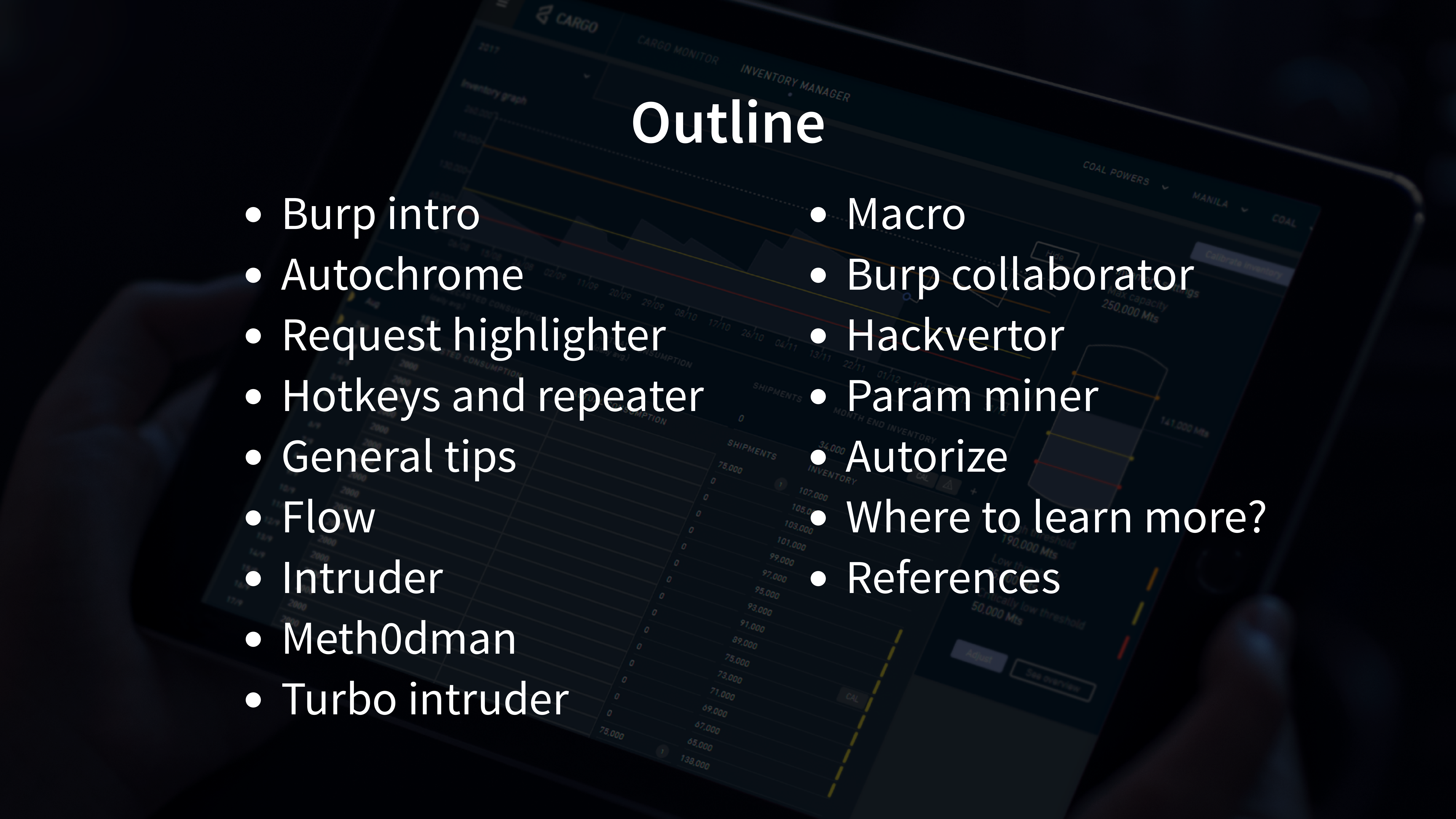
Burp suite - ninja tricks!

@webhak

Thomas Gøytil

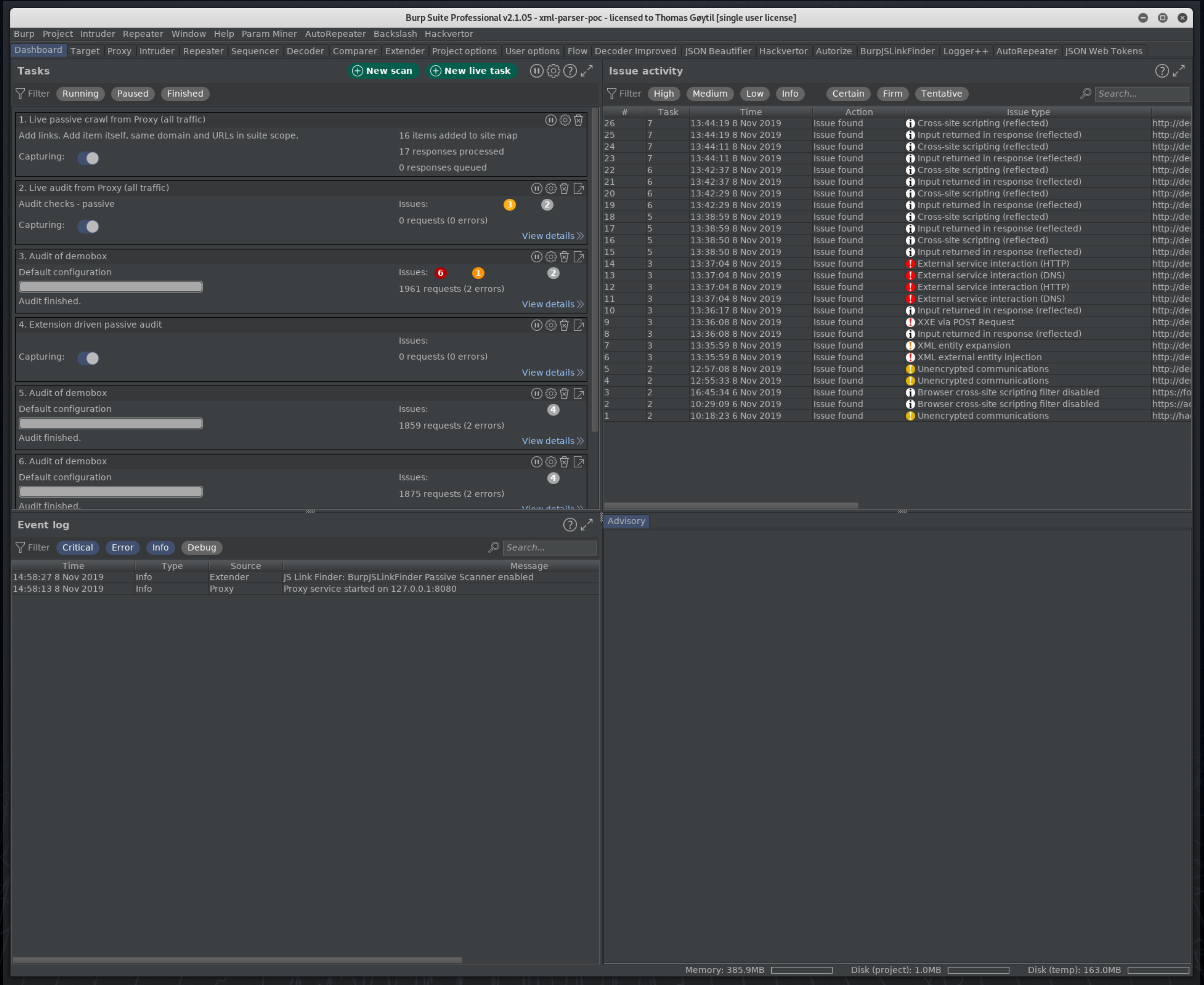
- Head of security @ Klaveness Digital
- Developer reformed to security professional
- Hacker, bug bounty hunter, speaker, etc.
- Love everything security: hardware, software, radio-hacking, lockpicking etc.

Outline



- Burp intro
- Autochrome
- Request highlighter
- Hotkeys and repeater
- General tips
- Flow
- Intruder
- Meth0dman
- Turbo intruder
- Macro
- Burp collaborator
- Hackvertor
- Param miner
- Autorize
- Where to learn more?
- References

Burp suite


Burp Suite Professional v2.1.05 - xml-parser-poc - licensed to Thomas Gøytil [single user license]
Burp Project Intruder Repeater Window Help Param Miner AutoRepeater Backslash Hackvertor
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Flow Decoder Improved JSON Beautifier Hackvertor Autorize BurpJSLinkFinder Logger++ AutoRepeater JSON Web Tokens
New scan
New live task
Filter Running Paused Finished
Filter High Medium Low Info Certain Firm Tentative
Search...
Filter Critical Error Info Debug
Search...
Advisory

Tasks

1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
16 items added to site map
17 responses processed
0 responses queued

2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Issues: 3 2
0 requests (0 errors)
View details »

3. Audit of demobox
Default configuration
Audit finished.
Issues: 6 1 2
1961 requests (2 errors)
View details »

4. Extension driven passive audit
Capturing:
Issues:
0 requests (0 errors)
View details »

5. Audit of demobox
Default configuration
Audit finished.
Issues: 4
1859 requests (2 errors)
View details »

6. Audit of demobox
Default configuration
Audit finished.
Issues: 4
1875 requests (2 errors)

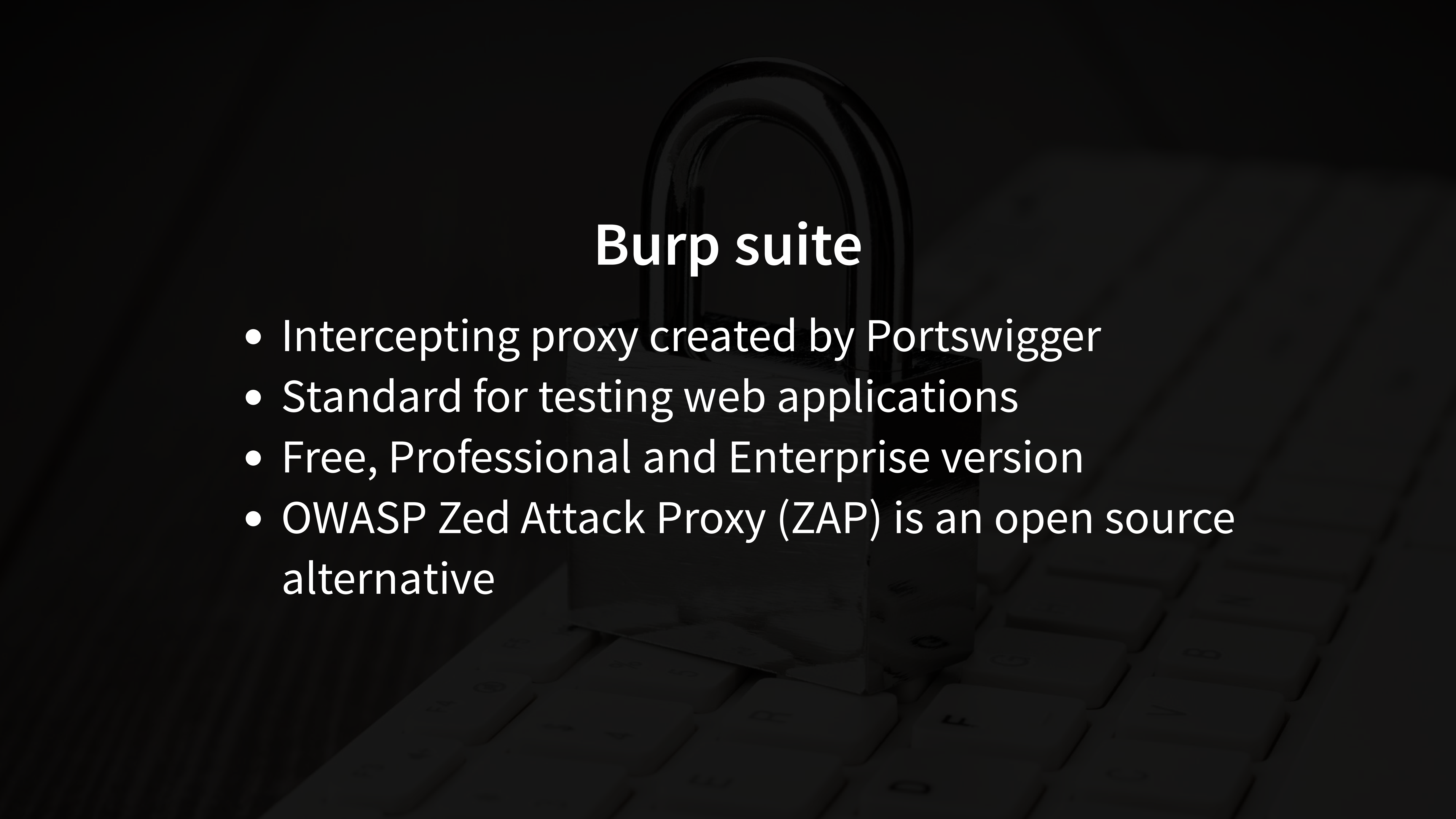
Issue activity

#	Task	Time	Action	Issue type	
26	7	13:44:19 8 Nov 2019	Issue found	ⓘ Cross-site scripting (reflected)	http://de
25	7	13:44:19 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
24	7	13:44:11 8 Nov 2019	Issue found	ⓘ Cross-site scripting (reflected)	http://de
23	7	13:44:11 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
22	6	13:42:37 8 Nov 2019	Issue found	ⓘ Cross-site scripting (reflected)	http://de
21	6	13:42:37 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
20	6	13:42:29 8 Nov 2019	Issue found	ⓘ Cross-site scripting (reflected)	http://de
19	6	13:42:29 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
18	5	13:38:59 8 Nov 2019	Issue found	ⓘ Cross-site scripting (reflected)	http://de
17	5	13:38:59 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
16	5	13:38:50 8 Nov 2019	Issue found	ⓘ Cross-site scripting (reflected)	http://de
15	5	13:38:50 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
14	3	13:37:04 8 Nov 2019	Issue found	! External service interaction (HTTP)	http://de
13	3	13:37:04 8 Nov 2019	Issue found	! External service interaction (DNS)	http://de
12	3	13:37:04 8 Nov 2019	Issue found	! External service interaction (HTTP)	http://de
11	3	13:37:04 8 Nov 2019	Issue found	! External service interaction (DNS)	http://de
10	3	13:36:17 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
9	3	13:36:08 8 Nov 2019	Issue found	! XXE via POST Request	http://de
8	3	13:36:08 8 Nov 2019	Issue found	ⓘ Input returned in response (reflected)	http://de
7	3	13:35:59 8 Nov 2019	Issue found	! XML entity expansion	http://de
6	3	13:35:59 8 Nov 2019	Issue found	! XML external entity injection	http://de
5	2	12:57:08 8 Nov 2019	Issue found	! Unencrypted communications	http://de
4	2	12:55:33 8 Nov 2019	Issue found	! Unencrypted communications	http://de
3	2	16:45:34 6 Nov 2019	Issue found	ⓘ Browser cross-site scripting filter disabled	https://fo
2	2	10:29:09 6 Nov 2019	Issue found	ⓘ Browser cross-site scripting filter disabled	https://ac
1	2	10:18:23 6 Nov 2019	Issue found	! Unencrypted communications	http://ha

Event log

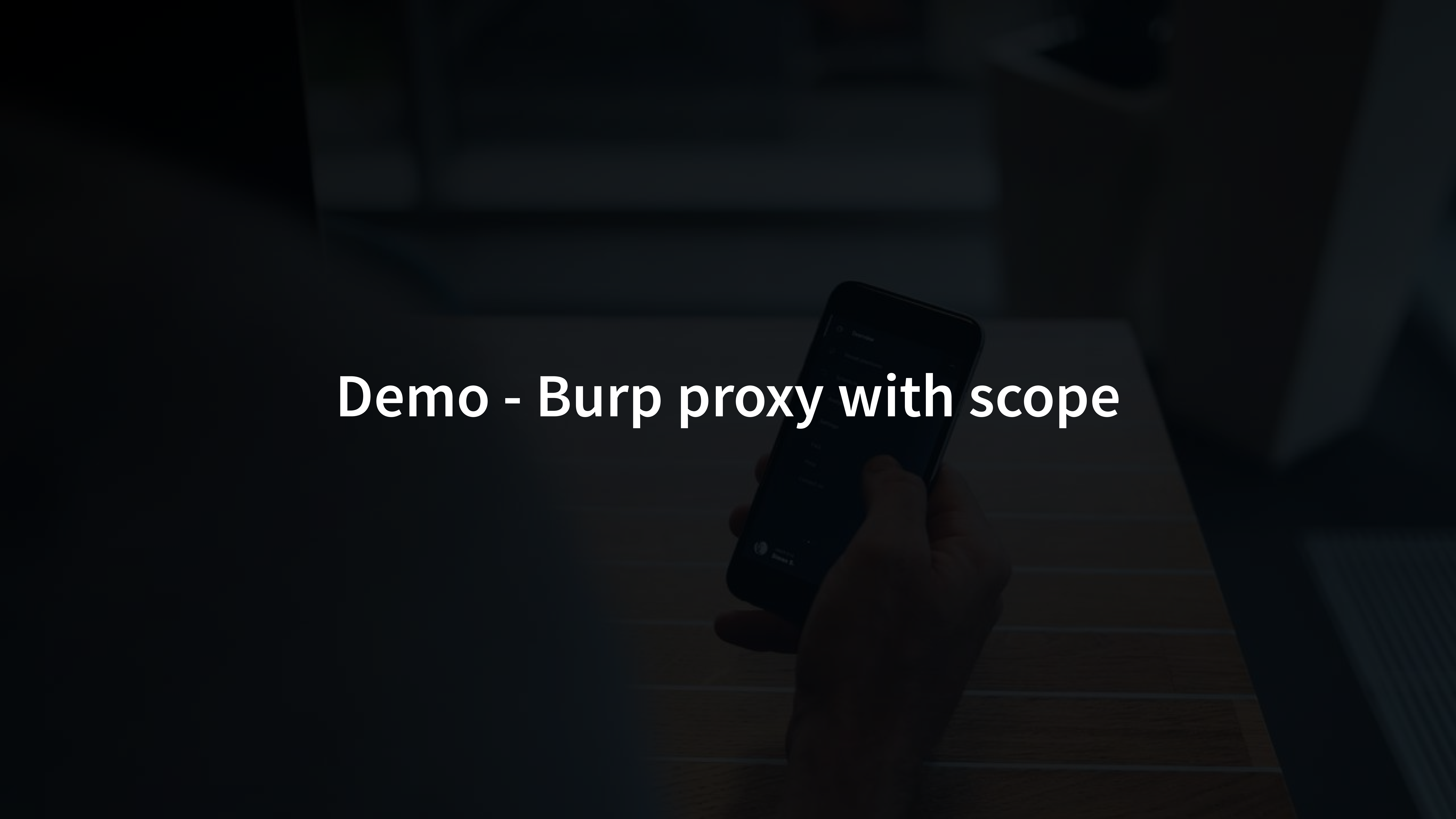
Time	Type	Source	Message
14:58:27 8 Nov 2019	Info	Extender	JS Link Finder: BurpJSLinkFinder Passive Scanner enabled
14:58:13 8 Nov 2019	Info	Proxy	Proxy service started on 127.0.0.1:8080

Memory: 385.9MB Disk (project): 1.0MB Disk (temp): 163.0MB



Burp suite

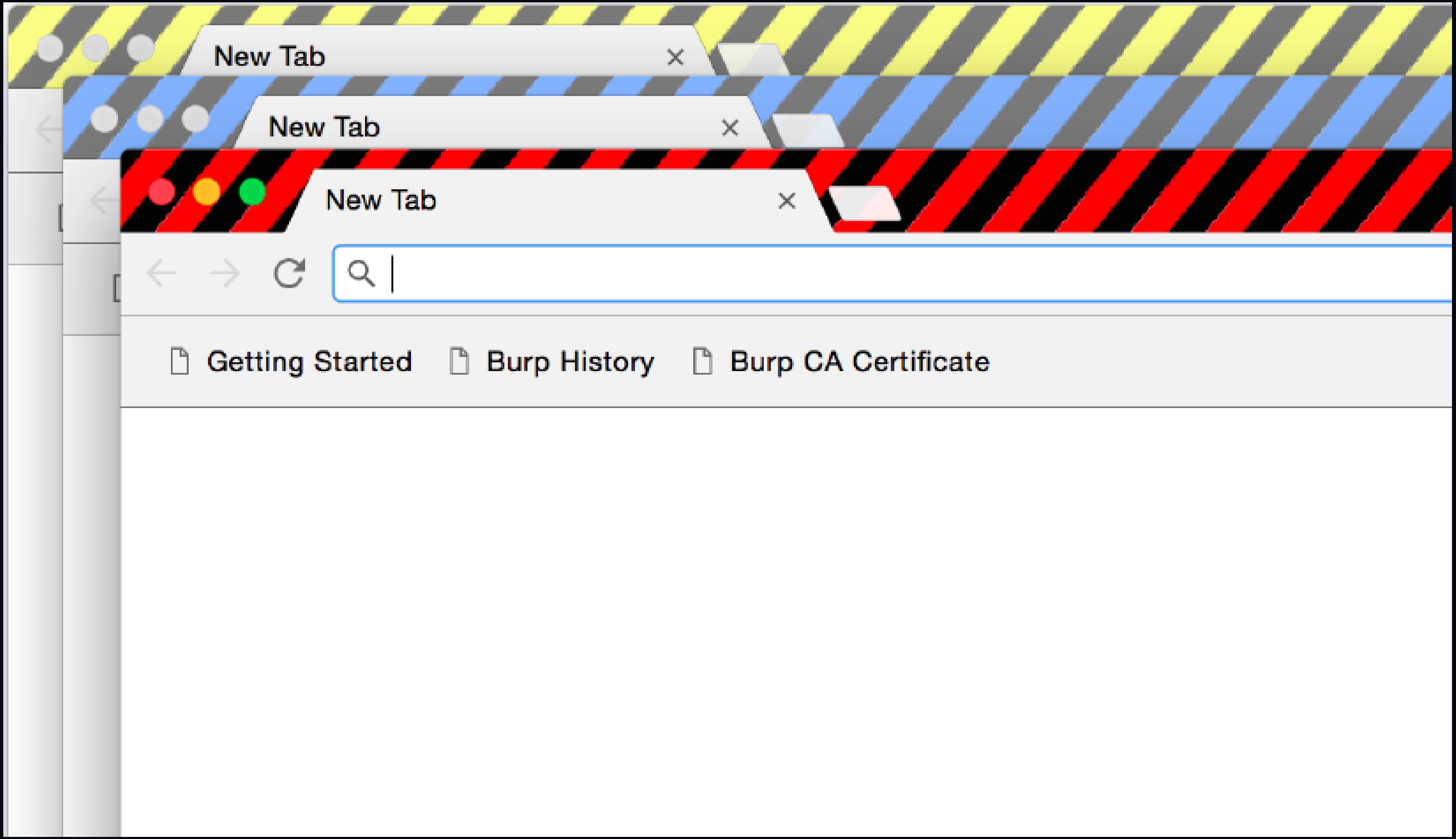
- Intercepting proxy created by Portswigger
- Standard for testing web applications
- Free, Professional and Enterprise version
- OWASP Zed Attack Proxy (ZAP) is an open source alternative



Demo - Burp proxy with scope

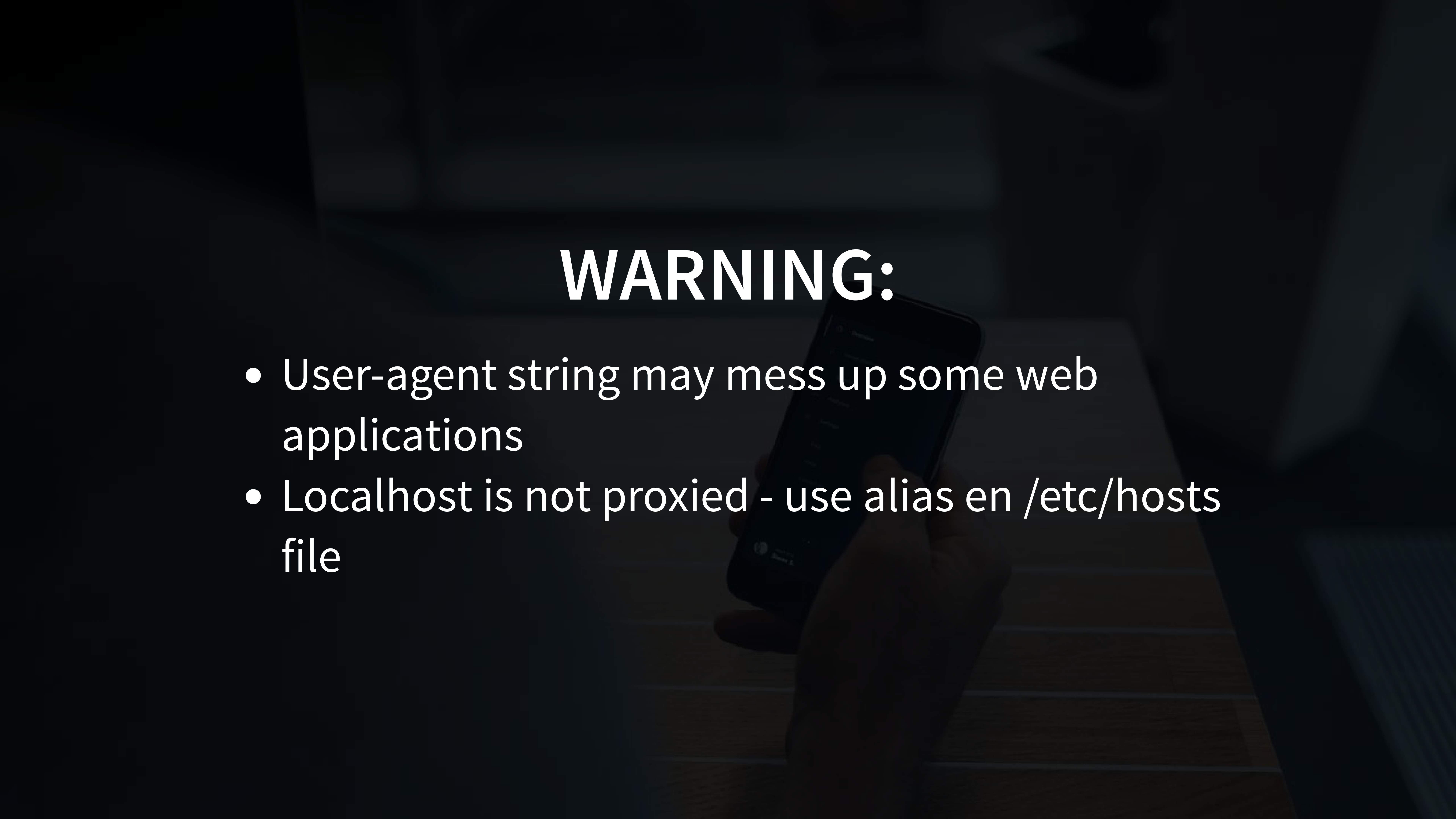
Autochrome

- Downloads Chromium and adds different profiles
- Profiles does not share cookies - one profile each user
- Default proxy localhost:8080
- Disable checking of certificates
- Sweet colored profiles!
- Adds separate user agent for each profile


New Tab
New Tab
New Tab
Getting Started
Burp History
Burp CA Certificate

Autochrome - Installation

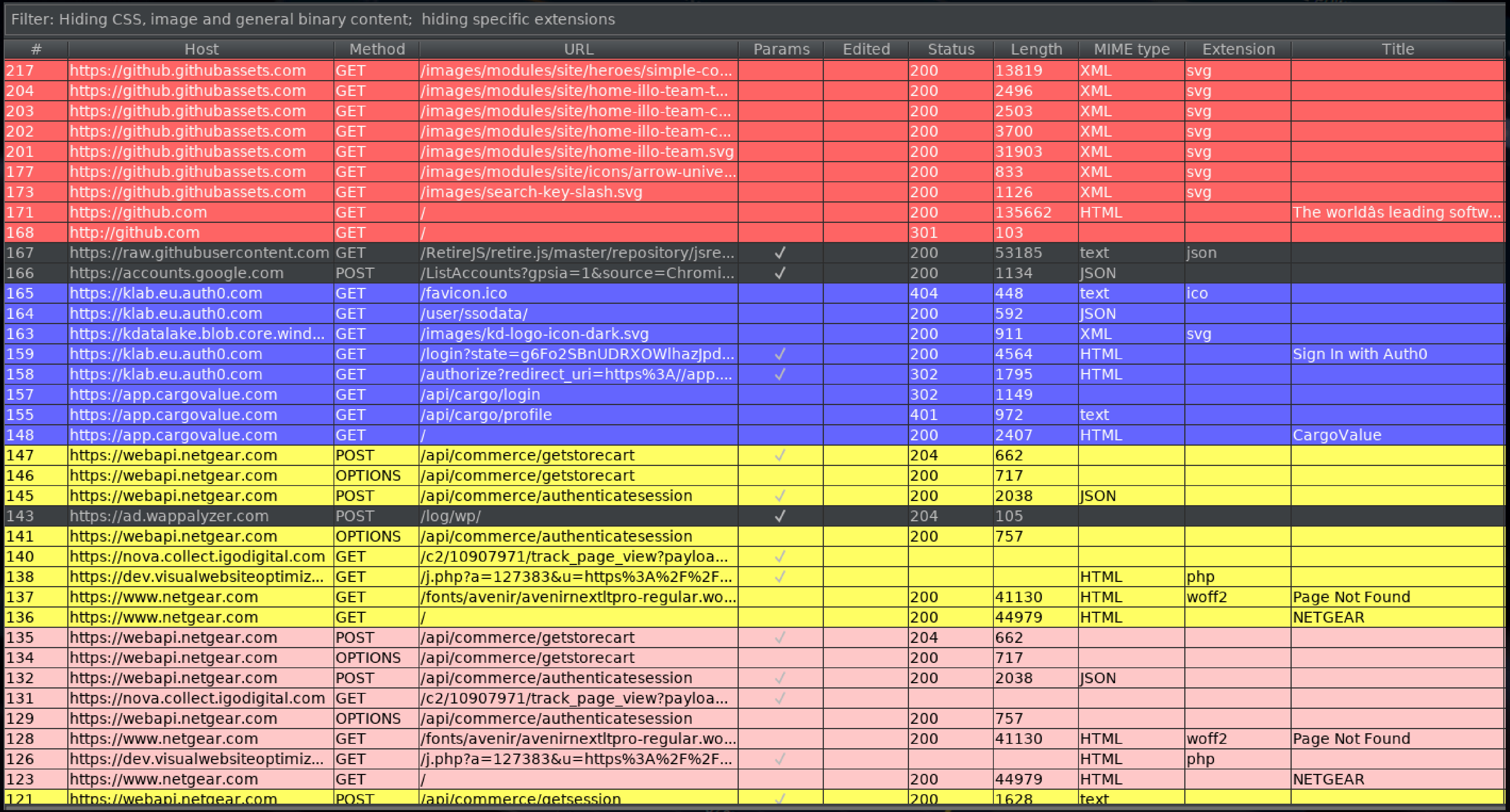
```
git clone https://github.com/nccgroup/autochrome
cd autochrome
ruby autochrome.rb
```



WARNING:

- User-agent string may mess up some web applications
- Localhost is not proxied - use alias en /etc/hosts file

Demo: Plugin - Request highlighter

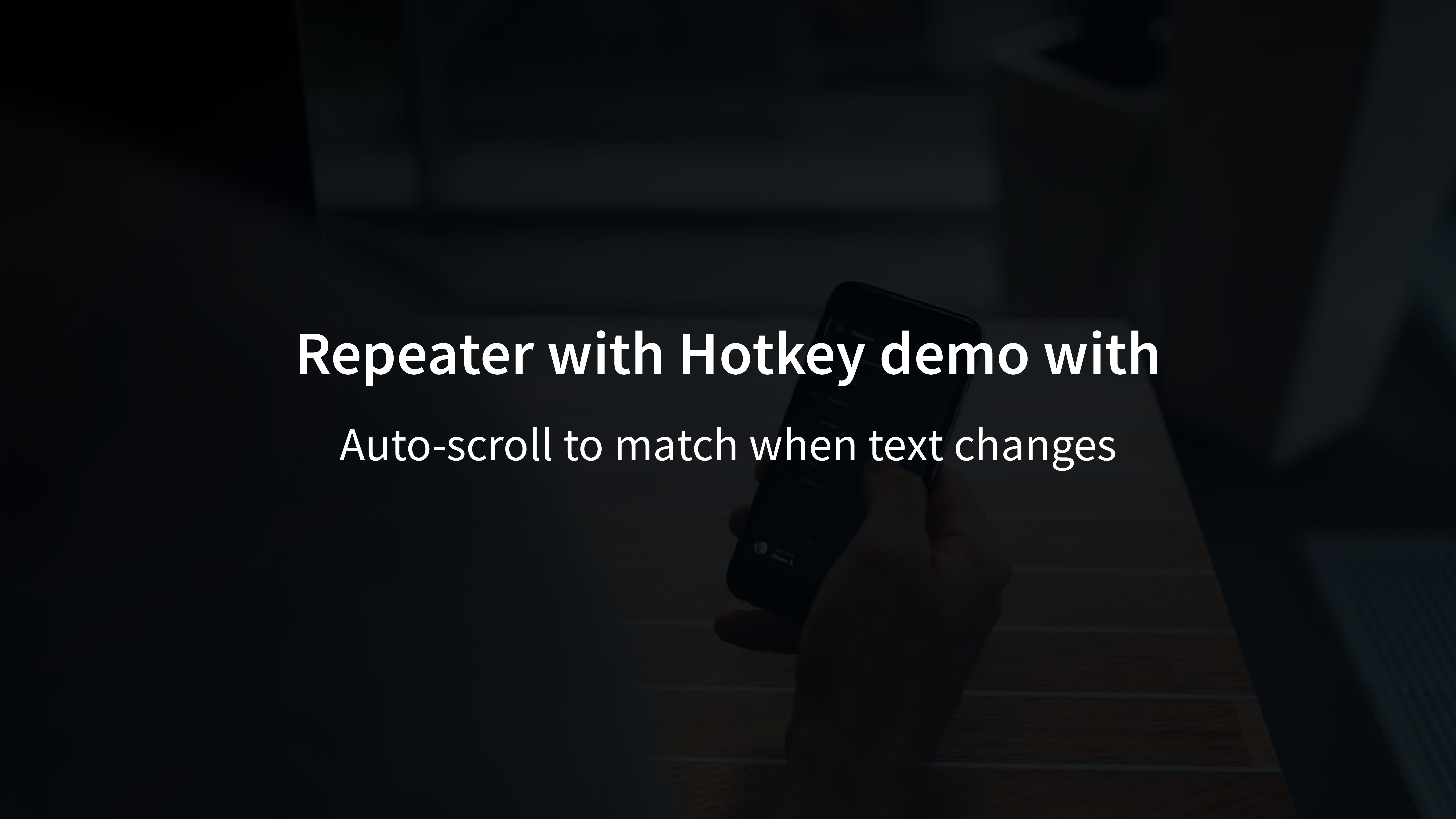


Filter: Hiding CSS, image and general binary content; hiding specific extensions

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
217	https://github.githubassets.com	GET	/images/modules/site/heroes/simple-co...			200	13819	XML	svg	
204	https://github.githubassets.com	GET	/images/modules/site/home-illo-team-t...			200	2496	XML	svg	
203	https://github.githubassets.com	GET	/images/modules/site/home-illo-team-c...			200	2503	XML	svg	
202	https://github.githubassets.com	GET	/images/modules/site/home-illo-team-c...			200	3700	XML	svg	
201	https://github.githubassets.com	GET	/images/modules/site/home-illo-team.svg			200	31903	XML	svg	
177	https://github.githubassets.com	GET	/images/modules/site/icons/arrow-unive...			200	833	XML	svg	
173	https://github.githubassets.com	GET	/images/search-key-slash.svg			200	1126	XML	svg	
171	https://github.com	GET	/			200	135662	HTML		The worldâs leading softw...
168	http://github.com	GET	/			301	103			
167	https://raw.githubusercontent.com	GET	/RetireJS/retire.js/master/repository/jsre...	✓		200	53185	text	json	
166	https://accounts.google.com	POST	/ListAccounts?gpsia=1&source=Chromi...	✓		200	1134	JSON		
165	https://klab.eu.auth0.com	GET	/favicon.ico			404	448	text	ico	
164	https://klab.eu.auth0.com	GET	/user/ssodata/			200	592	JSON		
163	https://kdatalake.blob.core.wind...	GET	/images/kd-logo-icon-dark.svg			200	911	XML	svg	
159	https://klab.eu.auth0.com	GET	/login?state=g6Fo2SBnUDRXOWlhazJpd...	✓		200	4564	HTML		Sign In with Auth0
158	https://klab.eu.auth0.com	GET	/authorize?redirect_uri=https%3A//app....	✓		302	1795	HTML		
157	https://app.cargovalue.com	GET	/api/cargo/login			302	1149			
155	https://app.cargovalue.com	GET	/api/cargo/profile			401	972	text		
148	https://app.cargovalue.com	GET	/			200	2407	HTML		CargoValue
147	https://webapi.netgear.com	POST	/api/commerce/getstorecart	✓		204	662			
146	https://webapi.netgear.com	OPTIONS	/api/commerce/getstorecart			200	717			
145	https://webapi.netgear.com	POST	/api/commerce/authenticatesession	✓		200	2038	JSON		
143	https://ad.wappalyzer.com	POST	/log/wp/	✓		204	105			
141	https://webapi.netgear.com	OPTIONS	/api/commerce/authenticatesession			200	757			
140	https://nova.collect.igodigital.com	GET	/c2/10907971/track_page_view?payloa...	✓						
138	https://dev.visualwebsiteoptimiz...	GET	/j.php?a=127383&u=https%3A%2F%2F...	✓				HTML	php	
137	https://www.netgear.com	GET	/fonts/avenir/avenirnextltpro-regular.wo...			200	41130	HTML	woff2	Page Not Found
136	https://www.netgear.com	GET	/			200	44979	HTML		NETGEAR
135	https://webapi.netgear.com	POST	/api/commerce/getstorecart	✓		204	662			
134	https://webapi.netgear.com	OPTIONS	/api/commerce/getstorecart			200	717			
132	https://webapi.netgear.com	POST	/api/commerce/authenticatesession	✓		200	2038	JSON		
131	https://nova.collect.igodigital.com	GET	/c2/10907971/track_page_view?payloa...	✓						
129	https://webapi.netgear.com	OPTIONS	/api/commerce/authenticatesession			200	757			
128	https://www.netgear.com	GET	/fonts/avenir/avenirnextltpro-regular.wo...			200	41130	HTML	woff2	Page Not Found
126	https://dev.visualwebsiteoptimiz...	GET	/j.php?a=127383&u=https%3A%2F%2F...	✓				HTML	php	
123	https://www.netgear.com	GET	/			200	44979	HTML		NETGEAR
121	https://webapi.netgear.com	POST	/api/commerce/getsession	✓		200	1628	text		

Hotkeys

- (Good) developers usually use hotkeys in their IDE - You should start doing it in Burp
- Ctrl+Shift+P - Proxy
- Ctrl+Shift+R - Repeater
- Ctrl+Shift+I - Intruder
- Ctrl+R - Send this request to repeater
- Ctrl+I - Send this request to intruder
- Ctrl+- - Previous tab
- Custom: Ctrl++ - Next tab
- Custom: Ctrl+G - Repeater send request

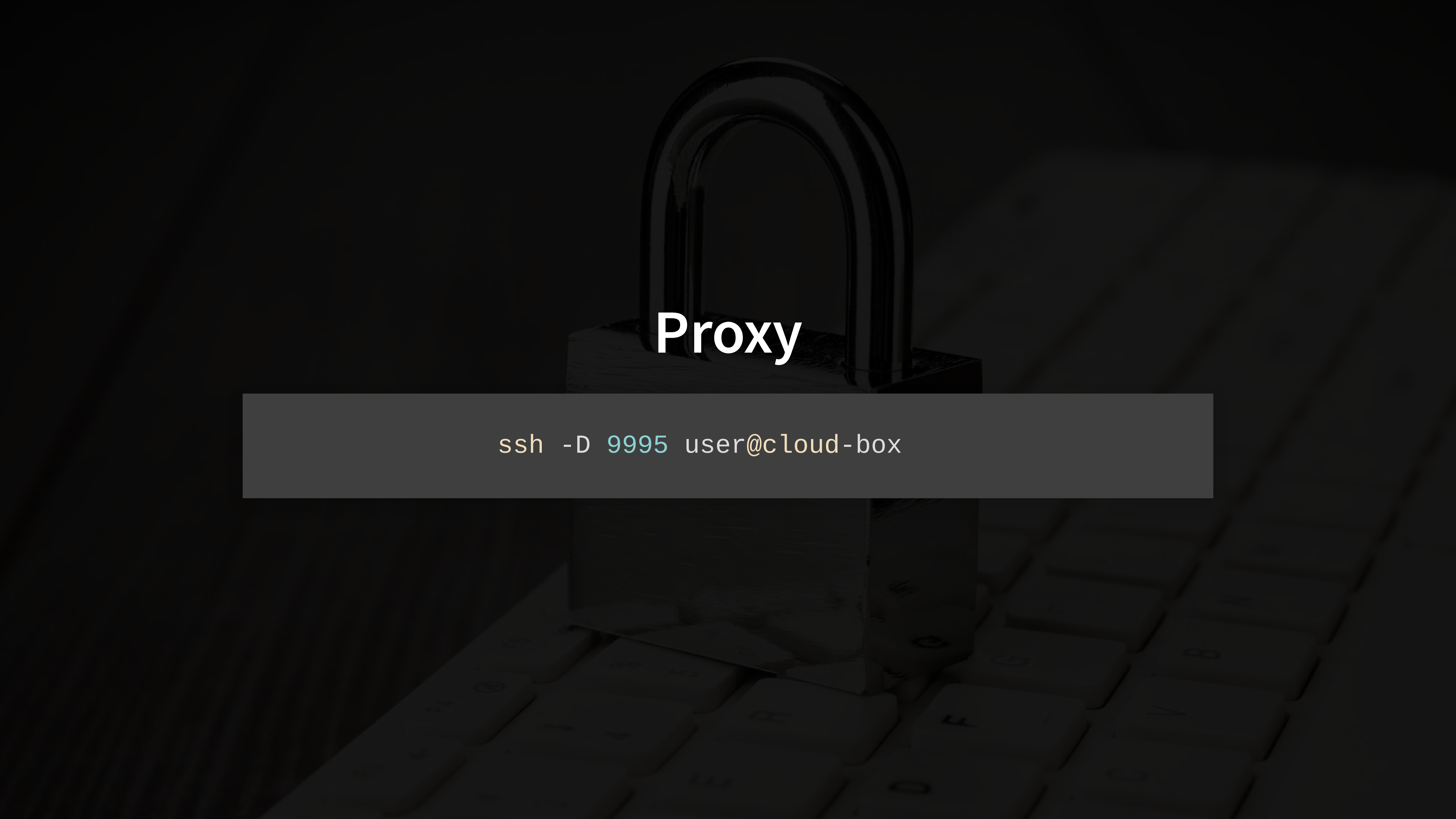


Repeater with Hotkey demo with

Auto-scroll to match when text changes

General tips

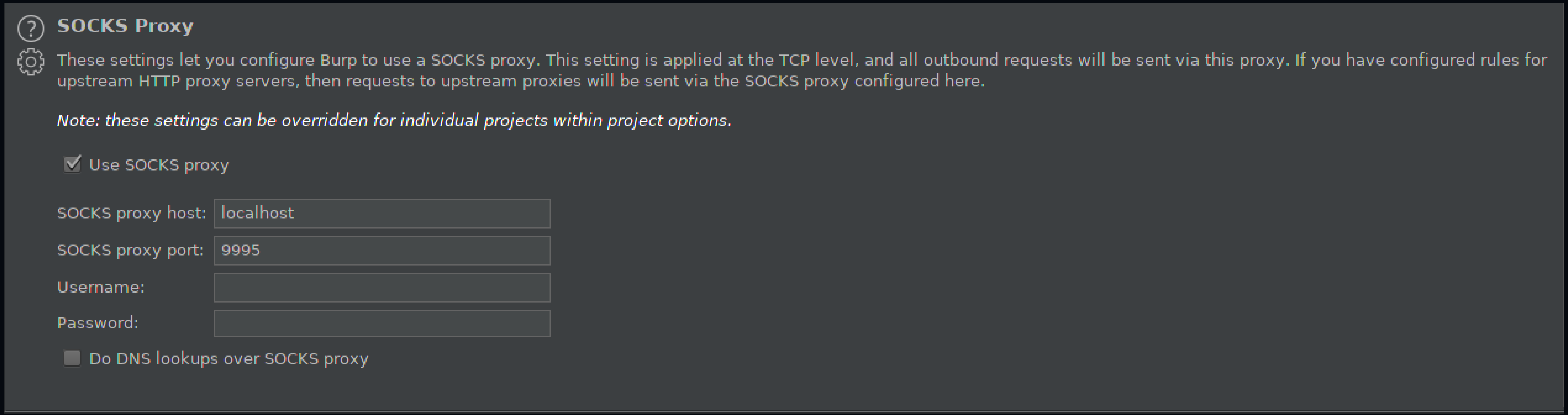
- Learn how to save session in Burp
- For intruder stuff - use SecList
- Some buttons are hard to find - know where the buttons is ;)
- Learn the advanced features - they save you a lot of time
- Use your cloud box as a SOCKS proxy



Proxy

```
ssh -D 9995 user@cloud-box
```

User options --> Connections



SOCKS Proxy

These settings let you configure Burp to use a SOCKS proxy. This setting is applied at the TCP level, and all outbound requests will be sent via this proxy. If you have configured rules for upstream HTTP proxy servers, then requests to upstream proxies will be sent via the SOCKS proxy configured here.

Note: these settings can be overridden for individual projects within project options.

☑ Use SOCKS proxy

SOCKS proxy host: localhost

SOCKS proxy port: 9995

Username:

Password:

□ Do DNS lookups over SOCKS proxy

Debugging burp - Flow plugin

Intruder basics

- Demo - basic numbers
- Demo - scan defined insertion point
- Demo - scan EVERY char

Intruder plugins - Meth0dman

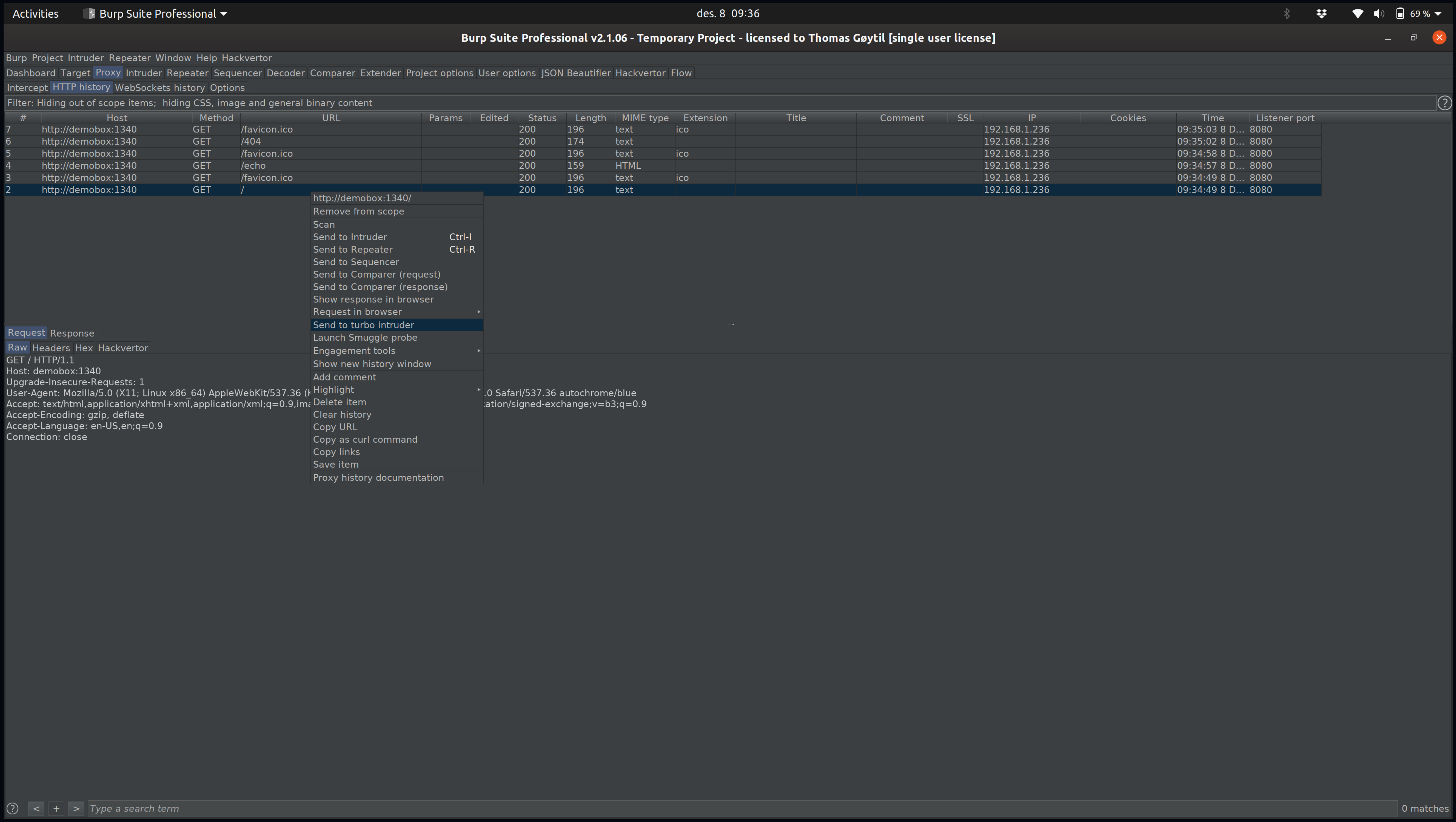
- For every endpoint on this site: do one request for each HTTP method !

Turbo intruder - Going beyond intruder

- Fast - custom HTTP stack
- Scalable - flat memory usage and headless support
- Flexible - Scripts are written in Python. Custom handling of malformed requests
- Convenient - Filtering non-relevant results

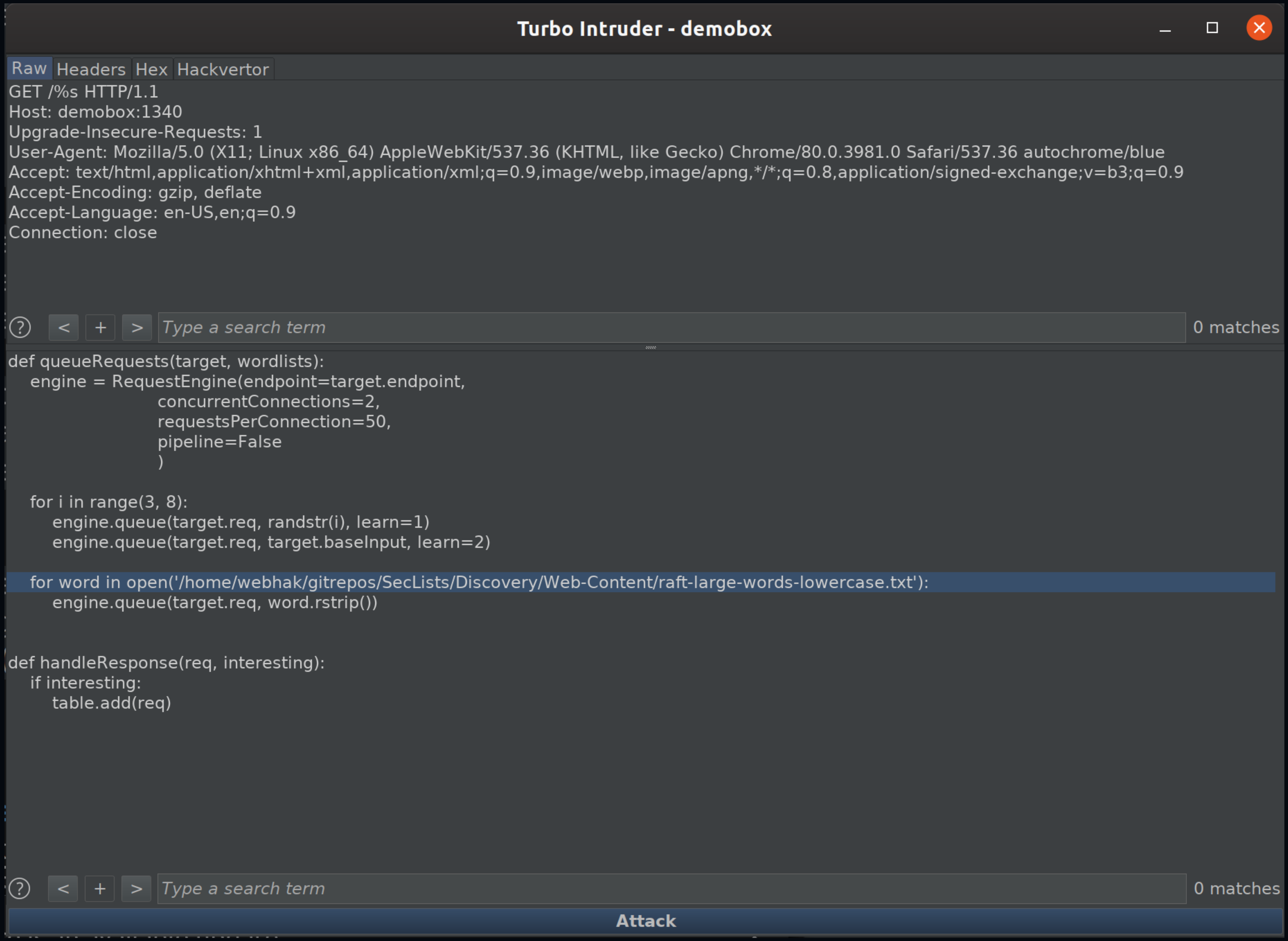
On the other hand it's undeniably harder to use, and the network stack isn't as reliable and battle-tested as core Burp's.

https://portswigger.net/research/turbo-intruder-embracing-the-billion-request-attack


Activities
Burp Suite Professional
des. 8 09:36
69 %
Burp Suite Professional v2.1.06 - Temporary Project - licensed to Thomas Gøytil [single user license]
Burp Project Intruder Repeater Window Help Hackvertor
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options JSON Beautifier Hackvertor Flow
Intercept HTTP history WebSockets history Options
Filter: Hiding out of scope items; hiding CSS, image and general binary content
http://demobox:1340/
Remove from scope
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Send to turbo intruder
Launch Smuggle probe
Engagement tools
Show new history window
Add comment
Highlight
Delete item
Clear history
Copy URL
Copy as curl command
Copy links
Save item
Proxy history documentation
Request Response
Raw Headers Hex Hackvertor
Type a search term
0 matches

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
7	http://demobox:1340	GET	/favicon.ico			200	196	text	ico				192.168.1.236		09:35:03 8 D...	8080
6	http://demobox:1340	GET	/404			200	174	text					192.168.1.236		09:35:02 8 D...	8080
5	http://demobox:1340	GET	/favicon.ico			200	196	text	ico				192.168.1.236		09:34:58 8 D...	8080
4	http://demobox:1340	GET	/echo			200	159	HTML					192.168.1.236		09:34:57 8 D...	8080
3	http://demobox:1340	GET	/favicon.ico			200	196	text	ico				192.168.1.236		09:34:49 8 D...	8080
2	http://demobox:1340	GET	/			200	196	text					192.168.1.236		09:34:49 8 D...	8080

```
GET / HTTP/1.1
Host: demobox:1340
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (k                              .0 Safari/537.36 autochrome/blue
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,ima                              cation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```



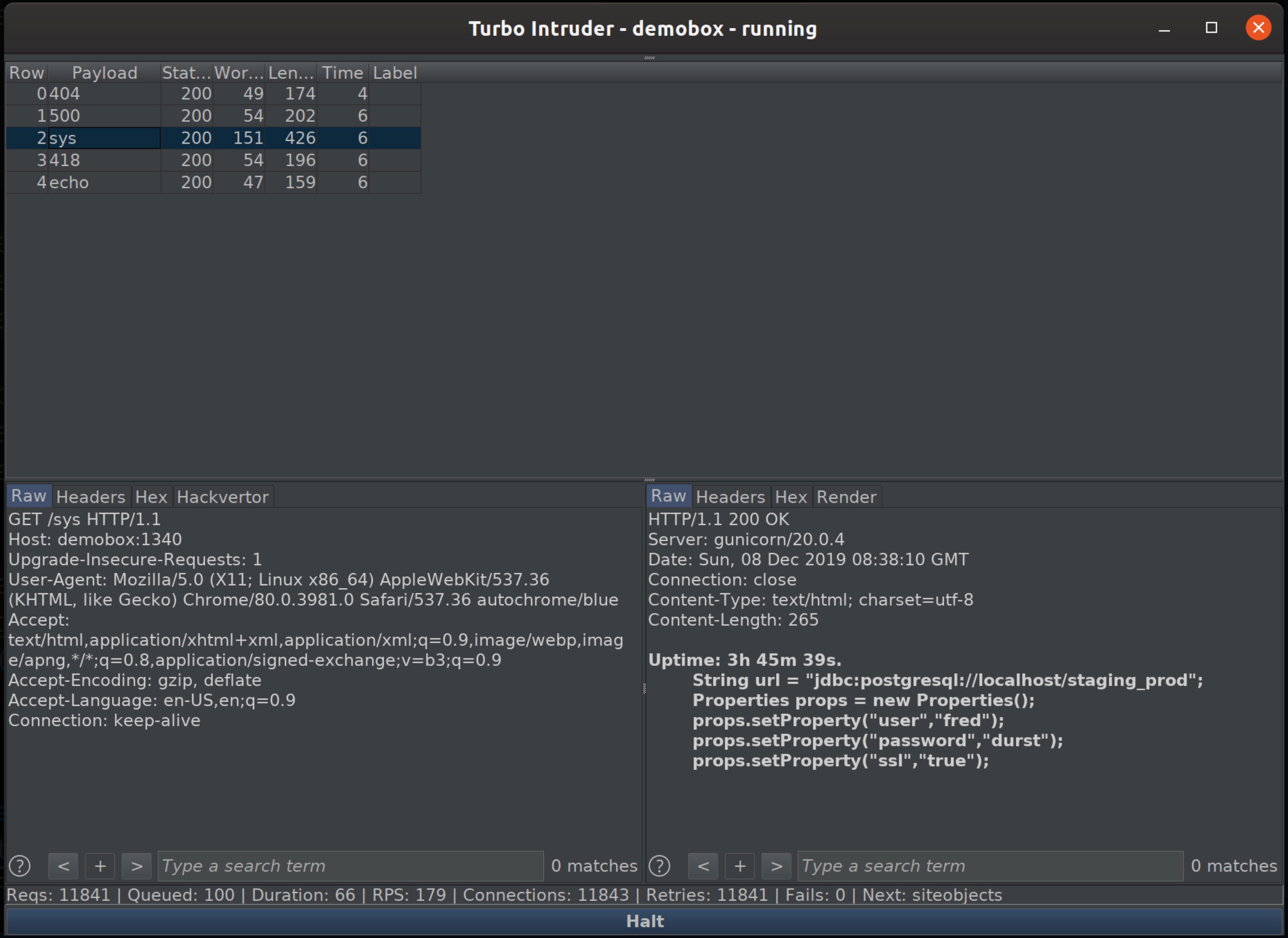
```
GET /%s HTTP/1.1
Host: demobox:1340
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3981.0 Safari/537.36 autochrome/blue
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
def queueRequests(target, wordlists):
    engine = RequestEngine(endpoint=target.endpoint,
                           concurrentConnections=2,
                           requestsPerConnection=50,
                           pipeline=False
                           )

    for i in range(3, 8):
        engine.queue(target.req, randstr(i), learn=1)
        engine.queue(target.req, target.baseInput, learn=2)

    for word in open('/home/webhak/gitrepos/SecLists/Discovery/Web-Content/raft-large-words-lowercase.txt'):
        engine.queue(target.req, word.rstrip())


def handleResponse(req, interesting):
    if interesting:
        table.add(req)
```



Row	Payload	Stat...	Wor...	Len...	Time	Label
0	404	200	49	174	4	
1	500	200	54	202	6	
2	sys	200	151	426	6	
3	418	200	54	196	6	
4	echo	200	47	159	6	

```
GET /sys HTTP/1.1
Host: demobox:1340
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/80.0.3981.0 Safari/537.36 autochrome/blue
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,imag
e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: gunicorn/20.0.4
Date: Sun, 08 Dec 2019 08:38:10 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 265

Uptime: 3h 45m 39s.
        String url = "jdbc:postgresql://localhost/staging_prod";
        Properties props = new Properties();
        props.setProperty("user","fred");
        props.setProperty("password","durst");
        props.setProperty("ssl","true");
```

Reqs: 11841 | Queued: 100 | Duration: 66 | RPS: 179 | Connections: 11843 | Retries: 11841 | Fails: 0 | Next: siteobjects

Standard wordlist

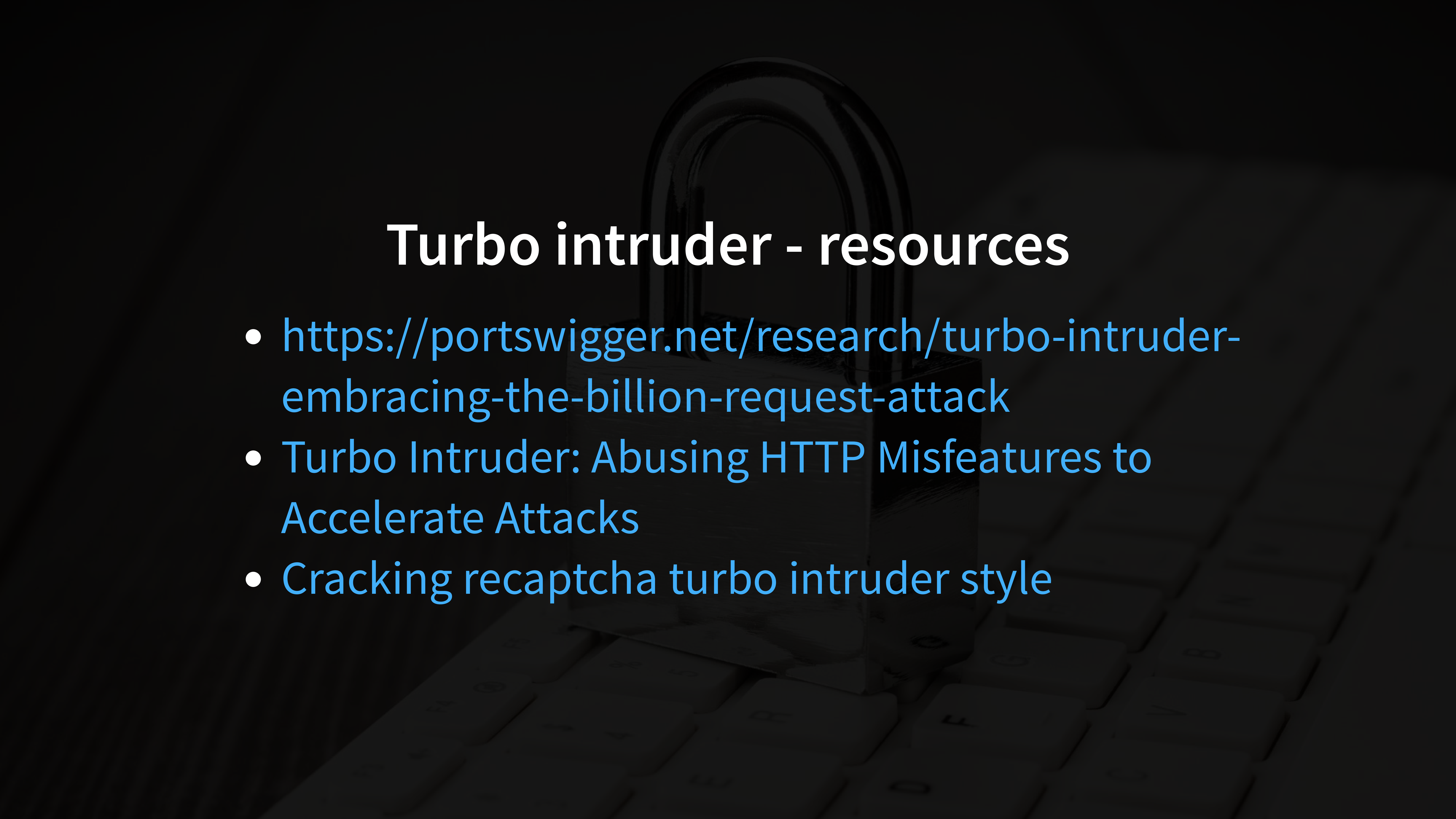
```
# regular wordlist
for line in open('/home/user/wordlist/a_wordlist.txt'):
        engine.queue(target.req, line.rstrip())
```

Observed words

```
# list of all words observed in traffic
for word in wordlists.observedWords:
        engine.queue(target.req, word)
```

Infinietly brute-force

```
# infinitely-running bruteforce (a, b ... aaa, aab etc)
seed = 0
while True:
        batch = []
        seed = wordlists.bruteforce.generate(
                seed,
                5000,
                batch
        )
        for word in batch:
                engine.queue(target.req, word)
```



Turbo intruder - resources

- https://portswigger.net/research/turbo-intruder-embracing-the-billion-request-attack
- Turbo Intruder: Abusing HTTP Misfeatures to Accelerate Attacks
- Cracking recaptcha turbo intruder style

Macro basics and debugging

Burp collaborator

Collaborator XXE demo

XXE exfil of /app/secret.txt with Burp collaborator

Private collaborator

Set up your own collaborator to not share data with Portswigger

Collaborator everywhere

- X-Forwarded-For
- X-Wap-Profile
- X-Real-Ip
- Forwarded
- etc....

https://portswigger.net/research/cracking-the-lens-targeting-https-hidden-attack-surface

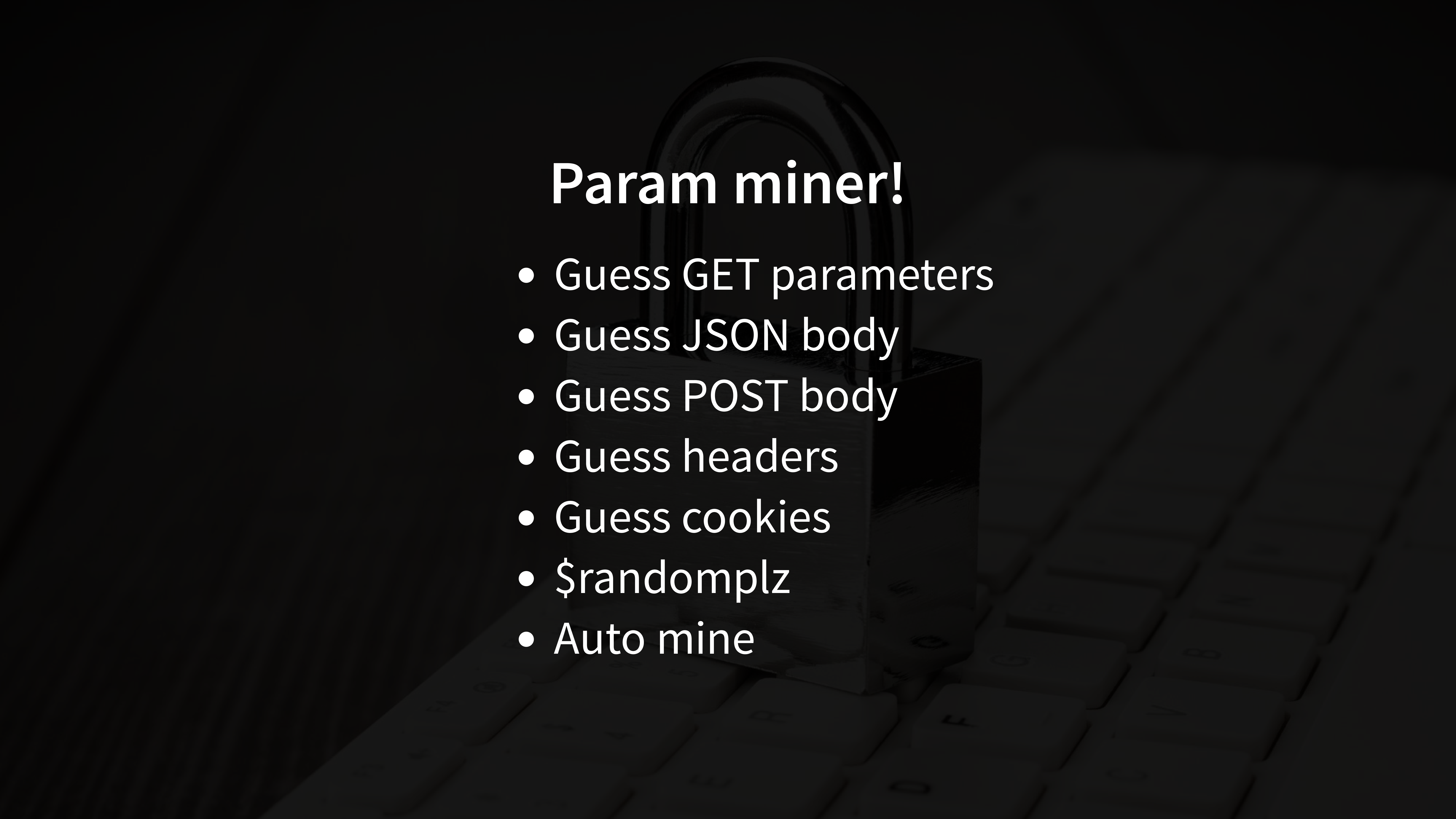
Collaborator everywhere

Tuning where collaborator is inserted

https://portswigger.net/research/adapting-burp-extensions-for-tailored-pentesting

Hackvertor

- Awesome plugin….
- … you just need to learn how to use it ;)
- Tags support parameters
- This plugin supports python code!
- Demo with URLencode in XSS-reflected demo

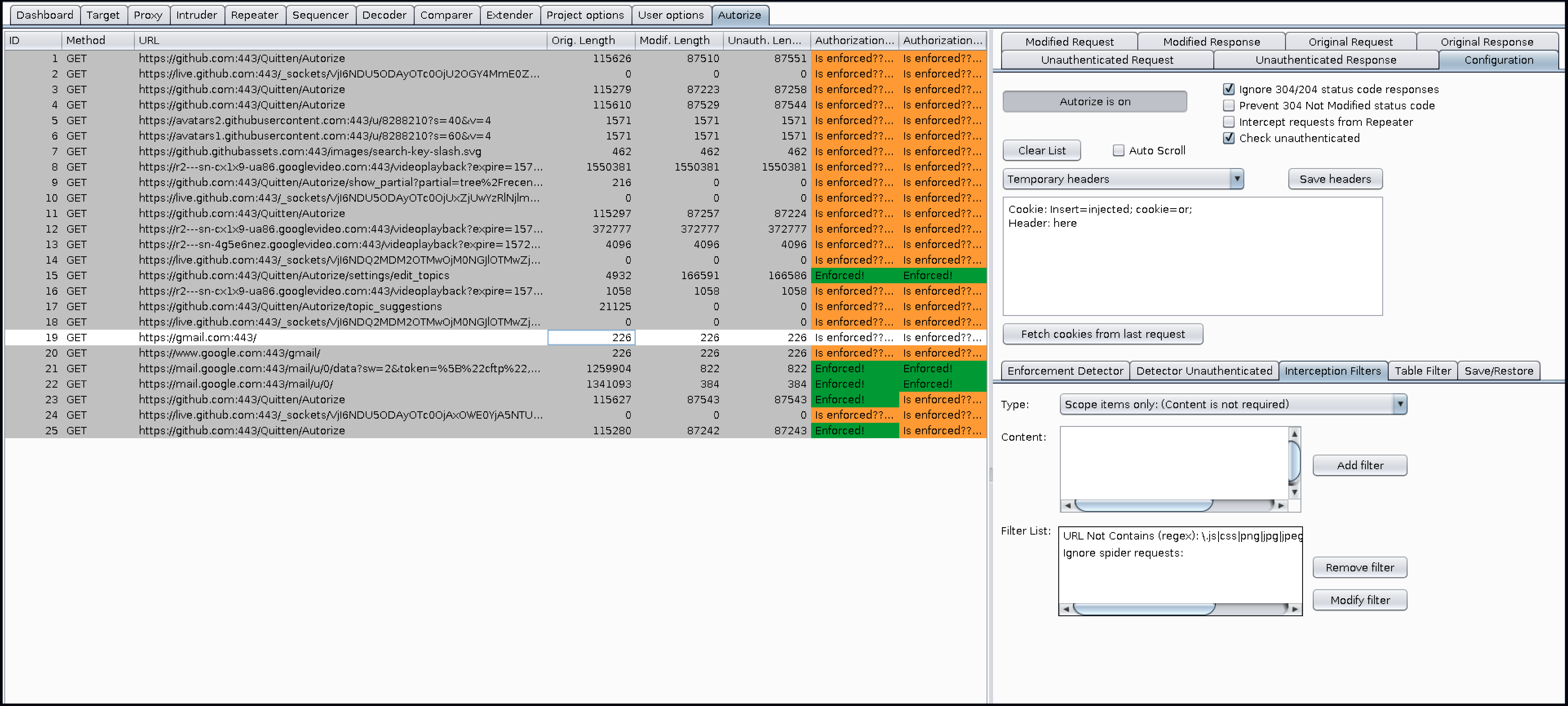


Param miner!

- Guess GET parameters
- Guess JSON body
- Guess POST body
- Guess headers
- Guess cookies
- $randomplz
- Auto mine

Param miner - Guess GET param

Autorize



ID	Method	URL	Orig. Length	Modif. Length	Unauth. Len...	Authorization...	Authorization...
1	GET	https://github.com:443/Quitten/Autorize	115626	87510	87551	Is enforced??...	Is enforced??...
2	GET	https://live.github.com:443/_sockets/VjI6NDU5ODAyOTc0OjU2OGY4MmE0Z...	0	0	0	Is enforced??...	Is enforced??...
3	GET	https://github.com:443/Quitten/Autorize	115279	87223	87258	Is enforced??...	Is enforced??...
4	GET	https://github.com:443/Quitten/Autorize	115610	87529	87544	Is enforced??...	Is enforced??...
5	GET	https://avatars2.githubusercontent.com:443/u/8288210?s=40&v=4	1571	1571	1571	Is enforced??...	Is enforced??...
6	GET	https://avatars1.githubusercontent.com:443/u/8288210?s=60&v=4	1571	1571	1571	Is enforced??...	Is enforced??...
7	GET	https://github.githubassets.com:443/images/search-key-slash.svg	462	462	462	Is enforced??...	Is enforced??...
8	GET	https://r2---sn-cx1x9-ua86.googlevideo.com:443/videoplayback?expire=157...	1550381	1550381	1550381	Is enforced??...	Is enforced??...
9	GET	https://github.com:443/Quitten/Autorize/show_partial?partial=tree%2Frecen...	216	0	0	Is enforced??...	Is enforced??...
10	GET	https://live.github.com:443/_sockets/VjI6NDU5ODAyOTc0OjUxZjUwYzRlNjlm...	0	0	0	Is enforced??...	Is enforced??...
11	GET	https://github.com:443/Quitten/Autorize	115297	87257	87224	Is enforced??...	Is enforced??...
12	GET	https://r2---sn-cx1x9-ua86.googlevideo.com:443/videoplayback?expire=157...	372777	372777	372777	Is enforced??...	Is enforced??...
13	GET	https://r2---sn-4g5e6nez.googlevideo.com:443/videoplayback?expire=1572...	4096	4096	4096	Is enforced??...	Is enforced??...
14	GET	https://live.github.com:443/_sockets/VjI6NDQ2MDM2OTMwOjM0NGJlOTMwZj...	0	0	0	Is enforced??...	Is enforced??...
15	GET	https://github.com:443/Quitten/Autorize/settings/edit_topics	4932	166591	166586	Enforced!	Enforced!
16	GET	https://r2---sn-cx1x9-ua86.googlevideo.com:443/videoplayback?expire=157...	1058	1058	1058	Is enforced??...	Is enforced??...
17	GET	https://github.com:443/Quitten/Autorize/topic_suggestions	21125	0	0	Is enforced??...	Is enforced??...
18	GET	https://live.github.com:443/_sockets/VjI6NDQ2MDM2OTMwOjM0NGJlOTMwZj...	0	0	0	Is enforced??...	Is enforced??...
19	GET	https://gmail.com:443/	226	226	226	Is enforced??...	Is enforced??...
20	GET	https://www.google.com:443/gmail/	226	226	226	Is enforced??...	Is enforced??...
21	GET	https://mail.google.com:443/mail/u/0/data?sw=2&token=%5B%22cftp%22,...	1259904	822	822	Enforced!	Enforced!
22	GET	https://mail.google.com:443/mail/u/0/	1341093	384	384	Enforced!	Enforced!
23	GET	https://github.com:443/Quitten/Autorize	115627	87543	87543	Enforced!	Is enforced??...
24	GET	https://live.github.com:443/_sockets/VjI6NDU5ODAyOTc0OjAxOWE0YjA5NTU...	0	0	0	Is enforced??...	Is enforced??...
25	GET	https://github.com:443/Quitten/Autorize	115280	87242	87243	Enforced!	Is enforced??...

☑ Ignore 304/204 status code responses

□ Prevent 304 Not Modified status code

□ Intercept requests from Repeater

☑ Check unauthenticated

□ Auto Scroll

Temporary headers ▾

```
Cookie: Insert=injected; cookie=or;
Header: here
```

Type: Scope items only: (Content is not required) ▾

Content:

Filter List:

URL Not Contains (regex): \.js|css|png|jpg|jpeg

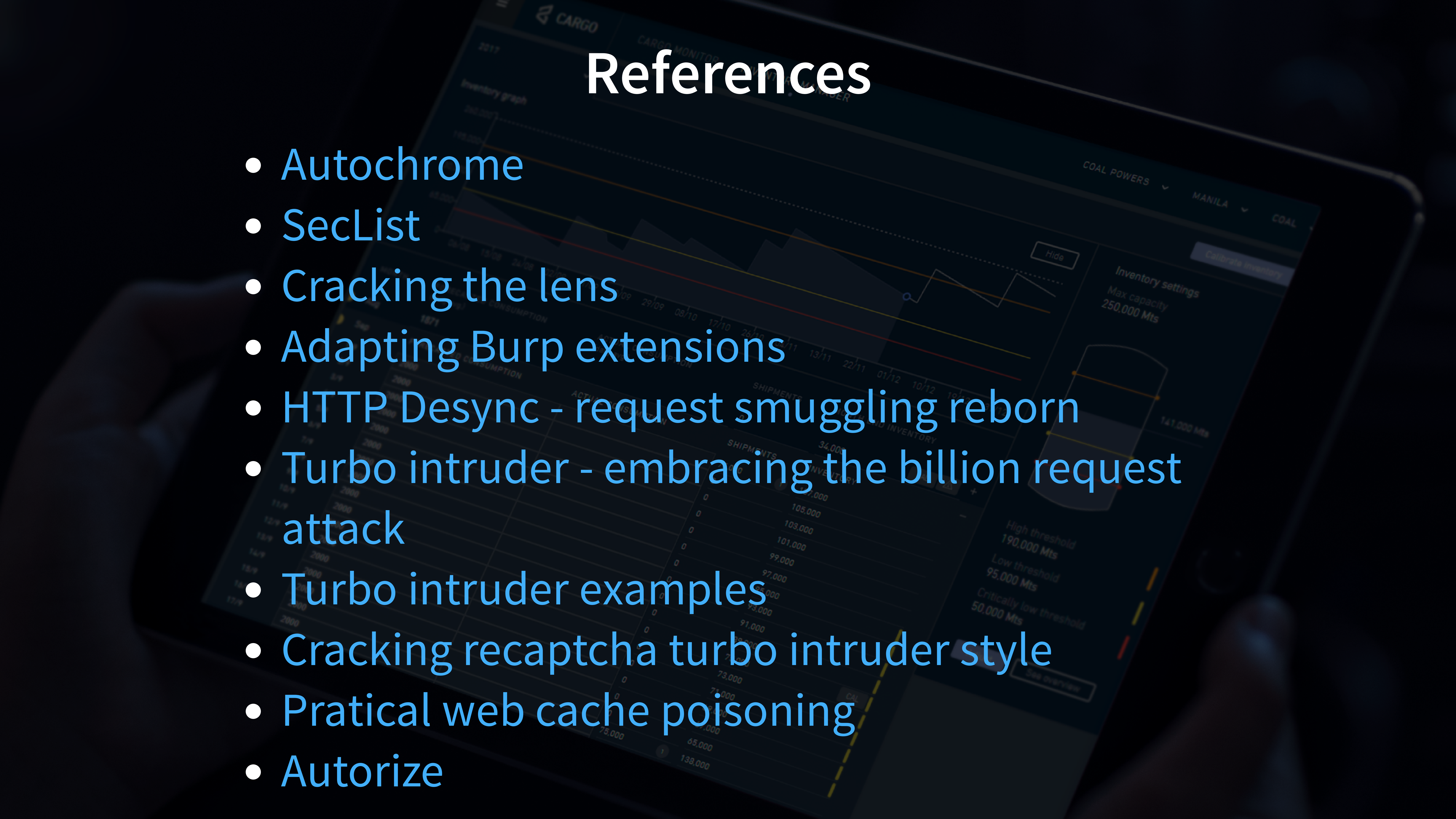
Ignore spider requests:

Where to learn more

- Mastering Burp Suite Pro: 100% Hands-On - Nicolas Gregoire (HiTB Amsterdam)
- Advanced Burp suite (Bugcrowd university)
- Portswigger - Burp testing methodologies

?

References



- Autochrome
- SecList
- Cracking the lens
- Adapting Burp extensions
- HTTP Desync - request smuggling reborn
- Turbo intruder - embracing the billion request attack
- Turbo intruder examples
- Cracking recaptcha turbo intruder style
- Pratical web cache poisoning
- Autorize