

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

Where do hackers spend time?

- **HTTP History:** Understanding flow of application
 - Orientation - “*Where 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	Extens...
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

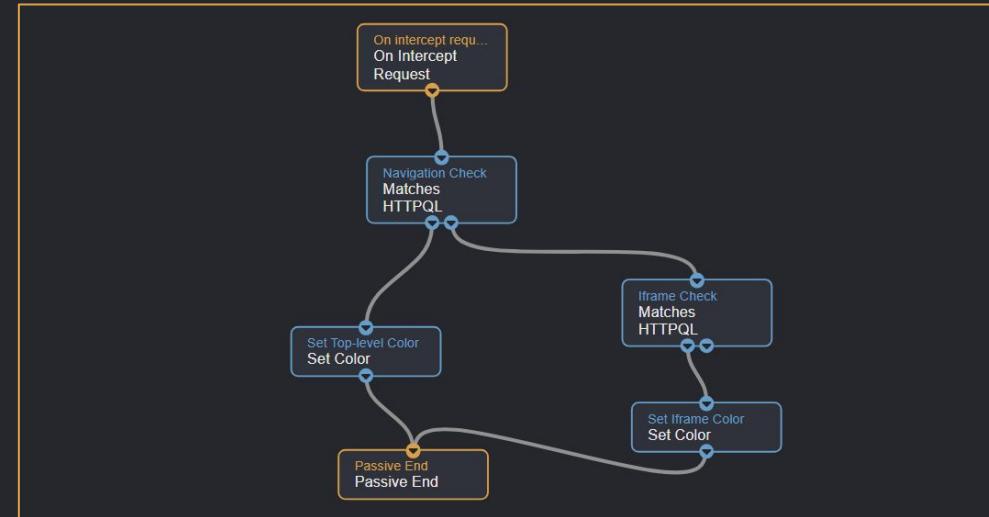


Iframe Navigation

Workflows

Passive 8

Top-Level Navigation



Simple Yet Common Passive Workflow Example

The screenshot shows the CAIDO proxy tool interface with the following details:

- Left Sidebar:** Overview, Sitemap, Scopes, Filters, Proxy (Intercept, HTTP History, WS History), Match & Replace.
- Middle Panel:**
 - Request Sent At:** 2025-09-05 10:24:05
 - Method:** POST 200 https://dashboard.rapyd.net
 - Headers:**

```

Host: dashboard.rapyd.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0) Gecko/20100101 Firefox/104.0
Accept: application/json, text/javascript, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 310
Origin: https://dashboard.rapyd.net
DNT: 1
Connection: keep-alive
Referer: https://dashboard.rapyd.net/settings/communication-center/support/open
    
```
 - Automated Edit:** A dropdown menu is open, showing "Automated Edit" as the selected option. Other options include "Replay", "Automate", "Workflows", "Assistant", and "Environment".
 - Match & Replace:** A sub-menu under "Match & Replace" is also open, showing "Default Collection" and "X-Bug-Bounty: GangGreenTemperTatum".
- Right Panel:**
 - Section:** Request Header
 - Name:** X-Bug-Bounty
 - Value:** String GangGreenTemperTatum
 - Condition:** Enter an HTTPQL query...
 - Buttons:** Update, Test, Delete, Download
 - Before:**

```

1 GET /path/?query=value HTTP/1.1
2 Host: example.com
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0) Gecko/20100101 Firefox/104.0
4 Connection: close
5 Content-Length: 15
6 {"key":"value"}
    
```
 - After:**

```

1 GET /path/?query=value HTTP/1.1
2 Host: example.com
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:104.0) Gecko/20100101 Firefox/104.0
4 Connection: close
5 Content-Length: 15
6 X-Bug-Bounty: GangGreenTemperTatum
7 {"key":"value"}
    
```

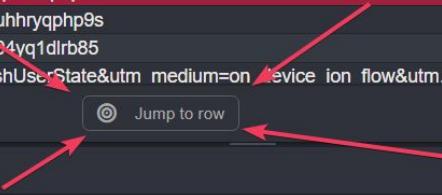
Jump to FREAKING Currently Selected Row

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

5279 my.1password.com:443 PUT /api/v2/perftrace 200
5278 poc.rhynorater.com:443 GET /qt/xss.php 200 .php
5277 poc.rhynorater.com:443 GET /qt/iframe.php 200 .php
5276 ssl.gstatic.com:443 GET /dynamite/ima... 200 .gif
5275 ssl.gstatic.com:443 GET /dynamite/ima... 200 .gif
5274 www.evernote.com:443 GET /DevicePaywa... refreshUser:State&utm medium=on 200

device ion flow&utm...

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



CAIDO

Overview Sitemap Scopes Filters

Proxy Intercept HTTP History WS History Match & Replace

Testing Replay Automate Workflows Assistant Environment

Logging Search Findings

Unset Scope Export Enter an HTTPQL query... Advanced Forwarding Environment Shift Launch

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

GET 200 https://poc.rhynorater.com/qt/test.html

ID	Host	Method	Path
8	cdnjs.cloudflare.com:443	GET	/ajax/libs/codemirror/5.65.2/mode/javascript/javascript.min.js
7	cdnjs.cloudflare.com:443	GET	/ajax/libs/codemirror/5.65.2/mode/xml/xml.min.js
6	cdnjs.cloudflare.com:443	GET	/ajax/libs/codemirror/5.65.2/codemirror.min.js
5	cdnjs.cloudflare.com:443	GET	/ajax/libs/codemirror/5.65.2/theme/monokai.min.css
4	cdnjs.cloudflare.com:443	GET	/ajax/libs/codemirror/5.65.2/codemirror.min.css
3	poc.rhynorater.com:443	GET	/qt/test.html
2	ssl.gstatic.com:443	GET	/ui/v1/icons/mail/images/cleardot.gif
1	ssl.gstatic.com:443	GET	/dynamite/images/cleardot.gif

Request Response

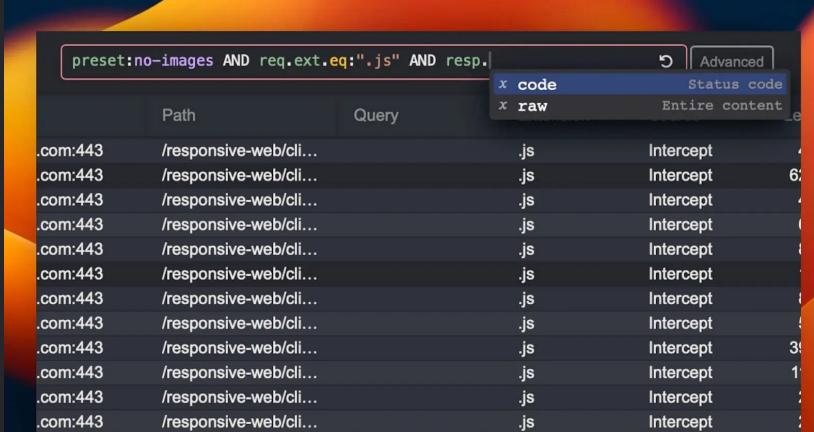
```
1 GET /qt/test.html HTTP/1.1
2 Host: poc.rhynorater.com
3 Connection: keep-alive
4 Pragma: no-cache
5 Cache-Control: no-cache
```

```
1 HTTP/1.1 200 OK
2 Date: Tue, 22 Jul 2025 19:12:32 GMT
3 Server: Apache/2.4.57 (Ubuntu)
4 Last-Modified: Mon, 05 May 2025 18:43:22 GMT
5 ETag: "108a-63467dfe1a72e-gzip"
```

Part 1

Caido Search

HTTPQL = Time for serious text-based filtering.



The screenshot shows the Caido Search interface with a search bar containing the query: `preset:no-images AND req.ext.eq:".js" AND resp..`. Below the search bar is a table with columns: Path, Query, Response Type, Status code, and Intercept count. The table lists multiple requests from .com:443, all ending in ".js" and having a status code of 6 or 3, with all intercepts set to "Intercept".

Path	Query	Response Type	Status code	Intercept
.com:443	/responsive-web/cli...	.js	Intercept	6
.com:443	/responsive-web/cli...	.js	Intercept	6
.com:443	/responsive-web/cli...	.js	Intercept	6
.com:443	/responsive-web/cli...	.js	Intercept	6
.com:443	/responsive-web/cli...	.js	Intercept	6
.com:443	/responsive-web/cli...	.js	Intercept	6
.com:443	/responsive-web/cli...	.js	Intercept	6
.com:443	/responsive-web/cli...	.js	Intercept	3
.com:443	/responsive-web/cli...	.js	Intercept	1
.com:443	/responsive-web/cli...	.js	Intercept	1
.com:443	/responsive-web/cli...	.js	Intercept	1
.com:443	/responsive-web/cli...	.js	Intercept	1

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



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

+ New Preset

Search...

- No Styling
- abc
- fromToday

Update preset

Name *

fromToday

Alias

fromtoday

Expression

`req.created_at.gt:"2025-07-22 15:07:00"`

Save Delete

Filters/Presets

The screenshot shows a browser developer tools Network tab with a list of requests. A red arrow points to a search input field containing "fromToday". Another red arrow points to a "Save as preset" dialog box where "fromToday" is selected as the name. A third red arrow points to a "Custom Presets" dropdown menu where "fromToday" is listed.

Part 1

Caido Search

common-filters (EvenBetter)

common-filters - EvenBetter Plugin

The screenshot shows the CAIDO application interface with the EvenBetter plugin installed. The sidebar on the left includes links for Overview, Sitemap, Scopes, Filters, Proxy, Intercept, HTTP History, WS History, Match & Replace, Testing, Replay, Automate, Workflows, Assistant, Environment, Logging, Search, Findings, Exports, Workspace, Files, Plugins, and Param Finder. The EvenBetter plugin is highlighted in the Plugins section.

The main area displays the EvenBetter plugin settings and a preset editor. The settings page shows a list of features with their descriptions and status (Kind, Requires Refresh?, Enabled). The features listed are:

Name	Description	Kind	Requires Refresh?	Enabled
share-scope	Share scope context menu button	frontend	No	<input checked="" type="checkbox"/>
quick-decode	Decode & encode selection on the Replay page	frontend	No	<input checked="" type="checkbox"/>
clear-all-findings	Adds a button to clear all findings	frontend	No	<input checked="" type="checkbox"/>
share-replay-collections	Export & import replay collections	frontend	No	<input checked="" type="checkbox"/>
share-mar	Import & export Match and Replace rules	frontend	No	<input checked="" type="checkbox"/>
exclude-host-path	Exclude Host/Path context menu buttons on the HTTP History page	frontend	Yes	<input checked="" type="checkbox"/>
quick-mar	Quick Match and Replace context menu button	frontend	Yes	<input checked="" type="checkbox"/>
colorize-by-method	Colorize session tabs by their HTTP methods in the Replay page	frontend	Yes	<input checked="" type="checkbox"/>
share-filters	Export & import filter presets	frontend	No	<input checked="" type="checkbox"/>
common-filters	Creates and automatically updates common filters you may want to use. 1hr, recent, 24hr, 6hr, 12hr	frontend	No	<input checked="" type="checkbox"/>
command-palette-workflows	Adds all your convert workflows to the command palette	frontend	Yes	<input checked="" type="checkbox"/>

The preset editor shows a search bar and a list of available filters: No Images, No Styling, recent, 1hr, 6hr, 12hr, and 24hr. A modal window is open to edit a preset named "recent". The modal fields are:

- Name: recent
- Alias: recent
- Expression: `req.created_at.gt:"2025-08-05 17:25:03"`

Buttons at the bottom of the modal include Save, Delete, and Download.

[https://github.com/bebiksi
or/EvenBetter](https://github.com/bebiksi/or/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.

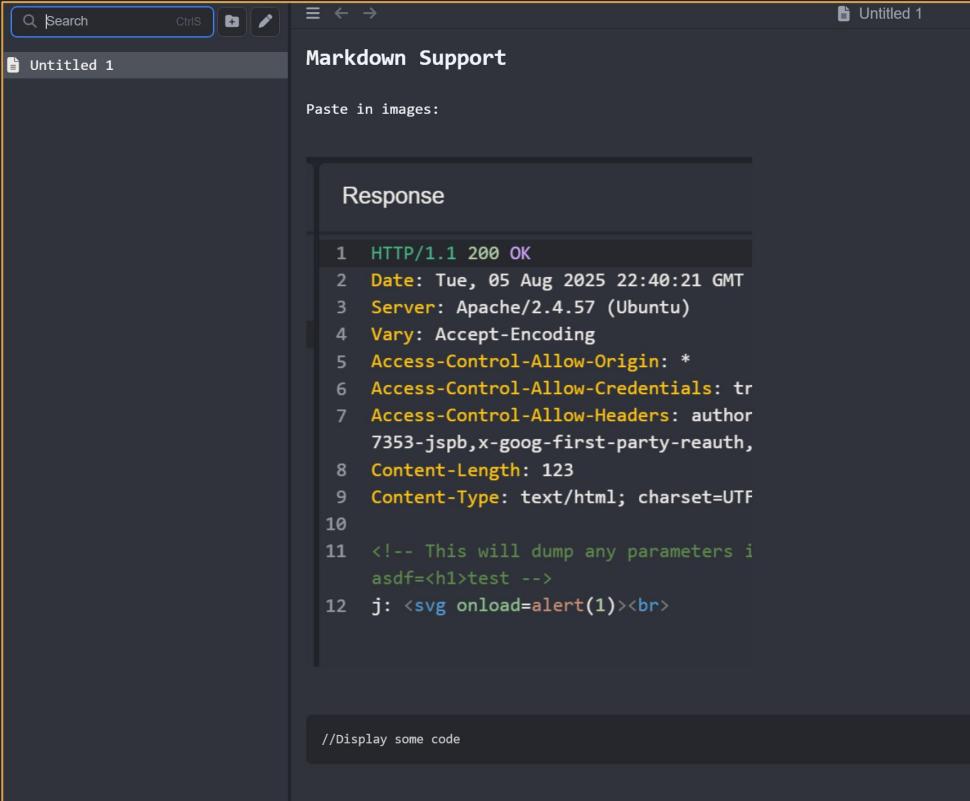
Part 2

Caido Replay

Notes++ Plugin - Organization

Organization

#1 - Directly in Notes++



The screenshot shows the Notes++ application interface. At the top, there's a toolbar with a search bar, a 'CtrlS' button, and other icons. Below the toolbar, a tab bar shows 'Untitled 1'. The main area has a dark background with light-colored text. A modal window titled 'Response' is open, displaying the following text:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 05 Aug 2025 22:40:21 GMT
3 Server: Apache/2.4.57 (Ubuntu)
4 Vary: Accept-Encoding
5 Access-Control-Allow-Origin: *
6 Access-Control-Allow-Credentials: true
7 Access-Control-Allow-Headers: author
7353-jspb,x-goog-first-party-reauth,
8 Content-Length: 123
9 Content-Type: text/html; charset=UTF
10
11 <!-- This will dump any parameters if
12 asdf=<h1>test -->
12 j: <svg onload=alert(1)><br>
```

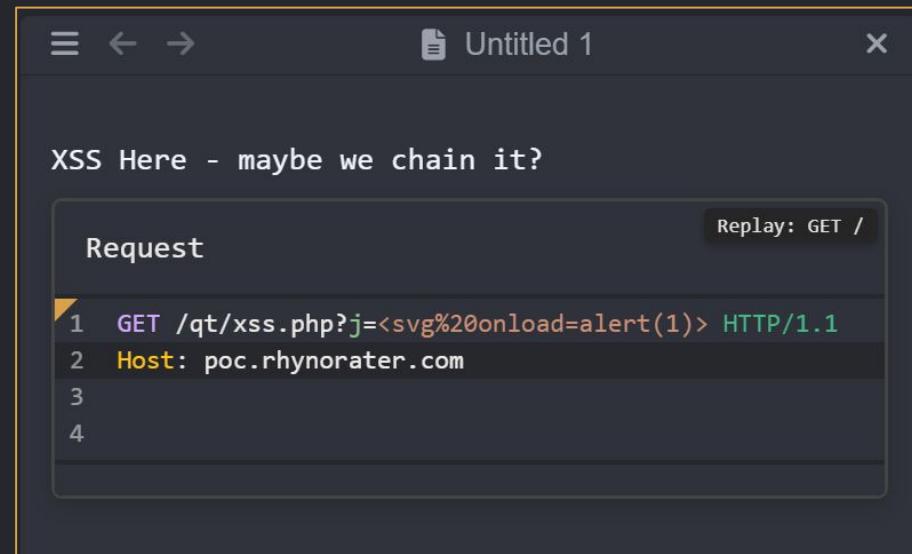
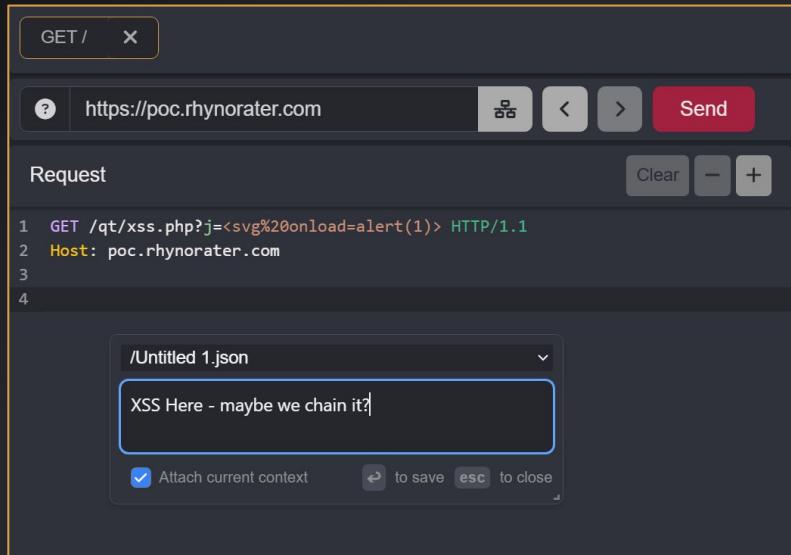
At the bottom of the main window, there's a footer bar with the text 'Display some code'.

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

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

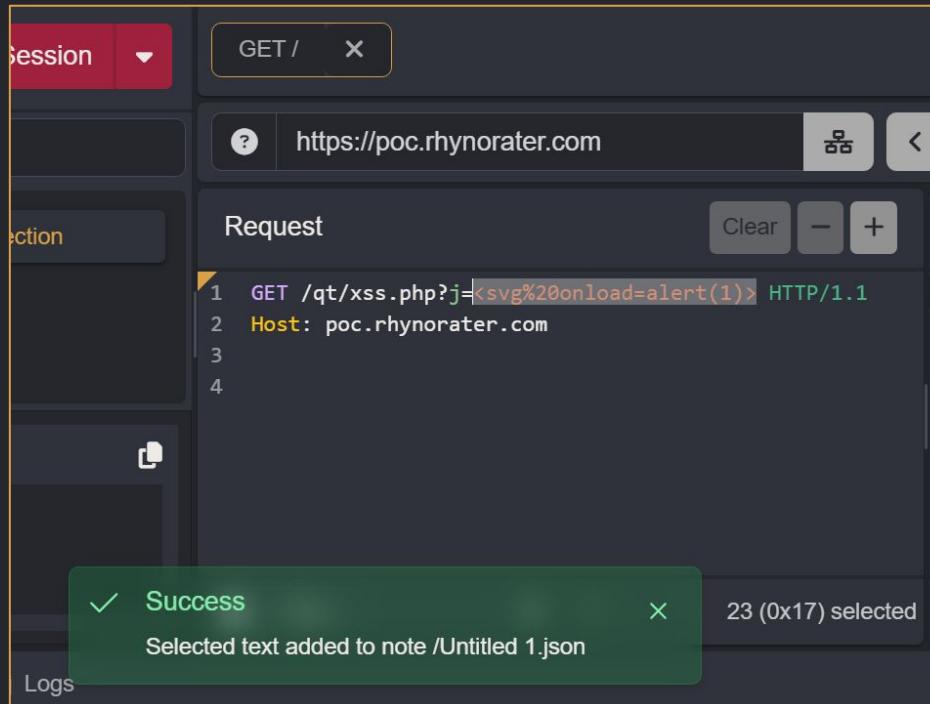
Organization

#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

The screenshot shows a user interface for a proxy tool. At the top left is a search bar with the placeholder "example". To its right is a URL input field containing "https://poc.rhynorater.com", followed by standard browser navigation buttons (refresh, back, forward) and a red "Send" button. Below the search bar is a dropdown menu showing "Default Collection" and a collection named "abc" which is currently selected. The main area displays a "Request" log with the following entries:

```
1 GET /qt/example HTTP/1.1
2 Authorization: Bearer 00000000-0000-0000-0000-000000000000
3 Host: poc.rhynorater.com
4
5
```

The screenshot shows the CAIDO application interface. On the left is a sidebar with various menu items: Overview, Sitemap, Scopes, Filters, Proxy (Intercept, Local History, WS Spy, Match & Replace), Testing (Reply, Automate, Workflows, Assistant, Environment), Logging (Search, Findings, Exports), Workspace (Files, Plugins, Workspaces), Plugins (403 Bypasser, EvenBetter, LoadPath, Port Selector, Themes). The "Reply" tab is selected. In the center, there's a search bar with "Search" placeholder and an "Enter a connection URL" input field with a "Send" button. A dropdown menu under "Reply" shows options: "public cloud" and "private cloud", with "public cloud" currently selected. The right side of the screen is divided into two panels: "Request" and "Response". Both panels show a placeholder image of two devices and the text "No reply session selected" and "No response to display". At the bottom center is a red "+ Create a session" button.

Replay Organization

Collection/Tab Management Features

The screenshot displays the Replay application interface with two main panels. The left panel shows a sidebar with a search bar and a list of collections: Default Collection, Vulns, Gadgets, api.siteexample.com, and Very Very Freaking Close. A red button at the top right says '+ New Session'. The right panel shows a session list for the 'Vulns' collection, which includes a POST request with 13 items. A context menu is open over the session list, showing options: '+ Add session', 'Open all sessions' (with a cursor), 'Rename', and a submenu under 'More' with 'Move', 'Close', 'Close Others', 'Close to the Left', 'Close to the Right' (with a cursor), and 'Close All'.

Replay

+ New Session

Search

> Default Collection

> Vulns

> Gadgets

> api.siteexample.com

> Very Very Freaking Close

Vulns

POST /?

13

Gadgets

+ Add session

Open all sessions

Rename

abc x bob x PC

Rename

Move

Close

Close Others

Close to the Left

Close to the Right

Close All

Part 2

Caido Replay

Replay Placeholders

Replay

Replay Placeholders

The screenshot shows the Requre tool interface. At the top, there's a URL input field with `https://poc.rhynorater.com`, a file selection button, and navigation arrows. To the right are a "Send" button and a "Add placeholder" button. Below the URL is a "Request" section containing a numbered list of log entries:

- 1 GET /qt/dumpreq.php HTTP/1.1
- 2 Authorization: Bearer 00000000-0000-0000-0000-000000000000
- 3 Host: poc.rhynorater.com
- 4
- 5

On the right side, under the "Response" heading, is another numbered list:

- 1 HTTP/1.1 200 OK
- 2 Date: Tue, 22 Ju
- 3 Server: Apache/2
- 4 Vary: Accept-Enc
- 5 Access-Control-A

A mouse cursor is hovering over the "Add placeholder" button.

A modal dialog titled "Placeholder Settings" is open. It contains a "From" field with "52" and a "To" field with "88". Below these fields is a "Input text" area containing the same log entries as the request section above. To the right, the "Type" dropdown is set to "Workflow", and the "Workflow" dropdown is set to "Random UUID Generator". A red arrow points from the "Input text" area to the "Workflow" dropdown. Another red arrow points from the "Workflow" dropdown to the "Actions" table below. The table has three columns: Type, Description, and Actions. It contains one entry: "Workflow" and "Random UUID Generator".

Placeholder Settings

Set the input text that will be transformed and inserted into the placeholder.

From: 52 To: 88

Input text

```
1 GET /qt/dumpreq.php HTTP/1.1
2 Authorization: Bearer 00000000-0000-0000-0000-000000000000
3 Host: poc.rhynorater.com
4
5
```

Type: Workflow

Workflow: Random UUID Generator

Procedure

Type	Description	Actions
Workflow	Random UUID Generator	

Replay

Replay Placeholders

The screenshot shows a network traffic capture interface with two panels: Request and Response.

Request:

```
1 GET /qt/dumpreq.php HTTP/1.1
2 Authorization: Bearer 00000000-0000-0000-0000-000000000000
3 Host: poc.rhynorater.com
4
5
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 22 Jul 2025 21:13:08 GMT
3 Server: Apache/2.4.57 (Ubuntu)
4 Vary: Accept-Encoding
5 Access-Control-Allow-Origin: *
6 Access-Control-Allow-Credentials: true
7 Access-Control-Allow-Headers: authorization,x-goog-authuser,x-goog-ext-3532
8 h,content-type
9 Content-Length: 126
10 Content-Type: text/html; charset=UTF-8
11 v <pre>GET /qt/dumpreq.php HTTP/1.1
12 Authorization: Bearer c1b5d176-ce7f-4eeb-934d-fbd46af2237a
13 Host: poc.rhynorater.com
14
15 </pre>
```

A red arrow points from the placeholder in the Request's Authorization header to the corresponding placeholder in the Response's Authorization header.

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

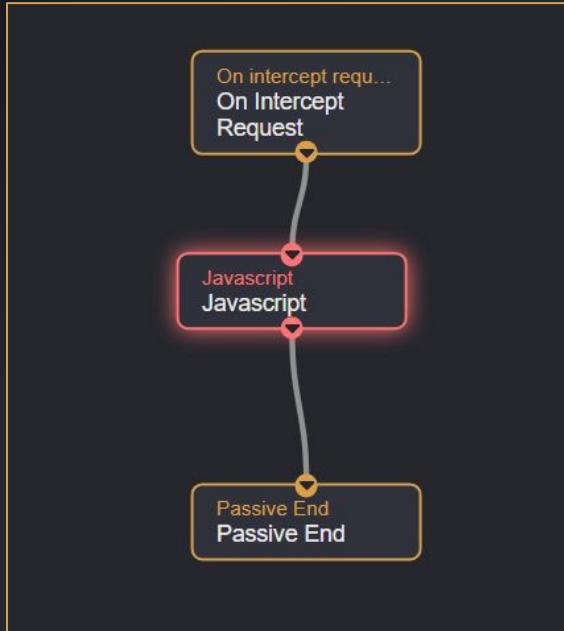
The screenshot shows the 'Environments' section of a software interface. At the top, there's a navigation bar with 'Environments', 'Forwarding' (green button), and a dropdown menu for 'Environment' currently set to 'No Environment'. Below this is a search bar and a 'New Environment' button. On the left, a sidebar lists environments: 'Global' (selected) and 'googleRPCIds', both highlighted with a red box. The main area shows an 'Update environment' card for 'Global' with a 'Name' field containing 'Global'. Under 'Environment Variables', it says 'Those variables will be available to tools and plugins when the environment is selected.' A 'Delete All' button and an 'Add' button are available. A table lists variables: 'sessionID' and 'PHPSESSID', both marked as 'Secret'. Each variable has an 'Update' button and a delete icon. Red arrows point from the 'Key-Value Stores' text at the bottom to the 'sessionID' and 'PHPSESSID' rows.

Name	Value	Kind
sessionID	Secret
PHPSESSID	Secret

Key-Value Stores

Replay

Replay Placeholders - Auto Session Refresher



```

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";
}
  
```

Environment Variables		
Those variables will be available to tools and plugins when the environment is selected.		
Name	Value	Kind
sessionId	autoUpdated	Secret

Replay

Replay Placeholders

Request
Clear
-
+

```

1 GET /qt/dumpreq.php HTTP/1.1
2 Cookie: sessionId=0000
3 Host: poc.rhynorater.com
4
5

```


Response
Clear
-
+

```

1 HTTP/1.1 200 OK
2 Date: Tue, 22 Jul 2025 22:20:51 GMT
3 Server: Apache/2.4.57 (Ubuntu)
4 Vary: Accept-Encoding
5 Access-Control-Allow-Origin: *
6 Access-Control-Allow-Credentials: true
7 Access-Control-Allow-Headers: authorization,x-goog-authuser,content-type
8 Content-Length: 97
9 Content-Type: text/html; charset=UTF-8
10
11 <pre>GET /qt/dumpreq.php HTTP/1.1
12 Cookie: sessionId=autoUpdated
13 Host: poc.rhynorater.com
14
15 </pre>

```

Placeholder Settings

Set the input text that will be transformed and inserted into the placeholder.

From	To	Type
48	52	Environment Variable

```

1 GET /qt/dumpreq.php HTTP/1.1
2 Cookie: sessionId=0000
3 Host: poc.rhynorater.com
4
5

```

Type

Environment Variable

sessionId

Add

Type	Description	Actions
Environment Variable	Variable: sessionId	Delete

Part 3

Caido Workflows

Workflow Generation with AI

AI Workflow Development

Caido Workflow GPT



Caido Workflow Developer GPT

By Justin Gardner ☺

Provides assistance to the user on how to use Caido's Workflows. NOTE:
will need to pull latest API reference from Cloudflare Worker. You may
have to tell it to use "getWorkflowJsNodeDocumentation".

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

Caido + Cursor

Adding Custom Docs to Caido

The screenshot shows a dark-themed application window titled "Workflow Advisor". The main title bar includes the application name and a subtitle "Caido + Cursor Adding Custom Docs to Caido". The menu bar contains File, Edit, Selection, View, Go, Run, Terminal, and Help. A tab bar shows "Untitled-1 - Cursor". The main content area has a header "Docs" with the sub-instruction "Crawl and index custom resources and developer docs". A button "+ Add Doc" is visible. Below this, three items are listed:

- Caido Docs (Developer)**
Indexed 7/8/25, 7:43 PM (Edit, Refresh, Copy, Delete icons)
- Caido Frontend SDK**
Indexed 7/7/25, 3:44 PM (Edit, Refresh, Copy, Delete icons)
- Caido Backend SDK**
Indexed 7/7/25, 3:44 PM (Edit, Refresh, Copy, Delete icons)

Part 3

Caido Workflows

Convert Workflows + Keyboard Shortcuts

Workflow

Shortcuts for Workflows

Shortcuts

Customize your keyboard shortcuts.

base Reset to defaults

Group	Name	Keybinding
Convert Workflow	Base64 Decode (Preview)	-
Convert Workflow	Base64 Decode (Replace)	⌃ ⌄ B
Convert Workflow	Base64 Encode (Preview)	-
Convert Workflow	Base64 Encode (Replace)	⌃ B

Request

```
1 GET /qt/dumpreq.php HTTP/1.1
2 Authorization: Bearer 00000000-0000-0000-0000-000000000000 [
3 Host: poc.rhynorater.com
4
5
```

Part 3

Caido Workflows

Convert Workflows + Command Palette (EvenBetter)

EvenBetter Plugin

Command Palette Workflows

The screenshot shows a command palette interface for the EvenBetter plugin. At the top, there's a search bar with 'abc' and a clear button. Below it is a header bar with a question mark icon, a URL field containing 'https://poc.rhynorater.com', and a red 'Send' button. The main area is divided into two sections: 'Request' on the left and 'Response' on the right. The Request section contains the following text:

```
1 GET /exampleRequest?queryParameter=abc1234/1234 HTTP/1.1
2 Host: poc.rhynorater.com
3
4
```

The Response section contains the following text:

```
1 HTTP/1.1 200 OK
2 Date: Mon, 28 Jul 2025 16:18:57 GMT
3 Server: Apache/2.4.57 (Ubuntu)
4 Last-Modified: Sat, 30 Dec 2023 21:37:49 GMT
5 ETag: "17-60dc0f5d4063a"
6 Accept-Ranges: bytes
7 Content-Length: 23
8 Access-Control-Allow-Origin: *
9 Access-Control-Allow-Credentials: true
10 Access-Control-Allow-Headers: authorization,x-goog-h-content-type
11 Content-Type: text/javascript
12
13 alert(document.domain)
```

common-filters	i	Creates and automatically updates common filters you may want to use. 1hr, recent, 24hr, 6hr, 12hr	frontend	No	<input checked="" type="checkbox"/>
command-palette-workflows		Adds all your convert workflows to the command palette	frontend	No	<input checked="" type="checkbox"/>

HTTPQL + Workflows = Finding

Example case study use-case

“hey, i never saw this endpoint before”

Update preset

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

Drop to...

Caido

Forwarding Environment lightspeed-re...

View Editor

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

```
dx = 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

The screenshot shows a passive workflow on the left and a code editor on the right.

Passive Workflow:

```

graph TD
    Start(( )) -- "On Intercept Response" --> Javascript1[Javascript]
    Javascript1 -- "On Intercept Response" --> Javascript2[Javascript]
    Javascript2 -- "Passive End" --> End(( ))
  
```

Code Editor (Javascript tab):

Name: Javascript
Alias: javascript

Required:

Code (code):

```

22 const text = body.toText();
23 const regex = /new \_.[a-zA-Z]{2}\("([A-Za-z0-9]{5,6})",[^"]{1,100}"/\[^"]+/g;
24
25 let match;
26 while ((match = regex.exec(text)) !== null) {
27     const [, key, value] = match;
28     sdk.console.log("RPCIDS:", match);
29     await sdk.env.setVar({
30         name: key,
31         value,
32         env: "googleRPCIds",
33         global: false,
34         secret: false,
35     });
36     sdk.console.log(`Set googleRPCIds.${key} = ${value}`);
37 }
  
```

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"])`

Buttons at the bottom:

- Save
- Run

Optional:

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

Environments

+ New Environment

Search...

Global

• googleRPCIds

Update environment
googleRPCIds

Name
googleRPCIds

Environment Variables
Those variables will be available to tools and plugins when the environment is selected.

Name	Value
Ok9j9b	/BardFrontendService.DeleteMemory
ZKcapf	/BardFrontendService.ListMemories
pUnU7	/BardFrontendService.WritePastConversationsInMemory
ra9Swb	/BardFrontendService.ContinueSharedConversation
q4uTj	/BardFrontendService.RouteLimRequest
rJGHib	/BardFrontendService.GetFirebaseAuthToken
zCCiu	/BardFrontendService.RenderCode
TjQSHc	/BardFrontendService.ExecuteCode



M&R - Case Study

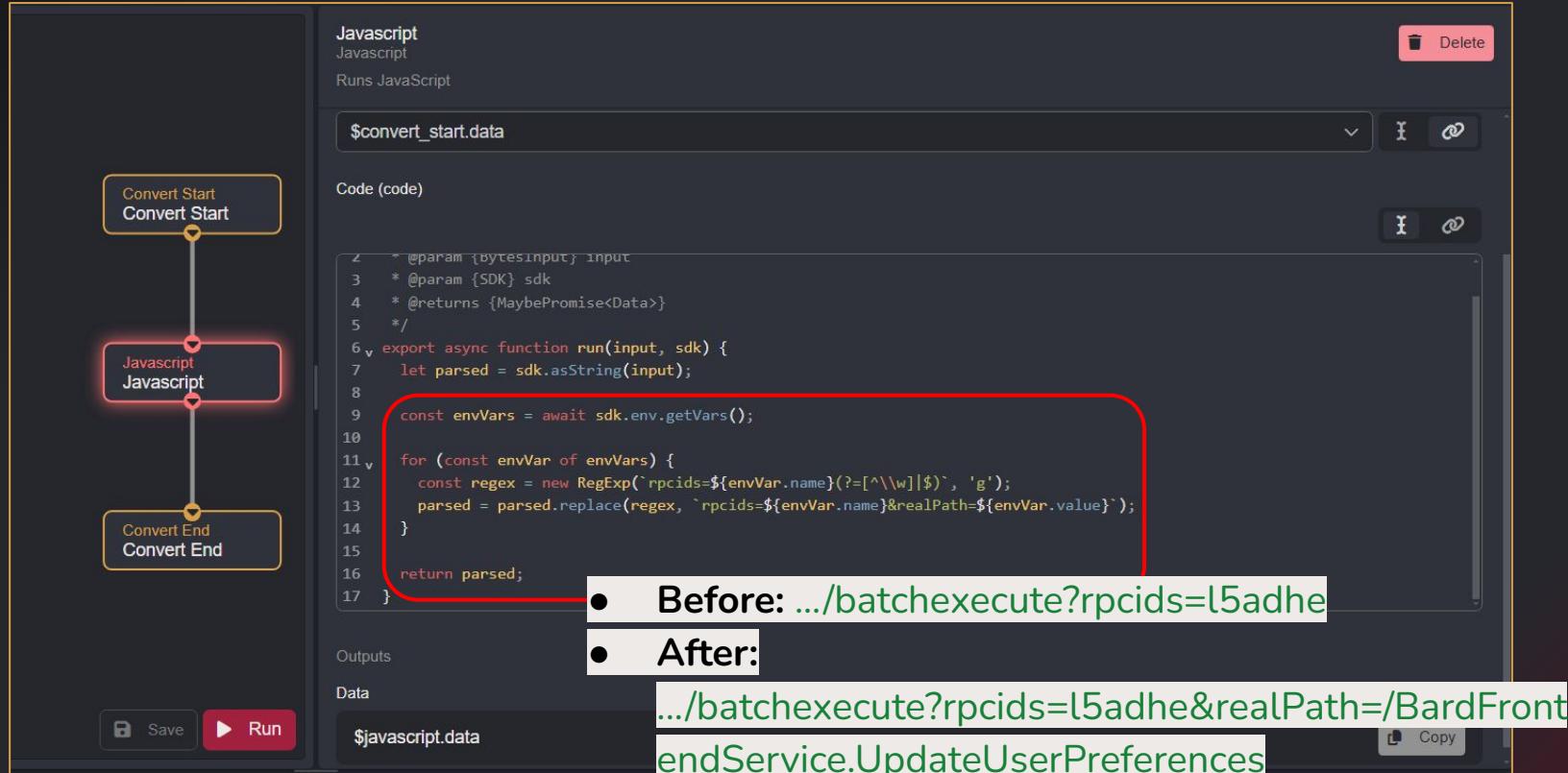
Google rpcids - Step 2 - Correlate & Enhance Data

```
1 POST /_/BardChatUi/data/batchexecute?rpcids=L5adheksource-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
```

The screenshot shows the "Match & Replace" tool interface. On the left, there's a sidebar with a tree view showing a "Default Collection" node and a "batchExecute Replacement" child node, which is selected and highlighted with a blue border. At the top center, there's a tab labeled "batchExecute Replacement" with a pencil icon. Below the tabs, there are two main sections: "Matcher" (set to "Regex") and "Replacer" (set to "Workflow"). The "Matcher" section contains a text input field with the regex pattern ".batchexecute.*". The "Replacer" section contains a dropdown menu with the option "RPCId Substituter", which is also highlighted with a red box. At the bottom of the interface, there are buttons for "Update", "Test", and "Delete".

M&R - Case Study

Google rpcids - Step 2 - Correlate & Enhance Data



The screenshot shows a workflow interface with the following components:

- Convert Start**: A yellow rounded rectangle labeled "Convert Start".
- Javascript**: A red rounded rectangle labeled "Javascript". This node contains the following code:

```

1 * @param {bytes} input
2 * @param {SDK} sdk
3 * @returns {MaybePromise<Data>}
4 */
5
6 v export async function run(input, sdk) {
7   let parsed = sdk.asString(input);
8
9   const envVars = await sdk.env.getVars();
10
11 v   for (const envVar of envVars) {
12     const regex = new RegExp(`rpcids=${envVar.name}(?=[^\\w]|$)`, 'g');
13     parsed = parsed.replace(regex, `rpcids=${envVar.name}&realPath=${envVar.value}`);
14   }
15
16   return parsed;
17 }
```

- Convert End**: An orange rounded rectangle labeled "Convert End".
- Code (code)**: A panel showing the code block from the Javascript node.
- Outputs**: A panel showing the output "\$javascript.data".
- Data**: A panel showing the output "\$javascript.data".

● Before: .../batchexecute?rpcids=l5adhe

● After:

.../batchexecute?rpcids=l5adhe&realPath=/BardFrontendService.UpdateUserPreferences

M&R - Case Study

Google rpcids - Step 2 - Correlate & Enhance Data

```
9  const envVars = await sdk.env.getVars();
10
11 v  for (const envVar of envVars) {
12    const regex = new RegExp(`rpcids=${envVar.name}(?=^[^\\w]|$)` , 'g');
13    parsed = parsed.replace(regex, `rpcids=${envVar.name}&realPath=${envVar.value}`);
14  }
15
16  return parsed;
17 }
```

M&R - Case Study

Google rpcids - Step 2 - Correlate & Enhance Data



Automated Edit

Pretty

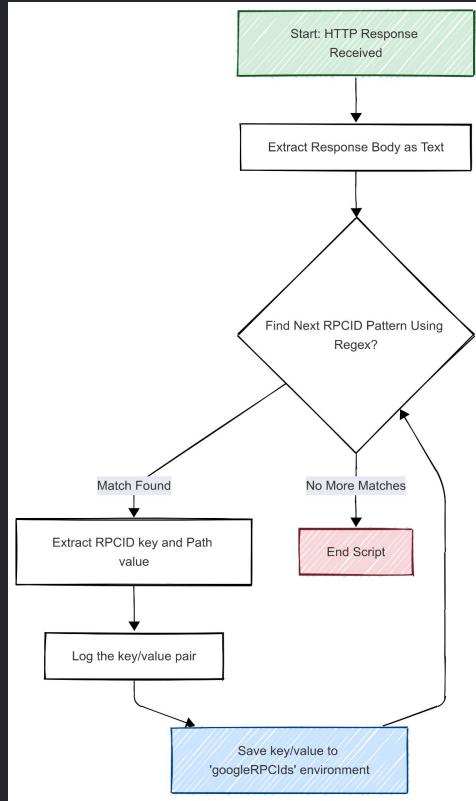
Raw

Drop to...

- 1 POST /_BardChatUi/data/batchexecute?rpcids=L5adhe&realPath=/BardFrontendService.UpdateUserPreferences&source-path=%2Fapp&bl=boq_assistant-bard-web-server_20250722.06_p1&f.sid=-8587937869850823709&hl=en&_reqid=1835262&rt=c HTTP/1.1
- 2 Host: gemini.google.com

M&R - Case Study

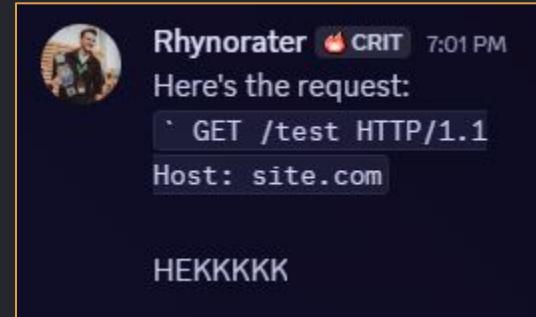
Recap - Stringing it all together



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)

Your Share Code (PGP Fingerprint)

Your Alias (shared along with Share Code)

Justin Gardner

Your Share Code



A7715791DDD1D1C52A926BB12F564048F43ECF25:SnVzdGluIEDhcmRuZXI=

Show Advanced Options

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

Friends

Paste share code here to add a new friend.

Justin Gardner

A7715791DDD1D1C52A926BB12F564048F43ECF25

Drop

Easy Collaboration within Caido

In Replay...

Request

```

1 GET /qt/dumpreq.php HTTP/1.1
2 Cookie: sessionId=0000
3 Host: poc.rhynorater.com
4
5

```

Response

In Filters...

Update preset

Name *

No Styling

Alias

no-styling

Expression

```
(req.ext.nlike: "%.css" AND
req.ext.nlike: "%.woff" AND
```

In
HTTP
History...

Request

Pretty Raw

```

1 GET /dynamite/images/cleardot.gif?zx=o0ti19vag8wc HTTP/1.1
2 Host: ssl.gstatic.com
3 Connection: keep-alive

```

In Scopes...

Update preset

How to use

Name *

testScope

In Scope

Out of Scope

```
poc.rhynorater.com
```

Add a domain or IP, one per line...

Example M&R

In M&R...

Section Response Body

Matcher String

Replacer String

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.

[Hide Advanced Options](#) 

The settings below should only be used if you're hosting your own server.

API Server URL

<https://yourCustomServer.com>

Key Server URL

<https://keys.openpgp.org/>

Part 5

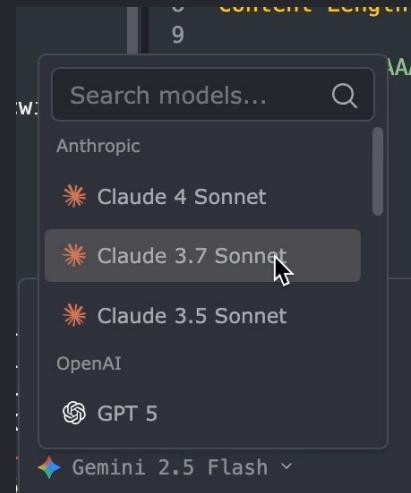
Caido Plugins

Shift

Shift Acquired

Seamless AI Integration into Caido

↑ shift + CAIDO

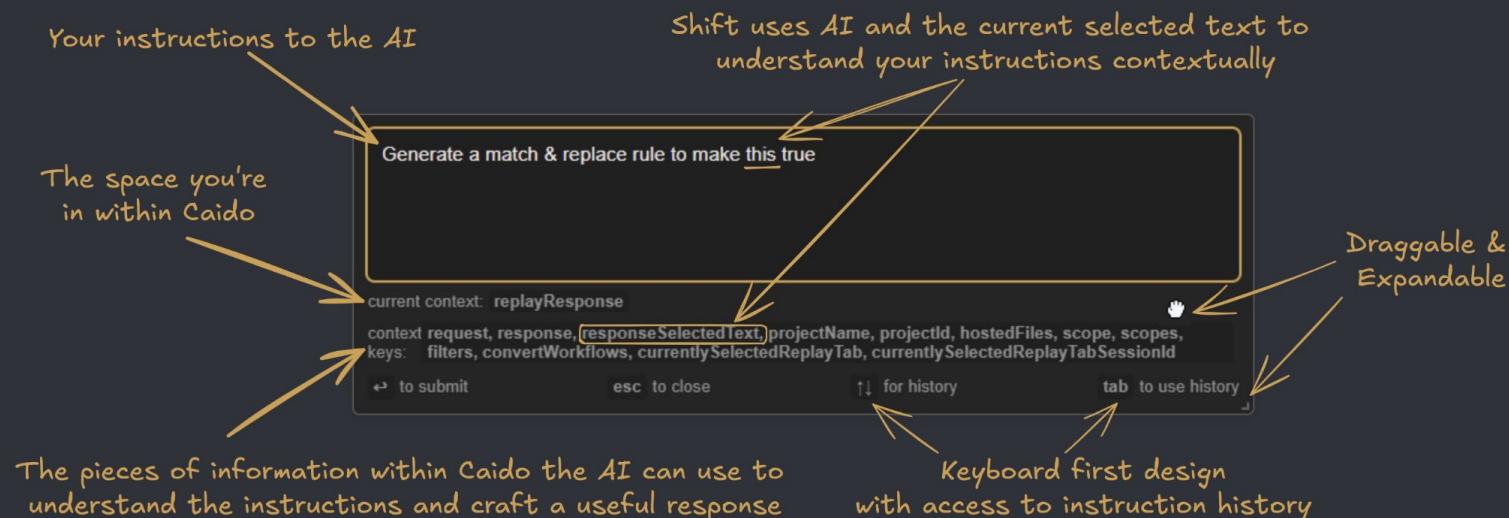


Shift

Seamless AI Integration into Caido

1. Press `<shift> + <space>`

2.



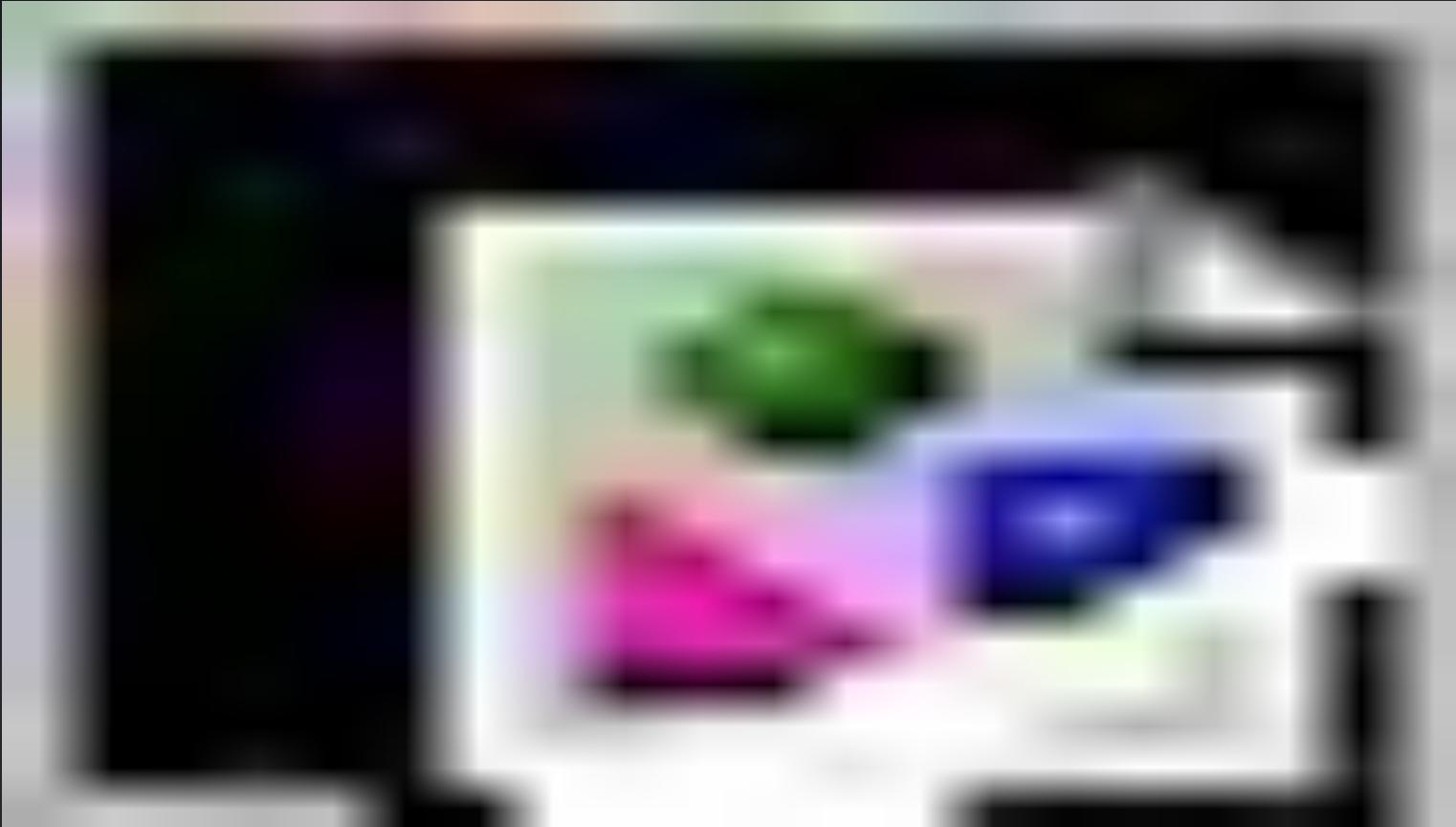
3. Profit?! The AI does the thing.

Taking following actions:
addMatchAndReplace



Shift

Seamless AI Integration into Caido



Shift

Case Study - Feature Flags on Google Jules

Make ONE match and replace rule to turn on all these feature flags. The feature flags are controlled by the boolean in the 3rd index of the nested arrays. Match the number starting with 4, then null, then the boolean. Change all falses to true

current context: httpHistoryResponse

context response, responseSelectedText, projectName, projectId, hostedFiles, keys: scope, scopes, filters, convertWorkflows, currentRow

→ to submit esc to close ↑ for history tab to use history

.0.0.0", "Chromium";v="138.0.7204.184", "Google Chrome";v=

; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.

tion/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.

Qo=

All rights reserved.

AQIwocsBCKOjywEihaDNAQim/M4BCIb9zgEIif30AQjtgM8BG0HizgEY6

Response

Pretty Raw Preview

279 "TSDtV": "%.@.#[[null,[45713273,null,true,null,null,null,\"yLITE\"],[45682235,null,false,null,null,null,\"sqKsie\"],[45700348,null,null,null,\"https://discord.gg/googlelabs\"],null,\"ueye\"],[45696048,null,false,null,null,null,\"k1zpG\"],[45694032,null,false,null,null,null,\"S1rRCD\"],[45654360,null,false,null,null,null,\"A8gef\"],[45700050,null,true,null,null,null,\"TiPcKe\"],[45700643,150000,null,null,null,null,\"dbnMsc\"],[45717420,null,false,null,null,null,\"Im04Qc\"],[45700048,null,null,1,null,\"Google does not train its generative AI models on content Jules receives from your private repositories unless you choose to include that content along with your feedback.\"],null,\"pNbTtY\"],[45716315,null,true,null,null,null,\"j4KNvc\"],[45713515,null,false,null,null,null,\"ZJkXtd\"],[45677491,null,false,null,null,null,\"dvb2ob\"],[45700019,null,false,null,null,null,\"prXHab\"],[45699063,null,false,null,null,null,\"igFK4\"],[45693746,null,false,null,null,null,\"yszwY\"],[45700047,null,null,null,\"Allow AI model training on content from public repositories\"],null,\"SANSEF\"],[45700508,null,false,null,null,\"zzBje\"],[45717403,null,null,null,\"https://mail.google.com/mail/u/0/?pli=\u003d1#chat/space/AQAQhTZlYE\"],null,\"jeVtv\"],[45717258,null,false,null,null,null,\"RiEogd\"],[45702554,null,false,null,null,null,\"Ca3g7\"],[45716193,null,null,null,null,null,\"zpFYNe\"],[\"[[\\\"Help me fix this error ...\\\",\\\"Diagnose this memory leak ...\\\",\\\"Write a g3doc for a project ...\\\",\\\"Write a test that mocks fetch ...\\\"]]\"]],[45716548,null,false,null,null,null,\"Xzz8Ce\"],[45668995,null,false,null,null,null,\"iETJDc\"],[45682221,null,false,null,null,null,\"zov3Sb\"],[45700445,4000,null,null,null,null,\"SDwrVc\"],[45682575,null,false,null,null,null,\"r7Xouf\"],[45700125,null,null,null,null,null,null,\"WMHHJc\"],[\"[[\\\"google3\\\",\\\"/labs/language/aida\\\",\\\"/learning/gemini/cms\\\",\\\"aida-tandem-server\\\"]]\"]],[45678716,null,true,null,null,null,\"nf3vSb\"],[45691590,null,false,null,null,null,\"MihKmc\"],[45699064,null,null,null,\"Jules is currently experiencing high load. You can view your existing tasks. Come back in a bit to create more tasks.\"]],null,\"MDTXKc\"],[45700349,null,null,null,\"https://x.com/julesagent\"],null,\"ArLNhb\"],[45706595,null,null,null,\"lynx\"],null,\"h5Bpgb\"],[45681765,null,true,null,null,null,\"oHCVmf\"],[45700046,null,null,null,\"Let Google use your future Jules conversations and code on content Jules receives from public repositories to train its generative AI models. Opting out does not apply to any feedback you may choose to provide.\"]],null,\"aRD8td\"],[45712655,null,false,null,null,null,\"k6bFvb\"],[45700824,null,false,null,null,null,\"HPs9hc\"],[45693526,null,true,null,null,null,\"zqXrie\"],[45717278,null,false,null,null,null,null,\"mznhdF\"],[45700823,null,false,null,null,null,\"Yqr4cc\"],[45682220,null,false,null,null,null,\"MO6sEf\"],[45660275,null,false,null,null,null,\"W9kaSe\"],[45715869,null,false,null,null,null,\"bbcXs\"],[45700049,null,false,null,null,null,null,\"oJMdc\"],[45696114,null,true,null,null,null,\"lQuuef\"],[45700607,null,false,null,null,null,\"i5gfu\"],[45700045,null,null,null,null,null,\"F90Zt\"],[\"[[\\\"Help me fix this error ...\\\",\\\"Diagnose this memory leak ...\\\",\\\"Write a README for this project ...\\\"]]\"]]

Shift

Case Study - Feature Flags on Google Jules

2 seconds later...

Taking following actions:
addMatchAndReplace



Turn on Feature Flags

Drop to...

Section Response Body

Matcher Regex

\|(4\d+,null,false

[\$1,null,true

Condition

Enter an HTTPQL query...

Update

Test

Delete

Download

Shift Rename

AI-Assisted Replay Tab Naming

The screenshot shows the CAIDO application interface. On the left, there's a sidebar with various tools: Overview, Sitemap, Scope, Filters, Proxy, Intercept, HTTP History, WS History, Match & Replace, Testing, Replay (which is highlighted in yellow), Automate, Workflows, Assistant, Logging, and Search. The main area has tabs at the top labeled 1, 2, 3, 4, 5, 6, and X. The tab labeled '4' is highlighted with a yellow border. Below the tabs, the URL is https://grehack.rhynorater.com. The interface is divided into Request and Response sections. The Request section shows a POST request with JSON data. The Response section shows an HTTP 404 Not Found error page. At the top of the main area, there's a red button labeled '+ New Session'. Above the tabs, there are buttons for 'Import Collection' and 'Options'. To the right of the tabs, there are icons for user profile and settings.

+ New Session

Import Collection Options

Overview Sitemap Scope Filters Proxy Intercept HTTP History WS History Match & Replace Testing Replay Automate Workflows Assistant Logging Search

1 2 3 4 5 6 X

https://grehack.rhynorater.com

Request

```
1 POST /endpoint HTTP/1.1
2 Host: grehack.rhynorater.com
3 Connection: close
4 Content-Type: application/json
5
6 {
    "data": "someVariable",
    "name": "someOtherVariable",
    "metadata": {
        "abc": 1
    },
    "objects": [
        "a",
        3
    ]
}
```

Response

```
1 HTTP/1.1 404 Not Found
2 Date: Wed, 13 Nov 2024 18:52:53 GMT
3 Server: Apache/2.4.57 (Ubuntu)
4 Access-Control-Allow-Origin: *
5 Access-Control-Allow-Headers: *
6 Content-Length: 285
7 Connection: close
8 Content-Type: text/html; charset=iso-8859-1
9
10 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//
11 <html>
12
13 <head>
14     <title>404 Not Found</title>
15 </head>
16
17 <body>
```

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

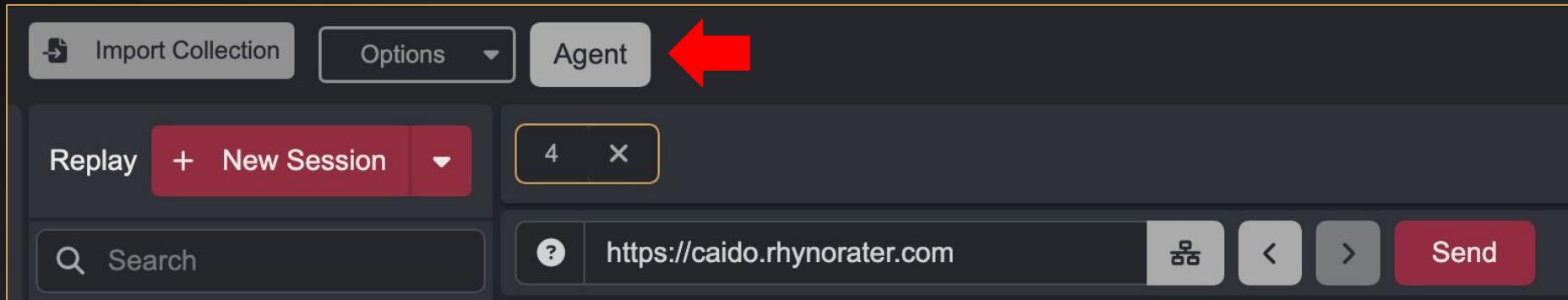
<https://github.com/caido-community/shift-agents>

Shift Agents

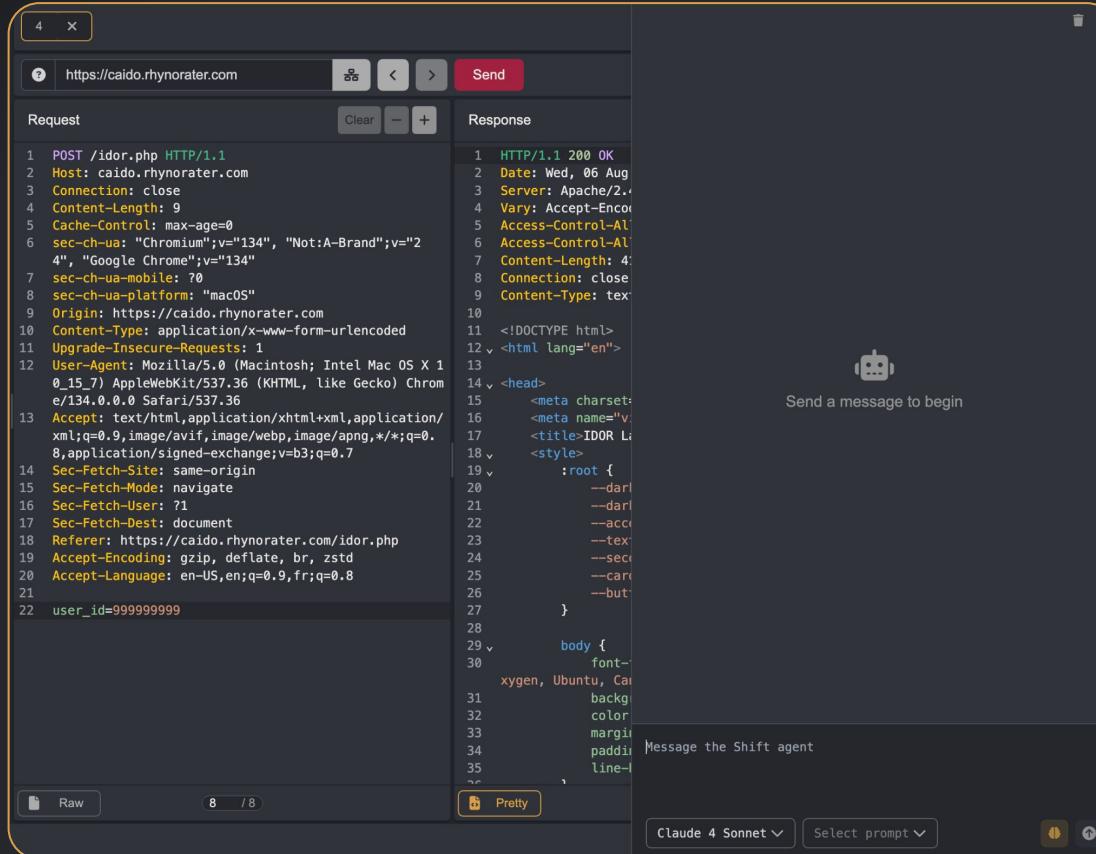
Shift Agents, the new micro-agent framework for Caido users.

Build personalized micro-agents for tasks like XSS exploitation, WAF bypassing, or anything you can think of.

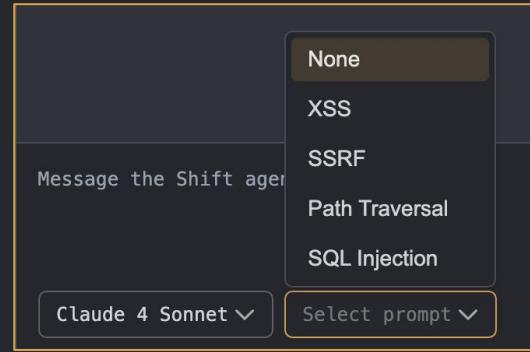
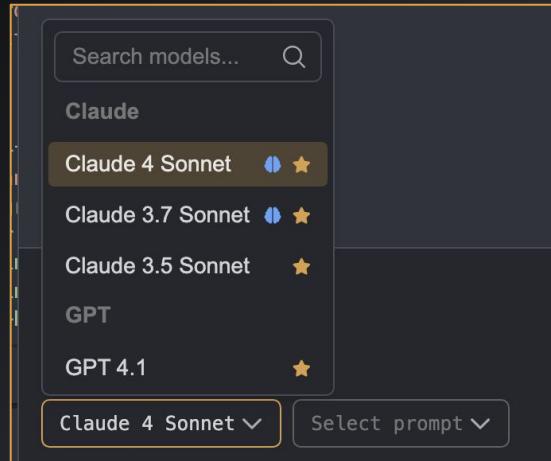
Delegate, delegate, delegate



Delegate, delegate, delegate



Build your own methodology



Custom Prompts		
Define reusable prompts for your AI interactions		+ Add Prompt
Title	Content	Actions
XSS Default	## XSS-Specific Testing Guidance - Test primarily reflected xss due to the nature of this running i...	
SSRF Default	## SSRF-Specific Testing Guidance - Test URL parameters that fetch external resources - Try interna...	
Path Traversal Default	## Path Traversal-Specific Testing Guidance - Test file path parameters with .. sequences - Try va...	
SQL Injection Default	## SQL Injection-Specific Testing Guidance - Test input parameters that interact with databases - S...	

Build your own methodology

XSS-Specific Testing Guidance

- Test primarily [reflected xss](#) due to the nature of this running in replay which doesn't 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>

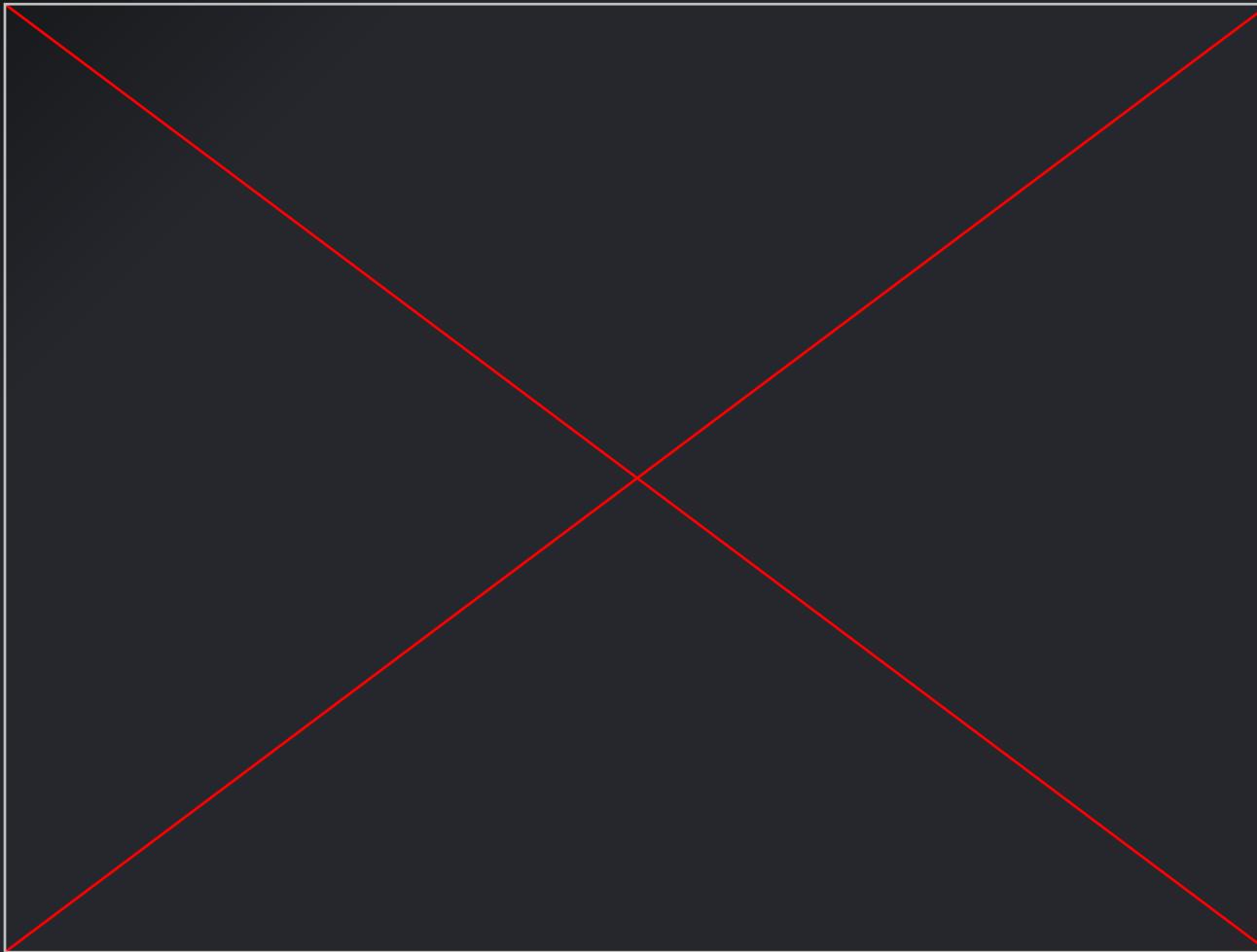
output: <script>alert(1)</script>

> 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)



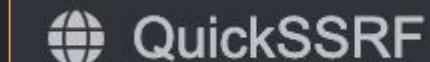
Compare

(Amr)



JXScout

(Francisco)



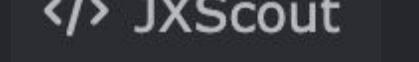
QuickSSRF

(Amr)



JWT Analyzer

(Amr)



OmniOAST

(Hahwul)



ReDocs

(Amr)

My plugins

Caido Plugins

My plugins

csp-auditor

Bytecap

The screenshot shows the Bytecap - File Size Monitor interface. On the left, there's a sidebar with various tools like WS History, Match & Replace, Testing, Replay, Automate, Workflows, Assistant, Environment, Logging, Search, Findings, Exports, Workspace, Plugins, Param Finder, Bypasser, QuickSRF, EvenBetter, YesWeCaido, Themes, Font Selector, Shift, Data Grep, Devtools, Squash, Exploit Generator, JWT Analyzer, Notes++, Compare, OmniDAST, Drop, Scanner, Chatio, and Bytecap. The main area has tabs for 'Forwarding' and 'Environment'. The 'Bytecap - File Size Monitor' tab is active, displaying 'Monitor and manage workspace file sizes'. It shows a 'Settings' section with a size threshold of 2980MB, a slider from 1MB to 20GB, and checkboxes for 'Enable Additional Warnings' at 75% and 90% of the threshold. Buttons for 'Apply Settings', 'Refresh Files', and 'Clear Alerts' are present. Below this, a section titled 'Caido Project Files (3) - Combined Size: 331.21 MB' lists files: database_raw.caido (309.47 MB), database.caido (21.71 MB), and config.caido (28 KB). A note states these are monitored as a combined unit. At the bottom, a table shows 'All Workspace Files (9) - Total: 340.53 MB' with columns for File Name, Size, and Status. The table includes rows for database_raw.caido, database.caido, database_raw.caido-wal, database.caido-wel, config.caido-shm, and database.caido-shn, each with its size and an 'OK' status indicator.

File Name	Size	Status
database_raw.caido	309.47 MB	Part of Combined Check
database.caido	21.71 MB	Part of Combined Check
database_raw.caido-wal	6.25 MB	OK
database.caido-wel	2.97 MB	OK
config.caido-shm	32 KB	OK
database.caido-shn	32 KB	OK

AI Plugin Development

Caido Developer Assistant



Caido Developer Assistant

By Justin Rhinehart  

A custom GPT to help developers make plugins/extensions for Caido.
Contains knowledge from developer documentation, the JS SDK, and
the UI kit.

<https://chatqpt.com/q/q-68095eb17eb08191ba19fd85f0a516ec-caido-developer-assistant>

Practical Takeaways



Web Security Labs

A collection of web security testing tools to help security professionals and enthusiasts audit web applications with efficiency and ease.

Match and Replace

Learn how to use M&R - a powerful tool for finding and replacing patterns in HTTP requests and responses.

[Open Lab](#)

IDOR Vulnerability

Explore how Insecure Direct Object References can expose sensitive user information and learn to identify these vulnerabilities.

[Open Lab](#)

Too Many Requests

Learn how to filter information with HTTPQL and how it can be used to scan for hidden information.

[Open Lab](#)

ShaSigned

Learn how to use convert workflows to really speed up your testing process.

[Open Lab](#)

CSRF via Content-Type

Explore how improper content-type handling can lead to CSRF vulnerabilities, even with SameSite cookies.

[Open Lab](#)

Session Monitor

Learn how to track session ID changes and monitor session behavior using Caldo workflows for session management testing.

[Open Lab](#)

XSS Lab

Discover two types of reflected XSS vulnerabilities, one in an HTML context and one in a JavaScript context.

[Open Lab](#)

Other Resources

 <https://links.caido.io/discord>

 <https://ctbb.show/discord>

 [https://www.bugcrowd.com/blog/the-ultimate-beginner
s-guide-to-caido/](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](#)



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.

