

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

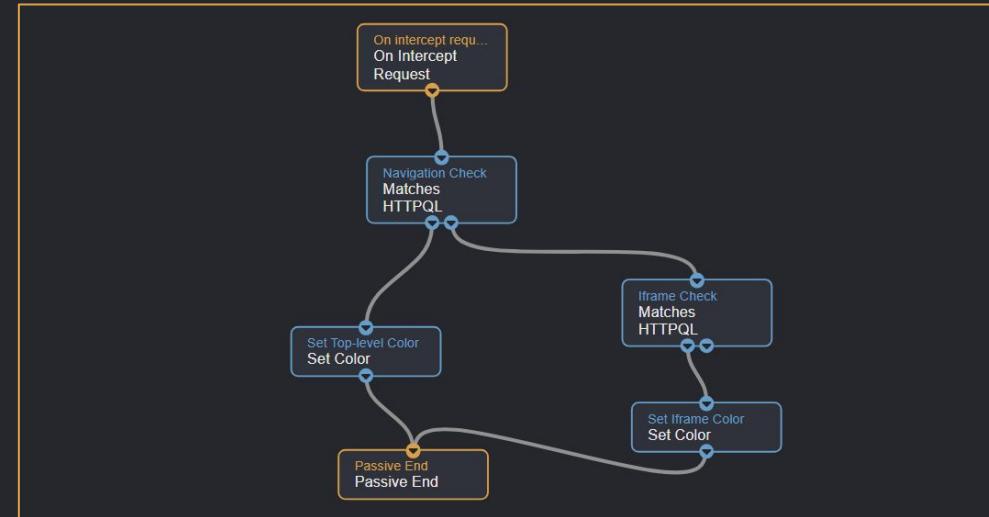


Iframe Navigation

Workflows

Passive 8

Top-Level Navigation



Simple Yet Common Passive Workflow Example

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

- Left Sidebar:** Overview, Sitemap, Scopes, Filters, Proxy (Intercept, HTTP History, WS History), Match & Replace.
- Middle Left Panel:** Request Sent At: 2025-09-05 10:24:05. Applied: 1XX 2XX 3XX 4XX 5X. Automated Edit dropdown is open, showing options: Original Request, Automated Edit, and a large preview area.
- Middle Right Panel:**
 - Match & Replace:** Default Collection contains a rule: X-Bug-Bounty: GangGreenTemperTatum.
 - Request Header:** Section: Request Header. Name: X-Bug-Bounty. Value: String. Value: GangGreenTemperTatum.
 - Condition:** Enter an HTTPQL query... (empty).
 - Buttons:** Update, Test, Delete, Download.
 - Before and After:**
 - Before:**

```

1 GET /path/?query=value HTTP/1.1
2 Host: dashboard.rapyd.net
3 User-Agent: Mozilla/5.0
4 Accept: application/json
5 Accept-Language: en-US
6 Accept-Encoding: gzip
7 Content-Type: application/json
8 fingerprint: ddb70cb5
9 token: 5c0c348b-f758-403b-ba8e-1234567890ab
10 Content-Length: 310
11 Origin: https://dashboard.rapyd.net
12 DNT: 1
13 Connection: keep-alive
14 Referer: https://dashboard.rapyd.net/settings/communication-center/support/open
15 
```
 - 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"}
8 
```
- Bottom Panel:** A large preview area showing the modified request with the X-Bug-Bounty header added.

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

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

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

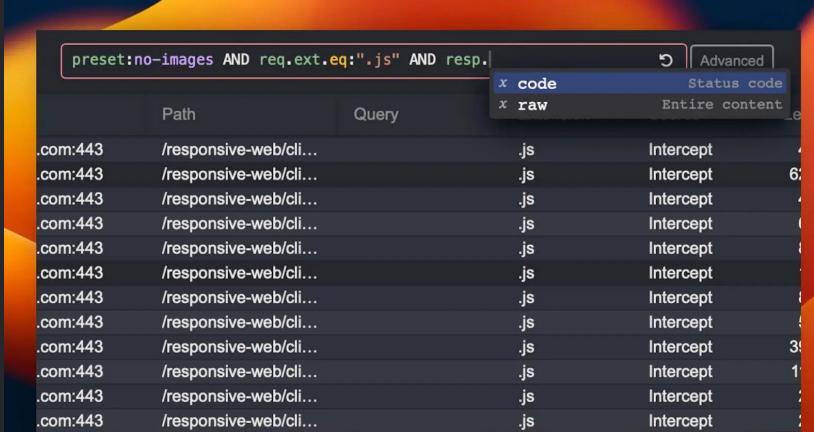
GET 200 https://poc.rhynorater.com/qt/test.html

Request	Pretty	Raw	Response	Pretty	Raw	Preview
1 GET /qt/test.html HTTP/1.1			1 HTTP/1.1 200 OK			
2 Host: poc.rhynorater.com			2 Date: Tue, 22 Jul 2025 19:12:32 GMT			
3 Connection: keep-alive			3 Server: Apache/2.4.57 (Ubuntu)			
4 Pragma: no-cache			4 Last-Modified: Mon, 05 May 2025 18:43:22 GMT			
5 Cache-Control: no-cache			5 ETag: "108a-63467dfe1a72e-gzip"			

Part 1

Caido Search

HTTPQL = Time for serious text-based filtering.



A screenshot of the Caido search interface. At the top, there is a search bar containing the query: `preset:no-images AND req.ext.eq:".js" AND resp..content ~ "script"`. Below the search bar is a table with columns: Path, Query, Status code, and Intercept. The table lists multiple entries, all of which have a status code of "Intercept".

Path	Query	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	
.com:443 /responsive-web/cli...	.js	Intercept	

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



The main interface shows the 'Filters' screen with the following details:

- Filters** header with a **+ New Preset** button.
- Search bar** with placeholder **Search...**.
- List of filters:**
 - No Styling
 - abc
 - **fromToday** (selected item)
- Update preset** section:
 - Name ***: **fromToday**
 - Alias**: **fromtoday**
 - Expression**: `req.created_at.gt:"2025-07-22 15:07:00"`
- Save** and **Delete** buttons at the bottom.

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. A third red arrow points to a "Custom Presets" dropdown menu where "fromToday" is selected.

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.

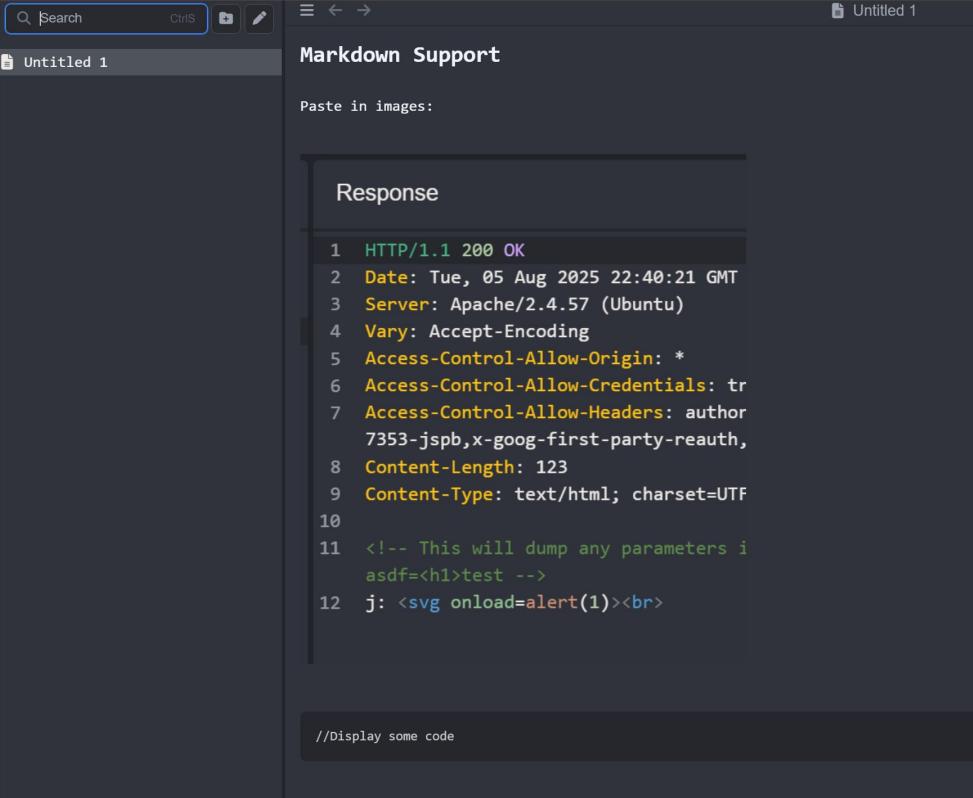
Part 2

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>
```

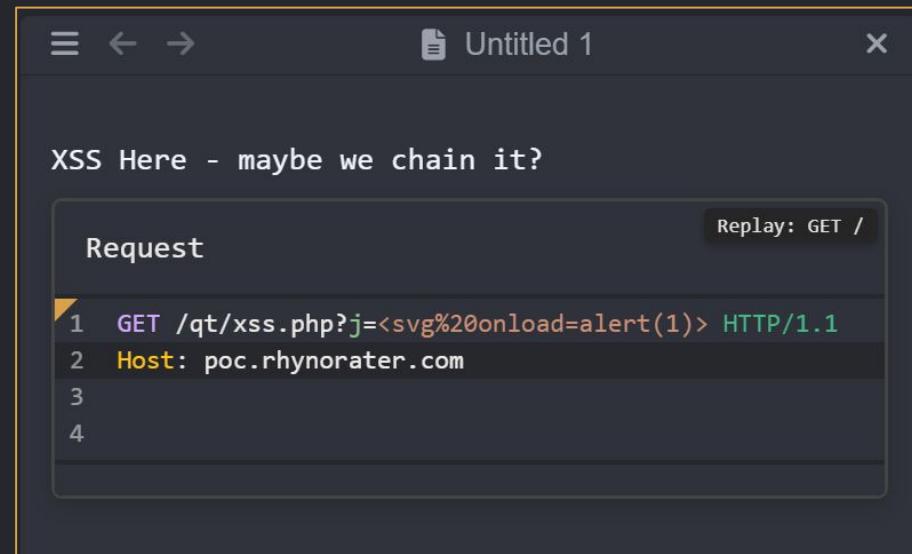
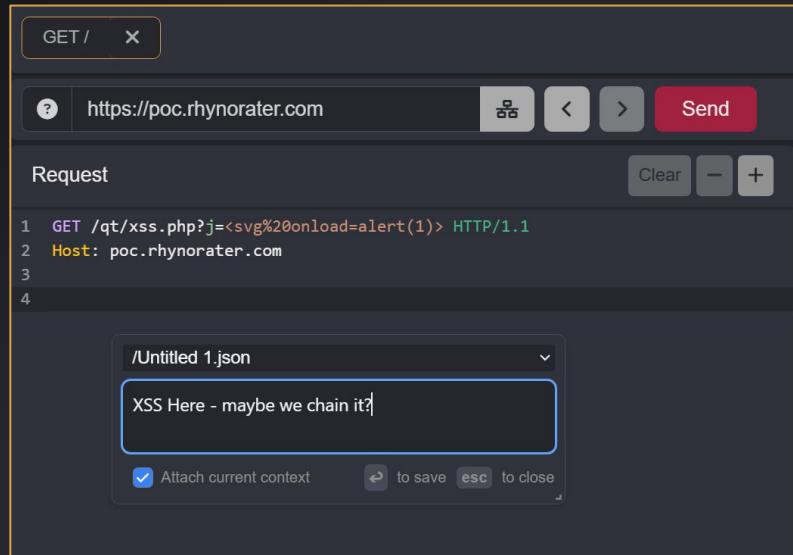
At the bottom of the main window, there's a footer bar with the text 'Display some code'.

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

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

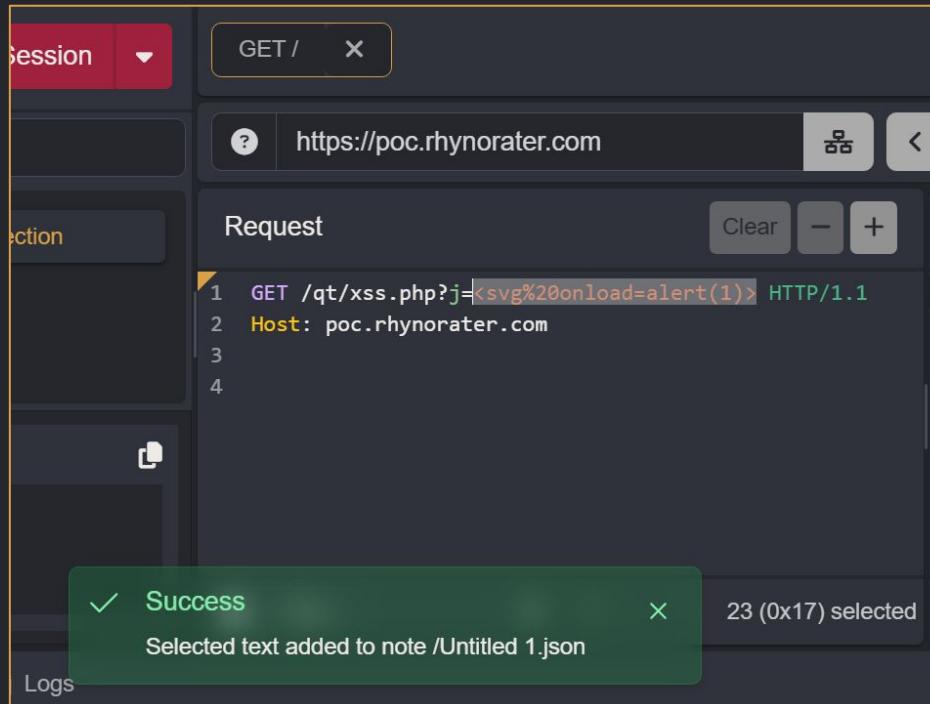
Organization

#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". Below these are several control buttons: a question mark icon, a refresh icon, a back arrow, a forward arrow, and a red "Send" button. On the left side, there's a sidebar with a dropdown menu set to "Default Collection" and a text input field containing "abc". The main area is titled "Request" and displays a list of five log 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. The top navigation bar includes "Import Collection", "Options", "Agent", and "Agent". The left sidebar has sections for Overview, Proxy (Intercept, Network History, WS Spy), Testing (Reply, Automate, Workflows, Assistant, Environment), Logging (Search, Findings, Exports), Workspace (Files, Plugins, Workspaces), and Plugins (403 Bypasser, EvenBetter, LoadPath, Port Selector, Themes). The main area has tabs for "Reply" (selected) and "New Session". A search bar at the top says "Enter a connection URL" with a "Send" button. Below it is a dropdown menu with options "public cloud" and "private cloud", with "private cloud" highlighted by a red box. The central part of the screen shows a "Request" section with two mobile device icons and a message: "No reply session selected". The right side shows a "Response" section with two mobile device icons and a message: "No response to display. Select a request with a response to view it here." 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 fields for "From" (52) and "To" (88), and a "Type" dropdown set to "Workflow". A sub-menu under "Workflow" is open, showing "Random UUID Generator" with a red arrow pointing to it. The "Input text" field on the left contains the same log entries as the main interface. At the bottom, a table lists placeholder configurations:

Type	Description	Actions
Workflow	Random UUID Generator	

A red arrow points from the "Procedure" label to the "Random UUID Generator" entry in the table.

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'. To the right are buttons for 'Vegas Google' and user profile.

The main area has tabs for 'Environments' (selected) and '+ New Environment'. A search bar contains 'Search...'. On the left, a sidebar lists environments: 'Global' (selected) and 'googleRPCIds', both highlighted with a red box.

The central part shows an 'Update environment' card for 'Global'. It includes fields for 'Name' (set to 'Global') and 'Environment Variables'. A note says: 'Those variables will be available to tools and plugins when the environment is selected.' Below this is a table of variables:

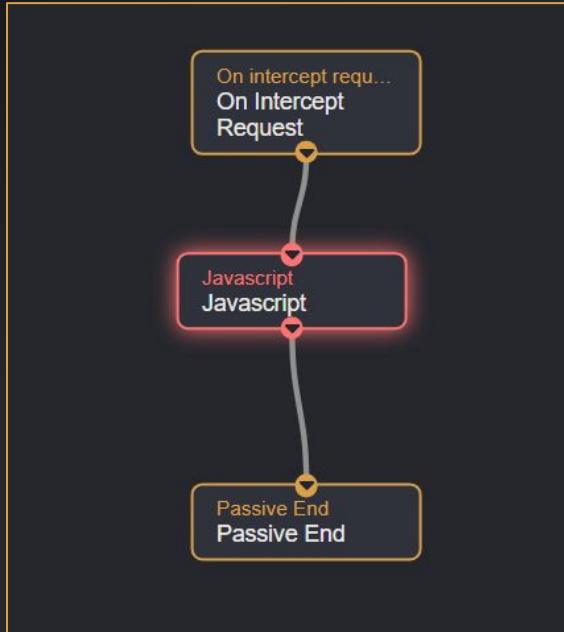
Name	Value	Kind
sessionID	Secret
PHPSESSID	Secret

Actions for each row include 'Update' and 'Delete' buttons, also highlighted with a red box. Red arrows point from the 'Key-Value Stores' text at the bottom to the 'Value' column of the table.

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

```
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.");
        }
    }
}
```

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 "Untitled-1 - Cursor". The menu bar includes File, Edit, Selection, View, Go, Run, Terminal, and Help. A toolbar with icons for file operations is at the top right. The main area displays a "Docs" section 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 🗑️
- Caido Frontend SDK**
Indexed 7/7/25, 3:44 PM Edit ⚙️ Refresh ⌛️ Copy 📁 Delete 🗑️
- Caido Backend SDK**
Indexed 7/7/25, 3:44 PM Edit ⚙️ Refresh ⌛️ Copy 📁 Delete 🗑️

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 the text "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 "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 Drop to...

Name *

Alias

Expression

Save Delete Download

```

graph TD
    A[On Intercept request] --> B[In Scope]
    B --> C[Matches HTTPQL]
    C --> D[Create Finding]
    D --> E[Passive End]
  
```

Matches HTTPQL

Matches a request/response against an HTTP...

Name: Matches HTTPQL

Alias: matches_httpql

Required Query (code)

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

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

```

graph TD
    A[On Intercept Res...] --> B[Javscript]
    B --> C[Passive End]
    
```

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 }

```

Capture group 1 - rpcid **Capture group 2 - path**

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"])`

Save
Run

Optional

```
/*
 * Caldo Workflow Script: RPCID Extractor
 *
 * This script runs on HTTP responses and is designed to parse JavaScript files
 * from Google services to extract the mapping between a short "rpcid" and its
 * full, descriptive service path. It then saves these mappings as environment
 * variables for a second "replacer" script to use.
 *
 * This is Step 1 of the Match & Replace process.
 */

// The 'sdk' and 'body' variables are provided by the Caldo workflow environment.
// 'body' represents the HTTP response body.

// 1. Get the full response body as a single string of text.
const text = body.toText();

// 2. Define the Regular Expression (Regex) to find the rpcid/path pattern.
// This regex is specifically crafted to find the JavaScript code structure
// seen in the case study, which looks like:
// "...new _Ix("l5adhe", class... "[...]/BardFrontendService.UpdateUserPreferences"]');
//
// - It looks for the constructor 'new _Ix(...)'.
// - Capture Group 1: `([a-zA-Z0-9]{5,6})` captures the short rpcid (e.g., "l5adhe").
// - `.*?` is a non-greedy match for all the code between the rpcid and the path.
// - Capture Group 2: `(\/.*)` captures the full descriptive path that starts with a '/'.
const regex = /new \w+\.\Ix\(("[a-zA-Z0-9]{5,6}")",.*?,["/.*?"]\)\;/g;

// 3. Loop through all matches in the text.
// The `regex.exec(text)` function finds the next match in the string.
// The `while` loop continues as long as new matches are being found.
let match;
while ((match = regex.exec(text)) !== null) {

    // The 'match' array contains the full match at index 0,
    // and the capture groups at subsequent indexes.
    // match[1] will be the rpcid (key).
    // match[2] will be the path (value).
    const key = match[1];
    const value = match[2];

    // For debugging, log the found pair to the tool's console.
    sdk.console.log(`Found RPCID Mapping: ${key} -> ${value}`);

    // 4. Save the discovered mapping into a dedicated environment.
    // This creates a "dictionary" that the next script can read from.
    // The 'sdk.env.setVar' function is specific to the proxy tool (Caldo).
    await sdk.env.setVar({
        name: key,           // The rpcid, e.g., "l5adhe"
        value: value,         // The path, e.g., "/BardFrontendService.UpdateUserPreferences"
        env: "googleRPCIDs", // The name of our "dictionary" or environment
        global: false,        // Set to 'false' to keep it in the current project
        secret: false,
    });
}
```

```
6)", [^"]{1,100}"(\/[^\"]+)

constructor(a){super(a)},  
UpdateUserPreferences"])|
```

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

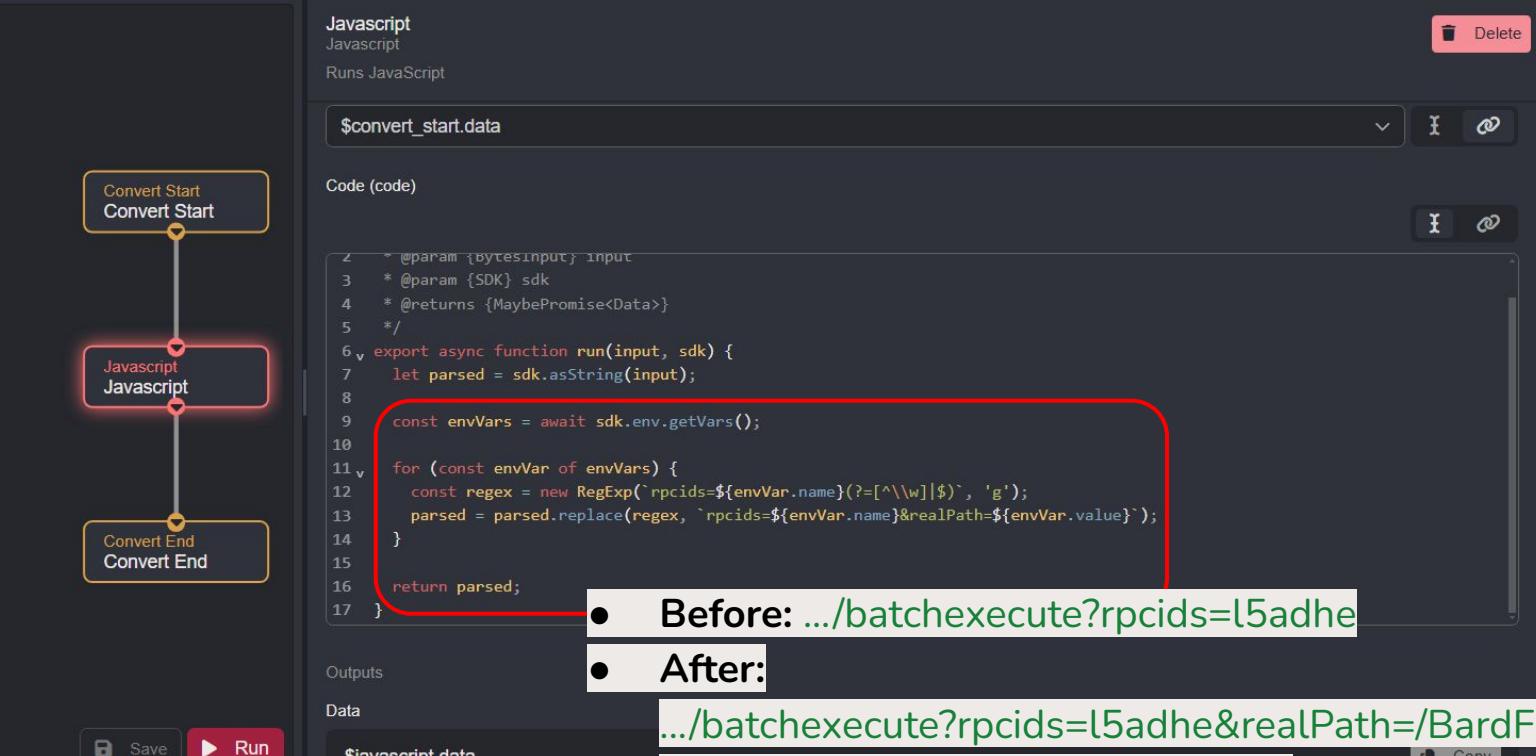
Google rpcids - Step 2 - Correlate & Enhance Data

```
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, both highlighted with a red box. The main area is titled "batchExecute Replacement" and contains several tabs: "Section" (selected), "Request First Line", "Matcher" (set to "Regex"), "Replacer" (set to "Workflow"), and "Condition". The "Matcher" field contains the regex ".batchexecute.*". The "Replacer" field has a dropdown menu with an item "RPCId Substituter" highlighted with a red box. At the bottom, there are buttons for "Update", "Test", and "Delete".

M&R - Case Study

Google rpcids - Step 2 - Correlate & Enhance Data



Javascript
Javascript
Runs JavaScript

\$convert_start.data

Code (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 Start
Convert Start

Javascript
Javascript

Convert End
Convert End

Save Run

Outputs

\$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

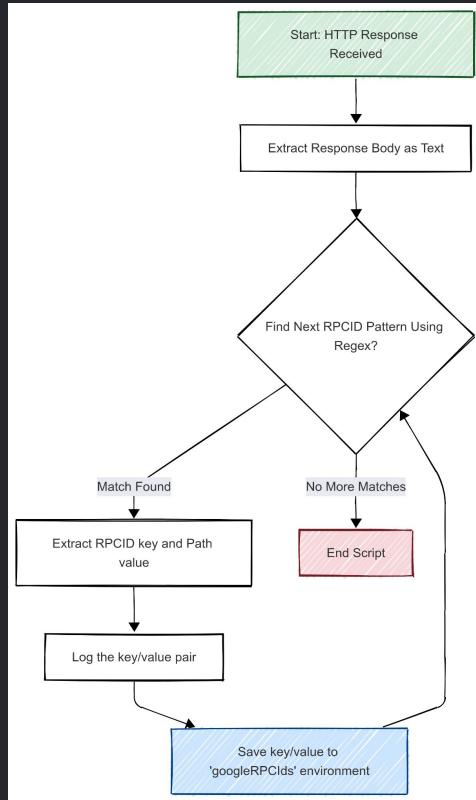
Raw

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

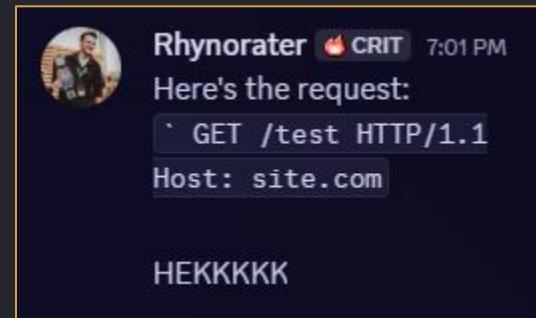
Recap - Stringing it all together



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

Drop to...

Name *

testScope

In Scope

Out of Scope

```
poc.rhynorater.com
```

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

Example M&R

In M&R...

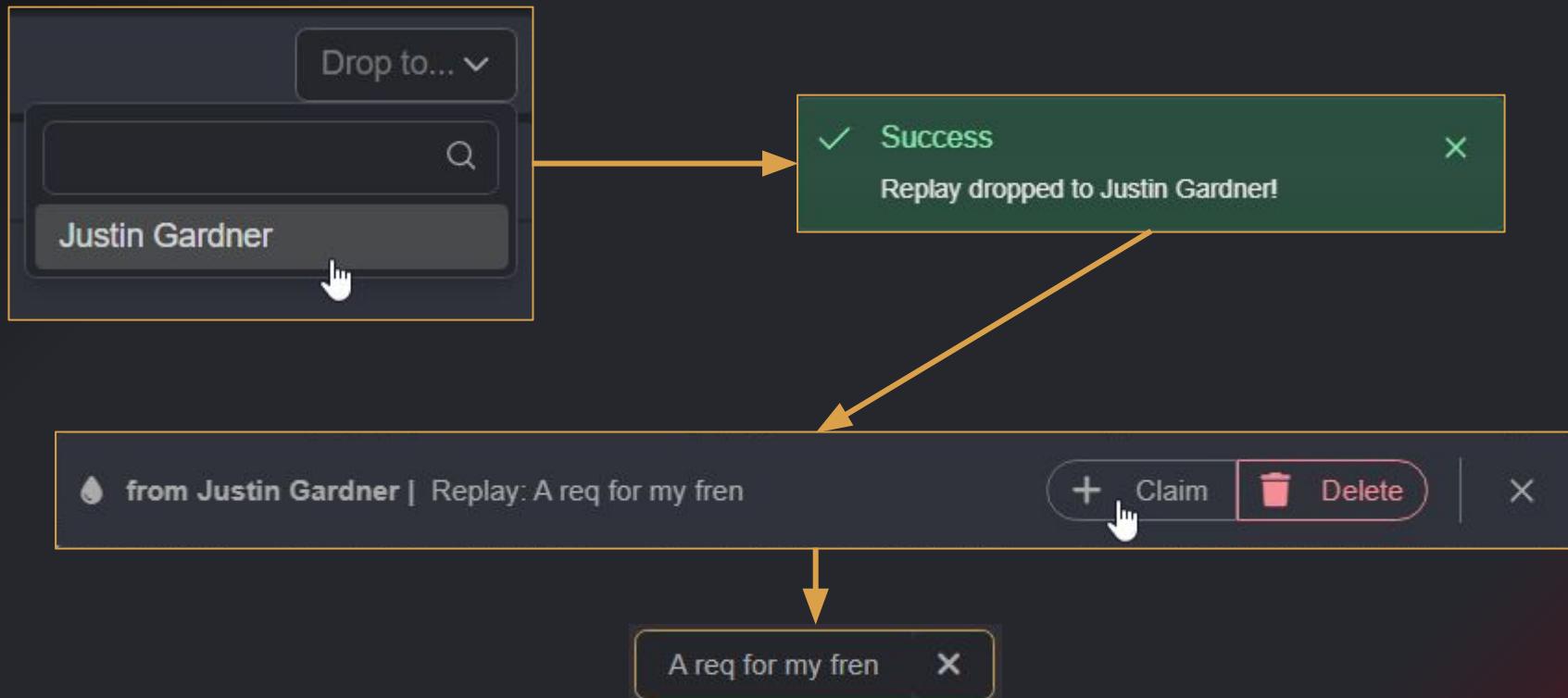
Section Response Body

Matcher String

Replacer String

Drop

Easy Collaboration within Caido



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

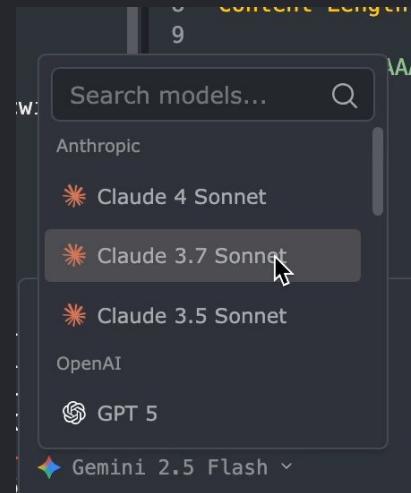
Caido Plugins

Shift

Shift Acquired

Seamless AI Integration into Caido

↑ shift + CAIDO

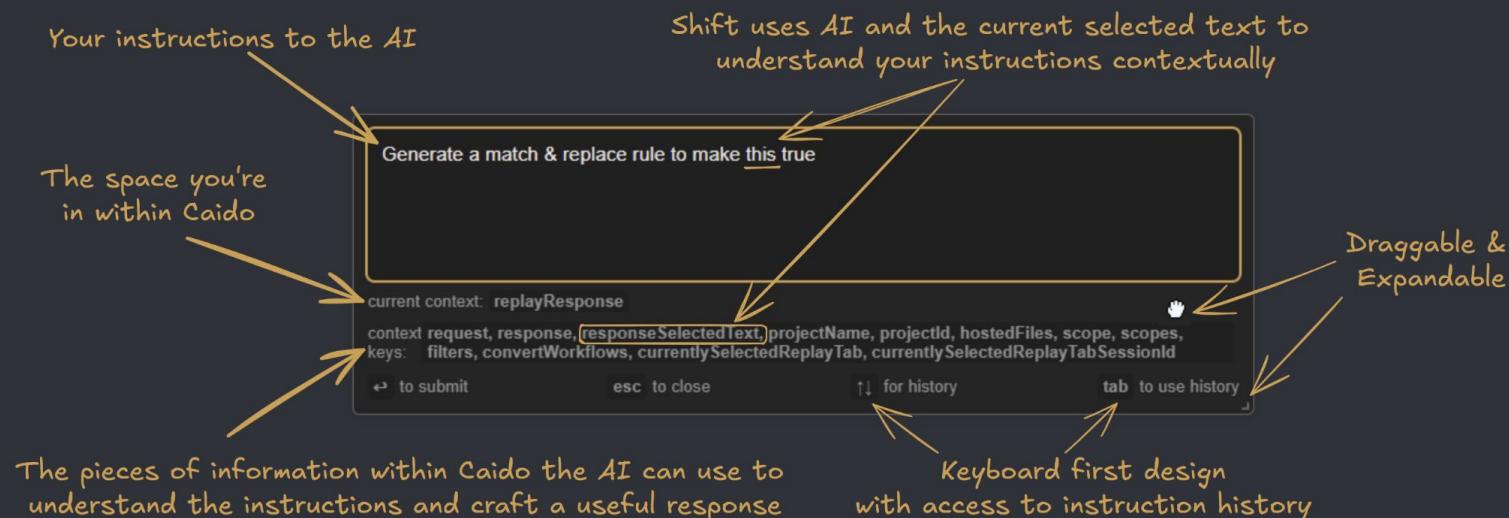


Shift

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

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 with the "Shift Rename" plugin active. The left sidebar contains navigation links for 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 workspace has tabs labeled 1, 2, 3, 4, 5, 6, and 7. Tab 4 is selected and titled "Abc". A search bar at the top of the workspace contains the URL "https://grehack.rhynorater.com". Below the search bar, the "Request" section shows a POST request with the following JSON payload:

```
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
    ]
}
```

The "Response" section displays the following 404 Not Found error page:

```
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

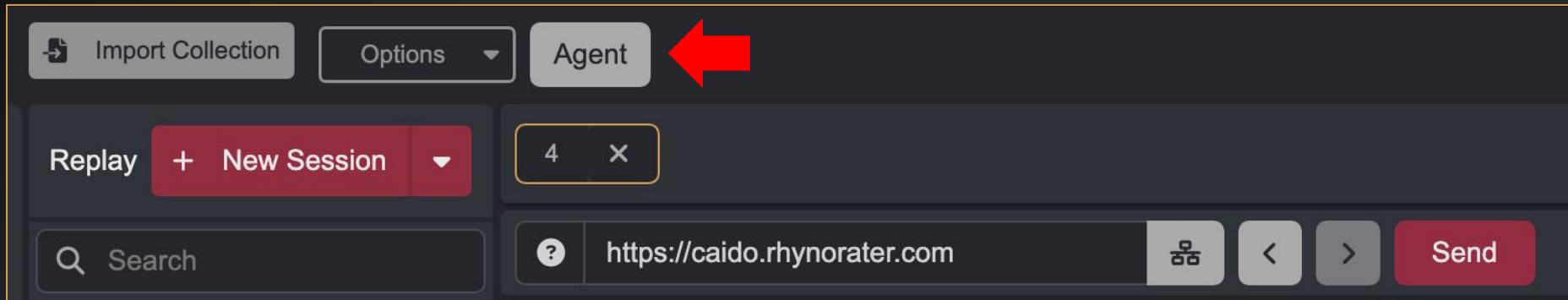
<https://github.com/caido-community/shift-agents>

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

The screenshot shows a browser-based proxy tool interface. The URL in the address bar is <https://caido.rhynorater.com>. The request and response are displayed in a split-pane view.

Request:

```
1 POST /idor.php HTTP/1.1
2 Host: caido.rhynorater.com
3 Connection: close
4 Content-Length: 9
5 Cache-Control: max-age=0
6 sec-ch-ua: "Chromium";v="134", "Not:A-Brand";v="2
4", "Google Chrome";v="134"
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: "macOS"
9 Origin: https://caido.rhynorater.com
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e/134.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://caido.rhynorater.com/idor.php
19 Accept-Encoding: gzip, deflate, br, zstd
20 Accept-Language: en-US,en;q=0.9,fr;q=0.8
21
22 user_id=999999999
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Wed, 06 Aug
3 Server: Apache/2.
4 Vary: Accept-Encoding
5 Access-Control-Allow-Origin: *
6 Access-Control-Allow-Methods: POST, GET, PUT, DELETE, PATCH, OPTIONS
7 Content-Length: 4
8 Connection: close
9 Content-Type: text/html
10
11 <!DOCTYPE html>
12 <html lang="en">
13 <head>
14   <meta charset="UTF-8">
15   <meta name="viewport" content="width=device-width, initial-scale=1.0">
16   <title>IDOR Lab</title>
17   <style>
18     :root {
19       --color-primary: #007bff;
20       --color-secondary: #6c757d;
21       --color-link: #0056b3;
22       --color-link-hover: #00497c;
23       --font-family: sans-serif;
24       --font-size: 16px;
25       --font-weight: bold;
26       --text-decoration: underline;
27     }
28
29   body {
30     font-family: var(--font-family);
31     background-color: #f9f9f9;
32     color: #333;
33     margin: 0;
34     padding: 0;
35     line-height: 1.5;
36   }
37
38   .container {
39     width: 100%;
40     height: 100vh;
41     display: flex;
42     align-items: center;
43     justify-content: center;
44     gap: 20px;
45   }
46
47   .form {
48     width: fit-content;
49     border: 1px solid #ccc;
50     padding: 10px;
51     border-radius: 5px;
52     background-color: #fff;
53   }
54
55   .form input {
56     width: 100%;
57     height: 30px;
58     margin-bottom: 10px;
59     padding: 5px;
60     border: 1px solid #ccc;
61     border-radius: 3px;
62   }
63
64   .form button {
65     width: 100px;
66     height: 35px;
67     background-color: var(--color-primary);
68     color: white;
69     border: none;
70     border-radius: 5px;
71     font-weight: bold;
72     cursor: pointer;
73   }
74
75   .form button:hover {
76     background-color: var(--color-secondary);
77   }
78
79   .output {
80     width: fit-content;
81     border: 1px solid #ccc;
82     padding: 10px;
83     border-radius: 5px;
84     background-color: #fff;
85     margin-top: 20px;
86   }
87
88   .output p {
89     margin: 0;
90     padding: 0;
91     font-size: 14px;
92     color: #333;
93   }
94
95   .output pre {
96     margin: 0;
97     padding: 0;
98     font-family: monospace;
99     font-size: 12px;
100    color: #333;
101  }
```

A message input field with a robot icon and placeholder text "Send a message to begin". A message history section with placeholder text "Message the Shift agent".

Bottom navigation buttons: Raw, Pretty, Claude 4 Sonnet, Select prompt, and other UI elements.

Build your own methodology

Search models... Q

Claude

- Claude 4 Sonnet** 4 ★
- Claude 3.7 Sonnet 4 ★
- Claude 3.5 Sonnet 3 ★

GPT

- GPT 4.1 ★

Claude 4 Sonnet ▼

Select prompt ▼

Message the Shift agent

None

XSS

SSRF

Path Traversal

SQL Injection

Claude 4 Sonnet ▼

Select prompt ▼

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

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>

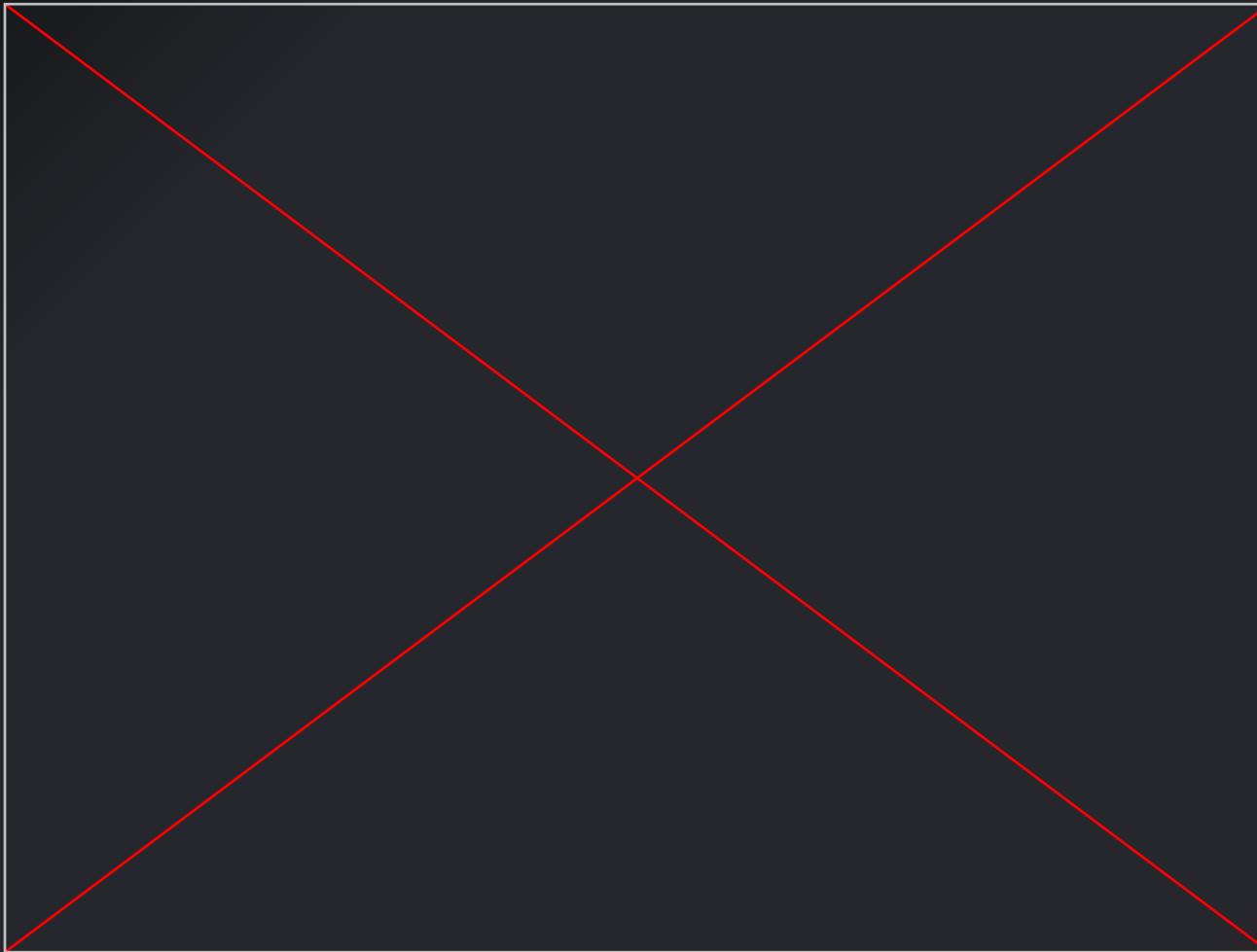
output: <script>alert(1)</script>

> 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)



(Francisco)



QuickSSRF



Compare

(Amr)

(Amr)



JWT Analyzer



OmniOAST

(Hahwul)



ReDocs

(Amr)

Caido Plugins

My plugins

csp-auditor

Info (0.0%)

CSP Analyses (13 total)

Request ID | Timestamp | Host / Path

Request ID	Timestamp	Host / Path
71512	6/5/2025, 4:32:49 PM	www.google-analytics.com
71488	6/5/2025, 4:32:44 PM	growfile.com
71486	6/5/2025, 4:32:44 PM	growfile.com

Forwarding | Environment | Help

Logs | Environment | Findings | Exports | Workspace | Plugins | Param Finder | Font Selector | Themes | Data Grep | Workflows Store | DevTools | 403 Bypasser | YesWeCaido | EvenBetter | QuickSRF | Squash | Shift | JWT Analyzer | Exploit Generator | OmniOAST | Notes+ | Compare | Automatch | SSH Agents | Cerebrum | Drop | Repos | Drop | Scanner | Chatio | CSP Auditor

v0.50.1 (Latest) | Commands | Logs

Bytecap

Forwarding | Environment | Help

CAIDO

WS History | Match & Replace | Testing | Replay | Automate | Workflows | Assistant | Environment | Logging | Search | Findings | Exports | Workspace | Plugins | Param Finder | Font Selector | Themes | Data Grep | Workflows Store | DevTools | 403 Bypasser | YesWeCaido | EvenBetter | QuickSRF | Squash | Shift | JWT Analyzer | Exploit Generator | OmniOAST | Notes+ | Compare | Automatch | SSH Agents | Cerebrum | Drop | Repos | Drop | Scanner | Chatio | Bytecap

Bytecap - File Size Monitor

Monitor and manage workspace file sizes

Size Threshold: 2980MB

1MB | 2GB | 20GB

Enable Additional Warnings: Warning at 75% of threshold | Warning at 90% of threshold

Apply Settings | Refresh Files | Clear Alerts

Caido Project Files (3) - Combined Size: 331.21 MB

Note: These .caido files are monitored as a combined unit for size threshold checks.

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

All Workspace Files (9) - Total: 340.53 MB

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

v0.50.2 (Latest) | Commands | Logs

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](#)

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 Caido workflows for session management testing.

[Open Lab](#)

Reflected XSS Lab

Learn the basics of how to identify reflected XSS with two different vulnerabilities in the same lab.

[Open Lab](#)

HTTP Hunt Lottery

Learn how to use Caido's HTTP History to discover hidden information in responses and access unintended functionality.

[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.

