Internals Deep-Dive

Emile Fugulin

Co-Founder of Caido

@TheSytten

Sytten

emile@caido.io

“Nice” weather in Bornholm

Part 1: Architecture & GraphQL

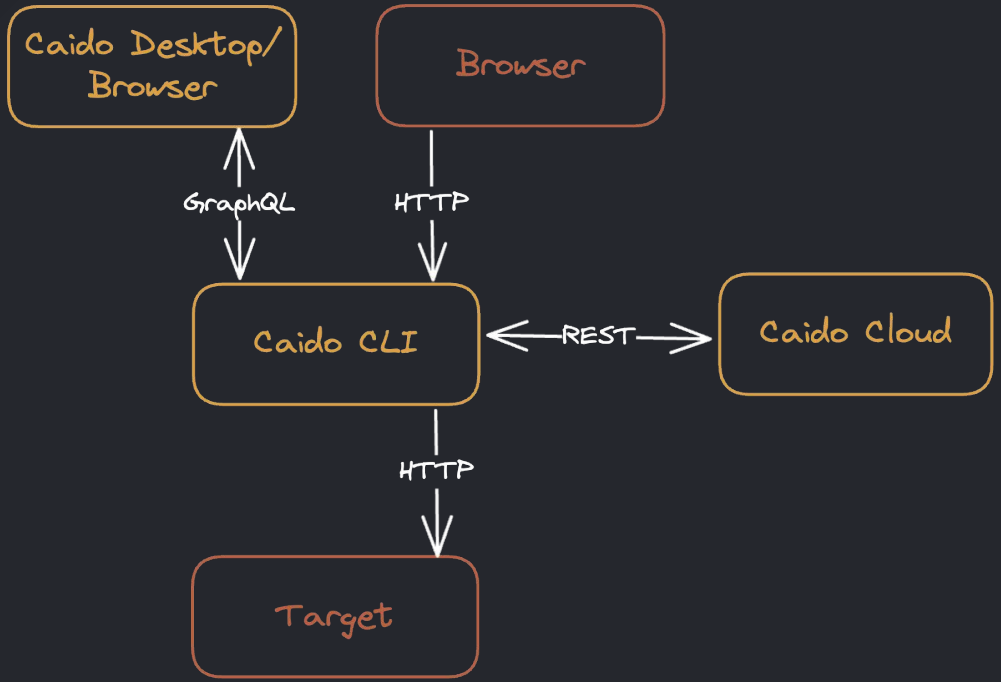
Part 2: Frontend and Backend Plugins

Part 3 (Optional): Workflows

Please asks questions as we go!

URL:
https://github.com/caido/workshop-defcon

Part 1: Architecture & GraphQL


Caido Desktop/
Browser
Browser
GraphQL
HTTP
Caido CLI
REST
Caido Cloud
HTTP
Target

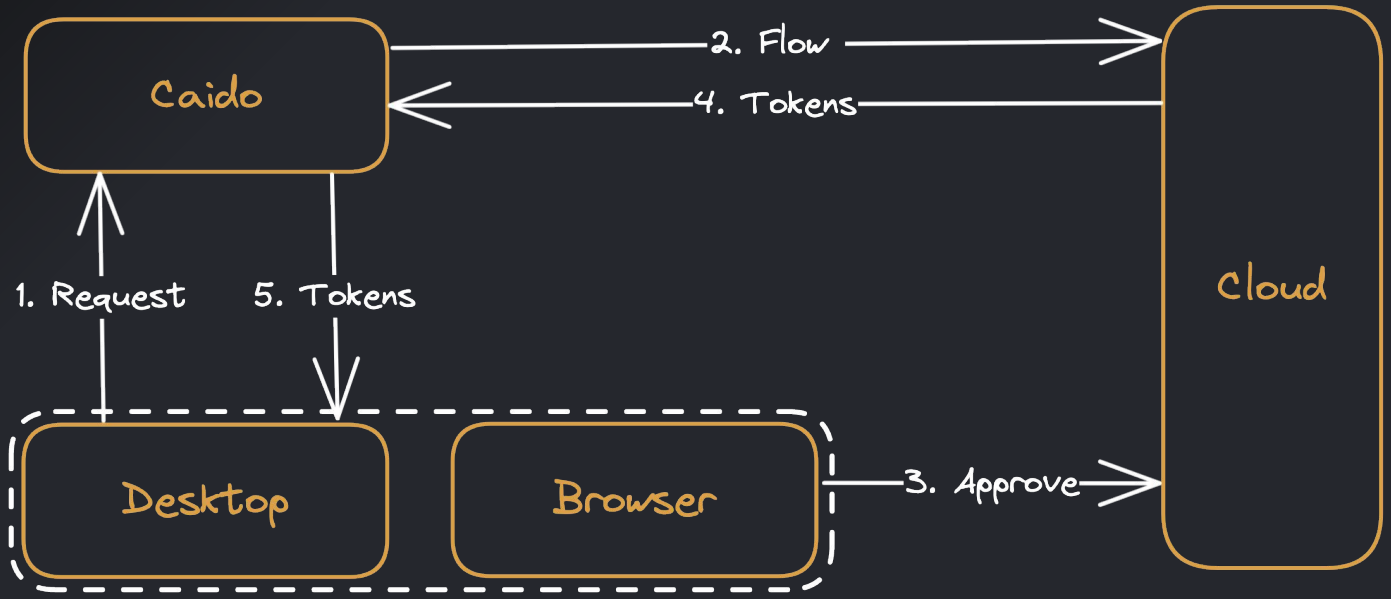
Schema: https://graphql-explorer.caido.io

Playground: http://localhost:8080/graphql

Let's explore!

1. Fetch existing requests
2. Subscribe to new requests
3. Analyze the requests
4. Create findings

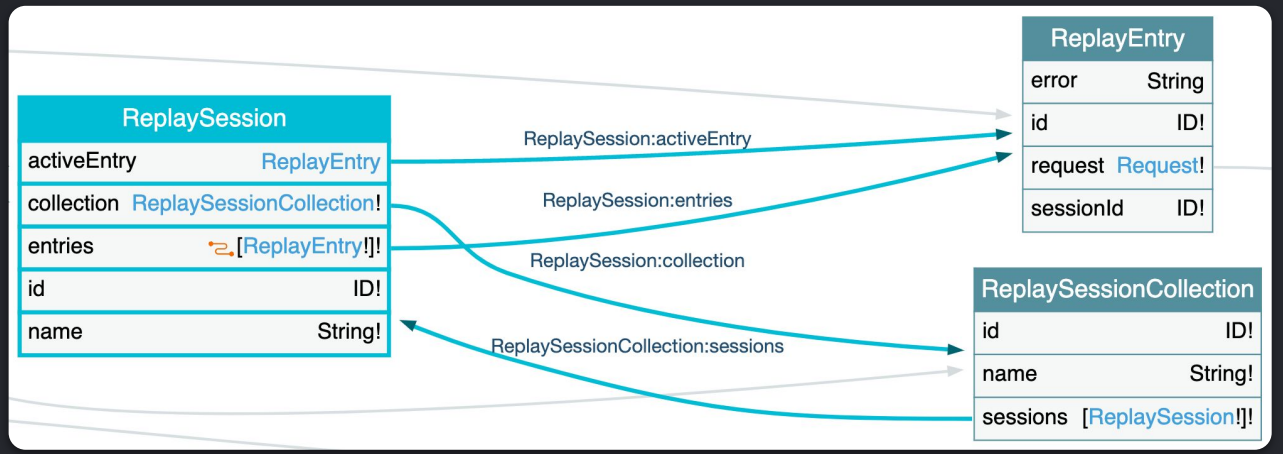
URL: https://github.com/caido/workshop-defcon
Branch: tool-starter



https://docs.caido.io/concepts/internals/authentication.html

- Design
  - Mutations
    - Format: [present tense verb][Model] (deleteRequest)
    - Return: Payload with optional value and error
  - Query
    - Format: [model(s)] (requests)
    - Return: Object or Collection
  - Subscription
    - Format: [past tense verb][Model] (createdProject)
    - Return: Payload with snapshot

- Nesting
  - Entry => Session => Collection



- Connection: Used for lazy loading
  - Input
    - Pagination: Cursor (faster) or Offset
    - Filtering: Migrating to HTTPQL
    - Ordering & Scope: Custom for Caido
  - Output
    - Count
    - PageInfo
  - Example:
    - `requests(after: String, before: String, first: Int, last: Int, filter: FilterClauseRequestResponseInput, order: RequestResponseOrderInput, scopeId: ID): RequestConnection!`
    - `requestsByOffset(limit: Int, offset: Int, filter: FilterClauseRequestResponseInput, order: RequestResponseOrderInput, scopeId: ID): RequestConnection!`

- Snapshot: Allows you to know if an operation was included in a result set
  - Query requests with snapshot 10
  - Subscription createdRequest with snapshot 9 (already in requests, ignore)
  - Subscription createdRequest with snapshot 11 (not in requests, process)

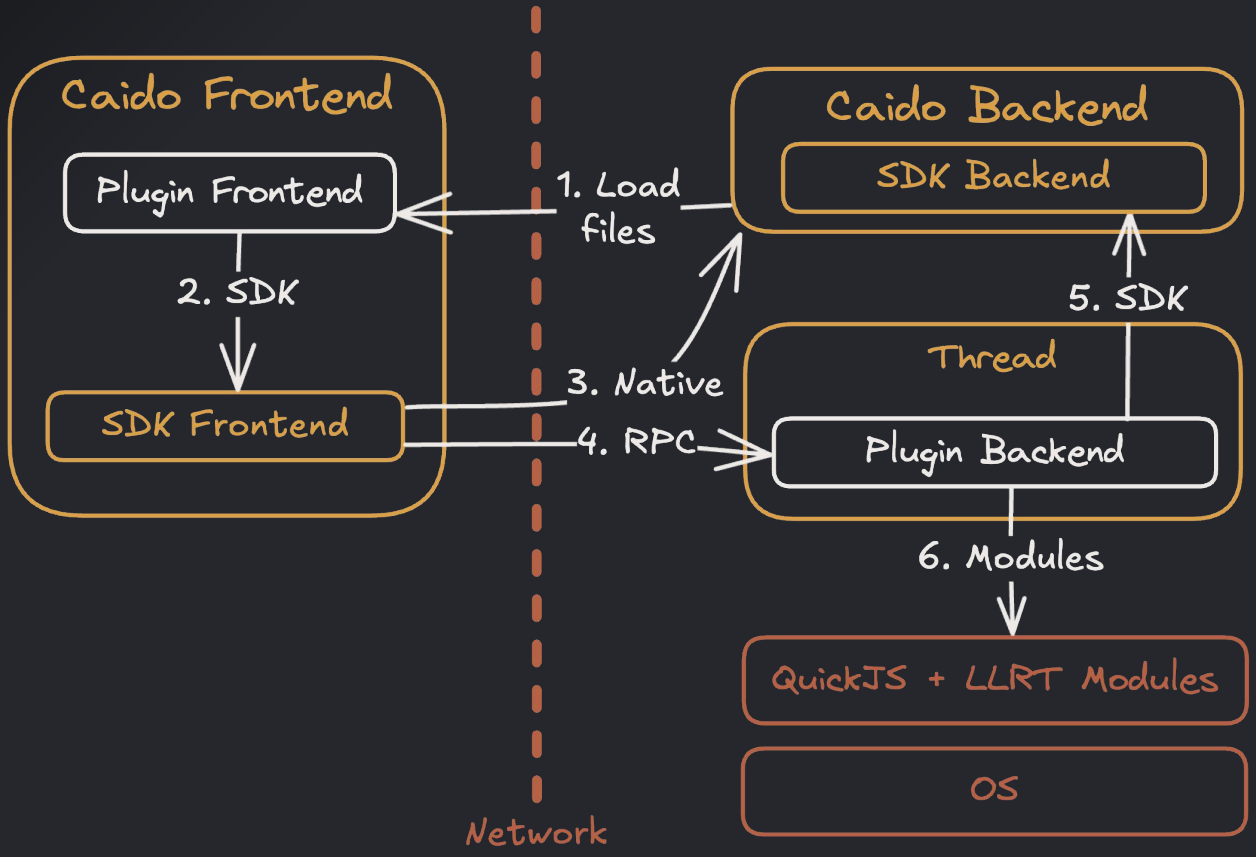
Part 2: Frontend and Backend Plugins

Frontend

- Technologies: HTML, CSS, JS (Bring your own framework)
- Capabilities
  - Interact with Caido Frontend
  - Add UI elements (Menu, Page, etc.)
  - Use the GraphQL API
- It can run multiple times in parallel

Backend

- Technologies: JS (Quickjs on steroids)
- Capabilities
  - Hooks in the system (async only for now)
  - Interact with Caido Backend
  - Interact with the OS (FS, Process, etc)
- It runs once


Caido Frontend
Plugin Frontend
2. SDK
SDK Frontend
1. Load files
3. Native
4. RPC
Network
Caido Backend
SDK Backend
5. SDK
Thread
Plugin Backend
6. Modules
QuickJS + LLRT Modules
OS

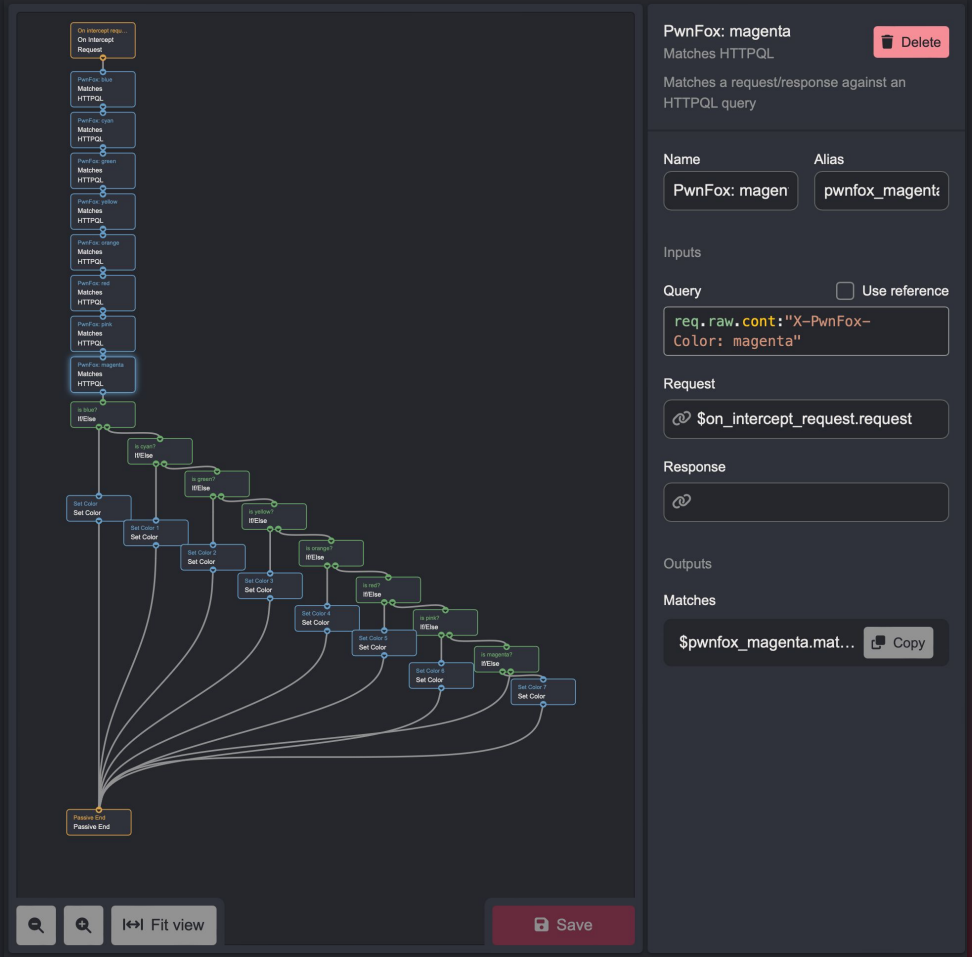
- API to analyze existing requests
- Subscribe to new requests
- Create findings when needed

URL: https://github.com/caido/workshop-defcon
Branch: plugin-starter

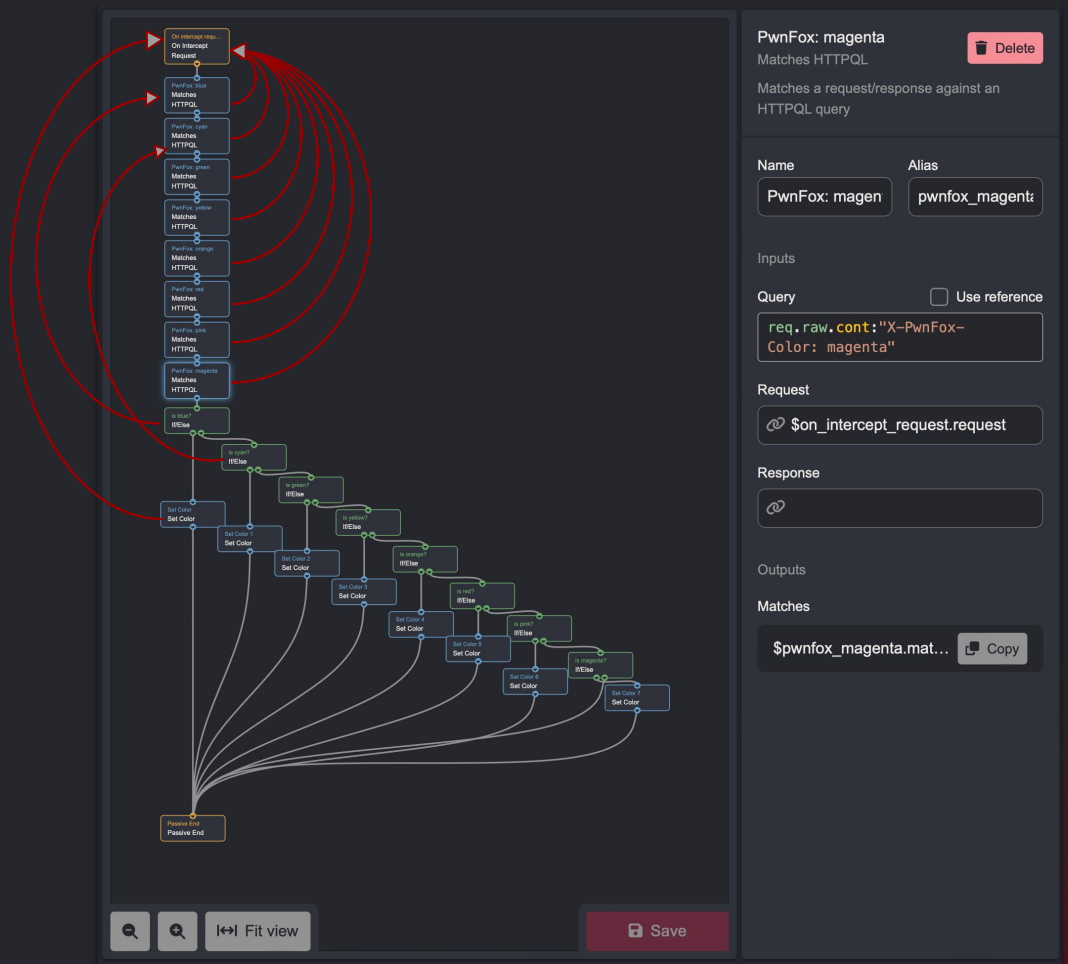
Part 3 (Optional): Workflows

- Convert: Input Bytes, Output Bytes
- Passive: On Proxy Request/Response Event (Async)
- Active: User trigger on Request

- Execution flow
  - Lines on the graph
  - Require a Control node to diverge



- Execution flow
  - Lines on the graph
  - Require a Control node to diverge
- Data flow
  - Each node has inputs and outputs
  - References link them
  - Doesn't require a direct relation



- JSON file representing a graph
  - https://github.com/caido/workflows/blob/main/convert/URL%20Decode/URL%20Decode.json

Node

```
{
  "id": 1,
  "alias": "end",
  "name": "End",
  "definition_id": "caido/convert-end",
  "version": "^0.1.0",
  "inputs": [
    {
      "alias": "data",
      "value": {
        "kind": "ref",
        "data": "$url_decode.data"
      }
    }
  ],
  "display": {
    "x": 0,
    "y": 230
  }
},
```

Edge

```
"edges": [
  {
    "source": {
      "node_id": 0,
      "exec_alias": "exec"
    },
    "target": {
      "node_id": 2,
      "exec_alias": "exec"
    }
  },
```

URL: https://docs.caido.io/guides/workflows/jwt_decode.html

Let's explore!

Contact

 info@caido.io

 @CaidoIO

 @caidoio@infosec.exchange

 https://links.caido.io/discord

 https://calendly.com/caido-emile