GET	/socket.io/?EIO=3&tr...	✓	200	359	JSON			16:36:28 9 ▾
Copy URLs in this host	GET	/socket.io/?EIO=3&tr...	✓	200	278	JSON			16:36:29 9 ▾
Copy links in this host									
Save selected items									
Show new site map window									
Site map help									

Headers Hex

```
?EIO=3&transport=websocket&sid=aPTAV4T3m2zE9CusAAAB HTTP/1.1
Host: https://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/71.0.3578.80
Sec-GRPC: brpc/2.0.0
Sec-WebSocket-Version: 13
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: cookieconsent_status=dismiss; io=aPTAV4T3m2zE9CusAAAB
Sec-WebSocket-Key: 8clFWFyb3RW0eqtN7ZsfhA==
```

Type a search term 0 matches

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 target tree and select "Spider" from the context menu.

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



OWASP
Open Web Application
Security Project

Burp Suite Community Edition v1.7.36 - Temporary Project

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

Control Options

Crawler Settings

These settings control the way the Spider crawls for basic web content.

Check robots.txt
 Detect custom "not found" responses
 Ignore links to non-text content
 Request the root of all directories
 Make a non-parameterized request to each dynamic page

Maximum link depth:

Maximum parameterized requests per URL:

Passive Spidering

Passive spidering monitors traffic through Burp Proxy to update the site map without making any new requests.

Passively spider as you browse
Link depth to associate with Proxy requests:

Form Submission

These settings control whether and how the Spider submits HTML forms.

Individuate forms by: Action URL, method and fields

Don't submit forms
 Prompt for guidance
 Automatically submit using the following rules to assign text field values:

Add	Enabled	Match type	Field name	Field value
<input type="button" value="Add"/>	<input checked="" type="checkbox"/>	Regex	mail	winter@example.com
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>	Regex	first	Peter
<input type="button" value="Remove"/>	<input checked="" type="checkbox"/>	Regex	last	Winter
	<input checked="" type="checkbox"/>	Regex	surname	Winter

Spider Options



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

	Host	Method	URL	Params	S
▼ 🔒 https://sf-owasp-juiceshop.herokuapp.com	https://sf-owasp-juic...	GET	/api/Challenges/		2
└ api	https://sf-owasp-juic...	GET	/api/Challenges/?nam...	✓	2
└ /	https://sf-owasp-juic...	GET	/api/		5
└ 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					

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=aPTAV4T3m2zE9CusAAAB; cookieconsent_status=dism
token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdGF0dXMiOiJ
CGFzc3dvcmQioiJjNGQzNTQ0NDbjYjQxZWUzOGUxNjJiYzFmNDMxZTk5Yi
BdCI6IjIwMTgtMTItMDQgMDM6NTe6MjQuNTM5ICswMDowMCJ9LCJpYXQiO
hnqgFyJdpW5PyvvNa-TB5ed081Z-ehXwN9j4Ek8bMBU9y-MpFOqofoof3
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

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@owasp.org

{"email": "paul.kern@owasp.org", "password": "Test!"}
```

Proxy Tab



OWASP
Open Web Application
Security Project

Burp Suite Community Edition v1.7.36 - Temporary Project

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
241	https://sf-owasp-juiceshop...	GET	/socket.io/?EIO=3&transport=polling...		✓	200	227	text	js
242	https://sf-owasp-juiceshop...	POST	/rest/user/login		✓				io/
243	https://sf-owasp-juiceshop...	GET	/socket.io/?EIO=3&transport=polling...		✓				io/
244	https://sf-owasp-juiceshop...	GET	/socket.io/?EIO=3&transport=polling...		✓				io/
245	https://sf-owasp-juiceshop...	GET	/socket.io/?EIO=3&transport=polling...		✓				io/
246	https://sf-owasp-juiceshop...	GET	/socket.io/?EIO=3&transport=polling...		✓				io/
247	https://sf-owasp-juiceshop...	GET	/socket.io/?EIO=3&transport=polling...		✓				io/
37	https://support.portswigger...	GET	/customer/portal/articles/178307...			200	249453	HTML	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



Burp Suite Community Edition v1.7.36 - Temporary Project

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

Filter by request type

- Show only in-scope items
- Hide items without responses
- Show only parameterized requests

Filter by MIME type

- HTML
- Script
- XML
- CSS
- Other text
- Images
- Flash
- Other binary

Filter by status code

- 2xx [success]
- 3xx [redirection]
- 4xx [request error]
- 5xx [server error]

Filter by search term [Pro only]

Show only:

Hide:

Filter by file extension

Filter by annotation

Filter by lister

Show all Hide all Revert changes

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
```

Scope Filter



Manual Tools

Burp Posts

<https://blog.sodaksec.com>

CONNECT.

LEARN.

GROW

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>



OWASP
Open Web Application
Security Project

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



OWASP
Open Web Application
Security Project