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://getfoxyproxy.org/downloads/)
- [https://chrome.google.com/webstore/detail/proxy-switchyomega/padekgcemlokbadohgkifijomclgjgif](https://chrome.google.com/webstore/detail/proxy-switchyomega/padekgcemlokbadohgkifijomclgjgif)
Foxy Proxy Quick Change
# Foxy Proxy Settings

## Proxies

<table>
<thead>
<tr>
<th>Enabled</th>
<th>Color</th>
<th>Proxy Name</th>
<th>Proxy Notes</th>
<th>Host or IP Address</th>
<th>Port</th>
<th>SOCKS proxy?</th>
<th>SOCKS Version</th>
<th>Auto PAC URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td></td>
<td>Burp Suite</td>
<td></td>
<td>127.0.0.1</td>
<td>8080</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td></td>
<td>127.0.0.1:3128</td>
<td></td>
<td>127.0.0.1</td>
<td>3128</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td></td>
<td>OWASP ZAP</td>
<td></td>
<td>127.0.0.1</td>
<td>8081</td>
<td></td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

- **Enabled**: Whether the proxy is active.
- **Color**: The color of the proxy in the list.
- **Proxy Name**: The name of the proxy service.
- **Proxy Notes**: Additional notes about the proxy.
- **Host or IP Address**: The IP address or host name of the proxy.
- **Port**: The port number used by the proxy.
- **SOCKS proxy?**: Indicates if the proxy uses the SOCKS protocol.
- **SOCKS Version**: The version of the SOCKS protocol used.
- **Auto PAC URL**: Whether the proxy uses a PAC file.

**Additional Options**:
- **Move Up**
- **Move Down**
- **Add New Proxy**
- **Edit Selection**
- **Copy Selection**
- **Delete Selection**

**Insert your proxies here from FoxyProxy on a Mobile device or from another computer.**

[Please Donate][1]  [Buy Proxy Service][2]
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](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
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/
BURP SUITE
About Burp Suite

- Developed and maintained by Portswigger
- [https://portswigger.net/burp/](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/](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

Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will see a row for each active listener:

- Click the [Add] button to create a new listener.
- Click the [Edit] button to modify an existing listener.
- Click the [Remove] button to remove an existing listener.

<table>
<thead>
<tr>
<th>Running</th>
<th>Interface</th>
<th>Invisible</th>
<th>Redirect</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>127.0.0.1:8080</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Each installation of Burp generates its own CA certificate that Proxy listeners can use when intercepting traffic:

- Click the [Import / export CA certificate] button to import or export the CA certificate.
- Click the [Regenerate CA certificate] button to regenerate the CA certificate.
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

[Image of Burp Suite interface with various data points and columns such as Method, URL, Params, Status, Length, HTML type, Title, and Comment.]

<table>
<thead>
<tr>
<th>Method</th>
<th>URL</th>
<th>Params</th>
<th>Status</th>
<th>Length</th>
<th>HTML type</th>
<th>Title</th>
<th>Comment</th>
<th>Time req</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>103</td>
<td>145</td>
<td></td>
<td></td>
<td></td>
<td>16:32:15</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>103</td>
<td>145</td>
<td></td>
<td></td>
<td></td>
<td>16:32:25</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>200</td>
<td>11031</td>
<td>HTML</td>
<td></td>
<td></td>
<td>16:32:35</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>200</td>
<td>934</td>
<td>JSON</td>
<td></td>
<td></td>
<td>16:32:45</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>200</td>
<td>11031</td>
<td>HTML</td>
<td></td>
<td></td>
<td>16:32:55</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>200</td>
<td>934</td>
<td>JSON</td>
<td></td>
<td></td>
<td>16:33:05</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>200</td>
<td>934</td>
<td>JSON</td>
<td></td>
<td></td>
<td>16:33:15</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>200</td>
<td>934</td>
<td>JSON</td>
<td></td>
<td></td>
<td>16:33:25</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>/socket.io/7500-58&amp;...</td>
<td></td>
<td>200</td>
<td>934</td>
<td>JSON</td>
<td></td>
<td></td>
<td>16:33:35</td>
<td></td>
</tr>
</tbody>
</table>

**Site Map Help:**

- **View site map**
- **Add site map**
- **Show site map window**
- **Save selected items**
- **Copy URLs in this host**
- **Copy links in this host**

**Toolbox:**

- **Add site map**
- **Remove from scope**
- **Manually scan this host**
- **Engagement tools**
- **Copy URL in this host**
- **Copy links in this host**
- **Save selected items**
- **Show new site map window**

**Site Map Generations:**

- **View site map**
- **Add site map**
- **Show site map window**
- **Save selected items**
- **Copy URLs in this host**
- **Copy links in this host**
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 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 tree.

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 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: 5
Maximum parameterized requests per URL: 50

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: 0

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:

<table>
<thead>
<tr>
<th>Add</th>
<th>Enabled</th>
<th>Match type</th>
<th>Field name</th>
<th>Field value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Regex</td>
<td>mail</td>
<td><a href="mailto:winter@example.com">winter@example.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex</td>
<td>first</td>
<td>Peter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex</td>
<td>last</td>
<td>Winter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex</td>
<td>surname</td>
<td>Winter</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Request to <a href="https://sf-owasp-juicebox.herokuapp.com:443">https://sf-owasp-juicebox.herokuapp.com:443</a> [52.45.22.48]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward</td>
</tr>
</tbody>
</table>

```plaintext
POST /ewt/user/login HTTP/1.1
Host: sf-owasp-juicebox.herokuapp.com
Connection: close
Content-Length: 56
Accept: application/json, text/plain, */*
Origin: https://sf-owasp-juicebox.herokuapp.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.9
Cookie: cookie_consent_status=dismiss; io=nPFAV4j3m2zERClAHAB; email=paul.kern@owasp.org

{"email":"paul.kern@owasp.org","password":"?test!"}
```
### Proxy History

<table>
<thead>
<tr>
<th>#</th>
<th>Host</th>
<th>Method</th>
<th>URL</th>
<th>Params</th>
<th>Edited</th>
<th>Status</th>
<th>Length</th>
<th>MIME type</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>242</td>
<td><a href="https://sf-owasp-juiceshop.com">https://sf-owasp-juiceshop.com</a></td>
<td>POST</td>
<td>/rest/user/login</td>
<td></td>
<td></td>
<td>✔</td>
<td>200</td>
<td>TEXT</td>
<td>io/</td>
</tr>
<tr>
<td>243</td>
<td><a href="https://sf-owasp-juiceshop.com">https://sf-owasp-juiceshop.com</a></td>
<td>GET</td>
<td>/socket.io?IE0=3&amp;transport=poll...</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>io/</td>
</tr>
<tr>
<td>244</td>
<td><a href="https://sf-owasp-juiceshop.com">https://sf-owasp-juiceshop.com</a></td>
<td>GET</td>
<td>/socket.io?IE0=3&amp;transport=poll...</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>io/</td>
</tr>
<tr>
<td>245</td>
<td><a href="https://sf-owasp-juiceshop.com">https://sf-owasp-juiceshop.com</a></td>
<td>GET</td>
<td>/socket.io?IE0=3&amp;transport=poll...</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>io/</td>
</tr>
<tr>
<td>246</td>
<td><a href="https://sf-owasp-juiceshop.com">https://sf-owasp-juiceshop.com</a></td>
<td>GET</td>
<td>/socket.io?IE0=3&amp;transport=poll...</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>io/</td>
</tr>
<tr>
<td>247</td>
<td><a href="https://sf-owasp-juiceshop.com">https://sf-owasp-juiceshop.com</a></td>
<td>GET</td>
<td>/socket.io?IE0=3&amp;transport=poll...</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>io/</td>
</tr>
<tr>
<td>248</td>
<td><a href="https://www.bing.com">https://www.bing.com</a></td>
<td>POST</td>
<td>/ajax/RLinkPing.htm?guid=0a4...</td>
<td></td>
<td></td>
<td>✔</td>
<td>204</td>
<td>JSON</td>
<td></td>
</tr>
<tr>
<td>249</td>
<td><a href="https://www.bing.com">https://www.bing.com</a></td>
<td>POST</td>
<td>/ajax/RLinkPing.htm?guid=6288...</td>
<td></td>
<td></td>
<td>✔</td>
<td>204</td>
<td>HTML</td>
<td>htm</td>
</tr>
<tr>
<td>250</td>
<td><a href="https://www.bing.com">https://www.bing.com</a></td>
<td>POST</td>
<td>/ajax/RLinkPing.htm?guid=481e...</td>
<td></td>
<td></td>
<td>✔</td>
<td>204</td>
<td>HTML</td>
<td>htm</td>
</tr>
<tr>
<td>251</td>
<td><a href="https://www.bing.com">https://www.bing.com</a></td>
<td>POST</td>
<td>/ajax/RLinkPing.htm?guid=0ac9...</td>
<td></td>
<td></td>
<td>✔</td>
<td>204</td>
<td>HTML</td>
<td>htm</td>
</tr>
<tr>
<td>252</td>
<td><a href="https://www.facebook.com">https://www.facebook.com</a></td>
<td>GET</td>
<td>/connect/ping?client_id=1907519...</td>
<td></td>
<td></td>
<td>✔</td>
<td>200</td>
<td>HTML</td>
<td>htm</td>
</tr>
<tr>
<td>253</td>
<td><a href="https://www.facebook.com">https://www.facebook.com</a></td>
<td>GET</td>
<td>/connect/ping?client_id=1907519...</td>
<td></td>
<td></td>
<td>✔</td>
<td>200</td>
<td>HTML</td>
<td>htm</td>
</tr>
<tr>
<td>254</td>
<td><a href="https://www.facebook.com">https://www.facebook.com</a></td>
<td>GET</td>
<td>/connect/ping?client_id=1907519...</td>
<td></td>
<td></td>
<td>✔</td>
<td>200</td>
<td>HTML</td>
<td>htm</td>
</tr>
<tr>
<td>255</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/analytics.js?_a...1544394600598</td>
<td></td>
<td></td>
<td>✔</td>
<td>200</td>
<td>script</td>
<td>js</td>
</tr>
<tr>
<td>256</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/analytics.js?_a...1544394717128</td>
<td></td>
<td></td>
<td>✔</td>
<td>200</td>
<td>script</td>
<td>js</td>
</tr>
<tr>
<td>257</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/analytics.js?_a...1544394745056</td>
<td></td>
<td></td>
<td>✔</td>
<td>200</td>
<td>script</td>
<td>js</td>
</tr>
<tr>
<td>258</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/cсе/cсе.js?cx=00408853463988...</td>
<td></td>
<td></td>
<td>✔</td>
<td>302</td>
<td>HTML</td>
<td>js</td>
</tr>
<tr>
<td>259</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/cсе/cсе.js?cx=00408853463988...</td>
<td></td>
<td></td>
<td>✔</td>
<td>302</td>
<td>HTML</td>
<td>js</td>
</tr>
<tr>
<td>260</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/cсе/cсе.js?cx=00408853463988...</td>
<td></td>
<td></td>
<td>✔</td>
<td>302</td>
<td>HTML</td>
<td>js</td>
</tr>
<tr>
<td>261</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/cсе/cсе.js?cx=00408853463988...</td>
<td></td>
<td></td>
<td>✔</td>
<td>302</td>
<td>HTML</td>
<td>js</td>
</tr>
<tr>
<td>262</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/cсе/cсе.js?cx=00408853463988...</td>
<td></td>
<td></td>
<td>✔</td>
<td>302</td>
<td>HTML</td>
<td>js</td>
</tr>
<tr>
<td>263</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/cсе/cсе.js?cx=00408853463988...</td>
<td></td>
<td></td>
<td>✔</td>
<td>302</td>
<td>HTML</td>
<td>js</td>
</tr>
<tr>
<td>264</td>
<td><a href="https://www.google-analytics.com">https://www.google-analytics.com</a></td>
<td>GET</td>
<td>/cсе/cсе.js?cx=00408853463988...</td>
<td></td>
<td></td>
<td>✔</td>
<td>302</td>
<td>HTML</td>
<td>js</td>
</tr>
</tbody>
</table>
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
  • 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