

API Security Workshop

Dan Barahona

Co-founder, APIsec University
dan@apisecuniversity.com

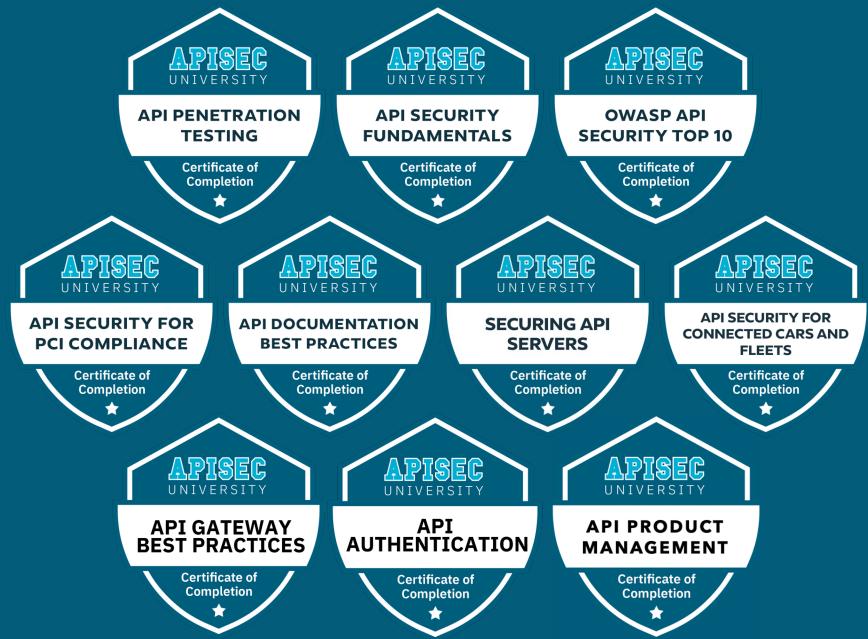


Free, Real-World API Security Training

Enroll in our hands-on university to access a wealth of expert content and improve your security skills.

[Sign Up Now!](#)

www.apisecuniversity.com



**Over 120,000 students
80%+ of Fortune 100**

coinbase

▼ Request Payload [view source](#)

```
▼ {client_order_id: "274fce73-edd3-4fc5-b2a3-86290  
  client_order_id: "274fce73-edd3-4fc5-b2a3-86290  
▼ order_configuration: {limitLimitGtc: {baseSize:  
  ▼ limitLimitGtc: {baseSize: "0.02433012", limit  
    baseSize: "0.02433012"  
    limitPrice: "3000"  
    postOnly: false  
  
product_id: "ETH-EUR"  
side: "SELL"  
source_account_id: "74f5810e-bda4-5277-ba28-90c  
target_account_id: "e64ba5fc-7db3-5e04-81ee-ced
```

coinbase

[Sign up](#)



Retrospective: Recent Coinbase Bug Bounty Award

By Author

[Company](#), February 18, 2022, 3 min read time



At Coinbase, our number one priority is ensuring that we uphold our security commitments to our customers.

On February 11, 2022, we received a report from a third-party researcher indicating that they had uncovered a flaw in Coinbase's trading interface. We

Root Cause

The underlying cause of the bug was a missing logic validation check in a Retail Brokerage API endpoint, which allowed a user to submit trades to a specific order book using a mismatched source account. This API is only utilized by our Retail Advanced Trading platform, which is currently in limited beta release.

2/11/2022 10:22:11 AM UTC USD -> EUR Call

412.50731

0.00122010 BTC

100.00000

412.50730

Filled

Pro tip: your UI is not part of your security stack

Why do Attackers Love APIs?

API Explosion

83%

of all Internet traffic is API traffic



APIs Under Attack

#1

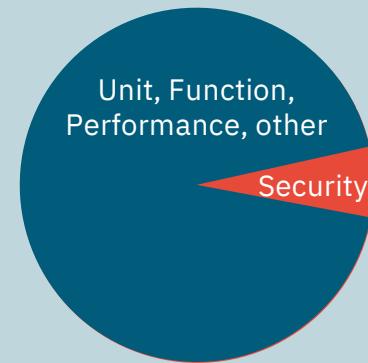
“API attacks will become the **most frequent attack vector**”

Gartner

APIs Under-Secured

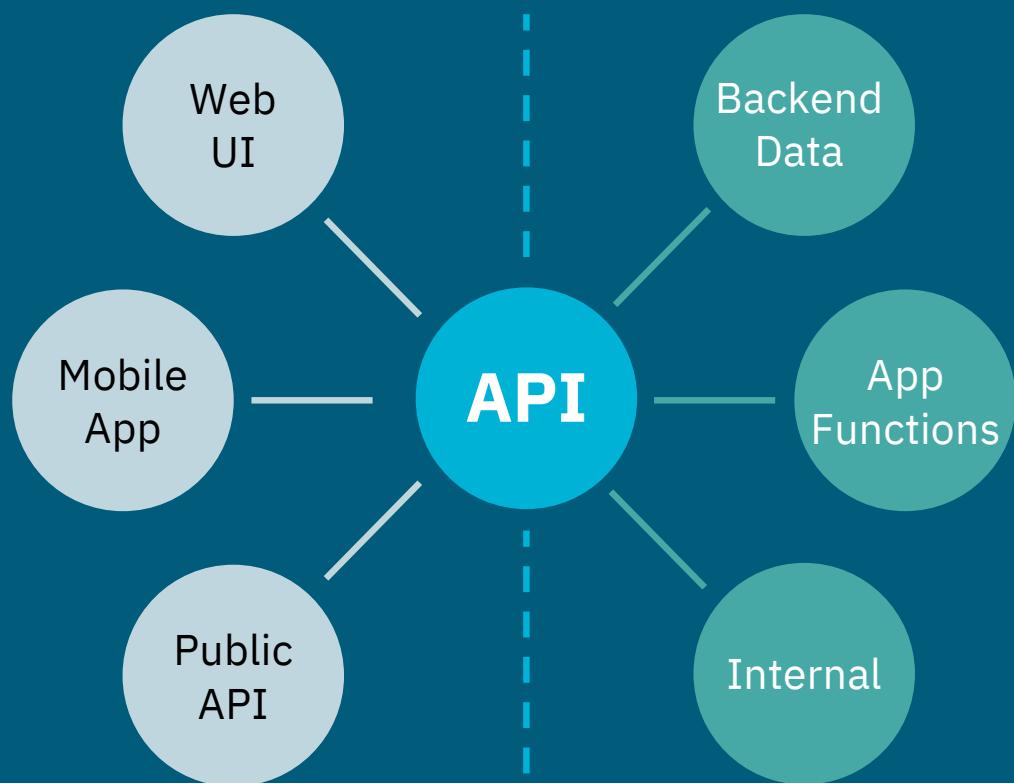
4%

of testing is Security



Source: stateofapis.com

What Makes APIs Prime Targets



APIs:

- Connect UIs to backend
- Provide direct access to data
- Can be easily discovered

APIs Hiding in Plain Sight

The screenshot shows a flight search results page from United.com. The flight details are as follows:

- Departure: SFO (San Francisco) at 12:15 AM
- Arrival: CVG (Cleveland) at 9:39 AM
- Date: August 16, 2024
- Flight Type: 1 STOP
- Flight Number: 7575
- Flight ID: 3517941830
- Carbon Emissions: 158 kg CO₂

A context menu is open over the flight information, showing options like Back, Forward, Reload, Save As..., Print..., Cast..., Search Images with Google, Send to Your Devices, Create QR Code for this Page, Translate to English, Open in Reading Mode, 1Password – Password Manager, View Page Source, Inspect (which is highlighted in blue), and AutoFill.

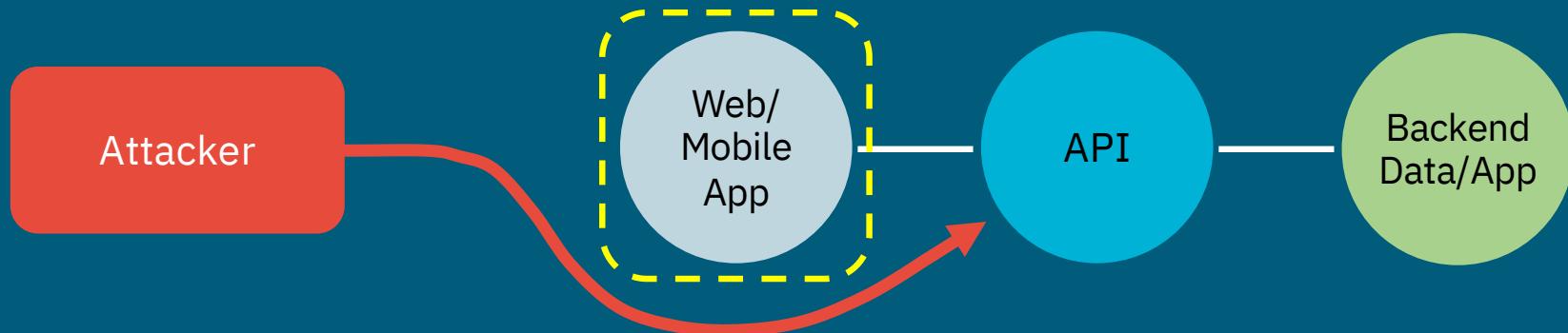
The browser's developer tools Network tab is active, showing a timeline of requests. A specific POST request to <https://www.united.com/api/flight/FetchFlights> is selected. The Headers and Payload sections are visible, with the Request URL and Method highlighted by a red box.

Name	Request URL	Request Method
lookup?airport=SFO&allAirp...	https://www.united.com/api/flight/FetchFlights	POST
lookup?airport=CVG&allAir...		
FetchFlights		
GetCarbonEmissions?cartId...		
7575?v=3.0&flavor=depend...		
3517941830		
advisories		
GetFareColumns		
RecommendedFlights?cartId...		
GetTeaserTexts?cartId=A9B...		
GetCarbonEmissions?cartId...		
FetchFareColumnEntlemen...		
register-trigger?partner_id=...		

Request Headers:

- Cache-Control: max-age=0, no-cache, no-store
- Content-Encoding: br
- Content-Length: 2039
- Content-Type: application/json; charset=utf-8
- Date: Sat, 22 Jun 2024 23:22:16 GMT
- Expires: Sat, 22 Jun 2024 23:22:16 GMT

How APIs Get Attacked



Attackers look for APIs that are:

- Over-permissioned
- Return too much information
- Access unauthorized functions
- Expose logic flaws



Federal Communications Commission

≡ Search

Home / EDOCS / Commission Documents

TracFone to Pay \$16M to Settle Data & Cybersecurity Investigation

“The investigations make clear that API security is paramount and should be on the radar of all carriers.”

“TracFone must perform continuous Static and Dynamic Security Testing (SAST/DAST) of Web Applications, **prioritizing APIs**, using **automated tools** that **test for vulnerabilities**.”

Loyaan A. Egal, Chief of Enforcement Bureau
Federal Communications Commission

fcc.gov/document/tracfone-pay-16m-settle-data-cybersecurity-investigation

What's Happening in the Real World?

API Breaches

Target	Impact
USPS	60M records
Coinbase	Fraudulent transactions
Experian	10s of millions
Instagram	Account takeover
Optus	10M records
T-Mobile	30M records
Dell	49M records
Parler	70TB data harvested
Peloton	4M records
Bumble	95M records
Zoom	Unauthorized access

Target	Impact
Facebook	530M records
John Deere	Account harvesting
Trello	15M
Twitter	5.4M records
Sumo Logic	Key leak
Pokemon Go	Data exposure
McDonald's	64M records
Yandex	Hacktivism
LinkedIn	700M
Tesla Backup	Data exposure
First American	885M

Target	Impact
7-Eleven 7Pay	Account takeover
Tinder	Data exposure
Wordle	Data manipulation
Duolingo	2.6M records
Echelon	Data exposure
Clubhouse	1.3M
Grindr	Account takeover
Venmo	207M records
Ring App	Data exposure
Plenty of Fish	Data exposure
JustDial	100M

2023 OWASP API Security Top 10

API1 Broken Object Level Authorization

API2 Broken Authentication

API3 Broken Object Property Level Authorization

API4 Unrestricted Resource Consumption

API5 Broken Function Level Authorization

API6 Unrestricted Access to Sensitive Business Flows

API7 Server Side Request Forgery

API8 Security Misconfiguration

API9 Improper Inventory Management

API10 Unsafe Consumption of APIs



Incomplete | Candidate Experience

mchire.com/candidates/incomplete?selected=72036918961549

All Apps **McHire**

Candidate Inbox

Incomplete

Recent activity ▾

Ian Carroll 49 m
Ha Jobsearch
1101 N. Osborn, Phoenix, 85001
Capture Incomplete

Unknown Candidate 50 m
Ha Jobsearch
1101 N. Osborn, Phoenix, 85001
Capture Incomplete

Ian Carroll

Conversation

to contact you?
052222222

Great! Can you please provide me with your email address as well?
no

I'd like to have the ability for a recruiter to follow up so I need to get your email.
i dont want to give you my email

In order to get you to the right person, I need to get your email.

About **Resume** **Notes** **Hire Details**

Add a note...

Candidate Summary

Ha Jobsearch +43 5222 2222
1101 N. Osborn, Phoenix, 85001 No Email Address Assigned

Resume **Add Resume**

Internal Notes

Add a note...

Add Forms

Nga FS viewed Ian Carroll

Send a text message to Ian

While viewing our test conversations, we noticed an interesting API to fetch the candidate information `PUT /api/lead/cem-xhr`, which seems to be a reference to proxying to some kind of Customer or Candidate Experience Manager (CEM) via an XHR request. The main parameter of this request was the `lead_id` of the chat, which for our test applicant was about `64,185,742`. We tried decrementing this number, and were immediately faced with PII



OWASP-1: Broken Object Level Authorization

Example: can User A access User B's data.

Request

Pretty Raw Hex

```
6 Content-Type: application/json
7 Origin: https://www.mchire.com
8 Priority: u=1, i
9 Referer:
  https://www.mchire.com/candidates/all-candidates?selected=7203691896154
9
10 Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138", "Google
  Chrome";v="138"
11 Sec-Ch-Ua-Mobile: ?0
12 Sec-Ch-Ua-Platform: "macOS"
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
17 X-Csrftoken: x9qmJgZ2rSuSuRb7VmWl7ANM236VJIqG
18 X-Requested-With: XMLHttpRequest
```

"lead_id":64185740,

```
order_type :0,
"time_filter":2,
"tz_str":"US/Arizona",
"lead_type":"all-candidates",
"filter_data":"",
"latest_candidate_id":"64185742",
"include_ui_filter":1,
"with_candidate_summary_data":1,
"support_auto_translation":1,
"page_type":"inbox"
}
```

Search 0 highlights

Done

Event log All issues

```
"linkedin_query_data":null,
"from_campaign":false,
"is_ask.olivia":false,
"resume_name":"Ayda_Portillo_Lopez_CLINTON",
"unmask_pii":{
  "email":{
    "key_name":"email",
    "privacy_setting":1,
    "value":"",
    "unmasked_value":""
  },
  "first_name":{
    "key_name":"first_name",
    "privacy_setting":1,
    "value":"Ayda",
    "unmasked_value":"Ayda"
  },
  "last_name":{
    "key_name":"last_name",
    "privacy_setting":1,
    "value":"Portillo Lopez",
    "unmasked_value":"Portillo Lopez"
  },
  "phone_number":{
    "key_name":"phone_number",
    "privacy_setting":1,
    "value":"+19845551234",
    "unmasked_value":"
  },
  "formatted_number": {
    "key_name": "formatted_number",
    "privacy_setting": 1,
    "value": "(984) 555-1234",
    "unmasked_value": "
  }
}
```

Search 0 highlights



SECURITY LEAKS

API Misuse: Hacker Exposes 2.6M Duolingo Users' Emails & Names

Duolingo Investigates Data Leak as Hacker Shares Personal User Information on Hacker Forums and Telegram.



OWASP-2: Broken Authentication

Weak/poor authentication. Often NO authentication.

```
{"users": [{"joinedClassroomIds": [], "streak": 624, "motivation": "work", "acquisitionSurveyReason": "friendsOrFamily", "shouldForceConnectPhoneNumber": false, "picture": "//simg-ssl.duolingo.com/avatars/858209554/PW1cepnuUj", "learningLanguage": "it", "hasFacebookId": false, "shakeToReportEnabled": null, "liveOpsFeatures": [], "canUseModerationTools": false, "id": 858209554, "betaStatus": "INELIGIBLE", "hasGoogleId": true, "privacySettings": ["DISABLE_THIRD_PARTY_TRACKING", "DISABLE_PERSONALIZED_ADS", "DISABLE_ADS_AND_TRACKING_CONTEXT"], "fromLanguage": "en", "hasRecentActivity15": true, "achievements": []}, {"observedClassroomIds": [4817870], "username": "DanBarahon1", "bio": "", "profileCountry": null, "chinaUserModerationRecords": [], "globalAmbassadorStatus": {}, "currentCourseId": "DUOLINGO_IT_EN", "hasPhoneNumber": true, "creationDate": 1638826461, "achievements": [], "hasPlus": true, "name": "Dan Corona", "roles": [{"users": [], "classroomLeaderboardsEnabled": false, "emailVerified": true, "courses": [{"preload": false, "placementTestAvailable": false, "authorId": "duolingo", "title": "Italian", "learningLanguage": "it", "xp": 45711, "healthEnabled": true, "fromLanguage": "en", "crowns": 94, "id": "DUOLINGO_IT_EN"}, {"preload": false, "placementTestAvailable": false, "authorId": "duolingo", "title": "Spanish", "l
```

Pro tip: Assume your “hidden” APIs will be discovered.



OWASP-3: Broken Object Property Level Authorization
Formerly “excess data exposure.” Return min data.

≡ WIRED

SUBSCRIBE

DAN SALMON SECURITY JUN 26, 2019 9:00 AM

I Scrapped Millions of Venmo Payments. Your Data Is at Risk

After proxying my phone traffic through my laptop, I watched the network traffic as I navigated through the app. I noticed that when you open the Venmo home page, you’re shown a live feed of transactions being made by strangers. I could see a public API endpoint that was returning the data for this feed, meaning that anyone could make a GET request (like a simple page load) to see the latest 20 transactions made on the app by anyone around the world. To my surprise, this endpoint was accessible even outside the app, with no authorization needed. After some experimenting, I found that I could make two requests for transaction data per minute, per IP address.

ZDNET

Home / Tech / Security

Venmo has no good reason to make user transactions public by default

"I used Venmo's public API to pull in all public transactions of 2017 -- a total of 207,984,218 transactions," he said in an email. "By looking through them, I learned a scary amount about Venmo users. I was able to follow a drug dealer's sales, watch a couple fight viciously on Valentine's Day, and learn exactly how many mangos a Santa Barbara, CA food cart sells each week."

Pro tip: filter data in API,
not the UI



OWASP-4: Unrestricted Resource Consumption

Rate Limiting won't prevent determined attackers.

Trello.com 15 mil
by emo - Tuesday January 16, 2024 at 03:33 PM

01-16-2024, 03:33 PM (This post was last modified: 01-16-2024, 03:37 PM by emo.)
Trello.com, 15,115,516

Contains emails, usernames, full names and other account info. 15,115,516 unique lines.
Selling one copy to whoever wants it, message on me on-site or on telegram if you're interested.

A sample of all lines which match 'cheko'

```
{"id": "4f1baf05ac3860b532015168", "aaId": "557058:33d228e8-310e-4afc-b740-e4910042fcbd", "activityBlocked": false, "avatarHash": null, "avatarUrl": null, "bio": "", "bioData": null, "confirmed": true, "fullName": "Sergey Schekochikhin", "idEnterprise": null, "idEnterprisesDeactivated": null, "idMemberReferrer": null, "idPremOrgsAdmin": null, "initials": "SS", "memberType": "normal", "nonPublic": false, "nonPublicAvailable": true}
```

"Given the misuse of the API uncovered in this January 2024 investigation, we made a change to it so that unauthenticated users/services cannot request another user's public information by email."



OWASP-5: Broken Function Level Authorization
Don't allow users to execute unauthorized functions.



[Podcasts](#) / [Malware](#) / [Vulnerabilities](#) / [InfoSec Insiders](#)

Dating Site Bumble Leaves Swipes Unsecured for 100M Users

Instagram

OWASP-6: Unrestricted Access to Sensitive Business Flows.
Careless business logic can create opportunities for abuse.

The screenshot shows a news article from TIME magazine. At the top, there is a navigation bar with three horizontal lines on the left, the TIME logo in red in the center, and a red "SUBSCRIBE" button on the right. Below the navigation bar, the article has a red header that reads "TECH • INSTAGRAM". The main title of the article is "Instagram Says Bug Gave Hackers Data on 'High-Profile' Users". Underneath the title, there is a quote in a yellow box: "'We recently discovered that one or more individuals obtained unlawful access to a number of high-profile Instagram users'".

TIME

SUBSCRIBE

TECH • INSTAGRAM

Instagram Says Bug Gave Hackers Data on 'High-Profile' Users

“We recently discovered that one or more individuals obtained unlawful access to a number of high-profile Instagram users”

OWASP API 7-10

API7: Server Side Request Forgery (SSRF)

API8: Security Misconfiguration

API9: Improper Inventory Management

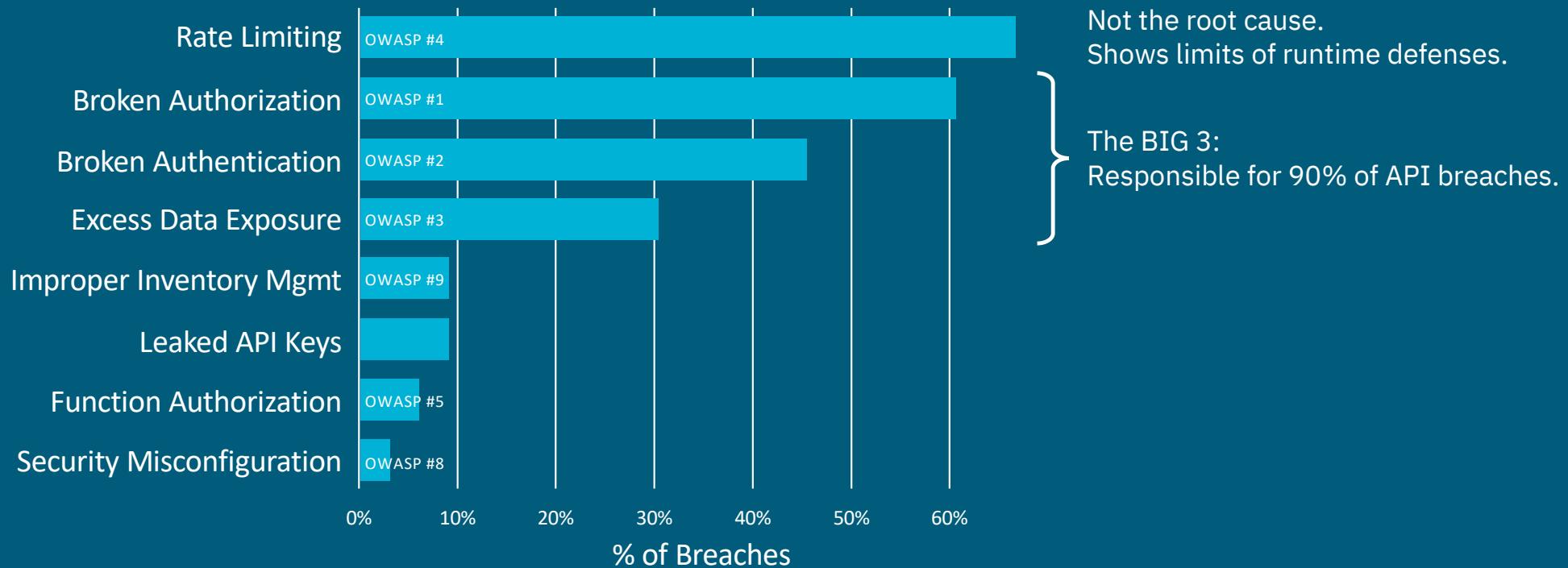
API10: Unsafe Consumption of APIs

How Can We Secure APIs?

API Breaches

Target	Impact	Target	Impact	Target	Impact
USPS	60M records	Facebook	530M records	7-Eleven 7Pay	Account takeover
Coinbase	Fraudulent transactions	John Deere	Account harvesting	Tinder	Data exposure
Experian	10s of millions	Trello	15M	Wordle	Data manipulation
Instagram	Account takeover	Twitter	5.4M records	Duolingo	2.6M records
Optus	10M records	Sumo Logic	Key leak	Echelon	Data exposure
T-Mobile	30M records	Pokemon Go	Data exposure	Clubhouse	1.3M
Dell	49M records	McDonald's	64M records	Grindr	Account takeover
Parler	70TB data harvested	Yandex	Hacktivism	Venmo	207M records
Peloton	4M records	LinkedIn	700M	Ring App	Data exposure
Bumble	95M records	Tesla Backup	Data exposure	Plenty of Fish	Data exposure
Zoom	Unauthorized access	First American	885M	JustDial	100M

Breach Analysis



Approaches to API Security

Testing

- Preventative
- “Hack yourself” approach
- Find vulns pre-production
- DAST, Pen-Testing

Monitoring

- Reactive
- Runtime threat detection
- Signature/anomaly detection
- WAF, SIEM

Why the WAF Missed the Attacks:

API attacks pass through defenses because they look legitimate.

BAD! GET /api/user?id=' OR 1=1--

OK? USER ID 10: DELETE /api/transfer?id=123

The Need for Testing

Security

- Unsecured Endpoints
- Incremental IDs
- Injection, XSS
- Fuzzing, input validation
- Error handling

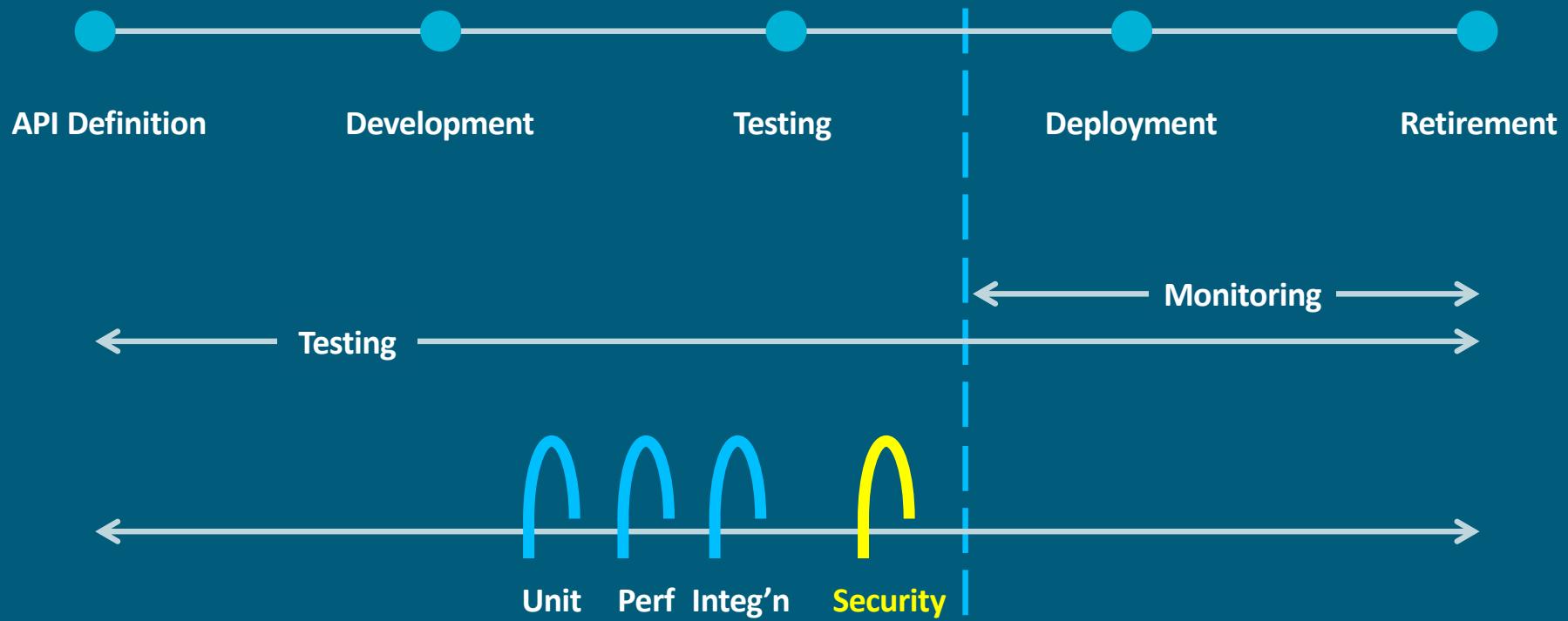
Data

- Excessive data exposure
- Sensitive data exposure
- Personal, health, bank data
- File, directory exposure
- Data exfiltration

Logic

- Object ID manipulation
- Cross-account access
- API function abuse
- Role-based access control
- Authorization gaps

Pre-production | Production



API Testing Approaches

Option 1:
Do nothing

Option 2:
Do it yourself



Option 3:
Pay someone
else to do it



Automated API Security Testing

The screenshot displays the APIsec web application interface. At the top, there's a navigation bar with tabs for 'Scan History', 'Scan All Endpoints', 'App Config', and user information ('Dan Barahona USER'). Below the header, the main content area shows a summary for the endpoint 'crapi 9/30'. It includes three donut charts: 'Sensitivity' (Total 42), 'Endpoint Authentication' (Total 42), and 'Method' (Total 42). The 'Method' chart shows distribution across GET, PUT, POST, DELETE, and PATCH. A table below lists specific endpoints with their methods, sensitivity levels, and parameters.

Method	Endpoint	Sensitivity	Endpoint Authentication	Total Parameters	Highly Sensitive Parameters
POST	/workshop/api/shop/orders	Critical	🔓	2	1
GET	/workshop/api/shop/orders/{order_id}	Critical	🔒	1	1
PUT	/workshop/api/shop/orders/{order_id}	Critical	🔓	3	2
GET	/workshop/api/shop/orders/all	Critical	🔒	0	0
POST	/workshop/api/shop/orders/return_order	Critical	🔓	1	1

On the right side, there's a section titled 'App Model' with a progress bar at 78.33% and several status indicators. A 'Recommended Action' box suggests providing values for parameters 'order_id, id' to improve test coverage on 2 endpoints, along with links to 'Configure for RBAC', 'Configure for BOLA', and 'Configure for Mass Assignments'.

PENETRATION
TESTING REPORT



Bolt by APIsec

craigslist

post an ad

search craigslist

event calendar

S	M	T	W	T	F	S
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25

help, faq, abuse, legal



apisecu.typeform.com/bolt-beta

SF bay area

sfc sby eby pen nby scz



community

activities
artists
childcare
classes
events
general
groups
local news

services

automotive
beauty
cell/mobile
computer
creative
cycle
event
farm+garden
financial
health/well
household

discussion forums

apple
arts
atheist
autos
beauty
bikes
celebs
comp
cosmos
diet
divorce
frugal
gaming
garden
help
history
housing
jobs
jokes
legal
manners
marriage
money
music
open
philos
photo
politics
psych
recover
religion
rofo
science
spirit
sports
super
tax
travel
tv
vegan

housing

apts / housing
missed
connections
musicians
pets
politics
rants & raves
rideshare
volunteers

for sale

antiques
appliances
arts+crafts
atv/utv/sno
auto parts
aviation
baby+kid
barter
beauty+hlth
bike parts
bikes
boat parts
books
business
cars+trucks
cds/dvd/vhs
cell phones
clothes+acc
collectibles
computer parts
computers
electronics
farm+garden
free
furniture
garage sale
general
heavy equip
household
jewelry
materials
motorcycle parts
motorcycles
music instr
photo+video
rvs+camp
sporting
tickets
tools
toys+games
trailers
video gaming
wanted
wheels+tires

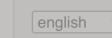
jobs

accounting+finance
admin / office
arch / engineering
art / media / design
biotech / science
business / mgmt
customer service
education
etc / misc
food / bev / hosp
general labor
government
human resources
legal / paralegal
manufacturing
marketing / pr / ad
medical / health
nonprofit sector
real estate
retail / wholesale
sales / biz dev
salon / spa / fitness
security

skilled trade / craft
software / qa / dba
systems / network
technical support
transport
tv / film / video
web / info design
writing / editing

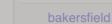
gigs

computer
creative
crew
domestic
event
labor
talent
writing



nearby cl

bakersfield
chico
fresno
gold country
hanford
humboldt
inland empire
klamath falls
las vegas
los angeles
medford
mendocino co
merced
modesto
monterey
orange co
palm springs
redding
reno
roseburg
sacramento
san luis obispo
santa barbara
santa maria
siskiyou co
stockton
susanneville
ventura
visalia-tulare
yuba-sutter



Bolt by APIsec

Bolt by APIsec



Bolt by APIsec

Traffic

Documentation

Base URL:

craigslist.org

Start

Enable automatic crawl

Bolt by APIsec v1.0

Last update: 7:13:55 AM

API Security Checklist

Authorization	<ul style="list-style-type: none"><input type="checkbox"/> Do applications restrict cross account data access?<input type="checkbox"/> Do applications restrict functional access to appropriate roles?<input type="checkbox"/> Are RBAC and multi-tenant permissions tested continuously?
Authentication	<ul style="list-style-type: none"><input type="checkbox"/> Are all sensitive API endpoints appropriately authenticated?<input type="checkbox"/> Are API keys, tokens, sessions properly secured?<input type="checkbox"/> Are all API endpoints tested to validate authentication is enforced?
Data Exposure	<ul style="list-style-type: none"><input type="checkbox"/> Are all inputs sanitized and validated before processed?<input type="checkbox"/> Is there PII, sensitive data, IP in API responses? Is it appropriate?<input type="checkbox"/> Are injection, mass assignment, input validation controls tested?
API Inventory	<ul style="list-style-type: none"><input type="checkbox"/> Is there a complete inventory of internal and 3rd party APIs?<input type="checkbox"/> Are APIs properly retired when required?
Governance & Risk	<ul style="list-style-type: none"><input type="checkbox"/> Are API dev/ops process standardized and documented?<input type="checkbox"/> Are APIs documented and managed in a central platform?<input type="checkbox"/> Are API security programs applied to internal and external APIs?<input type="checkbox"/> Are APIs comprehensively security tested before every release?
Training	<ul style="list-style-type: none"><input type="checkbox"/> Are Security & Engineering teams trained on API risks, best practices?

Thank you!

Dan Barahona

dan@apisecuniversity.com

Need CPEs?



apisecuniversity.com/workshop-cert