FWDSEC

We Taught Burp How to Speak GraphQL

Jared Meit

2024-5-27 | v0.2

About Me

Jared Meit

- Senior Application Security Consultant
- 16 years of web API design and development
- 7 years in security professionally + decades unprofessionally
- Designations & Certifications: OSWE, Azure Security Engineer

Quick Poll:

1. Who has heard of GraphQL?
2. Who uses Burp Suite?
3. Who has pentested GraphQL?
4. Who has pentested GraphQL with Burp?

Overview

- Intro (Already done)
- What is GraphQL
- GraphQL weaknesses + attacks
- Current security tools landscape
- Overview of my tool
- Demo
- Q&A

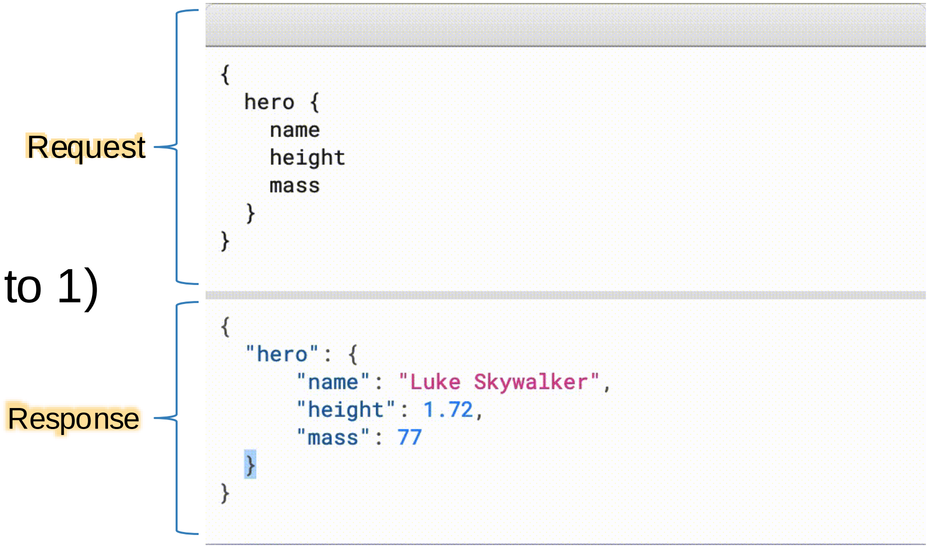
What even, like, is GraphQL?

FWDSEC

GraphQL

“A query language for your API"

- ✓ Body format
- ✓ Reduces calls to API
- ✓ Reduces endpoints (sometimes to 1)



```
{
  hero {
    name
    height
    mass
  }
}
```

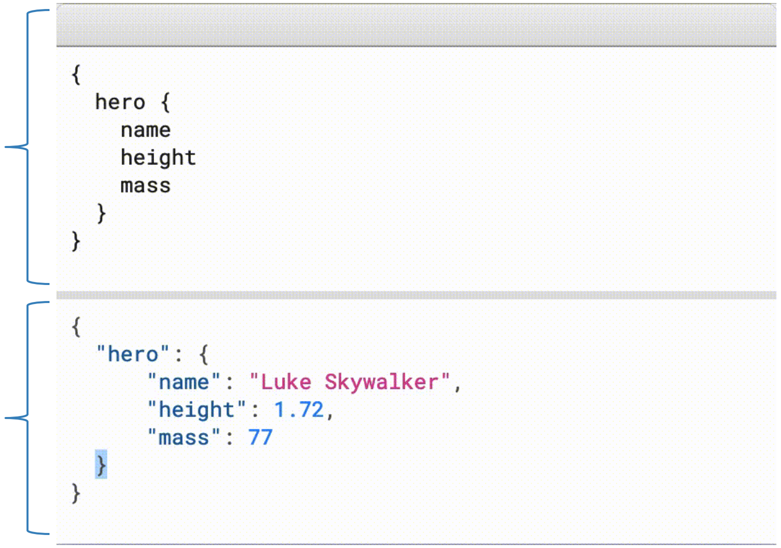
```
{
  "hero": {
      "name": "Luke Skywalker",
      "height": 1.72,
      "mass": 77
  }
}
```

FWDSEC

GraphQL

"A query language for your API"

- ✓ Body format
- ✓ Reduces calls to API
- ✓ Reduces endpoints (sometimes to 1)
- ✓ Just as vulnerable as regular REST
- ✓ Bonus DoS vulns
- ✓ It self-documents (Introspection)



Request

```
{
  hero {
    name
    height
    mass
  }
}
```

Response

```
{
  "hero": {
      "name": "Luke Skywalker",
      "height": 1.72,
      "mass": 77
  }
}
```

FWDSEC

What is GraphQL?

GraphQL

In your application code:

1. Import GraphQL library
2. Define GraphQL schema
3. Define “resolvers” that respond to the queries

Request Types:

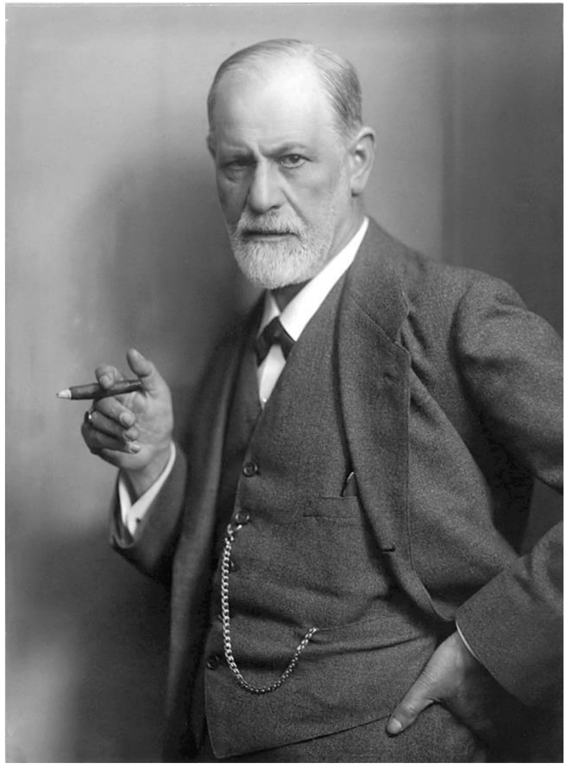
- Query
- Mutation
- Subscription

FWDSEC

GraphQL

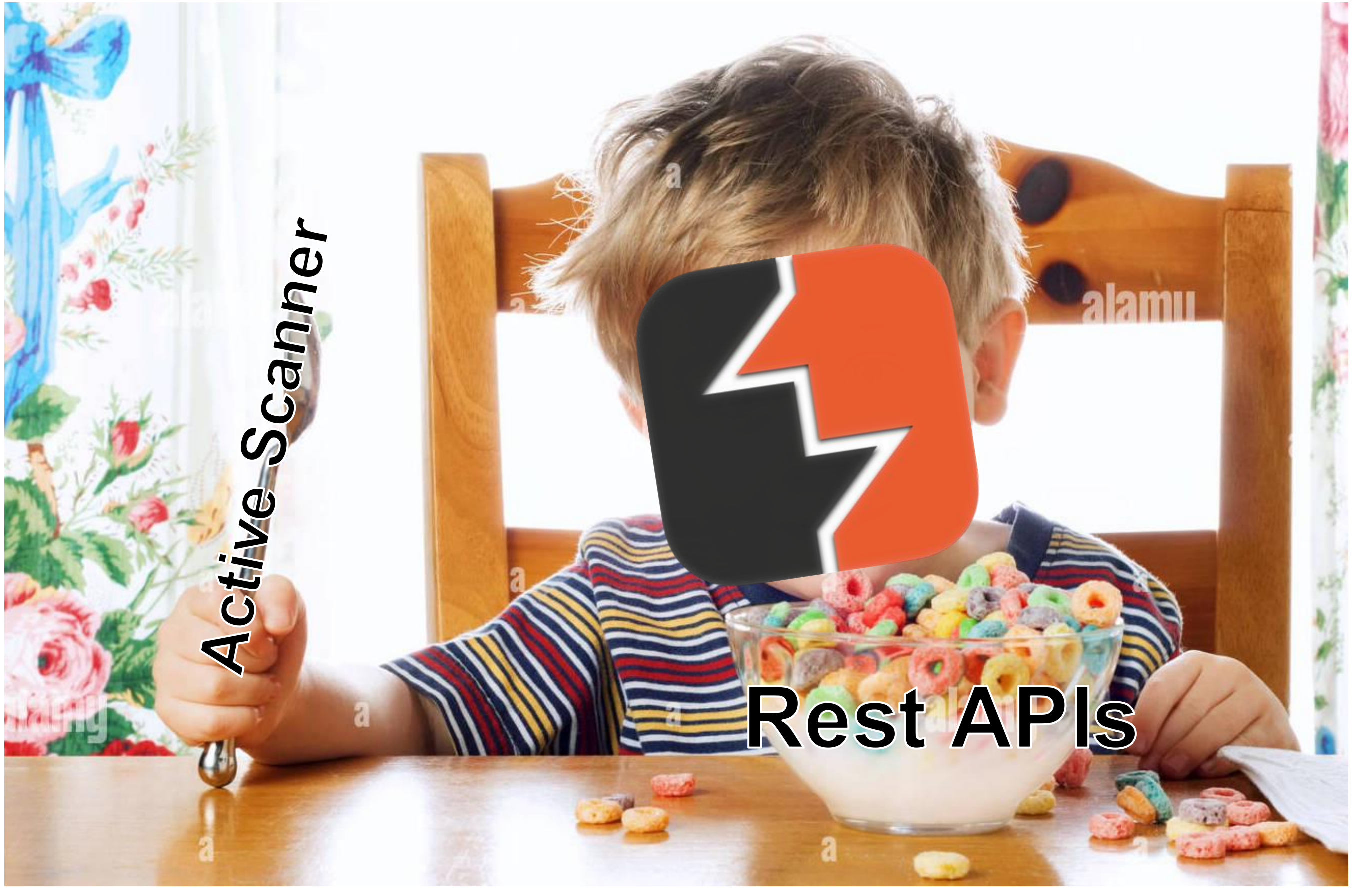
Introspection

- Special query
- Fetches entire schema
- Useful for frontend
- Vulnerability?



FWDSEC

What is GraphQL?



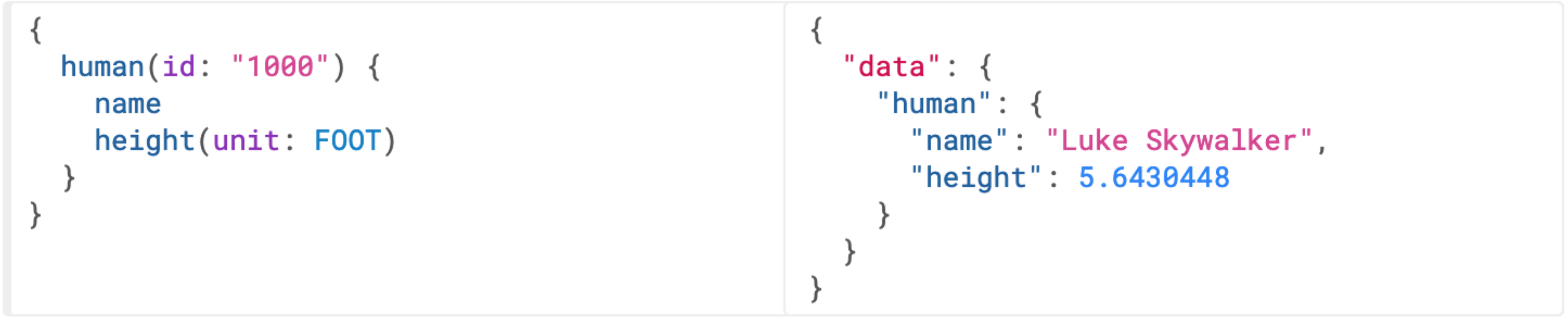
FWDSEC

Safe Injection Sites

FWDSEC

Ohhhhhhhhh… It takes params.

- Standard and custom data types



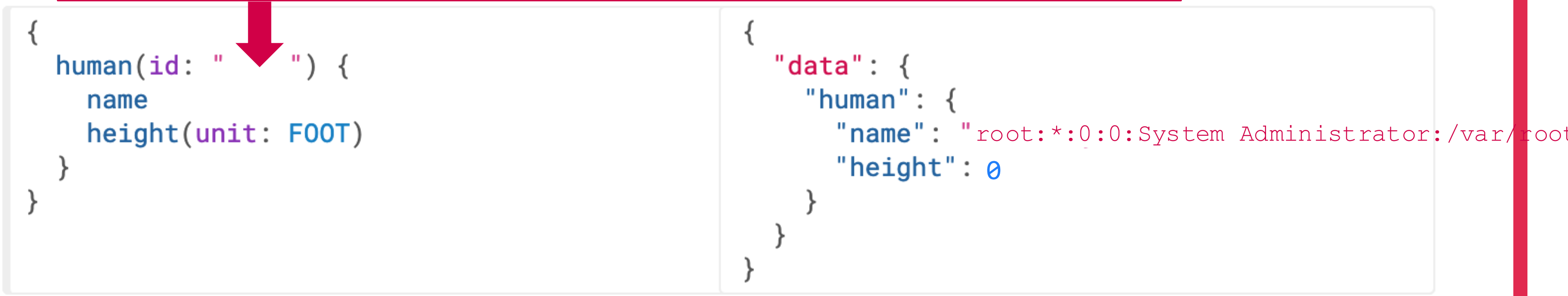
```
{
  human(id: "1000") {
    name
    height(unit: FOOT)
  }
}
```

```
{
  "data": {
    "human": {
      "name": "Luke Skywalker",
      "height": 5.6430448
    }
  }
}
```

FWDSEC

Old payloads
New locations

```
' UNION ALL SELECT LOAD_FILE('/etc/passwd') --
```



```
{
  human(id: "      ") {
    name
    height(unit: FOOT)
  }
}
```

```
{
  "data": {
    "human": {
      "name": "root:*:0:0:System Administrator:/var/root
      "height": 0
    }
  }
}
```

FWDSEC

Beautified:

```
{
  human(id: "1000") {
    name
    height(unit: FOOT)
  }
}
```

```
{
  "data": {
    "human": {
      "name": "Luke Skywalker",
      "height": 5.6430448
    }
  }
}
```

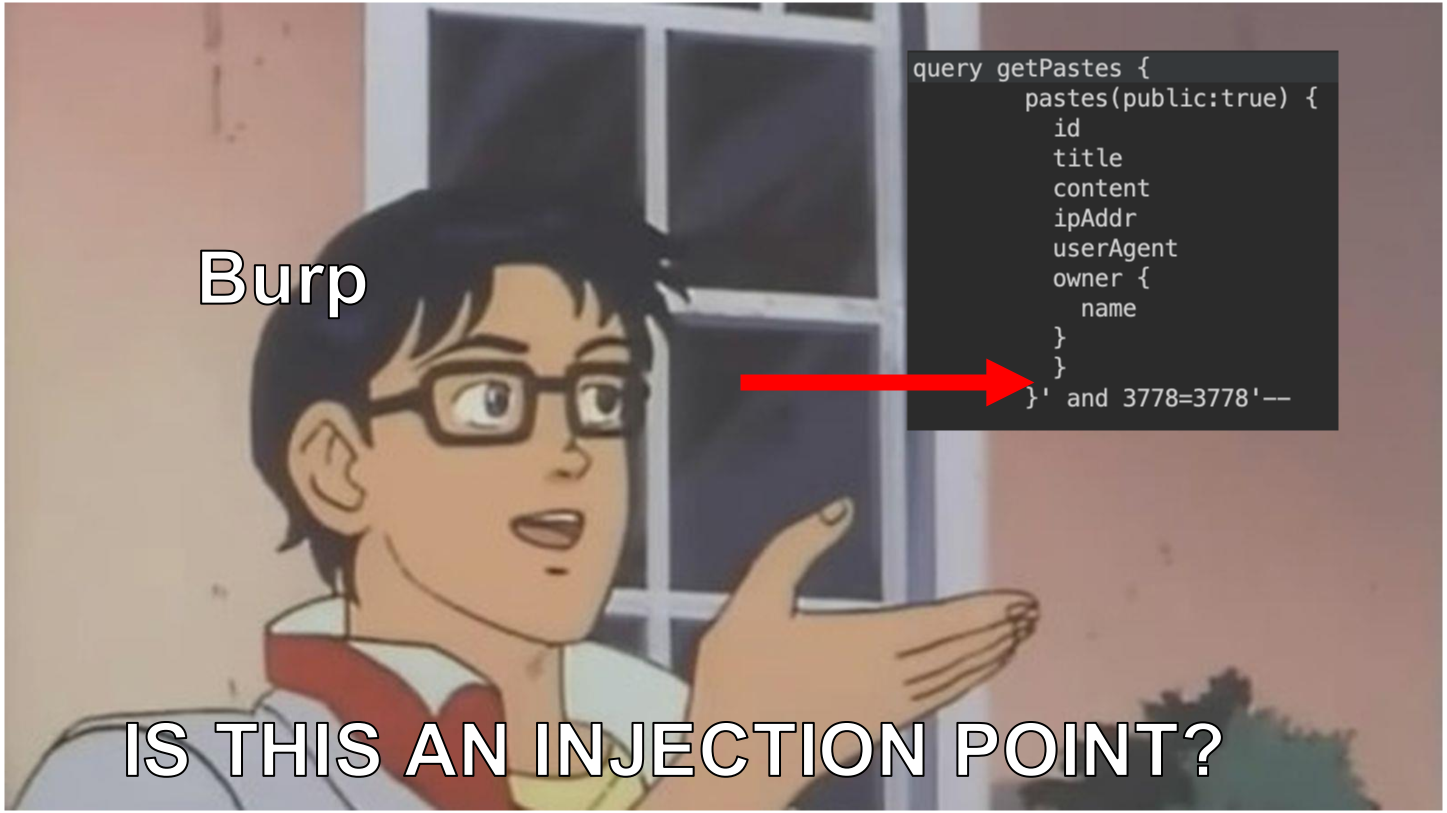
Actual request body:

```
1. {"query": "query {\n\thuman(id:\"1000\")
   {\n\t\tname\n\t\theight(unit:FOOT)\n}"}
```

FWDSEC

Burp is like:

FWDSEC



```
query getPastes {
        pastes(public:true) {
          id
          title
          content
          ipAddr
          userAgent
          owner {
            name
          }
          }
        }' and 3778=3778'--
```

Gently coaching Burp without being condescending

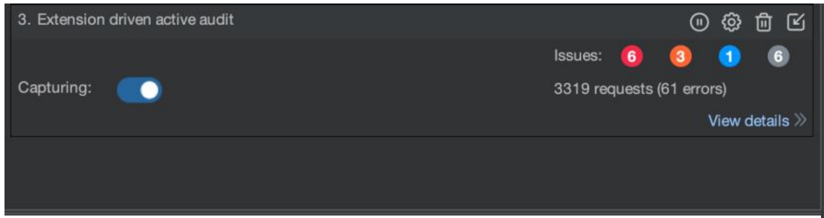
FWDSEC

Goals:

- Burp extension
- Auto find every possible request
- Leverage Active Scan

FWDSEC

Solution



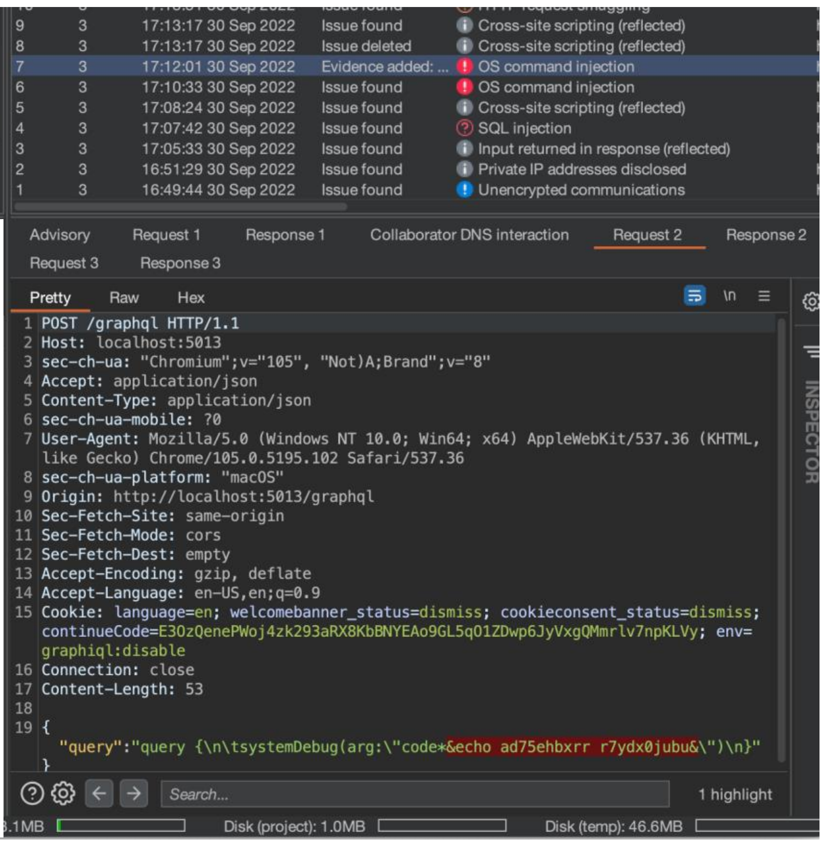
3. Extension driven active audit

Issues: 6 3 1 6

Capturing:

3319 requests (61 errors)

View details



```
9   3   17:13:17 30 Sep 2022   Issue found         Cross-site scripting (reflected)
8   3   17:13:17 30 Sep 2022   Issue deleted       Cross-site scripting (reflected)
7   3   17:12:01 30 Sep 2022   Evidence added: ... OS command injection
6   3   17:10:33 30 Sep 2022   Issue found         OS command injection
5   3   17:08:24 30 Sep 2022   Issue found         Cross-site scripting (reflected)
4   3   17:07:42 30 Sep 2022   Issue found         SQL injection
3   3   17:05:33 30 Sep 2022   Issue found         Input returned in response (reflected)
2   3   16:51:29 30 Sep 2022   Issue found         Private IP addresses disclosed
1   3   16:49:44 30 Sep 2022   Issue found         Unencrypted communications
```

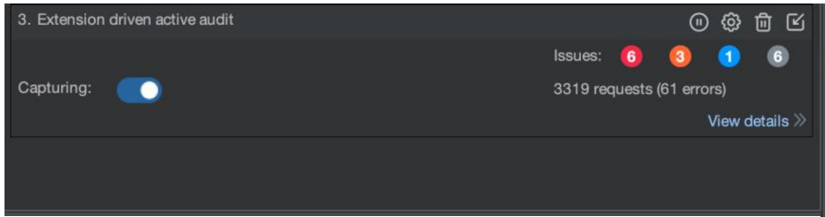
```
POST /graphql HTTP/1.1
Host: localhost:5013
sec-ch-ua: "Chromium";v="105", "Not)A;Brand";v="8"
Accept: application/json
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.5195.102 Safari/537.36
sec-ch-ua-platform: "macOS"
Origin: http://localhost:5013/graphql
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=E3OzQenePWoj4zk293aRX8KbBNYEAo9GL5q01ZDwp6JyVxgQMmrlv7npKLVy; env=
graphiql:disable
Connection: close
Content-Length: 53

{
  "query":"query {\n\tsystemDebug(arg:\"code*&echo ad75ehbxrr r7ydx0jubu&\")\n}"
}
```

Goals:

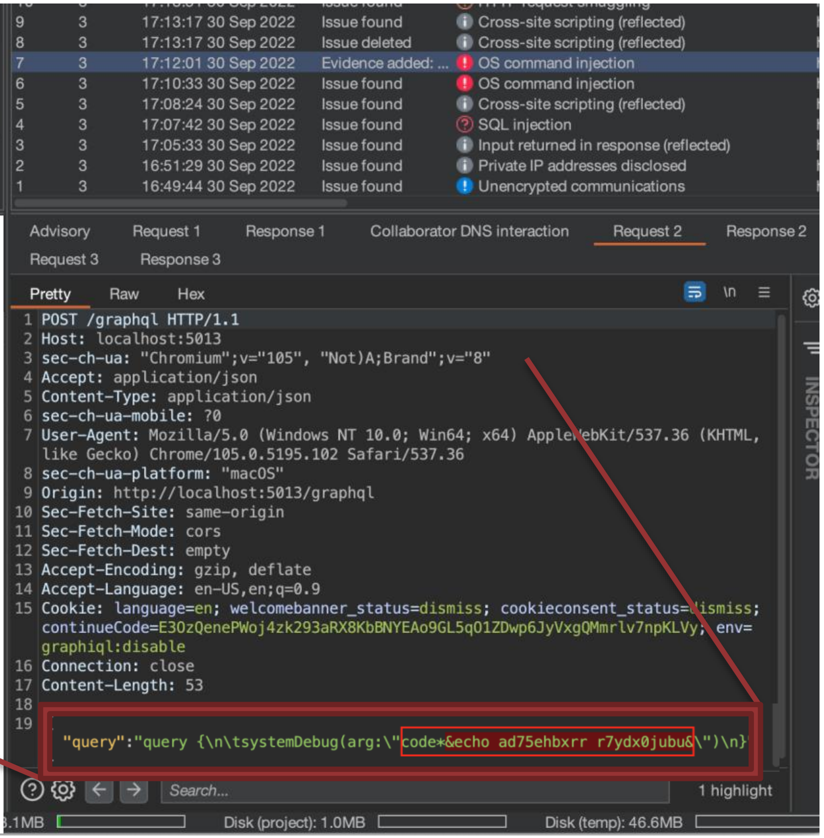
- Burp extension
- Auto find every possible request
- Leverage Active Scan

FWDSEC

Solution



```
3. Extension driven active audit
                    Issues: 6  3  1  6
Capturing:          3319 requests (61 errors)
                    View details »
```



```
9   3   17:13:17 30 Sep 2022   Issue found          Cross-site scripting (reflected)
8   3   17:13:17 30 Sep 2022   Issue deleted        Cross-site scripting (reflected)
7   3   17:12:01 30 Sep 2022   Evidence added: ...  OS command injection
6   3   17:10:33 30 Sep 2022   Issue found          OS command injection
5   3   17:08:24 30 Sep 2022   Issue found          Cross-site scripting (reflected)
4   3   17:07:42 30 Sep 2022   Issue found          SQL injection
3   3   17:05:33 30 Sep 2022   Issue found          Input returned in response (reflected)
2   3   16:51:29 30 Sep 2022   Issue found          Private IP addresses disclosed
1   3   16:49:44 30 Sep 2022   Issue found          Unencrypted communications
```

```
POST /graphql HTTP/1.1
Host: localhost:5013
sec-ch-ua: "Chromium";v="105", "Not)A;Brand";v="8"
Accept: application/json
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.5195.102 Safari/537.36
sec-ch-ua-platform: "macOS"
Origin: http://localhost:5013/graphql
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=E3OzQenePWoj4zk293aRX8KbBNYEAo9GL5q01ZDwp6JyVxgQMmrlv7npKLVy; env=
graphiql:disable
Connection: close
Content-Length: 53


 "query":"query {\n\tsystemDebug(arg:\"code*&echo ad75ehbxrr r7ydx0jubu&\")\n}
```

```
Search...                                   1 highlight
.1MB     Disk (project): 1.0MB     Disk (temp): 46.6MB
```

Goals:

- Burp extension
- Auto find every possible request
- Leverage Active Scan

FWDSEC

Auto GQL™ (aka Burp GraphQL Auto Scanner)

- Give it a URL
- Customize headers (optional)
- Click “Go”

Auto GQL™ (aka Burp GraphQL Auto Scanner)

- Give it a URL
- Customize headers (optional)
- Click “Go”

    1. Runs Introspection Query
    2. Determines every possible request
    3. Finds insertion/injection points
    4. Sends them all to Active Scanner
    5. You: profit

FWDSEC

Demo Time

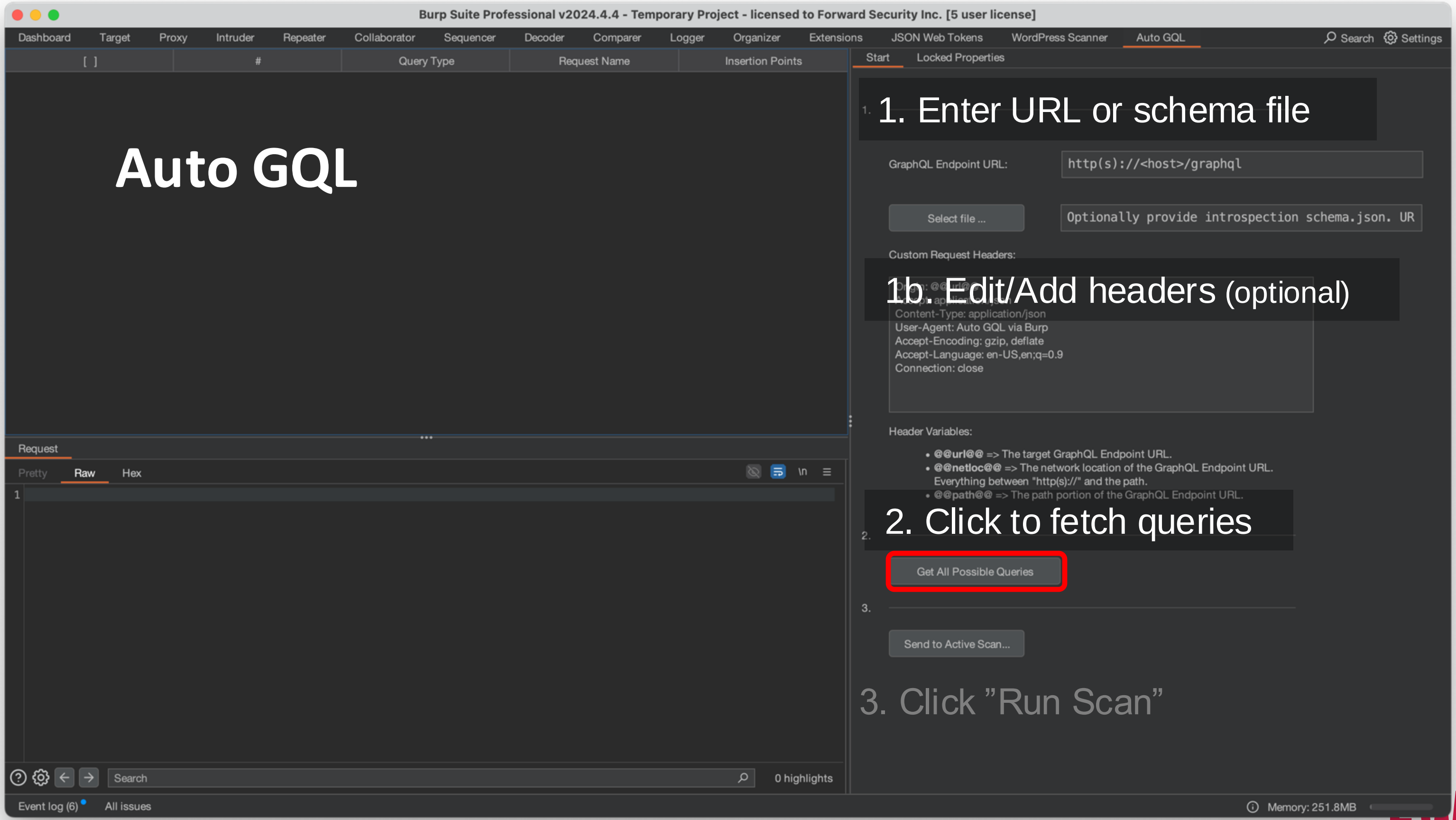
FWDSEC

Auto GQL™ (aka Burp GraphQL Auto Scanner)

- Give it a URL or schema file
- Customize headers (optional)
- Click “Go”

1. Runs Introspection Query
2. Determines every possible request
3. Finds insertion/injection points
4. Sends them all to Active Scanner
5. You: profit

Solution



Burp Suite Professional v2024.4.4 - Temporary Project - licensed to Forward Security Inc. [5 user license]

Auto GQL

1. Enter URL or schema file

GraphQL Endpoint URL: http(s)://<host>/graphql

Optionally provide introspection schema.json. UR

Custom Request Headers:

1b. Edit/Add headers (optional)

```
Content-Type: application/json
User-Agent: Auto GQL via Burp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

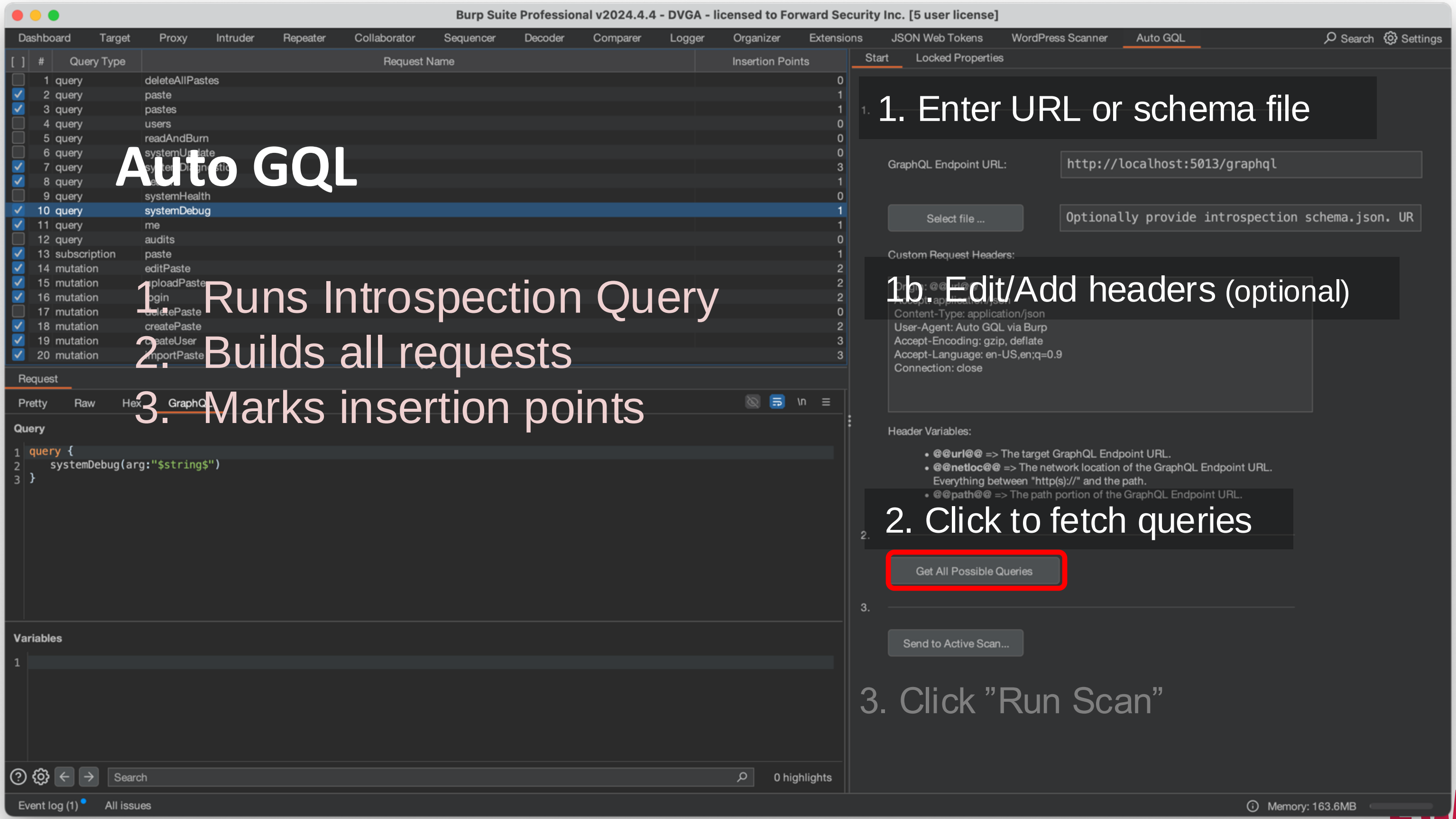
Header Variables:

- @@url@@ => The target GraphQL Endpoint URL.
- @@netloc@@ => The network location of the GraphQL Endpoint URL. Everything between "http(s)://" and the path.
- @@path@@ => The path portion of the GraphQL Endpoint URL.

2. Click to fetch queries

3. Click "Run Scan"

Solution



Burp Suite Professional v2024.4.4 - DVGA - licensed to Forward Security Inc. [5 user license]

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions JSON Web Tokens WordPress Scanner Auto GQL
Search Settings
Start Locked Properties

[ ]	#	Query Type	Request Name	Insertion Points
☐	1	query	deleteAllPastes	0
✓	2	query	paste	1
✓	3	query	pastes	1
☐	4	query	users	0
☐	5	query	readAndBurn	0
☐	6	query	systemUpdate	0
✓	7	query	systemDiagnostics	3
✓	8	query	[illegible]	1
☐	9	query	systemHealth	0
✓	10	query	systemDebug	1
✓	11	query	me	1
☐	12	query	audits	0
✓	13	subscription	paste	1
✓	14	mutation	editPaste	2
✓	15	mutation	uploadPaste	2
✓	16	mutation	login	2
☐	17	mutation	deletePaste	0
✓	18	mutation	createPaste	2
✓	19	mutation	createUser	3
✓	20	mutation	importPaste	3

Query

```
query {
  systemDebug(arg:"$string$")
}
```

Variables

Auto GQL

1. Runs Introspection Query
2. Builds all requests
3. Marks insertion points

1. Enter URL or schema file

GraphQL Endpoint URL: http://localhost:5013/graphql

Select file ... Optionally provide introspection schema.json. UR

Custom Request Headers:

1b. Edit/Add headers (optional)

```
Content-Type: application/json
User-Agent: Auto GQL via Burp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Header Variables:

- @@url@@ => The target GraphQL Endpoint URL.
- @@netloc@@ => The network location of the GraphQL Endpoint URL. Everything between "http(s)://" and the path.
- @@path@@ => The path portion of the GraphQL Endpoint URL.

2. Click to fetch queries

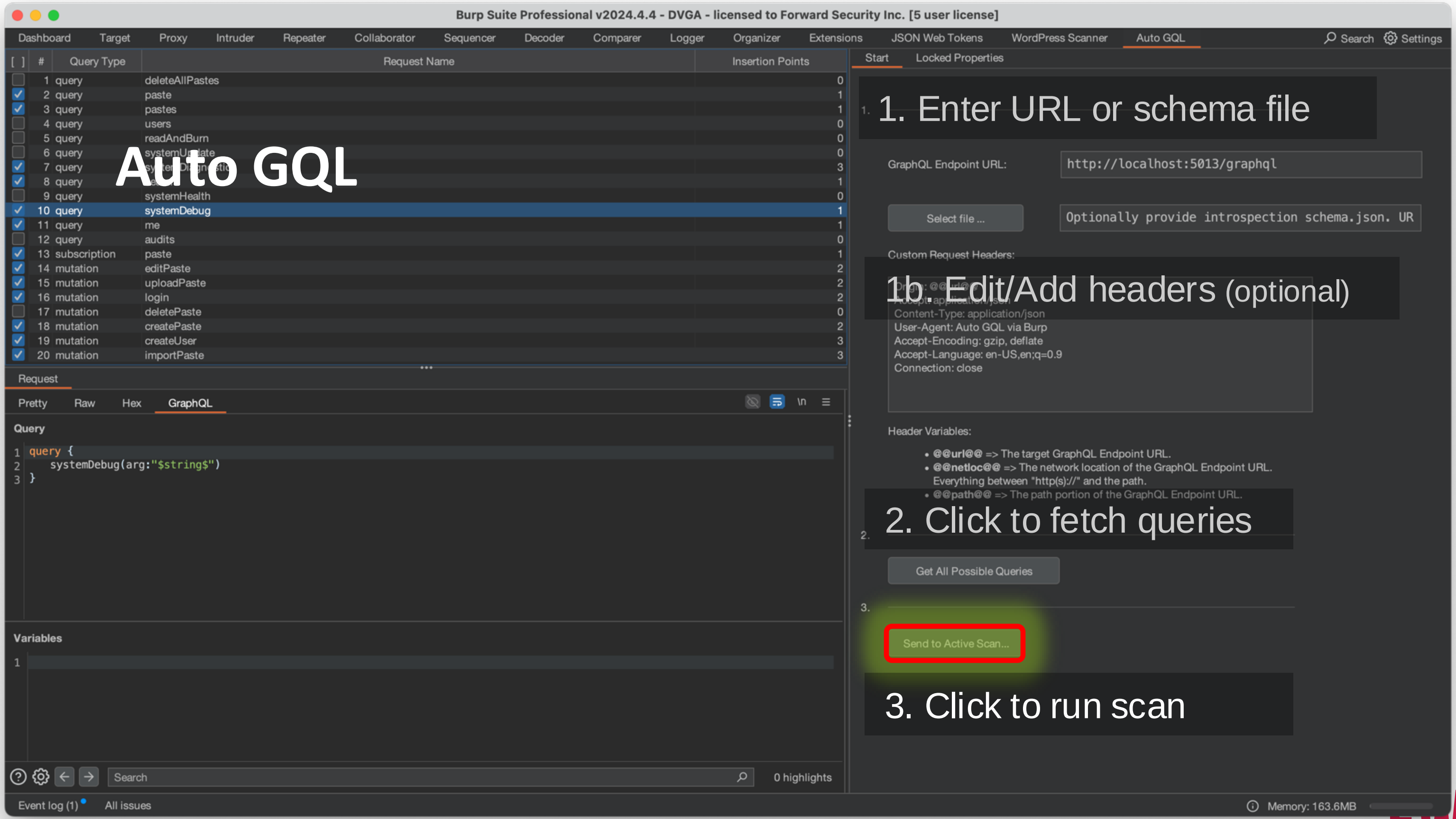
Get All Possible Queries

Send to Active Scan...

3. Click "Run Scan"

FWDSEC

Solution



Burp Suite Professional v2024.4.4 - DVGA - licensed to Forward Security Inc. [5 user license]

Auto GQL

[ ]	#	Query Type	Request Name	Insertion Points
☐	1	query	deleteAllPastes	0
✓	2	query	paste	1
✓	3	query	pastes	1
☐	4	query	users	0
☐	5	query	readAndBurn	0
☐	6	query	systemUpdate	0
✓	7	query	[illegible]	3
✓	8	query	[illegible]	1
☐	9	query	systemHealth	0
✓	10	query	systemDebug	1
✓	11	query	me	1
☐	12	query	audits	0
✓	13	subscription	paste	1
✓	14	mutation	editPaste	2
✓	15	mutation	uploadPaste	2
✓	16	mutation	login	2
☐	17	mutation	deletePaste	0
✓	18	mutation	createPaste	2
✓	19	mutation	createUser	3
✓	20	mutation	importPaste	3

Request

Query

```
query {
  systemDebug(arg:"$string$")
}
```

Variables

1. Enter URL or schema file

GraphQL Endpoint URL: `http://localhost:5013/graphql`

Select file ... `Optionally provide introspection schema.json. UR`

Custom Request Headers:

1b. Edit/Add headers (optional)

```
Content-Type: application/json
User-Agent: Auto GQL via Burp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Header Variables:

- @@url@@ => The target GraphQL Endpoint URL.
- @@netloc@@ => The network location of the GraphQL Endpoint URL. Everything between "http(s)://" and the path.
- @@path@@ => The path portion of the GraphQL Endpoint URL.

2. Click to fetch queries

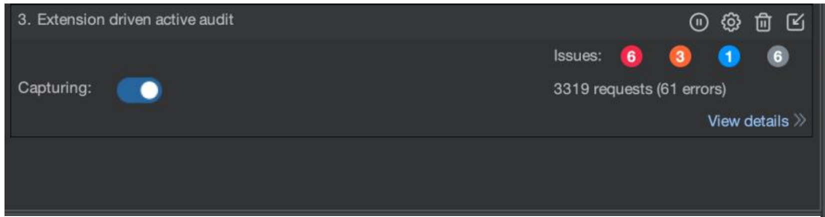
Get All Possible Queries

3. Send to Active Scan...

3. Click to run scan

FWDSEC

Solution



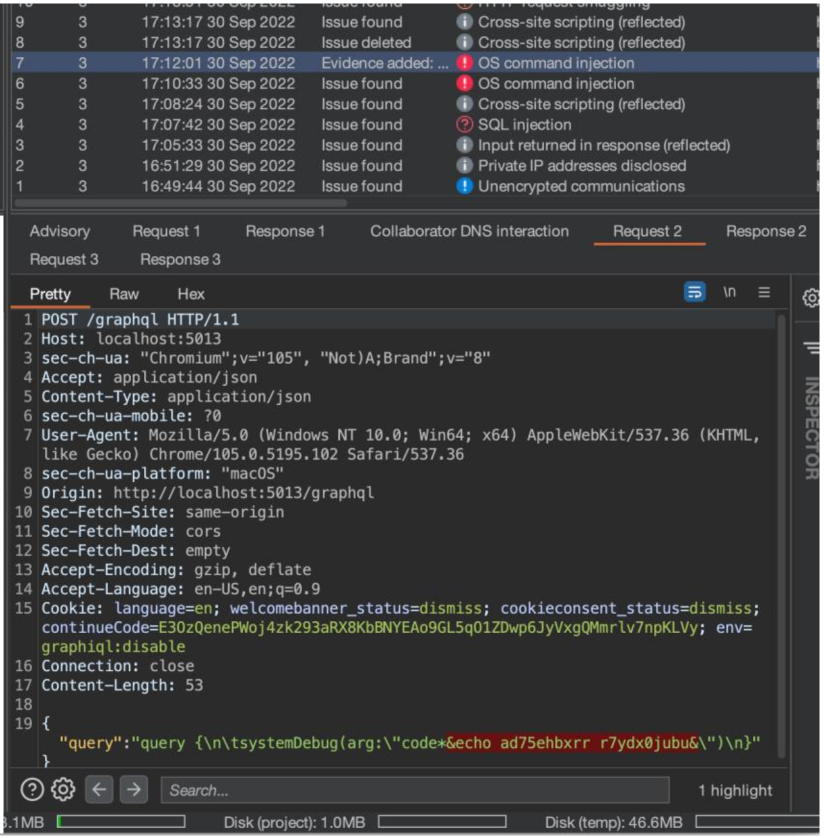
3. Extension driven active audit

Issues: 6 3 1 6

Capturing:

3319 requests (61 errors)

View details »



9	3	17:13:17 30 Sep 2022	Issue found	Cross-site scripting (reflected)
8	3	17:13:17 30 Sep 2022	Issue deleted	Cross-site scripting (reflected)
7	3	17:12:01 30 Sep 2022	Evidence added: ...	OS command injection
6	3	17:10:33 30 Sep 2022	Issue found	OS command injection
5	3	17:08:24 30 Sep 2022	Issue found	Cross-site scripting (reflected)
4	3	17:07:42 30 Sep 2022	Issue found	SQL injection
3	3	17:05:33 30 Sep 2022	Issue found	Input returned in response (reflected)
2	3	16:51:29 30 Sep 2022	Issue found	Private IP addresses disclosed
1	3	16:49:44 30 Sep 2022	Issue found	Unencrypted communications

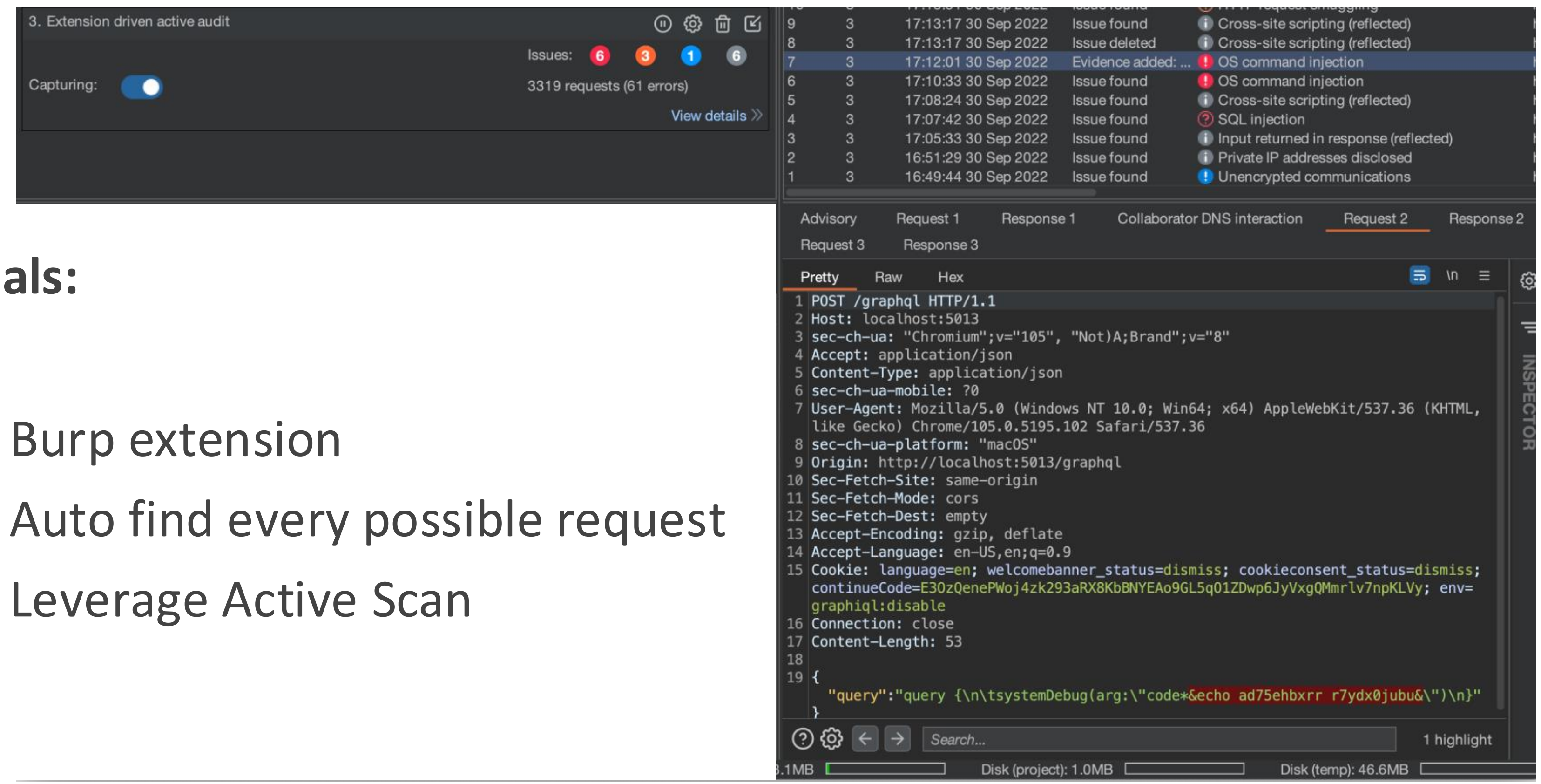
```
POST /graphql HTTP/1.1
Host: localhost:5013
sec-ch-ua: "Chromium";v="105", "Not)A;Brand";v="8"
Accept: application/json
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.5195.102 Safari/537.36
sec-ch-ua-platform: "macOS"
Origin: http://localhost:5013/graphql
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=E3OzQenePWoj4zk293aRX8KbBNYEAo9GL5qO1ZDwp6JyVxgQMmrlv7npKLVy; env=
graphiql:disable
Connection: close
Content-Length: 53

{
  "query":"query {\n\tsystemDebug(arg:\"code*&echo ad75ehbxrr r7ydx0jubu&\")\n}"
}
```

Goals:

- ❏ Burp extension
- ❏ Auto find every possible request
- ❏ Leverage Active Scan

FWDSEC

Solution



```
9   3   17:13:17 30 Sep 2022   Issue found         Cross-site scripting (reflected)
8   3   17:13:17 30 Sep 2022   Issue deleted       Cross-site scripting (reflected)
7   3   17:12:01 30 Sep 2022   Evidence added: ... OS command injection
6   3   17:10:33 30 Sep 2022   Issue found         OS command injection
5   3   17:08:24 30 Sep 2022   Issue found         Cross-site scripting (reflected)
4   3   17:07:42 30 Sep 2022   Issue found         SQL injection
3   3   17:05:33 30 Sep 2022   Issue found         Input returned in response (reflected)
2   3   16:51:29 30 Sep 2022   Issue found         Private IP addresses disclosed
1   3   16:49:44 30 Sep 2022   Issue found         Unencrypted communications
```

```
POST /graphql HTTP/1.1
Host: localhost:5013
sec-ch-ua: "Chromium";v="105", "Not)A;Brand";v="8"
Accept: application/json
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.5195.102 Safari/537.36
sec-ch-ua-platform: "macOS"
Origin: http://localhost:5013/graphql
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=E3OzQenePWoj4zk293aRX8KbBNYEAo9GL5qO1ZDwp6JyVxgQMmrlv7npKLVy; env=
graphiql:disable
Connection: close
Content-Length: 53

{
  "query":"query {\n\tsystemDebug(arg:\"code*&echo ad75ehbxrr r7ydx0jubu&\")\n}"
}
```

```
.1MB        Disk (project): 1.0MB        Disk (temp): 46.6MB
```

Goals:

- ✓ Burp extension
- ✓ Auto find every possible request
- ✓ Leverage Active Scan

FWDSEC

Take-away Considerations

- GraphQL is new and security is often lacking
- Burp’s Active Scanner automates vulnerability hunting
- Auto GQL extends Active Scanner to find GraphQL insertion points ***and*** automatically grabs all possible requests.
- Get it here: https://github.com/FWDSEC/burp-auto-gql
- Save massive amounts of time

Workshop Prerequisites

- Burp Suite (Community Edition is fine)
  - https://portswigger.net/burp/communitydownload
  - Click Go straight to downloads -->

- AutoGQL Burp Extension
  - https://github.com/FWDSEC/burp-auto-gql/

- Docker
  - https://www.docker.com/get-started/

- DVGA docker image
  - Pull image:

```
$ docker pull dolevf/dvga:latest
```

  - Run image:

```
$ docker run -t -p 5013:5013 -e WEB_HOST=0.0.0.0 dolevf/dvga
```

FWDSEC

Q&A

Contact Me:

Jared Meit

Email: j.meit@fwdsec.com

https://github.com/FWDSEC/burp-auto-gql

Contact FWDSEC:

Twitter: @FWD_SEC

FWDSEC