Becoming a CAIDO Power User

Ads Dawson x OWASP Toronto

September 17, 2025 - ~45 mins-1 hour

- Ads Dawson (LinkedIn: @adamdawson0)
- Ambassador @ CAIDO
- @GangGreenTemperTatum
- rads (@immapickle_nchill)
- OWASP Toronto chapter lead
- BugCrowd hacker and HAB member

Goal of tonight:

Highlight features of Caido that will make

YOU

a more efficient hacker.

Why Caido?

A personal story on finding a better workflow.

- Caido compliments skills and style as a hacker
- My previous proxy (Burp Suite) felt overly complex for my day-to-day needs.
- I was spending more time chasing noisy scans than finding actual bugs or creating my own methodology - deliberate and effective approach
- “Information overload" != real, foundational skills
- Caido does a ton of caching and compression to keep everything feel the opposite of clunky
  - **HTTPQL & Workflows > Bambas**
  - **Typescript > Java**
- The clean and intuitive UI let me focus on hacking, not wrestling with the tool.
- I host it on a VPS, allowing me to connect from any device, anywhere—even my phone.
- Caido makes me a better hacker

https://evanconnelly.com/post/my-first-100-hackerone-reports/

Where do hackers spend time?

- HTTP History: Understanding flow of application
  - Orientation - “W*here is that request I triggered?*”
  - Filtering - “***SCREW YOU ANALYTICS ENDPOINTS!!!***”
  - Comprehension - “Ah, that’s how this is implemented…”
- Replay: Implementing attack vectors
  - Friction Reduction - “*Eh, too hard*” == **missed bugs**
  - Organization - “*Oh, I’ll use this request with this…*”

Part 0

Caido Request Navigation

HTTP History

Navigation Highlighter - Passive Workflow

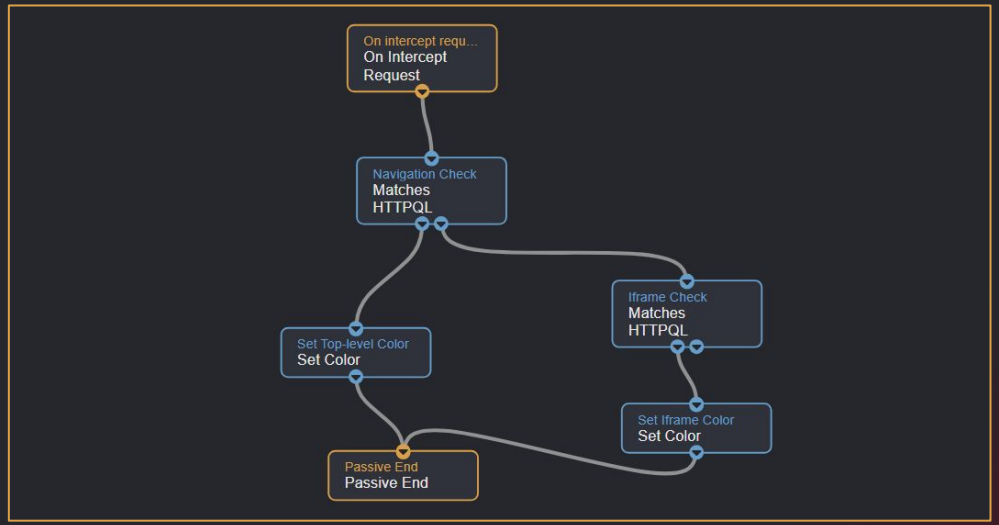
Unset Scope | Export | `req.host.cont:"poc" and row.id.gt:5270` | Advanced

ID	Host	Method	Path	Query	Status	Exten…
5278	poc.rhynorater.com:443	GET	/qt/xss.php	iframed	200	.php
5277	poc.rhynorater.com:443	GET	/qt/iframe.php	src=/qt/xss.php?iframed	200	.php

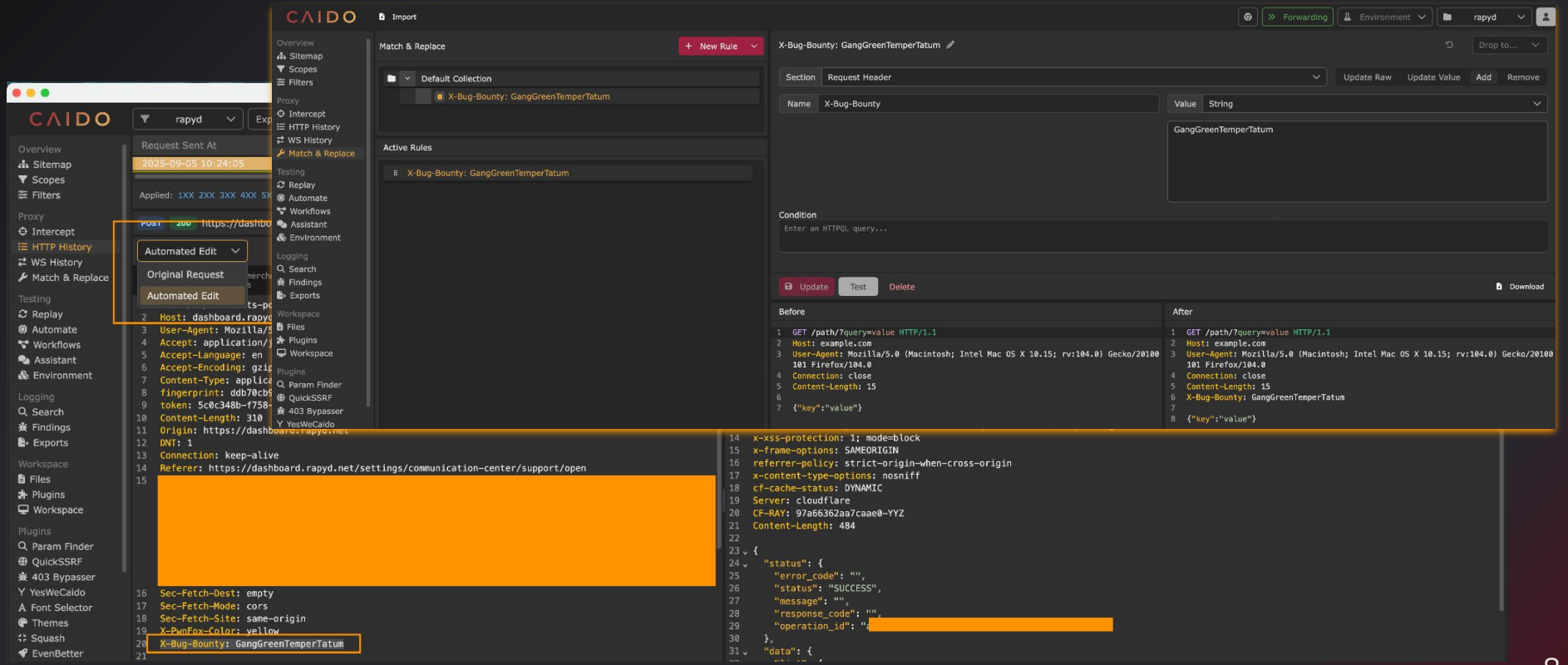
Iframe Navigation

Top-Level Navigation

Workflows | Passive 8



Simple Yet Common Passive Workflow Example



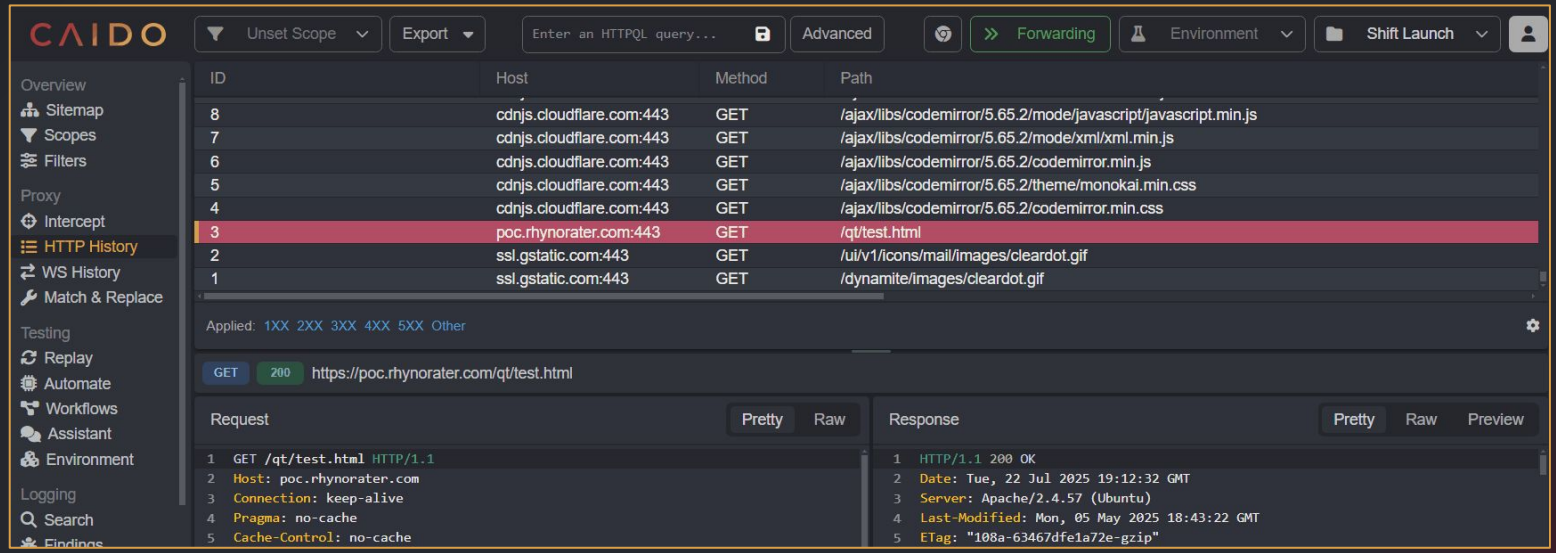
Jump to ~~FREAKING~~ Currently Selected Row

5279	my.1password.com:443	PUT	/api/v2/perftrace		200	
5278	poc.rhynorater.com:443	GET	/qt/xss.php	iframed	200	.php
5277	poc.rhynorater.com:443	GET	/qt/iframe.php	src=/qt/xss.php?iframed	200	.php
5276	ssl.gstatic.com:443	GET	/dynamite/ima…	zx=9uhhryqphp9s	200	.gif
5275	ssl.gstatic.com:443	GET	/dynamite/ima…	zx=qc34yq1dlrb85	200	.gif
5274	www.evernote.com:443	GET	/DevicePaywa…	refreshUserState&utm_medium=on…evice_ion_flow&utm…	200	

Applied: 1XX 2XX 3XX 4XX 5XX Other

Jump to row

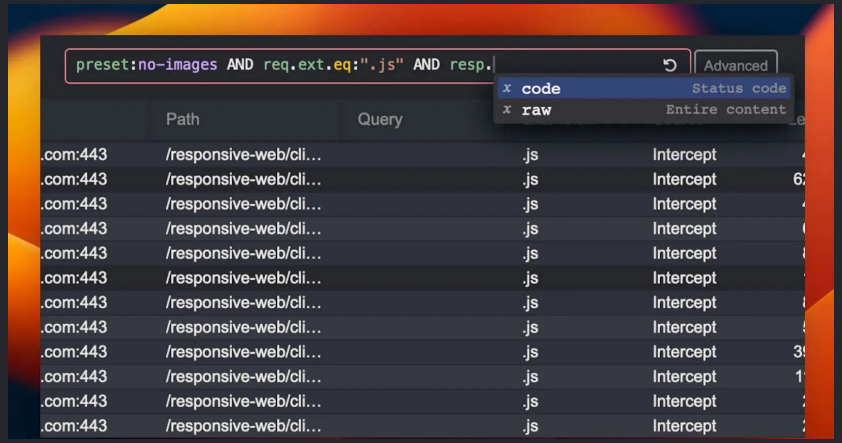
GET 200 https://poc.rhynorater.com/qt/xss.php?iframed



Part 1

Caido Search

HTTPQL = Time for serious text-based filtering.



HTTPQL - HTTP Query Language

Primitives

The constructing primitives of HTTPQL Filter Clause, in order of position, are the:

1. Namespace
2. Field
3. Operator
4. Value

https://caido.io/blog/2024-01-17-httpql
https://docs.caido.io/reference/httpql

HTTPQL - HTTP Query Language

```
req.raw.ncont:"abc123" and resp.raw.cont:"Set-Cookie: x=abc123"
```

Where did this cookie come from originally
that is reset every request?

```
req.path.regex:/v[1-3]/
```

Show me only legacy version on this API

HTTPQL - HTTP Query Language

```
req.host.cont:"api" and req.query.ncont:"xsrf_param" and
req.method.ncont:"GET"
```

Give me potentially CSRF-able requests on this API

```
req.query.cont:"cookieVal" and resp.raw.cont:"Set-Cookie:
j=cookieVal"
```

Find query parameter source for cookie sink

HTTPQL - HTTP Query Language

```
req.host.cont:"api.site.com" and req.method.cont:"PUT"
```

Give me potential PUT-based CSPT sinks on this API

```
req.ext.cont:"js" and resp.raw.cont:"/api/"
```

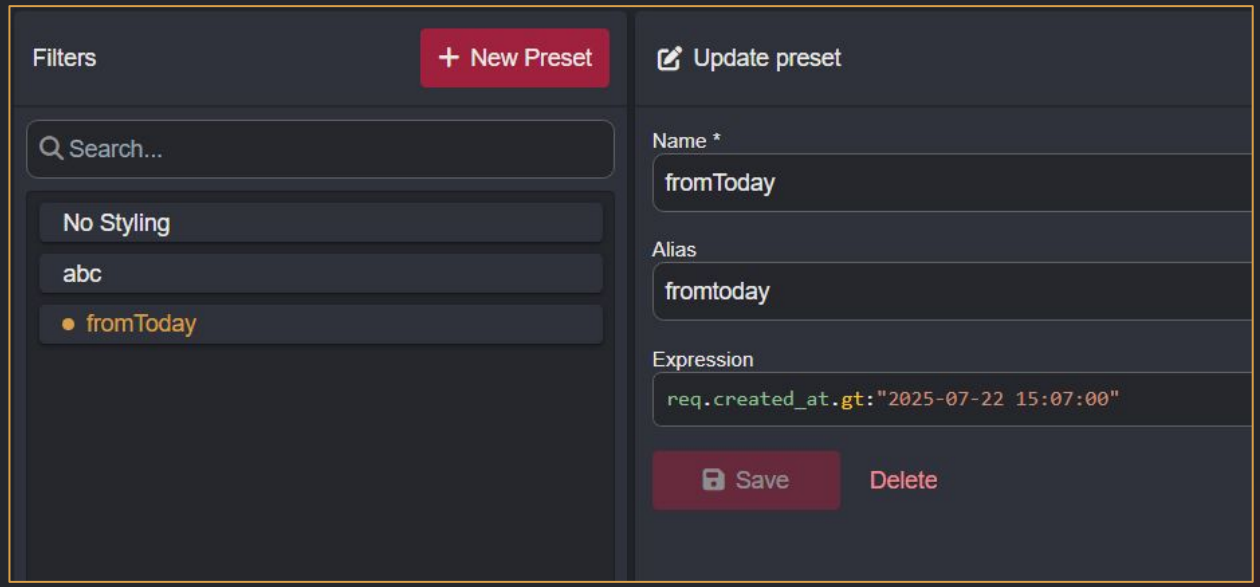
Give me all JS files that include endpoints for this API

HTTPQL - HTTP Query Language

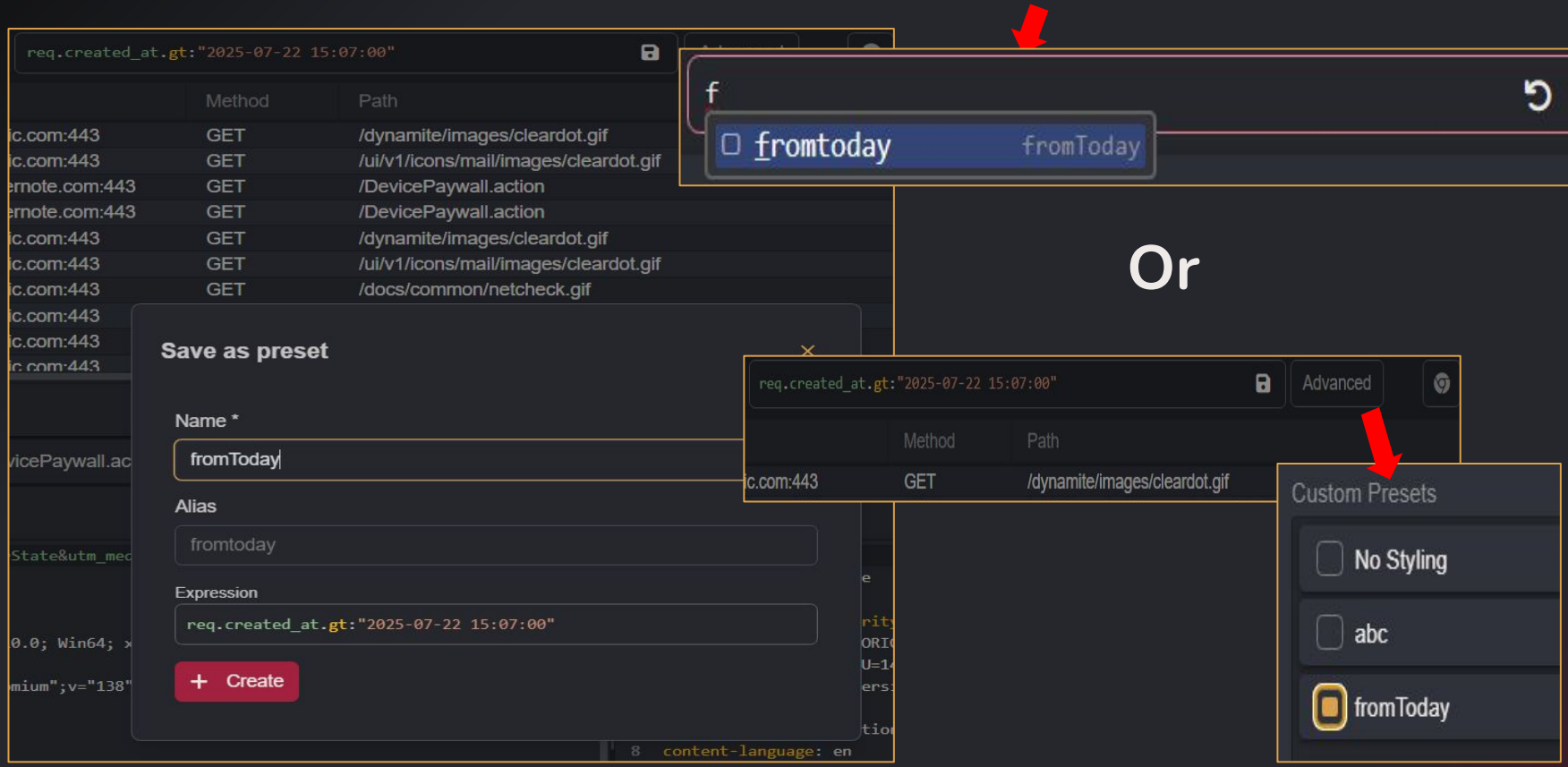
```
req.path.cont:"thatOneReq" and req.created_at.gt:"2025-07-22
16:00:00"
```

Give me that one request from 5 mins ago that I cannot find

Filters/Presets



Filters/Presets

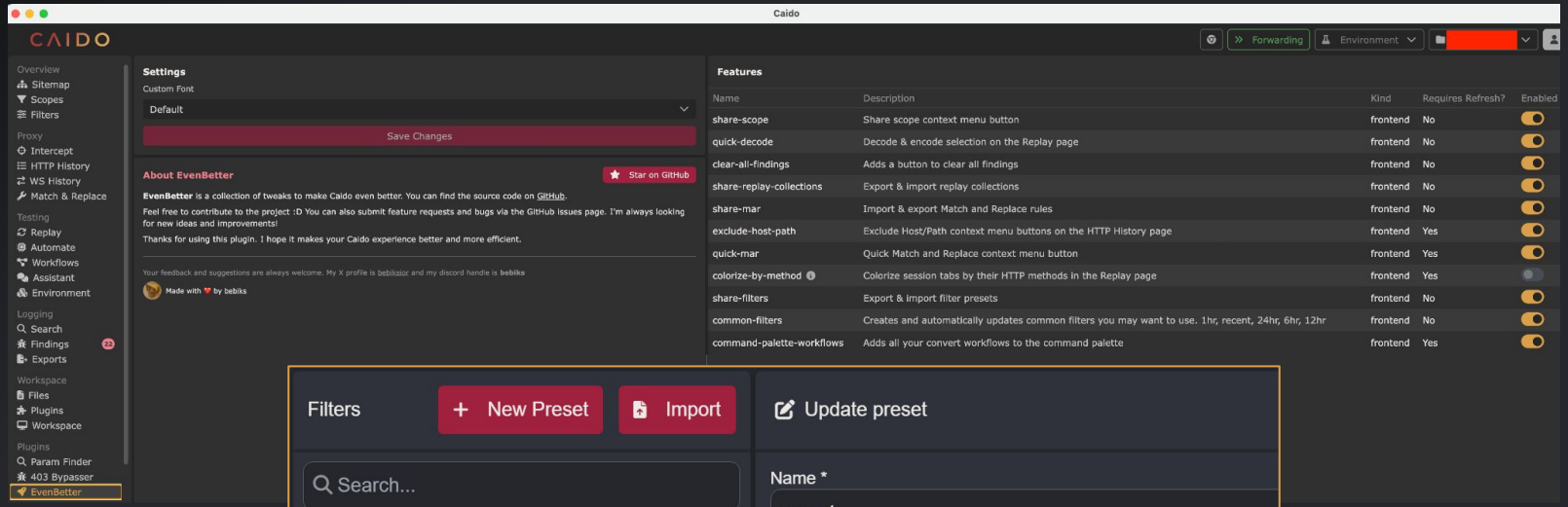


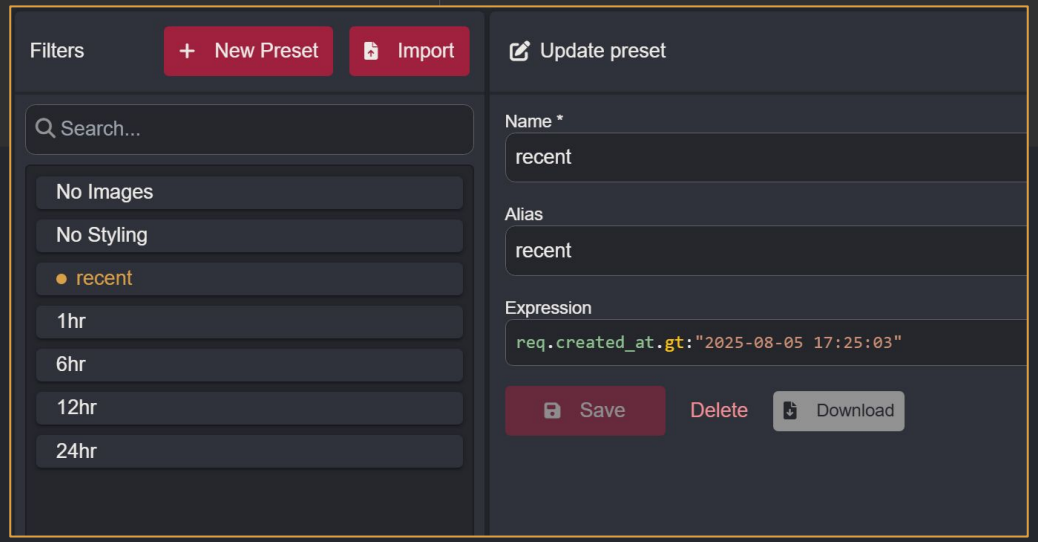
Part 1

Caido Search

common-filters (EvenBetter)

common-filters - EvenBetter Plugin





https://github.com/bebiksior/EvenBetter

https://github.com/bebiksior/EvenBetter/blob/28762c09ed5f37176e87e3485d71787d03cc5dd5/packages/frontend/src/features/common-filters/index.ts#L11-L17

Wishlist ✨🎅✨

- More Granular Selectors: Increased control
  - req/resp.headers
  - req.body
  - req.cookies
- Variables: Dynamic values in presets
  - Req.created_at.gt:now
- Search tabs, Emile. Tabs. I want tabs.

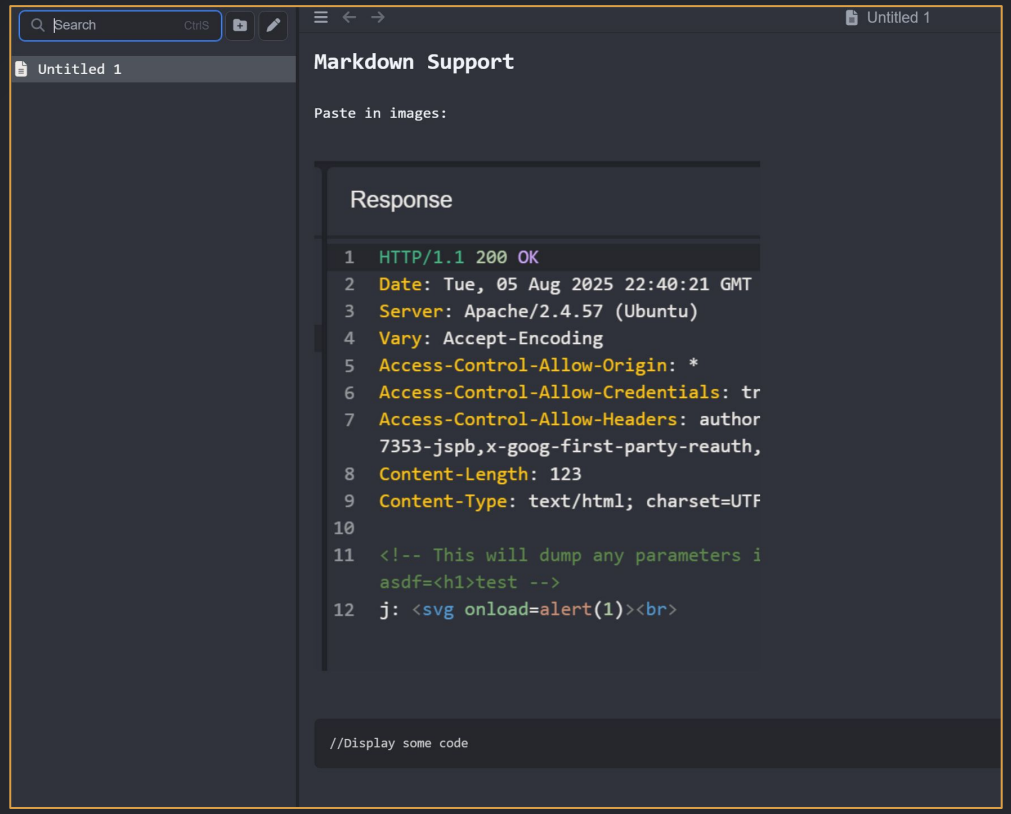
Part 2

Caido Replay

Notes++ Plugin - Organization

Organization

#1 - Directly in Notes++

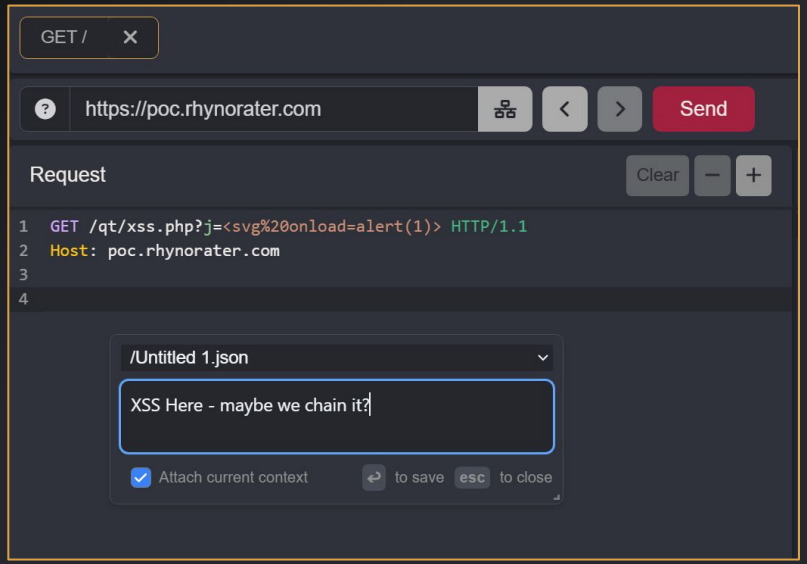


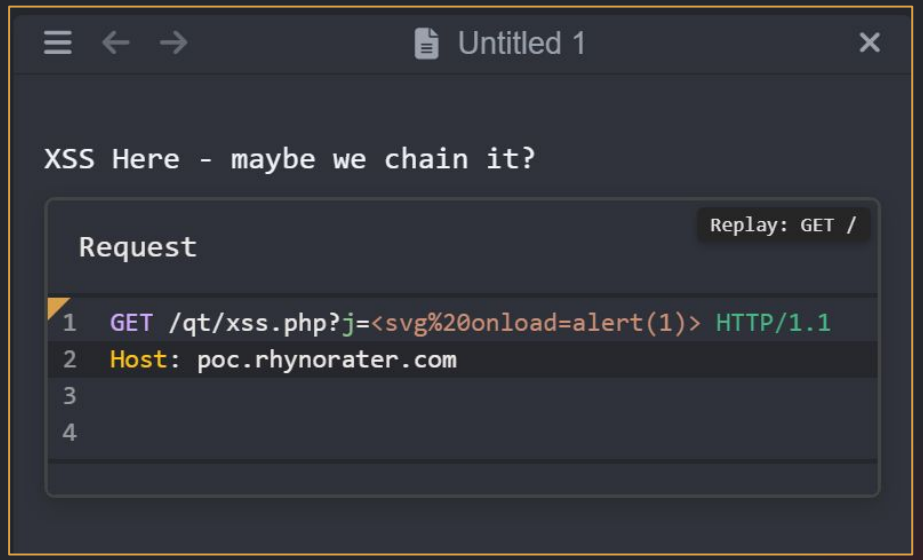
https://github.com/caido-community/NotesPlusPlus

https://github.com/caido-community/NotesPlusPlus/issues/20

Organization

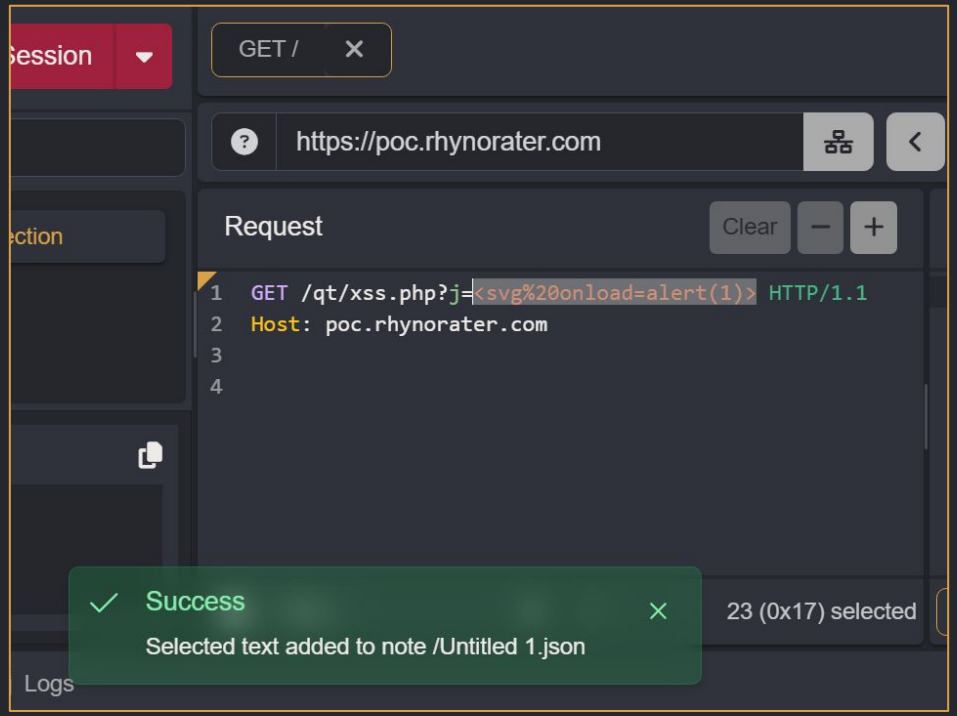
#2 - CTRL-ALT-N - Replay Notes with context





Organization

#3 - CTRL-ALT-Shift-N - Select Text & Send to Active Note



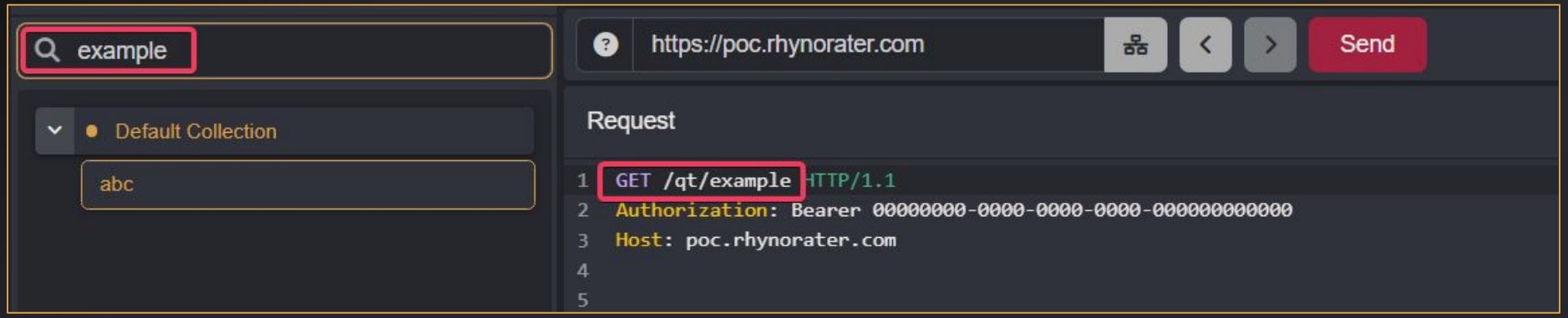
Part 2

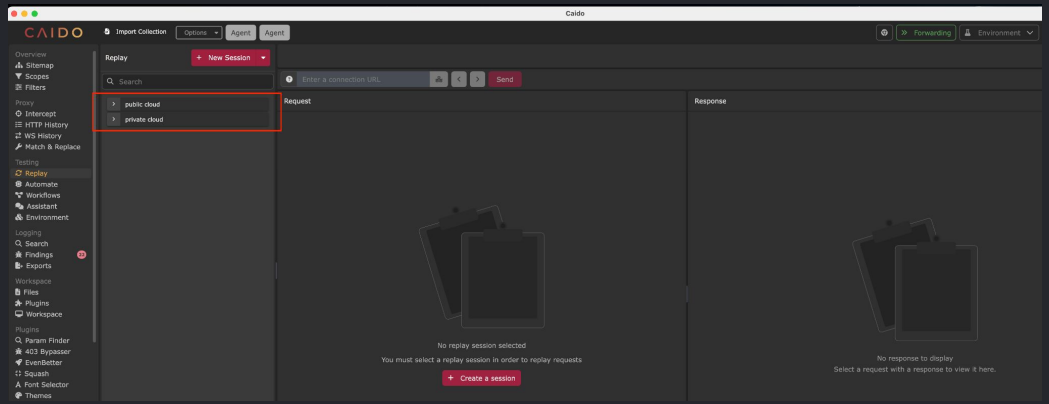
Caido Replay

Organization

Replay Organization

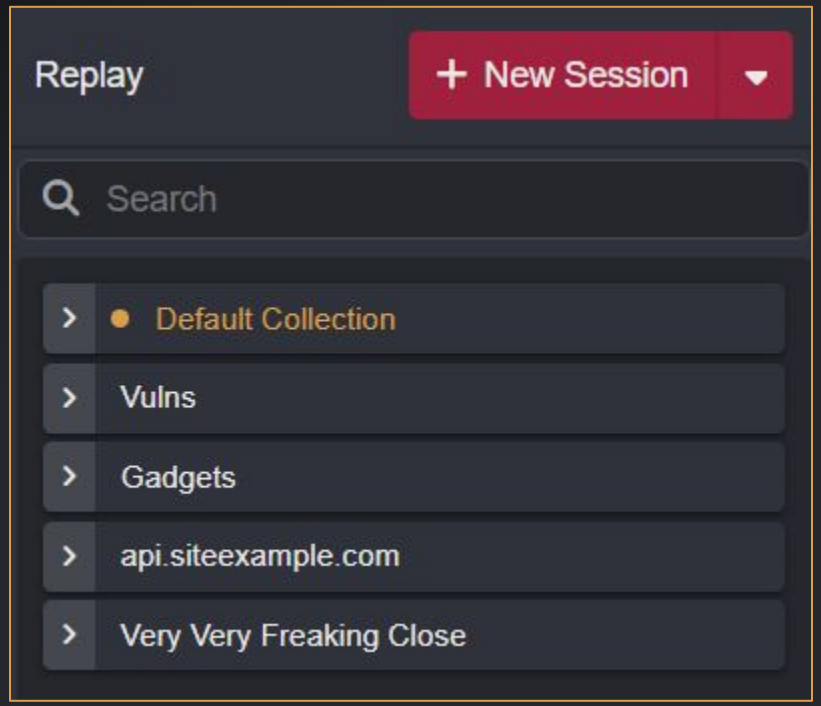
Replay Tab Search - Quick Index

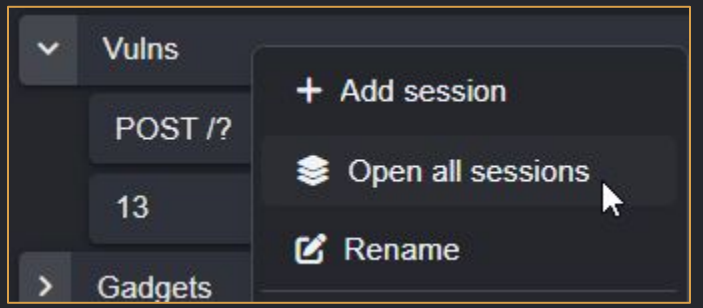


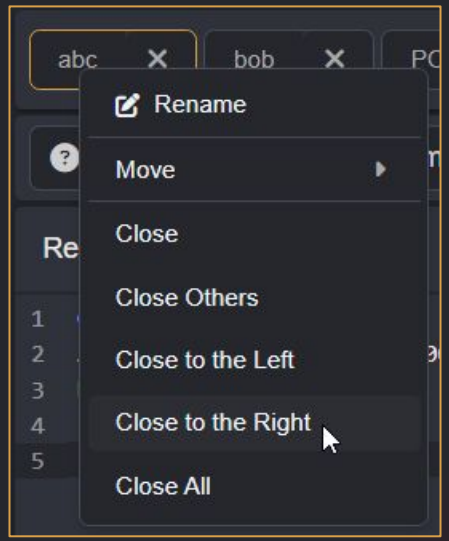


Replay Organization

Collection/Tab Management Features







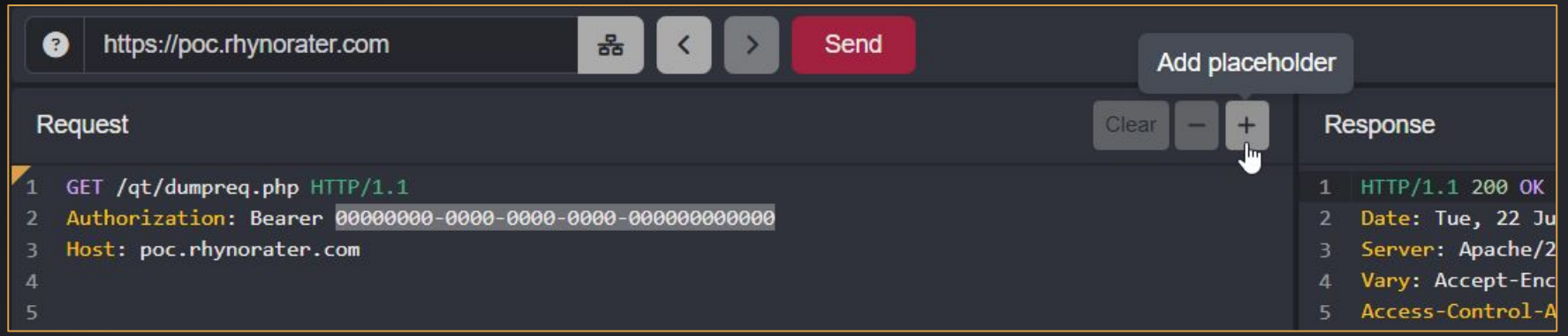
Part 2

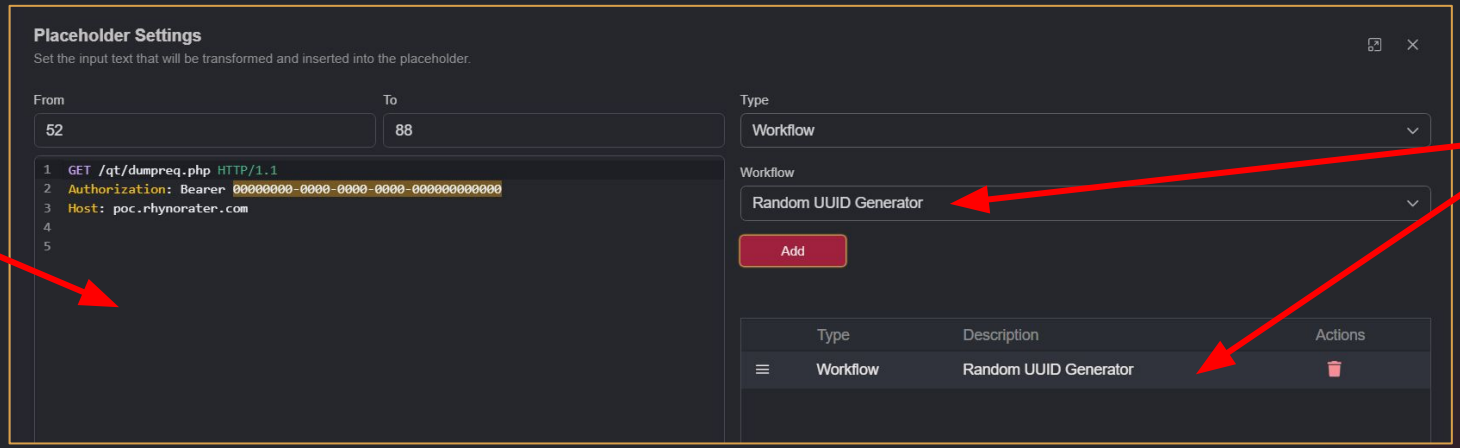
Caido Replay

Replay Placeholders

Replay

Replay Placeholders



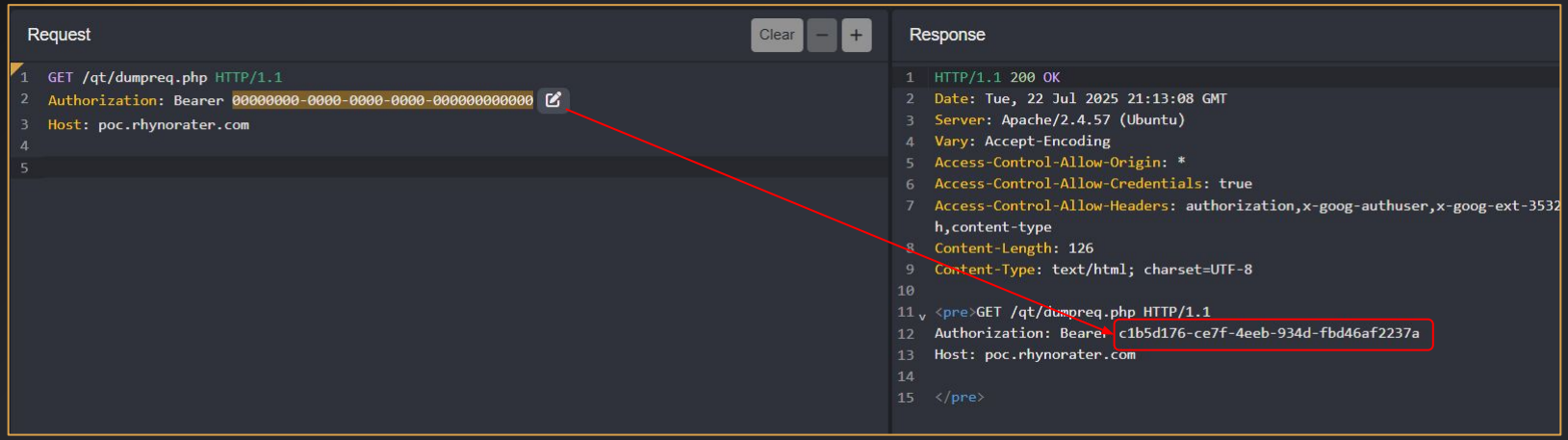


Input text

Procedure

Replay

Replay Placeholders

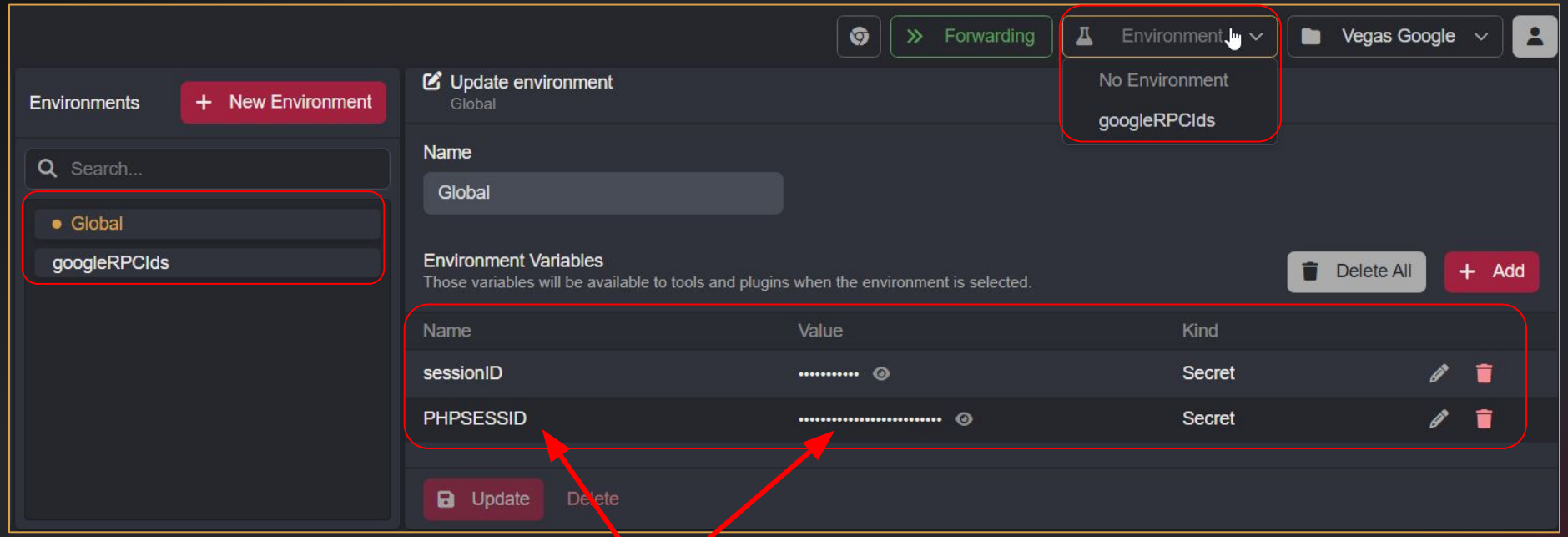


Use Cases

- High Friction Test Environments
  (binary format + base64 + url encoding + %3D truncation)
- Auth Refreshing (hint hint)
- CSRF Token Refreshing
- Request Signing Heavy Environments

Environments

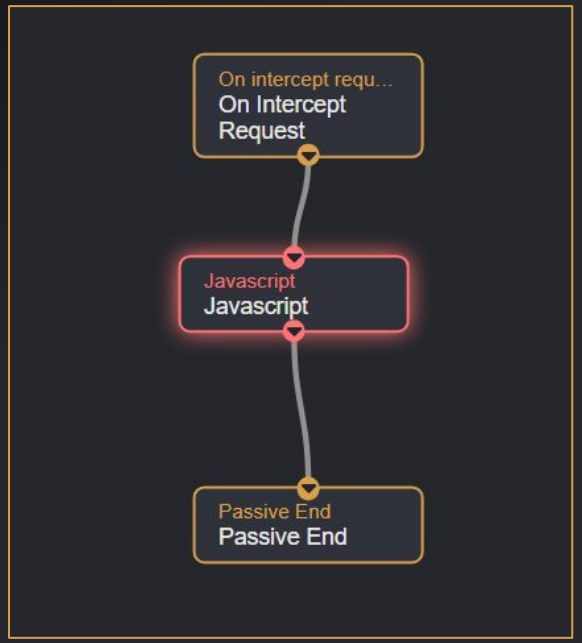
Data & Variable Store



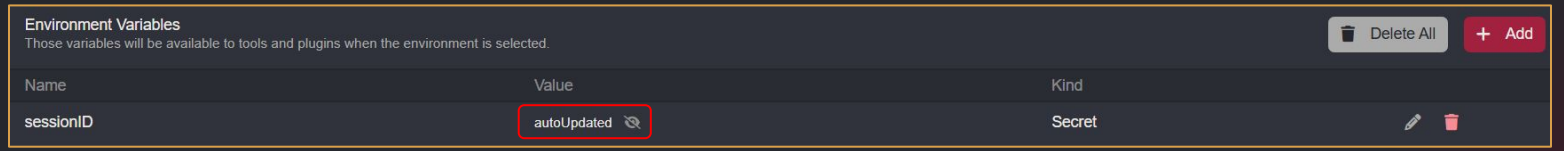
Key-Value Stores

Replay

Replay Placeholders - Auto Session Refresher

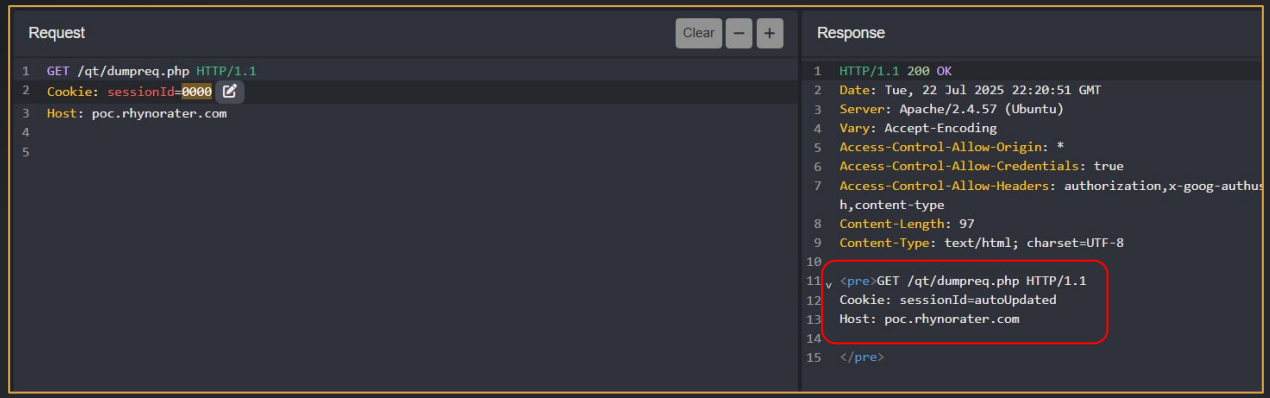


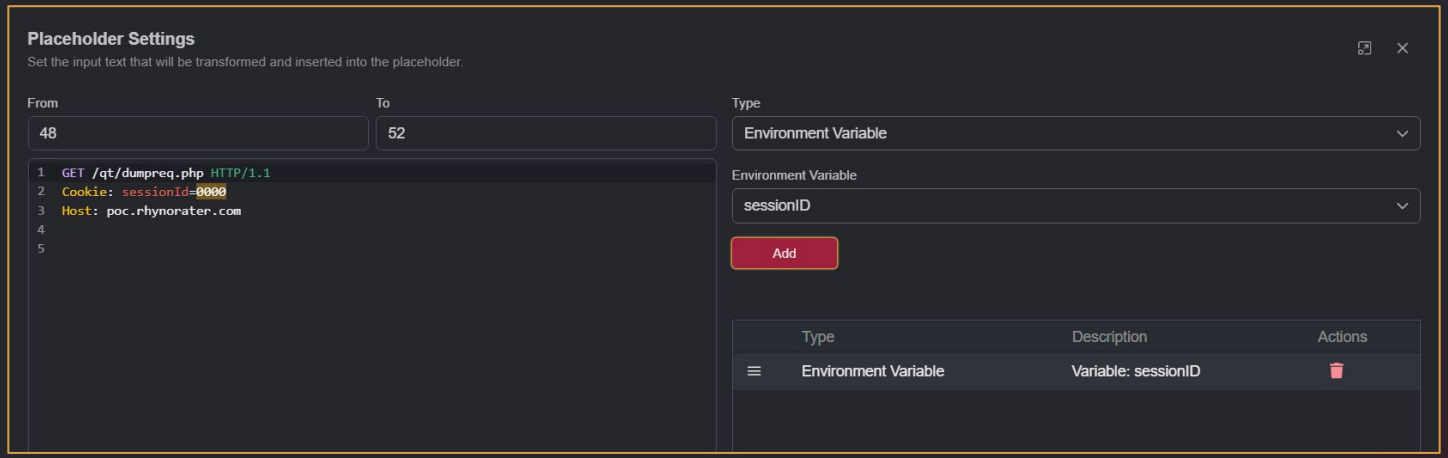

```javascript
export async function run(input, sdk) {
    if (!input.request || input.request.getHost() !== 'poc.rhynorater.com') {
        sdk.console.debug("Skipping non-target request or no request.");
        return;
    }

    const cookieHeaders = input.request.getHeader('Cookie');
    if (!cookieHeaders || cookieHeaders.length === 0) return;

    const cookieString = cookieHeaders.join('; ');
    const sessionIdMatch = cookieString.match(/(?:^|;)\s*sessionID=([^;]+)/);

    if (sessionIdMatch && sessionIdMatch[1]) {
        try {
            await sdk.env.setVar({
                name: "sessionID",
                value: sessionIdMatch[1],
                secret: true,
                global: true
            });
            sdk.console.log("Updated 'sessionID' env var.");
        } catch (error) {
            sdk.console.error(`Failed to set 'sessionID': ${error.message}`);
        }
    }
    return "success";
}
```



Replay

Replay Placeholders





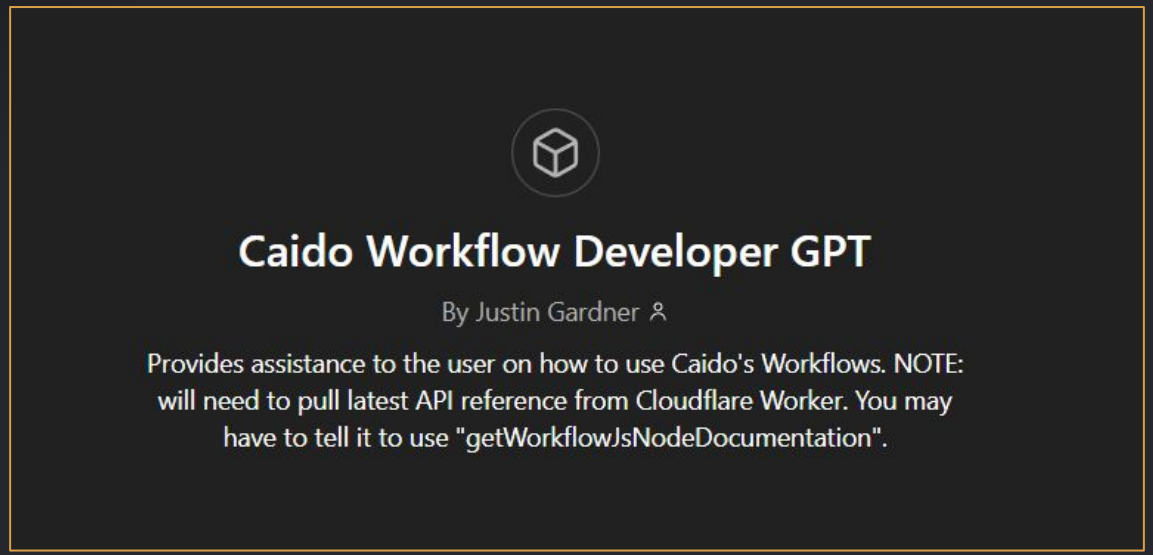
Part 3

Caido Workflows

Workflow Generation with AI

AI Workflow Development

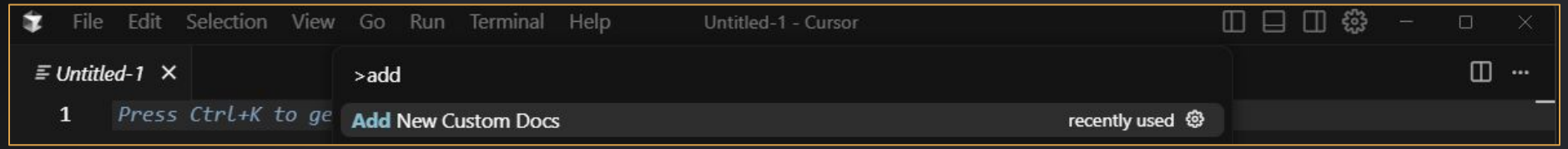
Caido Workflow GPT

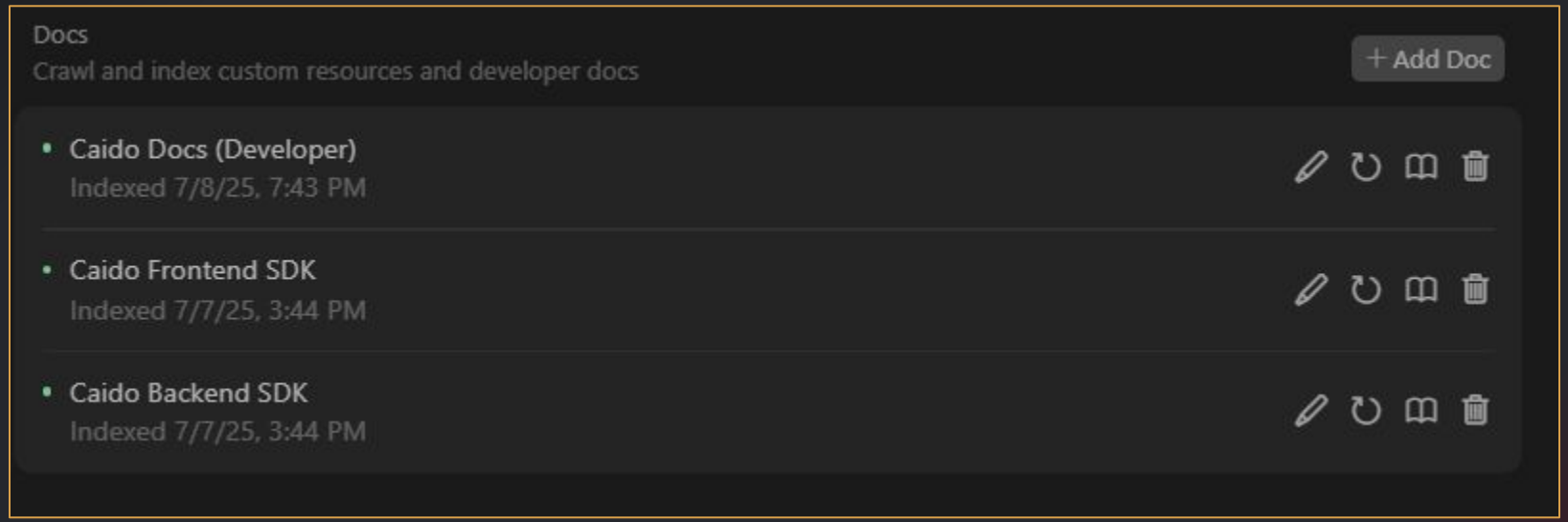


https://ctbb.show/caido-workflow-advisor

Caido + Cursor

Adding Custom Docs to Caido





https://developer.caido.io/guides/vibe_coding.html#using-ai-to-assist-in-plugin-development

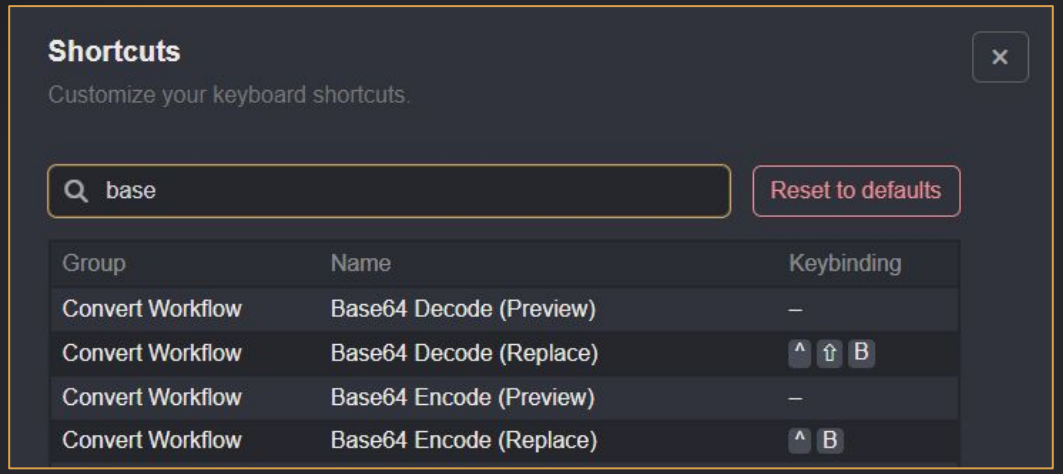
Part 3

Caido Workflows

Convert Workflows + Keyboard Shortcuts

Workflow

Shortcuts for Workflows



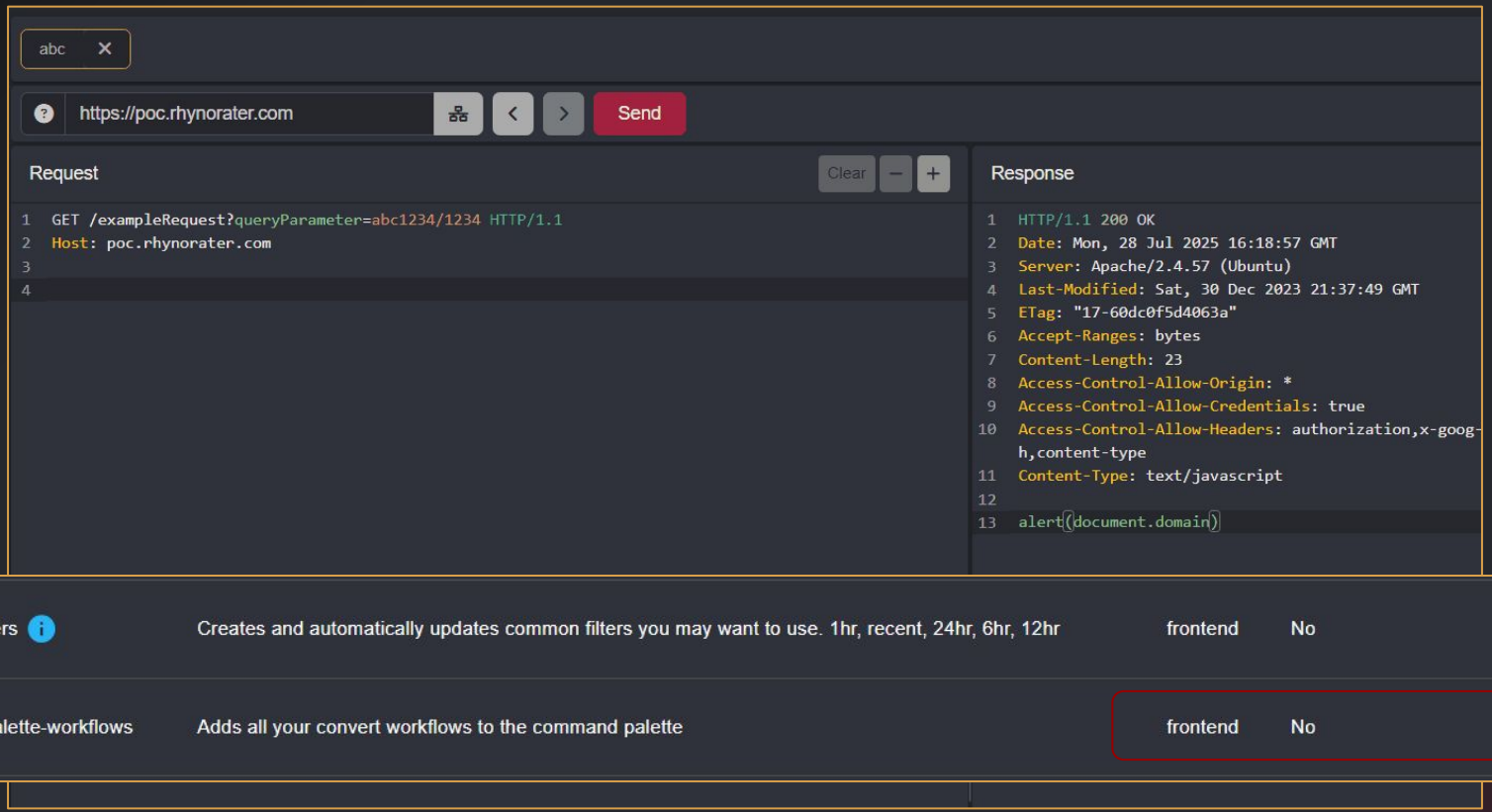
Part 3

Caido Workflows

Convert Workflows + Command Palette (EvenBetter)

EvenBetter Plugin

Command Palette Workflows



HTTPQL + Workflows = Finding

Example case study use-case

“hey, i never saw this endpoint before”

Update preset

Drop to...

Name *

all requests containing the current user and id in body 2

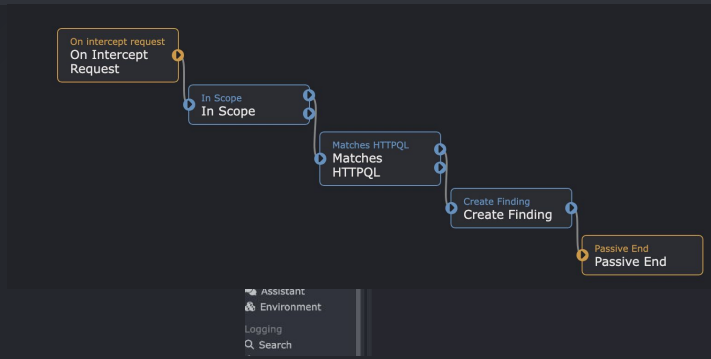
Alias

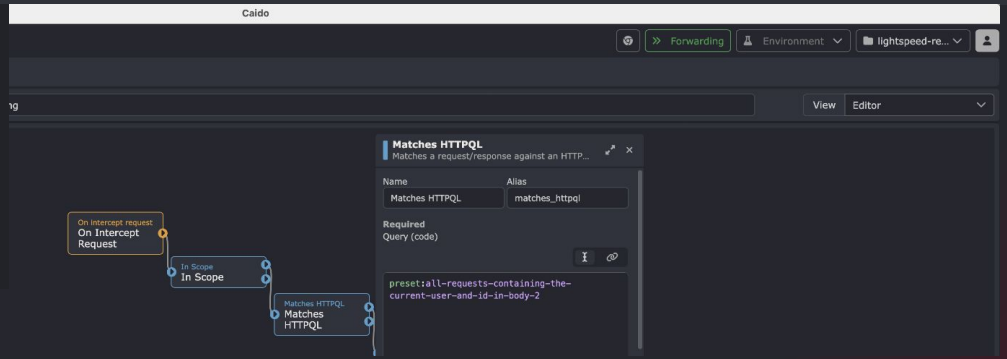
all-requests-containing-the-current-user-and-id-in-body-2

Expression

```
req.raw.cont:"X-PwnFox-Color: red" and req.raw.cont:"124041525" and req.path.ne:"/cp/api/v1/124041525/heartbeat" and req.method.ne:"GET" and req.path.ncont:"124041525"
```

Save Delete Download





Part 4

Caido M&R

New UI, M&R Workflows, and Environments

M&R - Case Study

Google rpcids

```
1  POST /_/BardChatUi/data/batchexecute?rpcids=L5adhe&source-path=%2Fapp&bl=boq_assistant-bard-web-server_20250722.06_p1&f.sid=-858
   7937869850823709&hl=en&_reqid=1835262&rt=c HTTP/1.1
2  Host: gemini.google.com
```

exp pathTraversal Script snippet #10 m=LQaXg,HwBxOc,...ipCoca.O%3A%3B ×

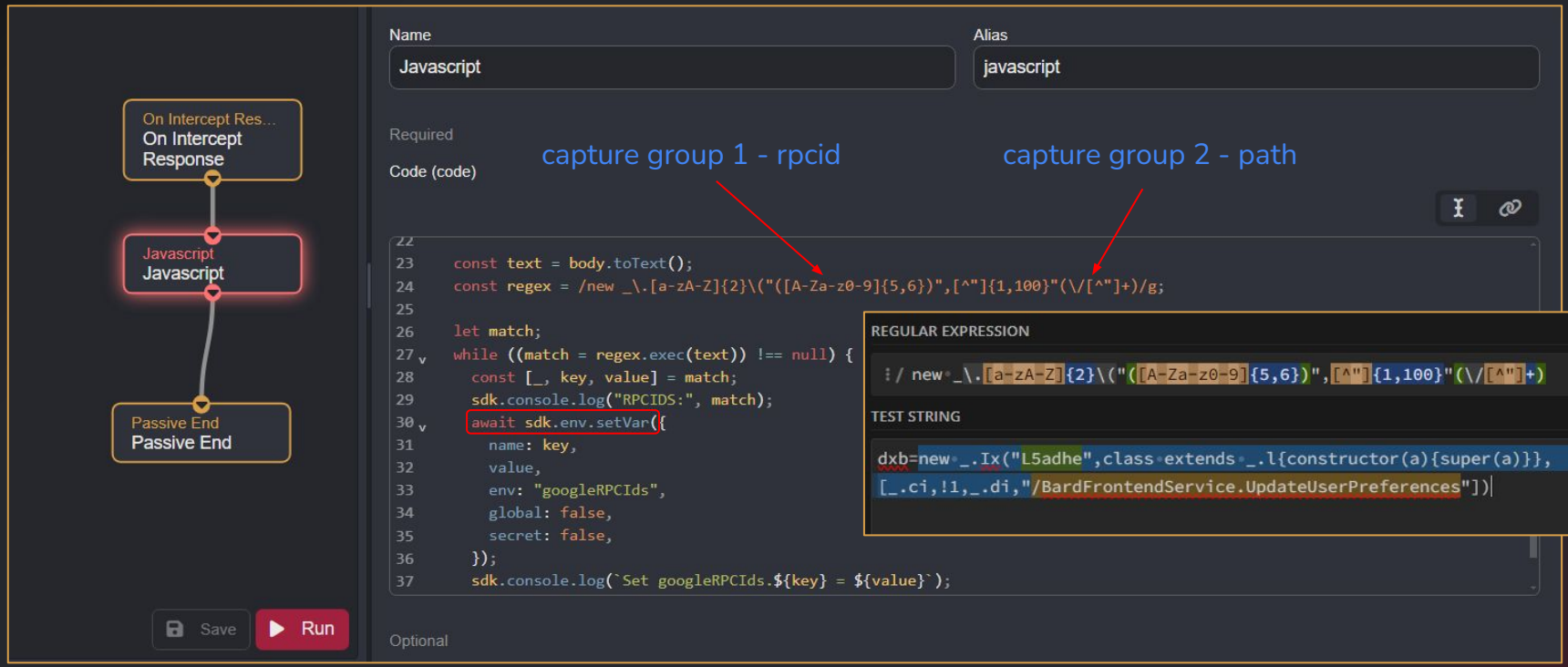
```
1373 ...er(a)}};dxb=new _.Ix("L5adhe",class extends _.l{constructor(a){super(a)}},[_.ci,!1,_.di,"/BardFrontendService.UpdateUserPreferences"]);_.WC
```

```
dxb = new _.Ix("L5adhe",class extends _.l {
    constructor(a) {
        super(a)
    }
}
,[_.ci, !1, _.di, "/BardFrontendService.UpdateUserPreferences"]);
```

Mission: Create something in Caido to help cross-correlate

M&R - Case Study

Google rpcids - Step 1 - Extract with Passive Workflow -> Env



M&R - Case Study

Google rpcids - Step 1 - Extract with Passive Workflow -> Env

REGULAR EXPRESSION

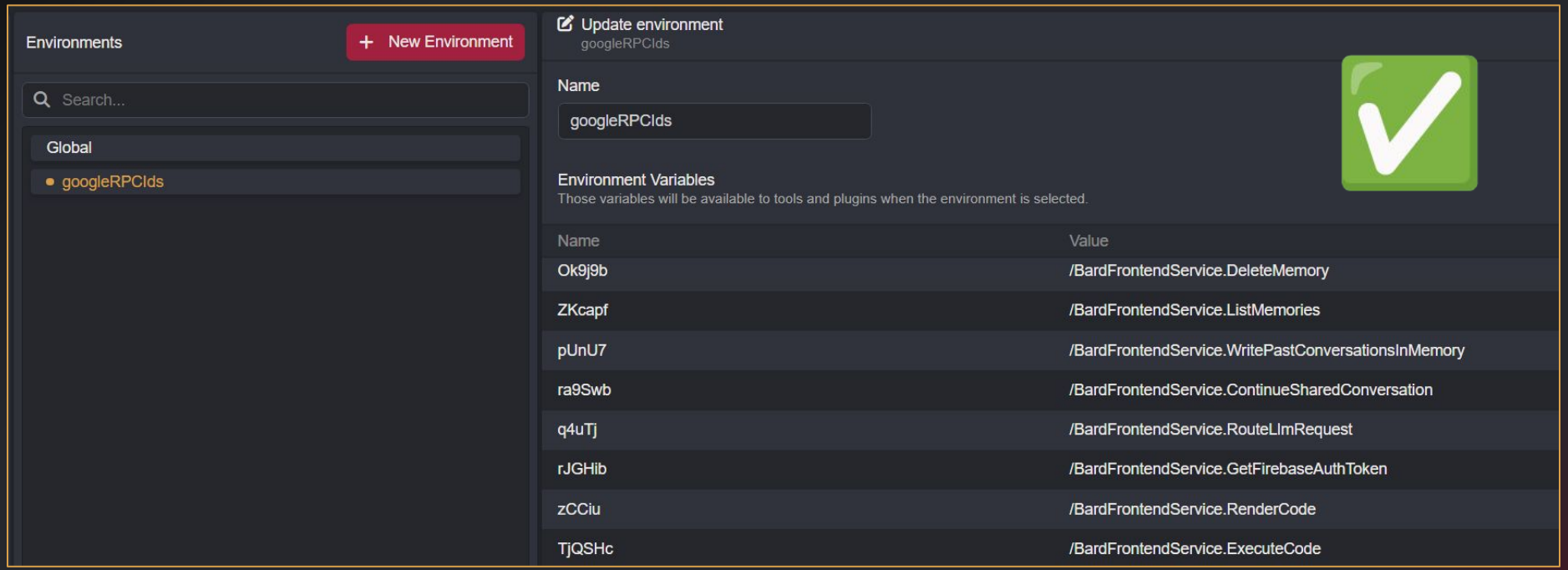
```
/ new _\.[a-zA-Z]{2}\("([A-Za-z0-9]{5,6})",[^"]{1,100}"(\/[^"]+)
```

TEST STRING

```
dxb=new _.Ix("L5adhe",class extends _.l{constructor(a){super(a)}},
[_.ci,!1,_.di,"/BardFrontendService.UpdateUserPreferences"])
```

M&R - Case Study

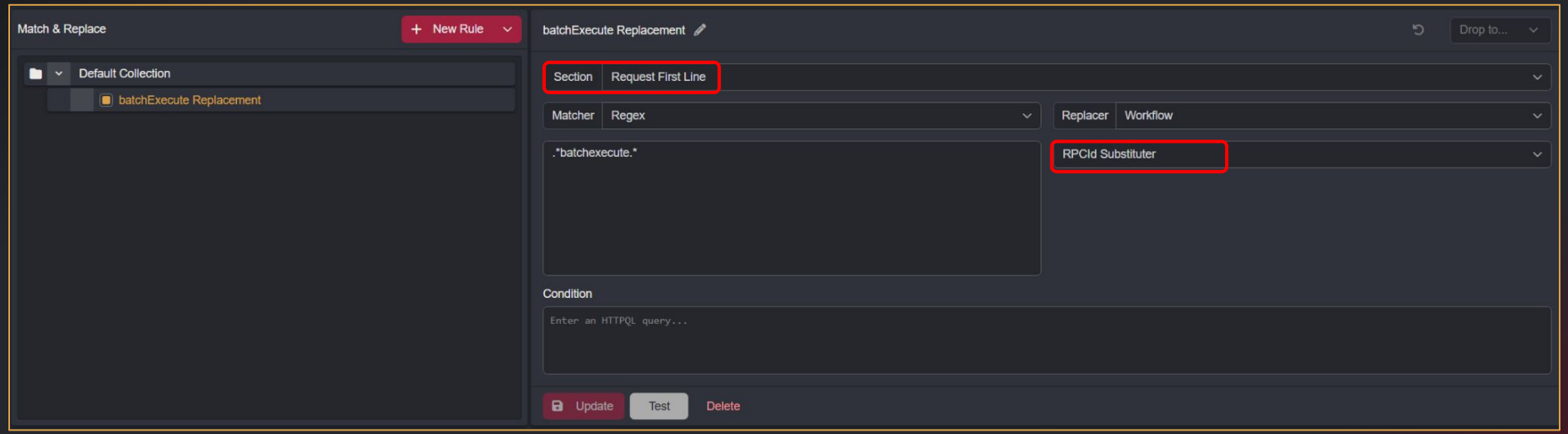
Google rpcids - Step 1 - Extract with Passive Workflow -> Env



M&R - Case Study

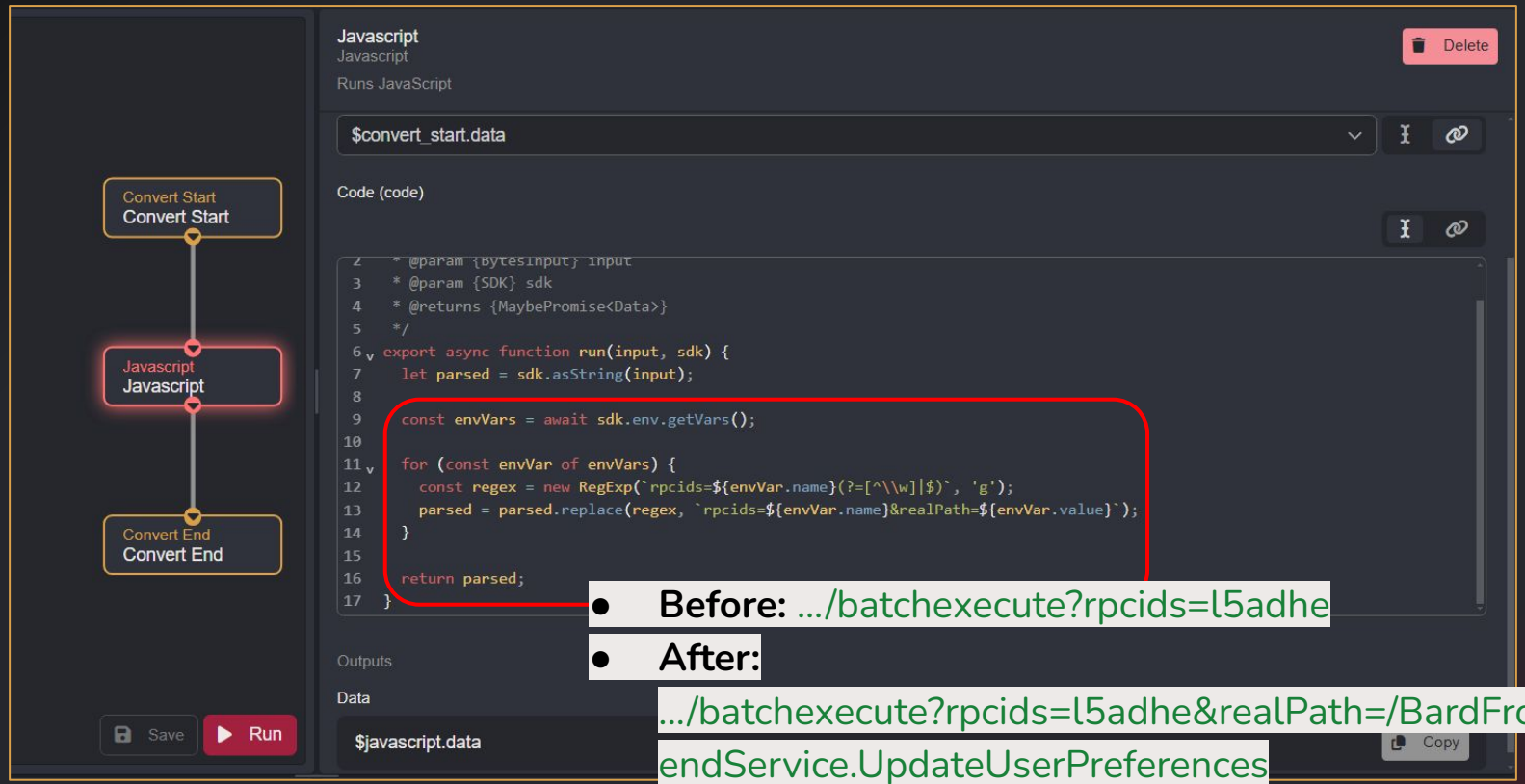
Google rpcids - Step 2 - Correlate & Enhance Data

```
1  POST /_/BardChatUi/data/batchexecute?rpcids=L5adhe&source-path=%2Fapp&bl=boq_assistant-bard-web-server_20250722.06_p1&f.sid=-858
   7937869850823709&hl=en&_reqid=1835262&rt=c HTTP/1.1
2  Host: gemini.google.com
```



M&R - Case Study

Google rpcids - Step 2 - Correlate & Enhance Data



- **Before:** .../batchexecute?rpcids=l5adhe
- **After:** .../batchexecute?rpcids=l5adhe&realPath=/BardFrontendService.UpdateUserPreferences

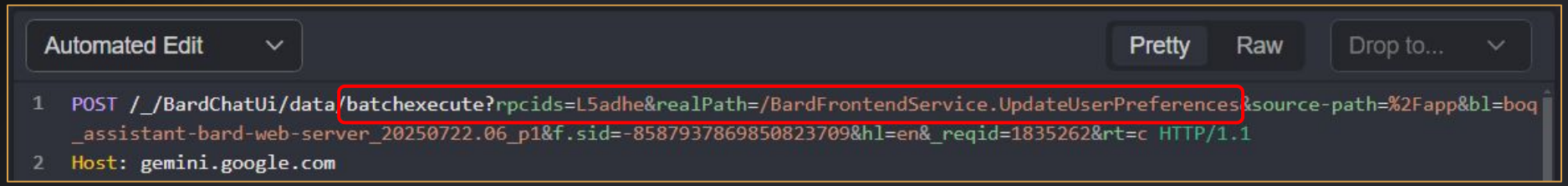
M&R - Case Study

Google rpcids - Step 2 - Correlate & Enhance Data

```
  const envVars = await sdk.env.getVars();

  for (const envVar of envVars) {
    const regex = new RegExp(`rpcids=${envVar.name}(?=[^\\w]|$)`, 'g');
    parsed = parsed.replace(regex, `rpcids=${envVar.name}&realPath=${envVar.value}`);
  }

  return parsed;
}
```

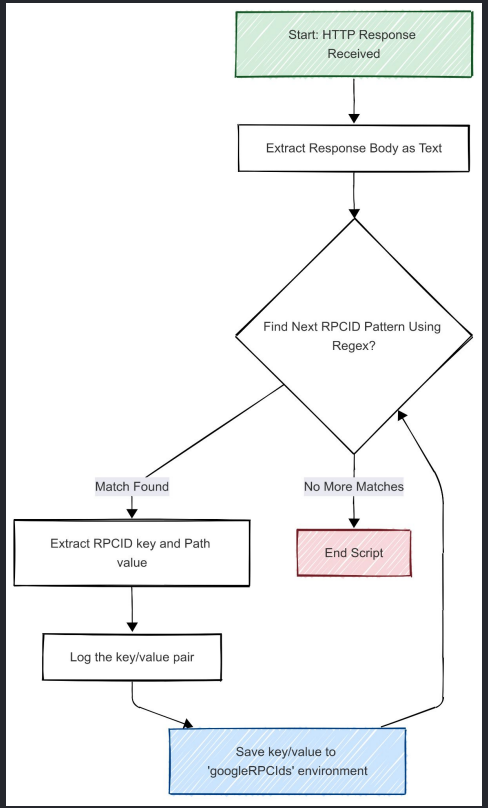
M&R - Case Study

Google rpcids - Step 2 - Correlate & Enhance Data



M&R - Case Study

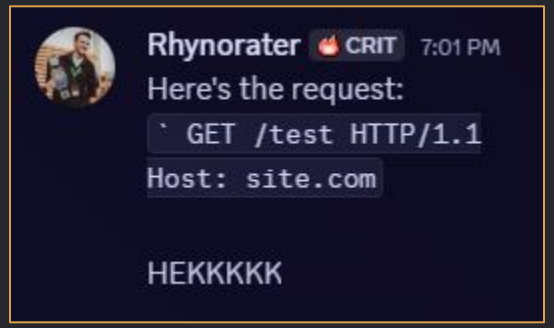
Recap - Stringing it all together



Part 5

Caido Plugins - Drop

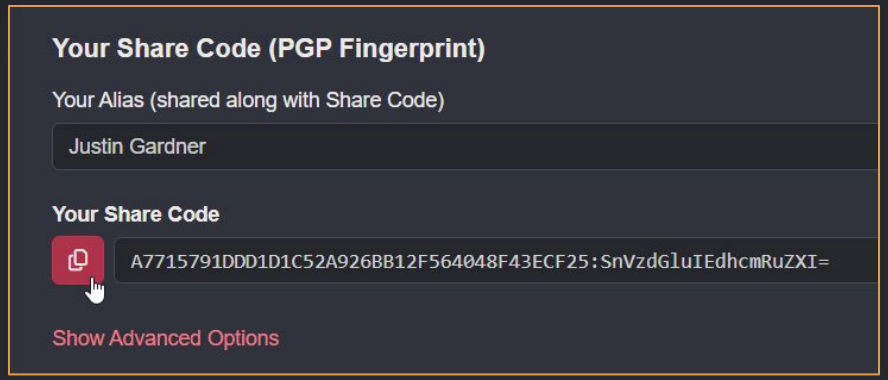
Easy Collaboration within Caido.



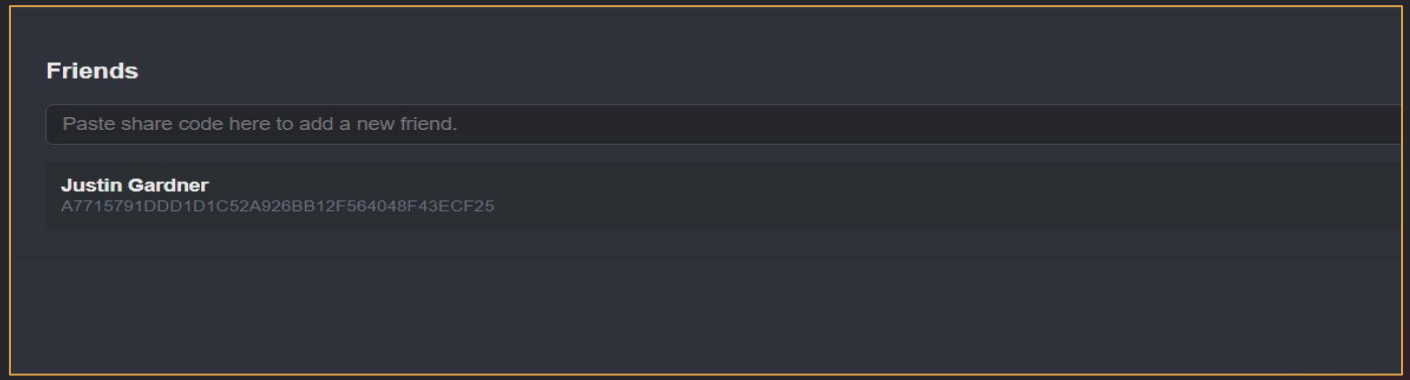
ads wishlist: Any bug bounty platform triage folks using Caido, put something in the platform so we can easily share requests through Drop in the platform - no more messy submission writeups

Drop

Easy Collaboration within Caido (PGP)



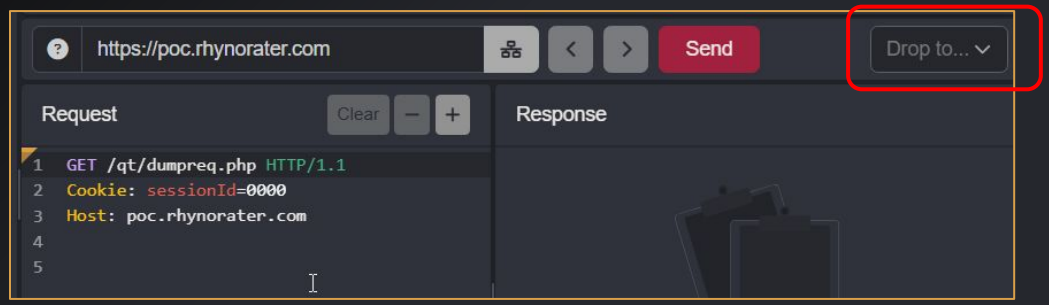
“Hey all, I’ve got this weird request ..”



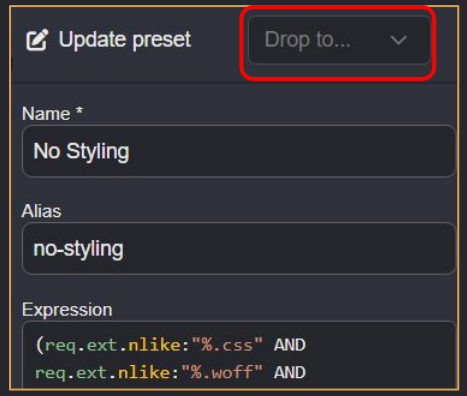
Drop

Easy Collaboration within Caido

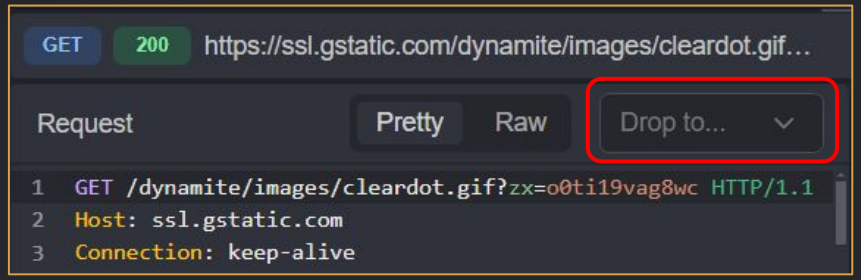
In Replay...



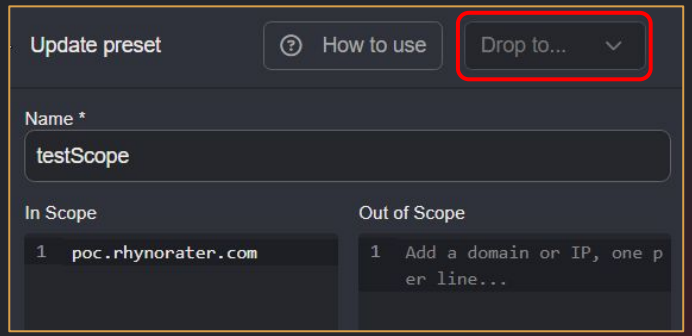
In Filters...

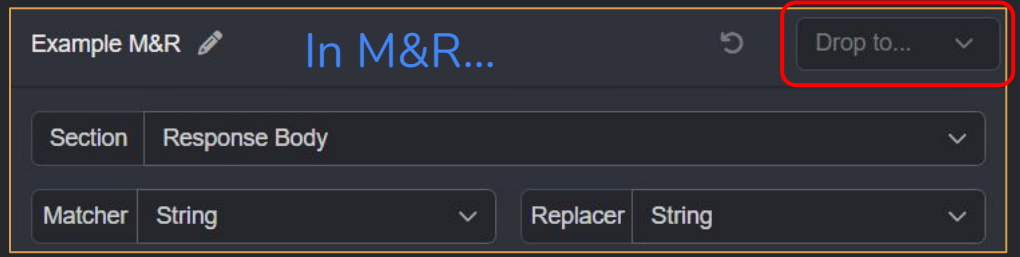


In HTTP History...



In Scopes...





Drop

Easy Collaboration within Caido

Server

To work, `Drop` requires a centralized server. The data that flows through the server is completely end-to-end encrypted using the target user's PGP public key, which is shared via the share code.

The code for the server is public, so you can host your own instance or use any of the public servers below. **We have a super easy to use docker image for hosting your own server**. Please see here for more info.

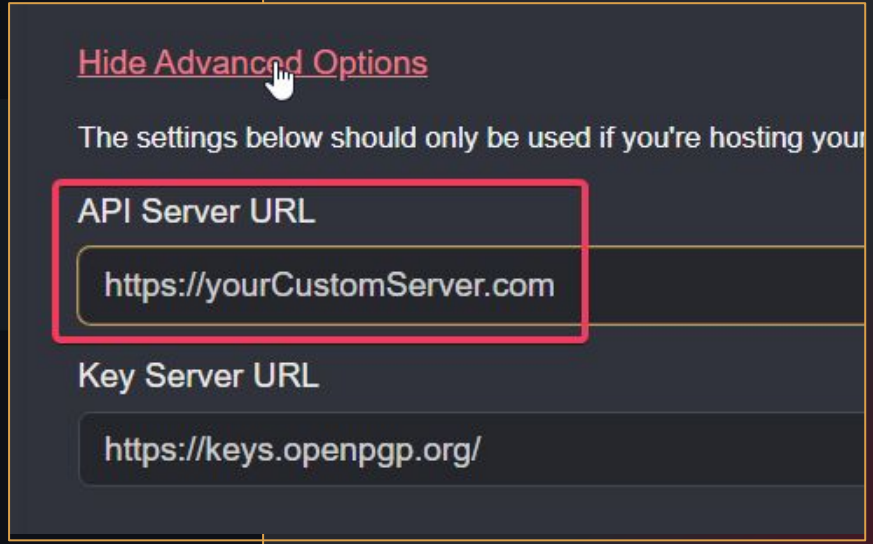
The API Server code can be found here. Our database schema is as follows:

```
CREATE TABLE IF NOT EXISTS messages (
  id INTEGER PRIMARY KEY AUTOINCREMENT,
  from_public_key TEXT NOT NULL,
  to_public_key TEXT NOT NULL,
  encrypted_data TEXT NOT NULL,
  created_at DATETIME DEFAULT CURRENT_TIMESTAMP
);
```

No unencrypted userdata is ever placed into the DB.

Public servers

Domain	Owner
`drop.cai.do`	`Caido Labs Inc.`



Part 5

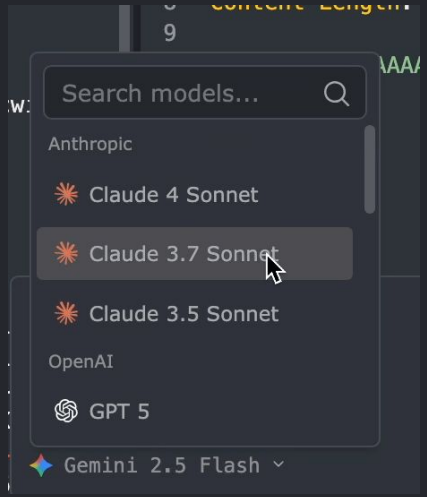
Caido Plugins

Shift

Shift Acquired

Seamless AI Integration into Caido

shift + CAIDO

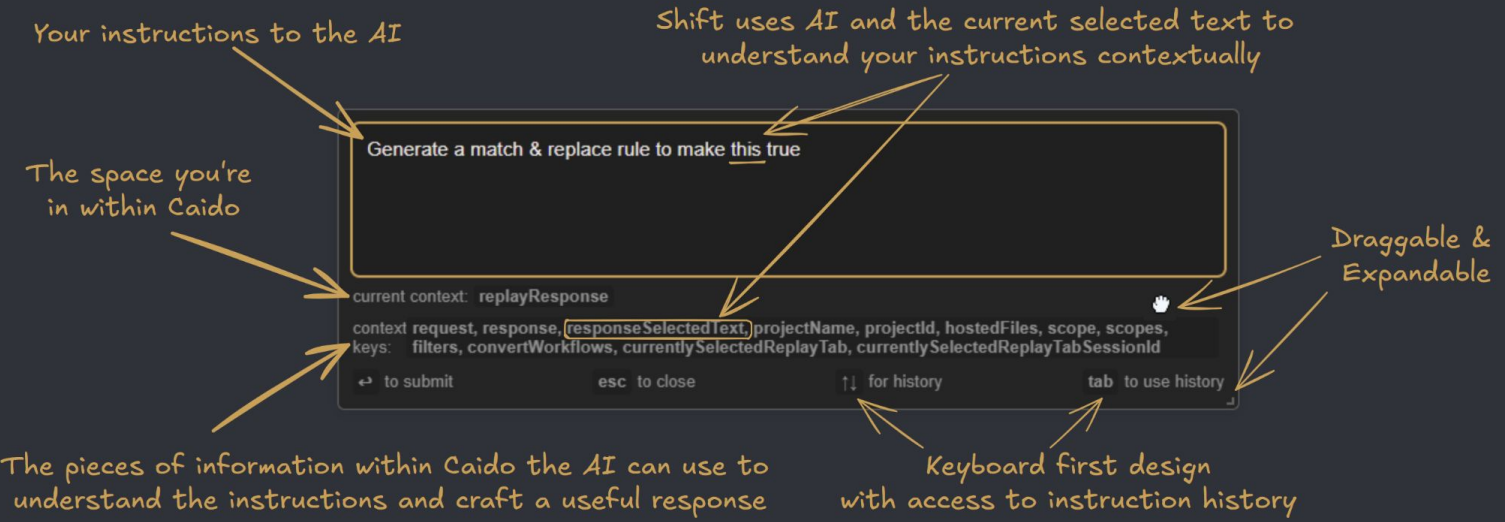


Shift

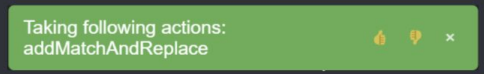
Seamless AI Integration into Caido

1. Press <shift> + <space>

2.



3. Profit?! The AI does the thing.

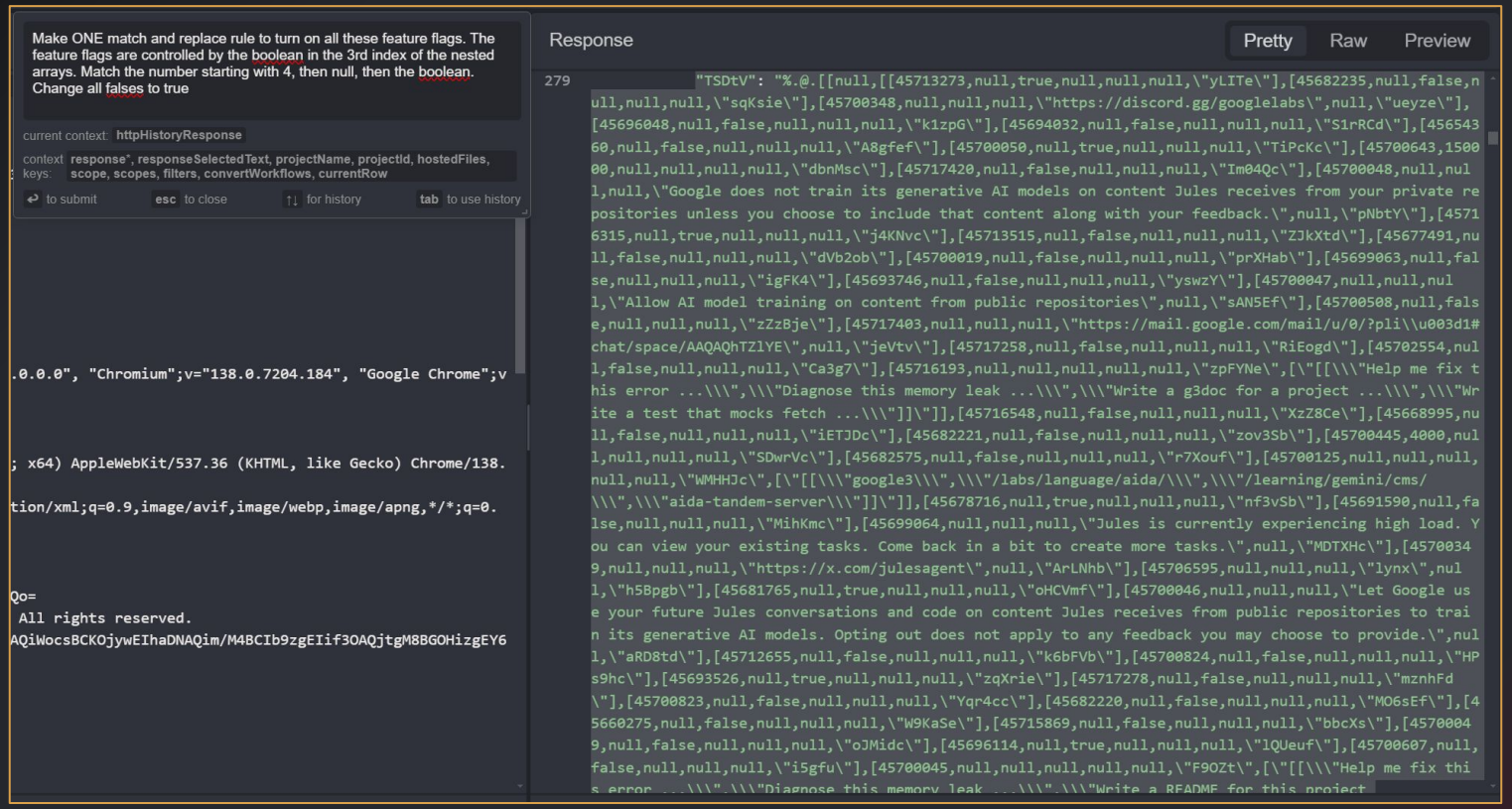


Shift

Seamless AI Integration into Caido

Shift

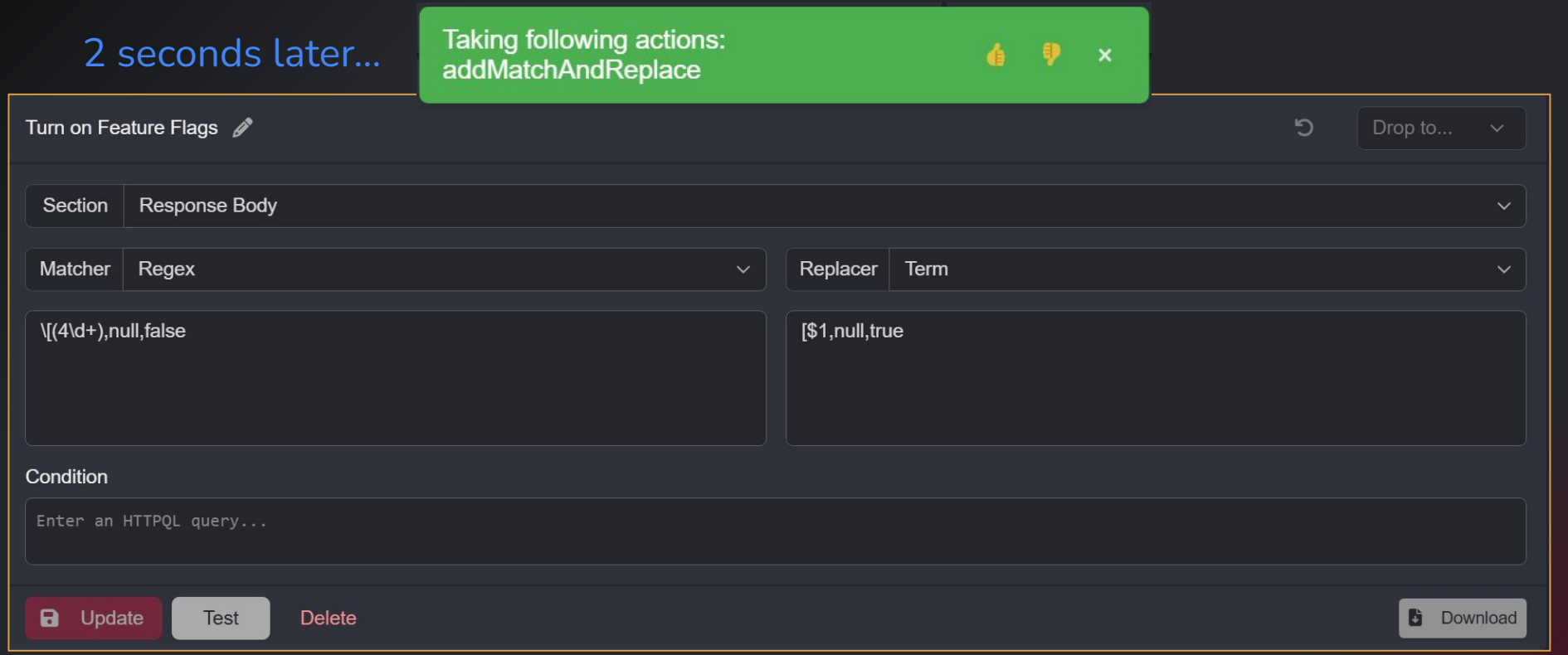
Case Study - Feature Flags on Google Jules



Shift

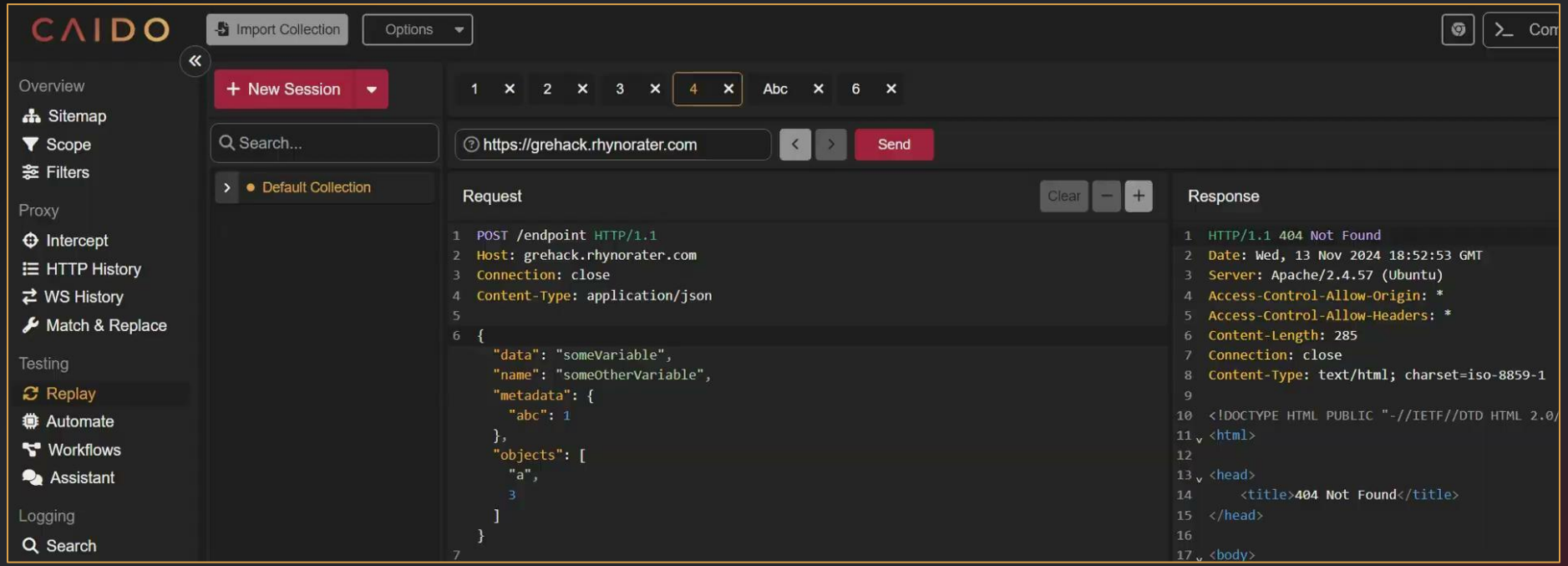
Case Study - Feature Flags on Google Jules

2 seconds later...



Shift Rename

AI-Assisted Replay Tab Naming



Shift Rename

Case Study - Google RPCs & GraphQL Operations

Rename Instructions

Include the HTTP Verb, and a concise version of the path in the tab name. Focus on the end of the path. Include only the first 4 characters of IDs.
Example: GET /api/v1/users/{id}/profile

If the request contains the `realPath` query parameter, use the value of that query parameter for the tab.
Example: GET /batchexecute?rpcIds=fJ3m2N&realPath=/example.Test
Result: /example.Test

If the request is a graphql request, use the `operationName` JSON body parameter to name the tab.
Example "operationName":"abc123"
Result: abc123

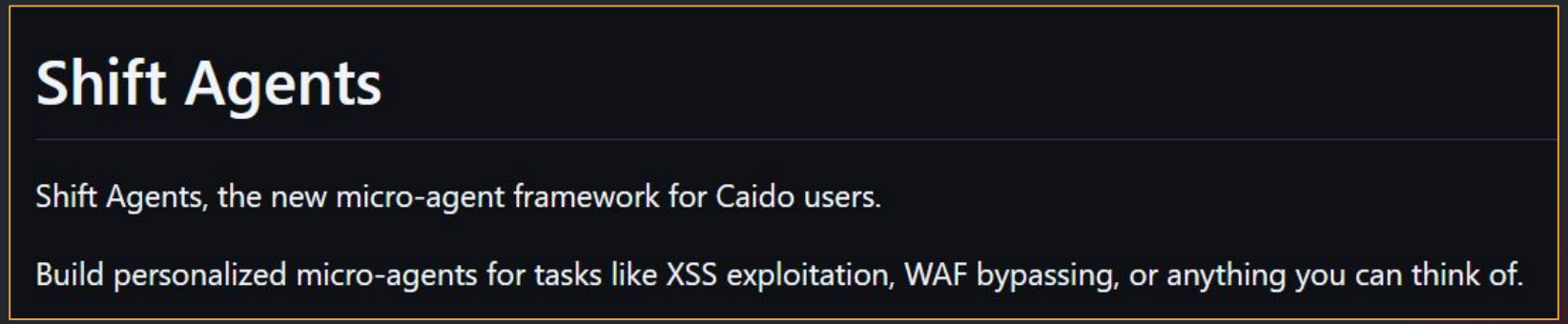
Custom instructions for the AI when renaming tabs

Part 5

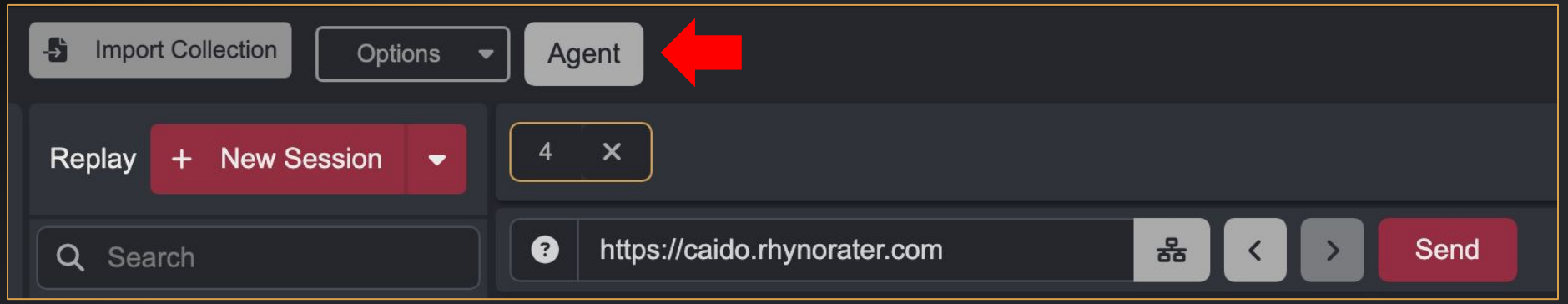
Caido Plugins

Shift Agents

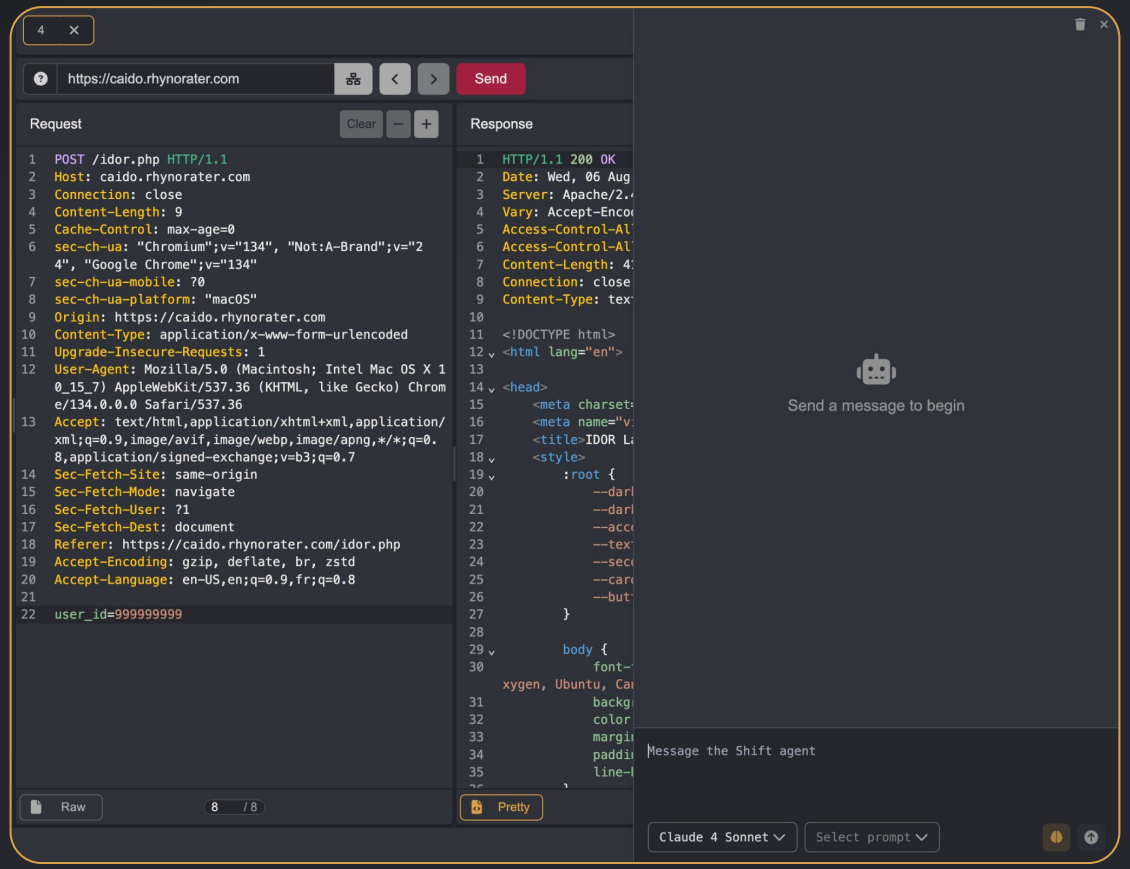
https://github.com/caido-community/shift-agents



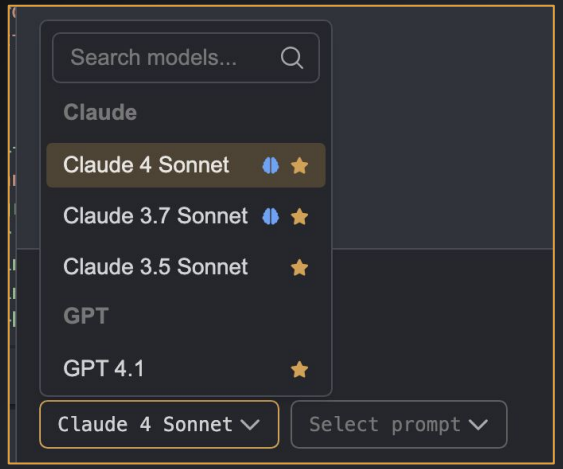
Delegate, delegate, delegate

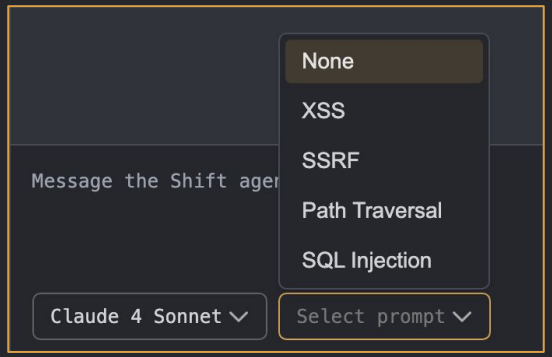


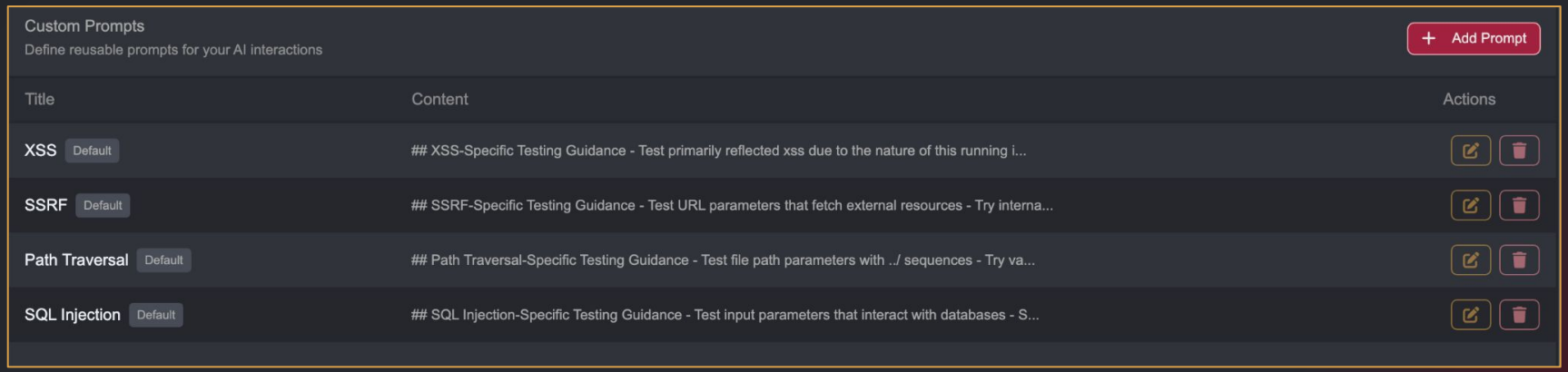
Delegate, delegate, delegate



Build your own methodology







Build your own methodology

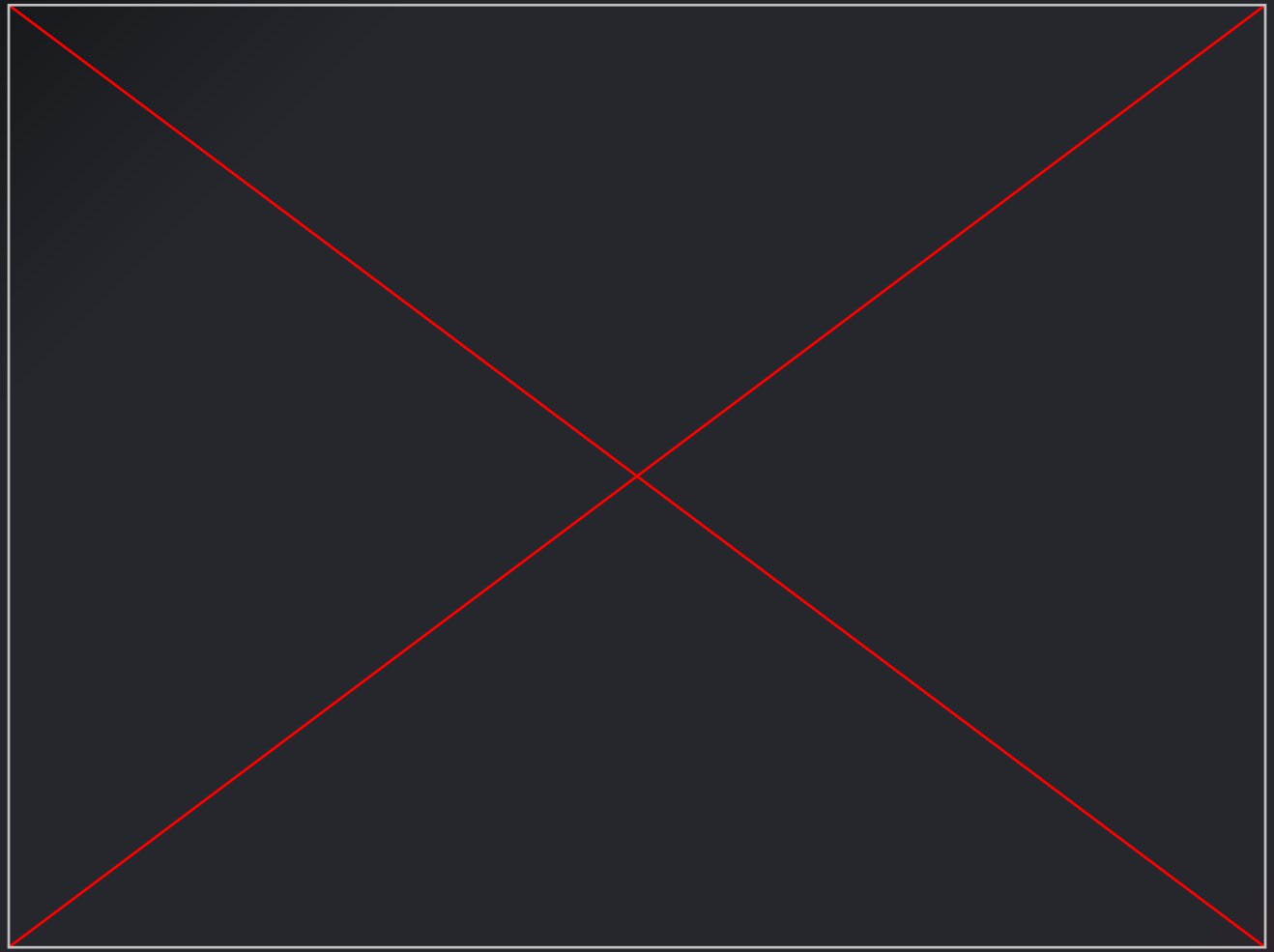
XSS-Specific Testing Guidance
- Test primarily reflected xss due to the nature of this running in replay which doesnt have a headless browser
- Test in different contexts: HTML, JavaScript, attributes, CSS

Below is example monologue of an expert attempting to exploit this vulnerability. This is similar to how your testing should look. REMEMBER, this just an example. Do not follow these exact steps.

Build your own methodology

target: example.com/search?q=
> let me start with a basic payload to see how the application handles special characters
input: <script>alert(1)</script>
output: <script>alert(1)</script>
> they're HTML encoding angle brackets. classic defense. let me try some other vectors

input: "><script>alert(1)</script>
output: "><script>alert(1)</script>
> still encoding, even when trying to break out of an attribute context. let me check if they're filtering the word 'script'



Part 5

Caido Plugins

Honorable Mentions

Squash (Evan Connelly) - Clean up your HTTP requests

403 Bypasser (Bebiks) - Super badass RevProxy/WAF bypass framework

Param Finder (Bebiks) - Bruteforce for parameters in various places

Authmatrix (Caido Dev Team) - Quick and Easy Authz Testing in Caido

Data Grep (...Bebiks) - Easily “grep” your Caido data for extractables

Chatio (Amr)

(w2xim3) QuickSSRF

Compare (Amr)

(Amr) JWT Analyzer

JXScout (Francisco)

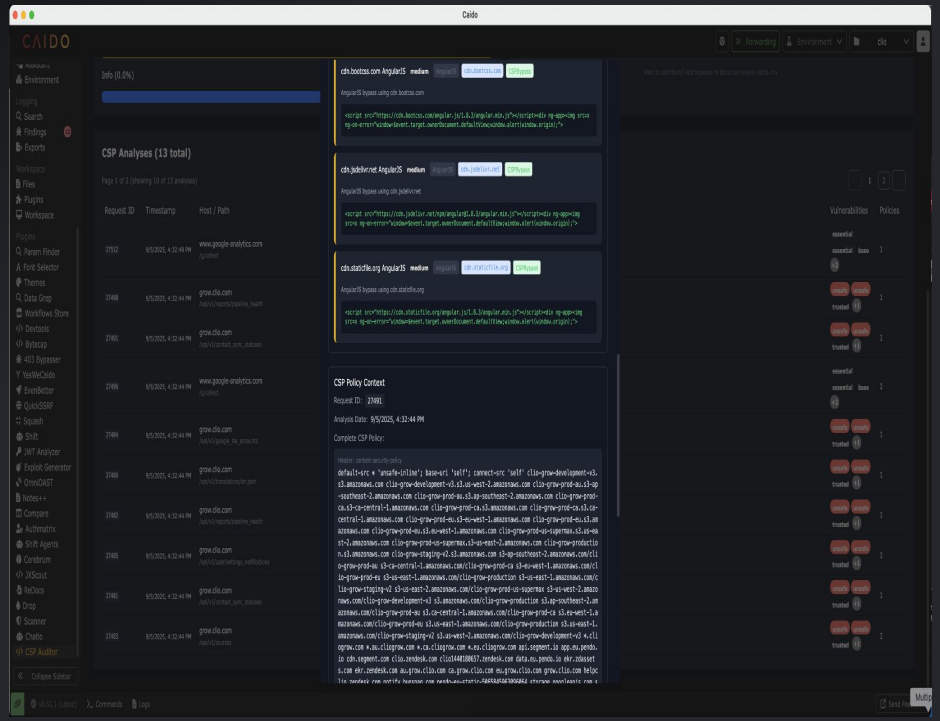
OmniOAST (Hahwul)

ReDocs (Amr)

Caido Plugins

My plugins

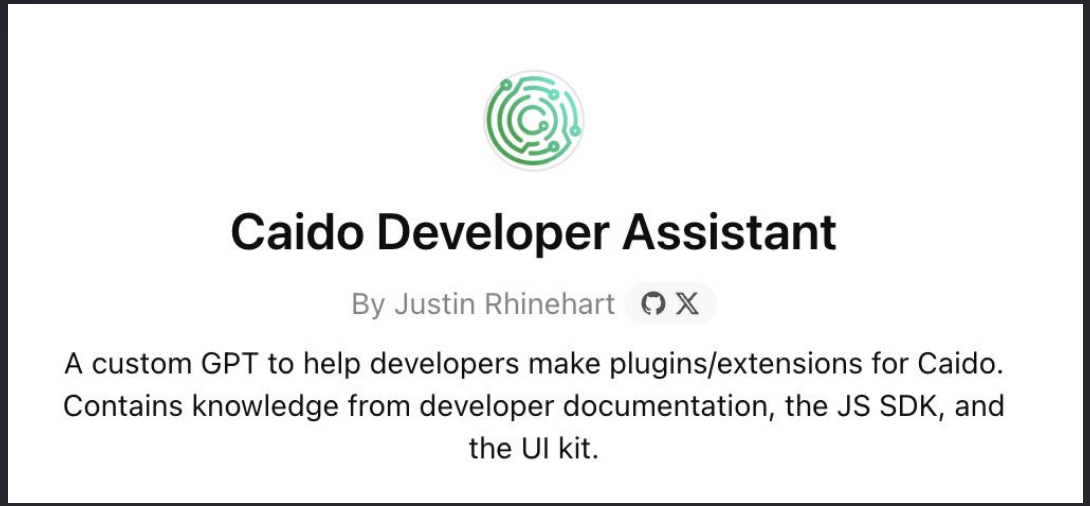
csp-auditor



Bytecap

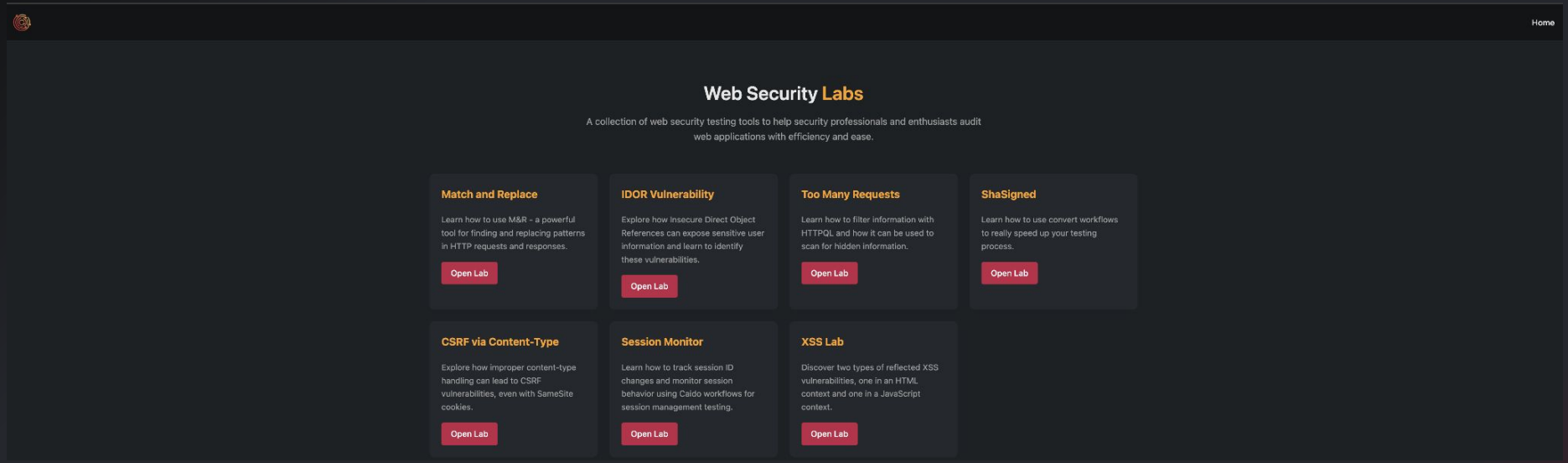
AI Plugin Development

Caido Developer Assistant



https://chatgpt.com/g/g-68095eb17eb08191ba19fd85f0a516ec-caido-developer-assistant

Practical Takeaways



https://caido.rhynorater.com/

Other Resources

- https://links.caido.io/discord
- https://ctbb.show/discord
- https://www.bugcrowd.com/blog/the-ultimate-beginners-guide-to-caido/

Thank You

Questions?

https://linktr.ee/adsdawson

@adamdawson0

https://links.caido.io/discord

Caido **20%** Discount Code: 0xmoose

Slides available in my github repo

Live hackathon

Practical bug bounty with Caido

Lightspeed Retail

Lightspeed Ecommerce E-Series

In Scope Targets

https://bugcrowd.com/engagements/lightspeed-retail

This is the Control Panel - https://my.ecwid.com

This is the Storefront Panel - [yourstore].company.site

API - https://app.ecwid.com/api/v3/

Please note that "yourstore" is a placeholder only in the target scope. When you register an account, you will have your own Instant site domain in your store that you can edit in the form of [yourstore].company.site.