Doyensec GraphQL

# GraphQL in Pills

**Describe** your data

```
type Project {
  name: String
  tagline: String
  contributors: [User]
}
```

# GraphQL in Pills

## **Ask** for what you want

```
{
  project(name: "GraphQL") {
    tagline
  }
}
```

# GraphQL in Pills

## **Get** predictable results

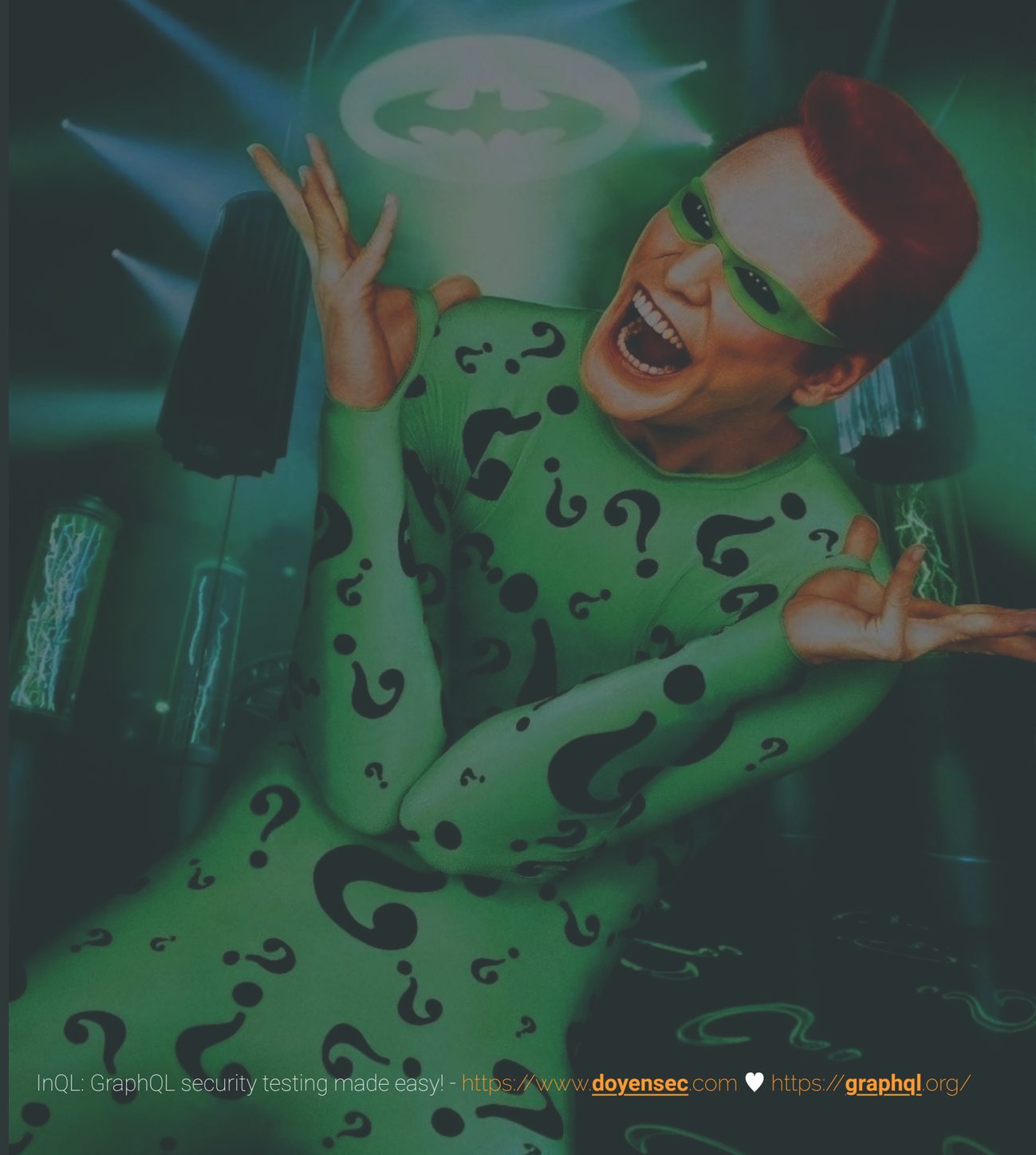
```
{
  "project": {
    "tagline": "A query language for APIs"
  }
}
```

# GraphQL in Action

## Request

```
POST /graphql HTTP/1.1
Host: domain2.local:8080
User-Agent: Mozilla/5.0 ...
Accept: application/json

{"query":"query testCORS {
  allDogs{
    name
  }
}",
"variables":null,
"operationName":"testCORS"}
```



# GraphQL in Action

## Response

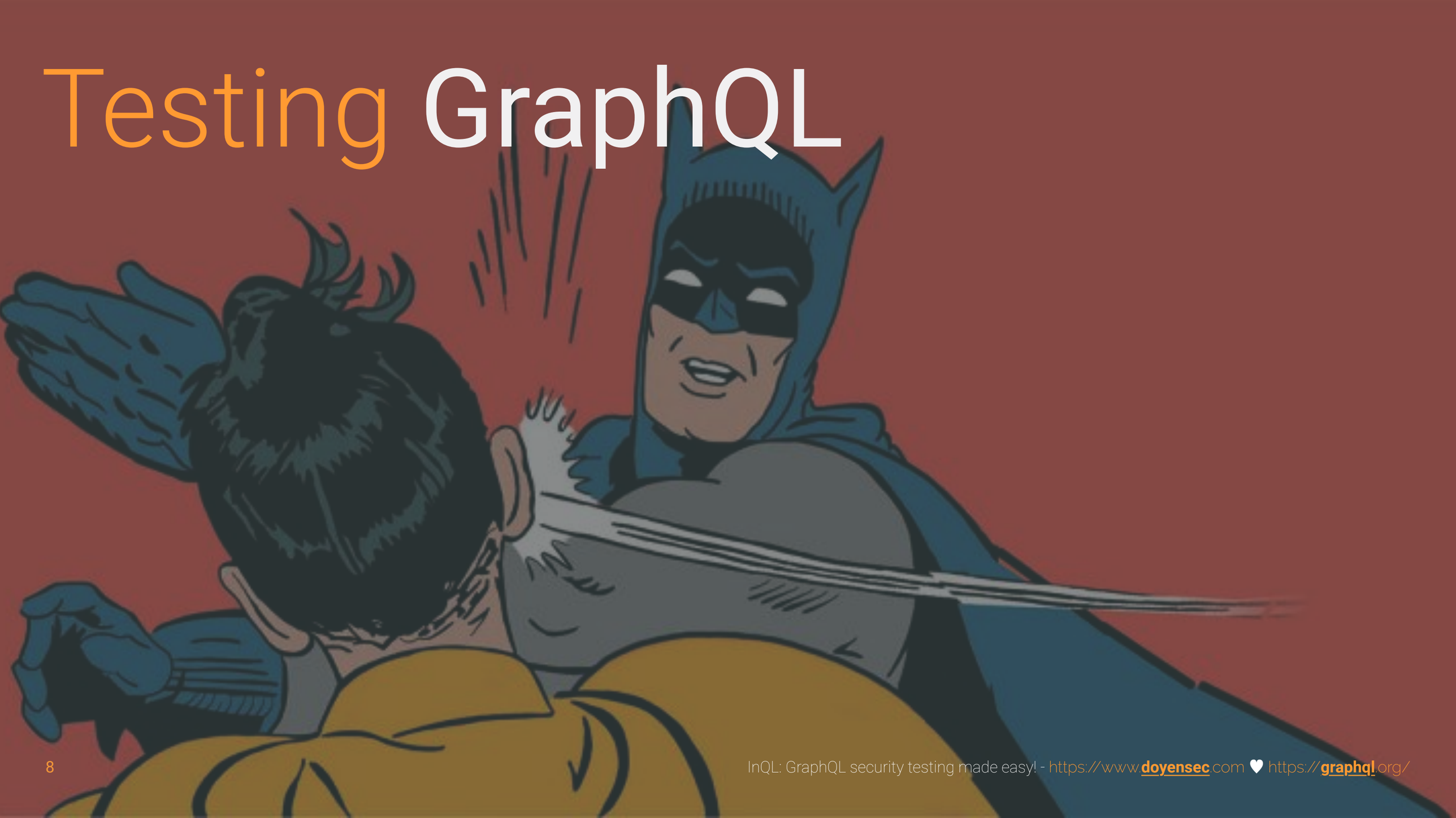
HTTP/1.1 200 OK
Connection: close
Content-Type: application/json

{"data":{"allDogs":[{"name":"Abi"},...

# GraphQL Vulnerabilities

- Missing Authentication/Authorization
- Resource Exhaustion
- Information Exposure
- IDOR

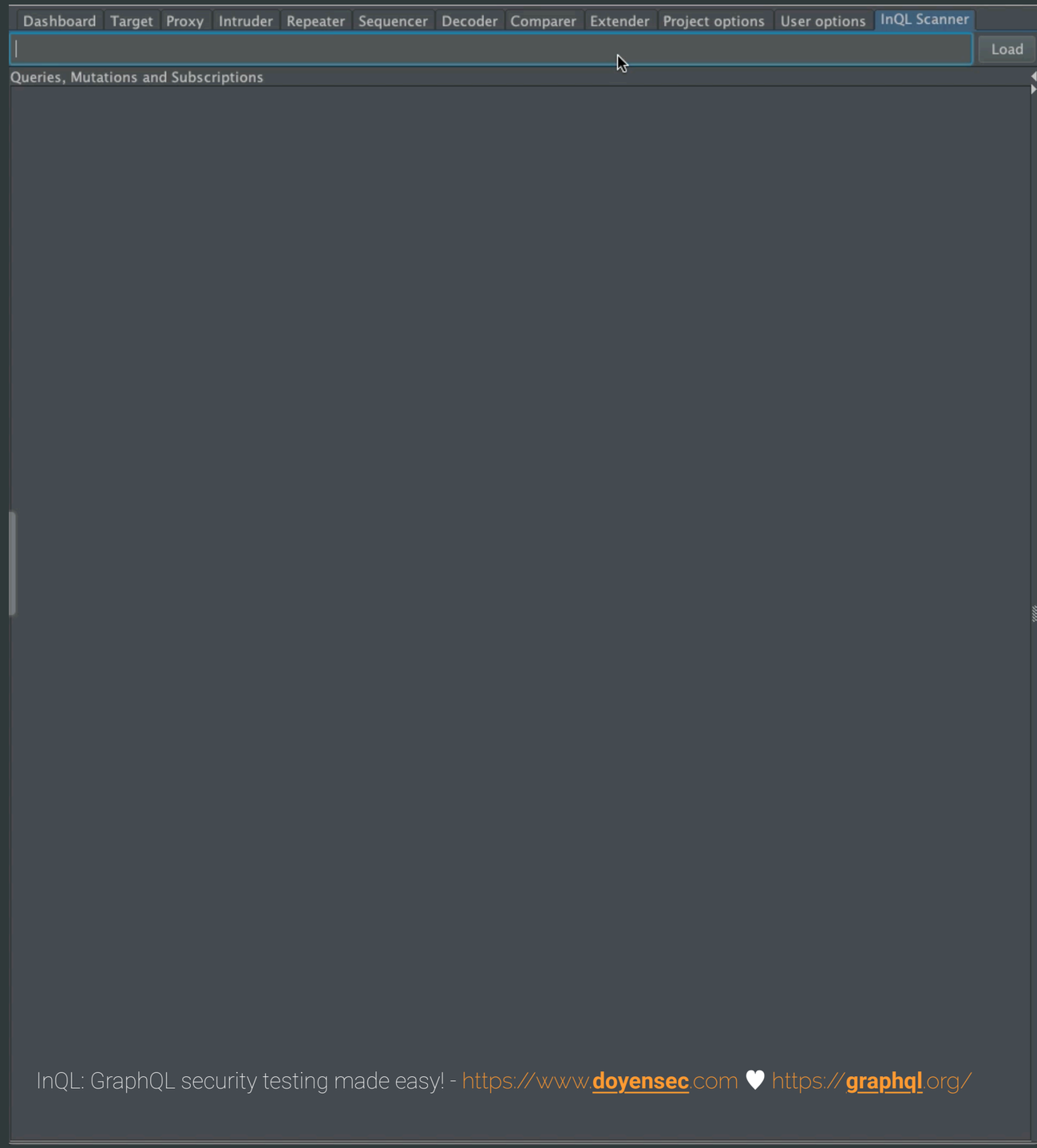
# Testing GraphQL

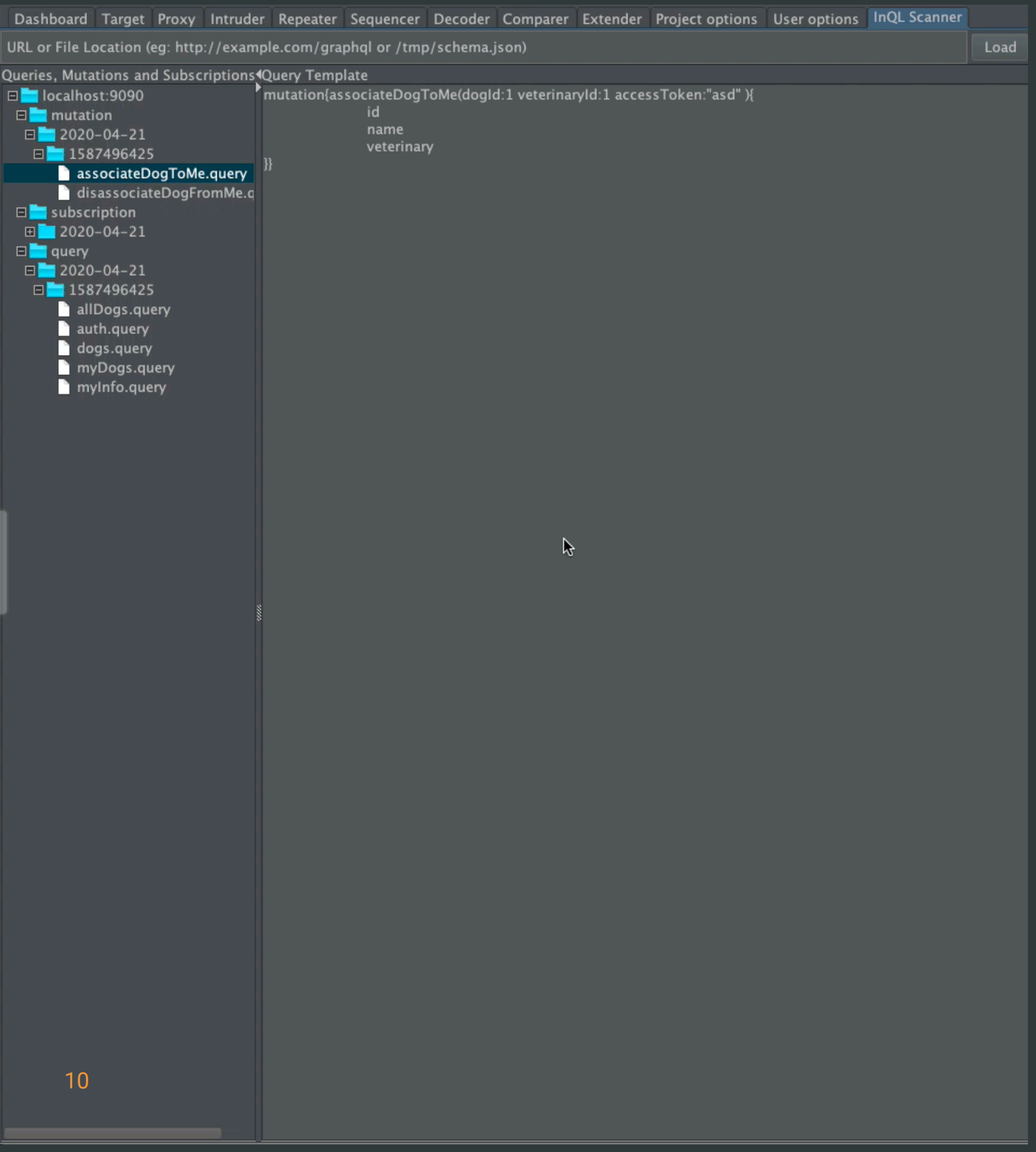


# InQL in Action

**In**trospection Graph**QL**

1. Query introspection endpoint
2. Generate API documentation
3. Blackbox approach
4. Works offline
5. Burp plugin **and** python package






# InQL in Action

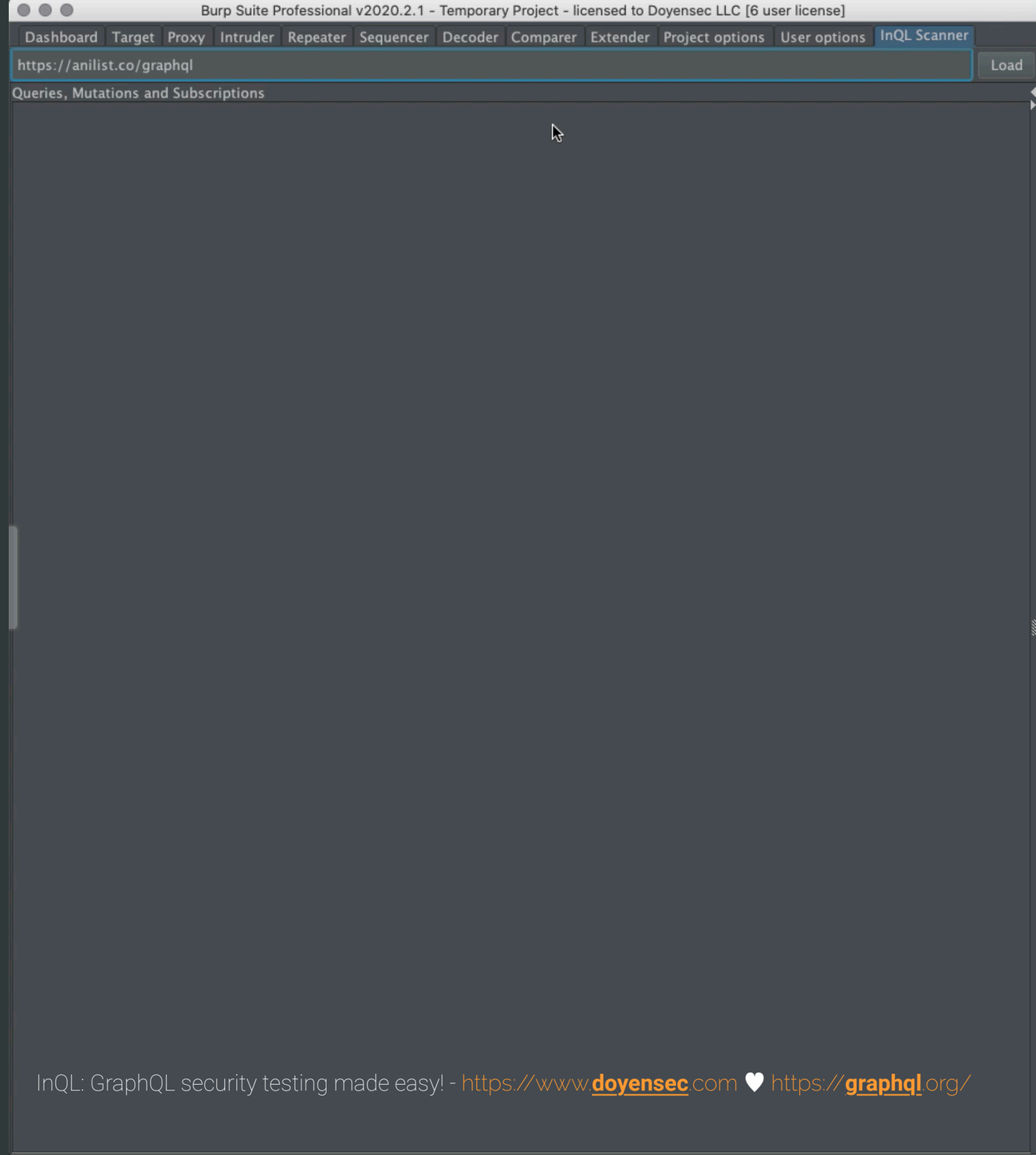
## **Detect** GraphQL Endpoints

1. Active Scanner Support
2. Passive Scanner Support

# InQL in Action

## **Send** to Repeater

1. Generates HTTP Header
2. Automatic Authentication
3. Custom Header Support



Doyensec GraphQL

thypon nJoyneer