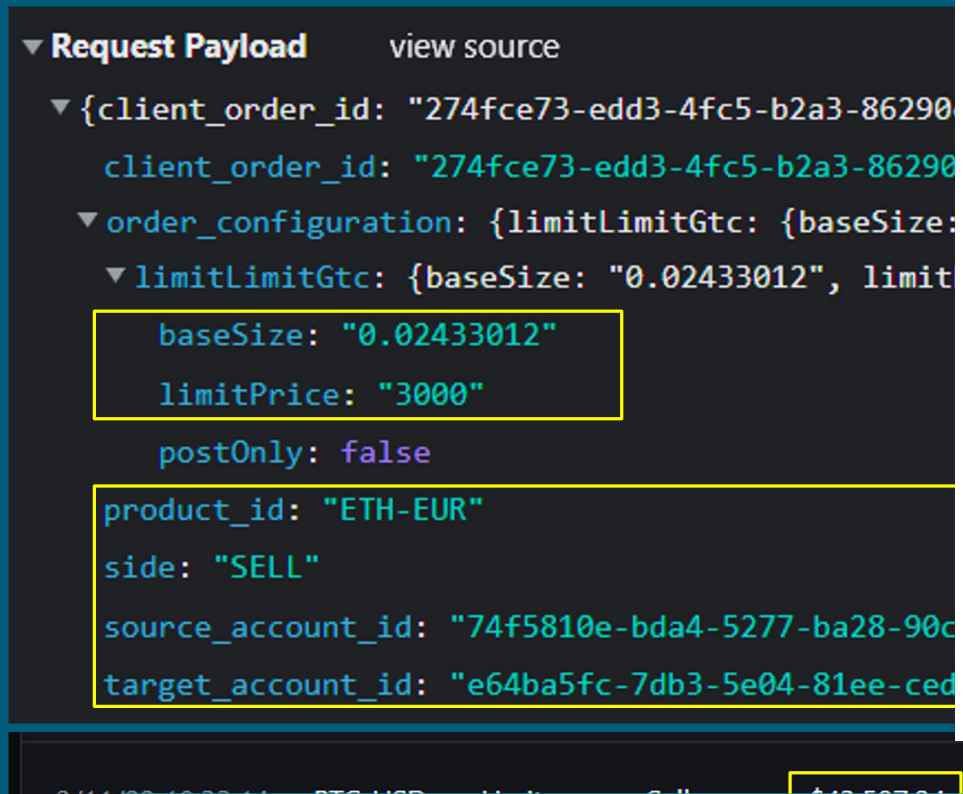
API Security Workshop

Dan Barahona
Co-founder, APIsec University
dan@apisecuniversity.com

APISEC
UNIVERSITY

coinbase



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

Akamai

APIs Under Attack

#1

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

Gartner

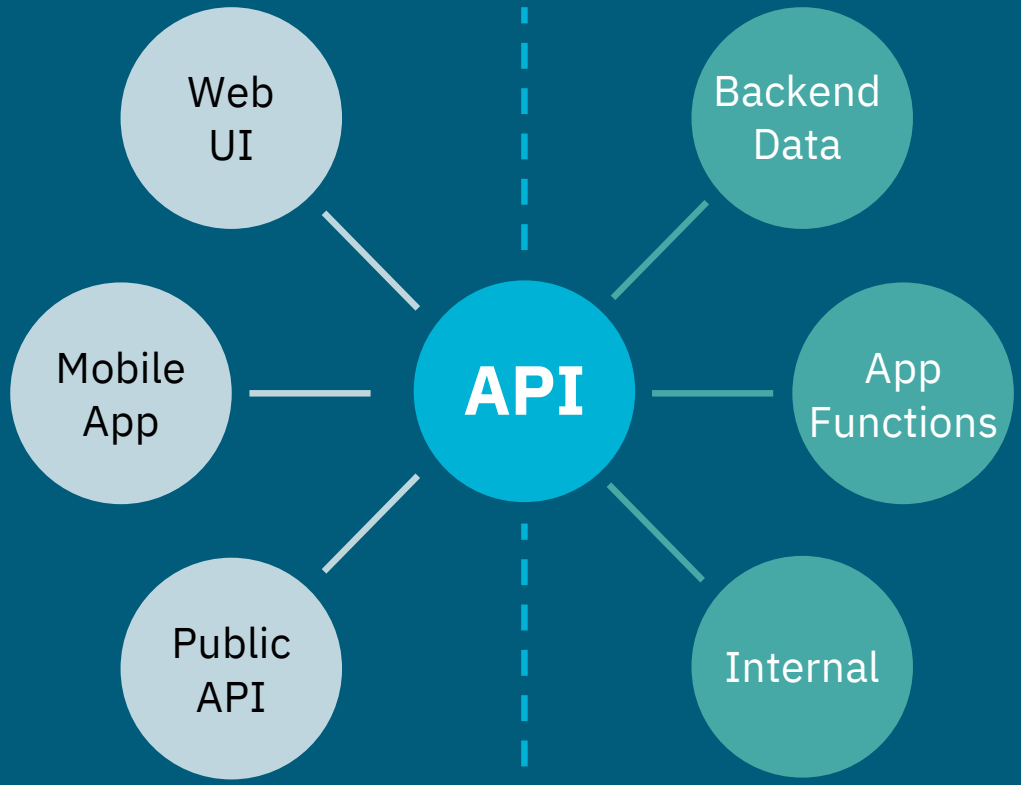
APIs Under-Secured

4%

of testing is Security

Source: stateofapis.com

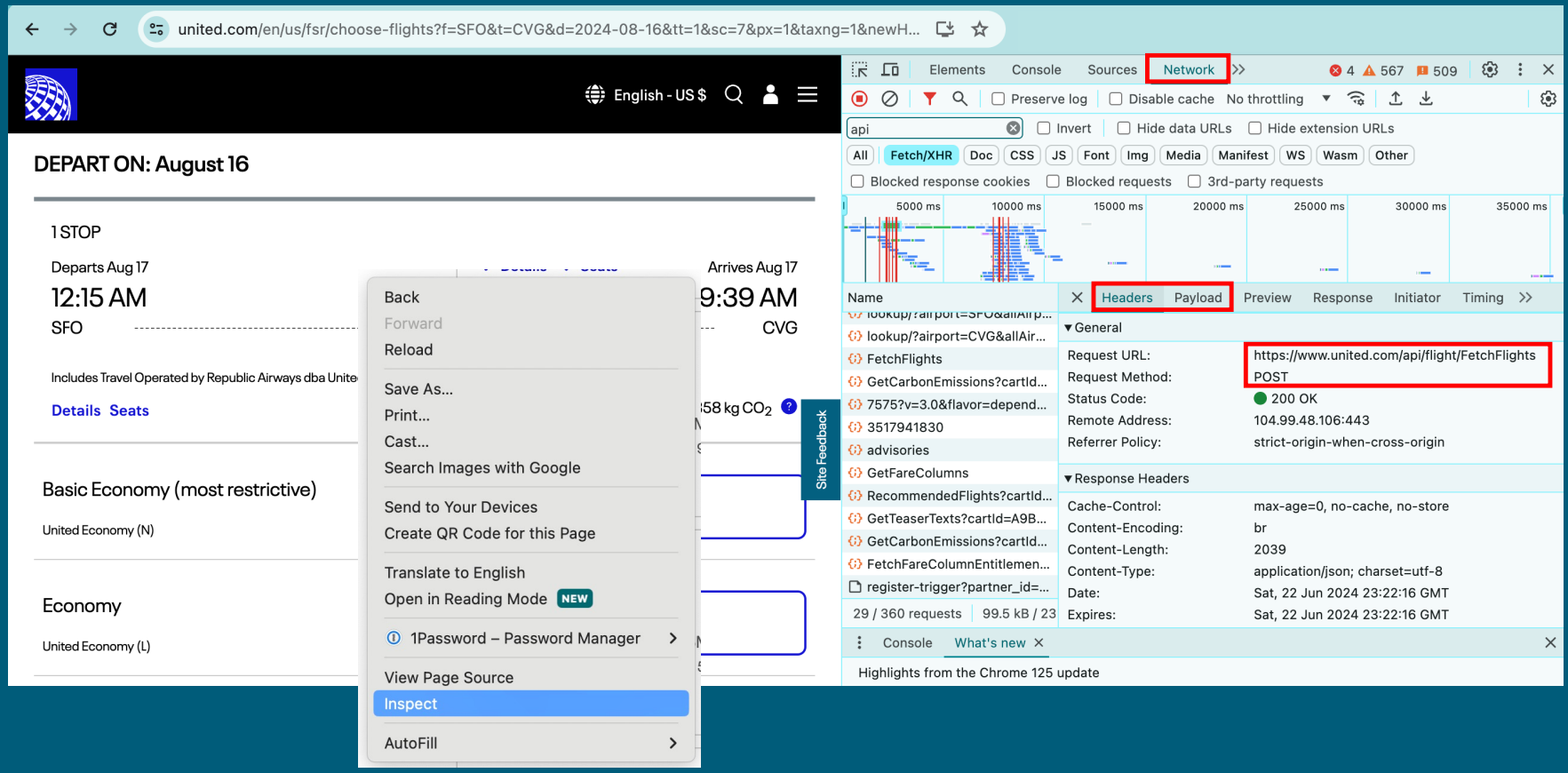
What Makes APIs Prime Targets



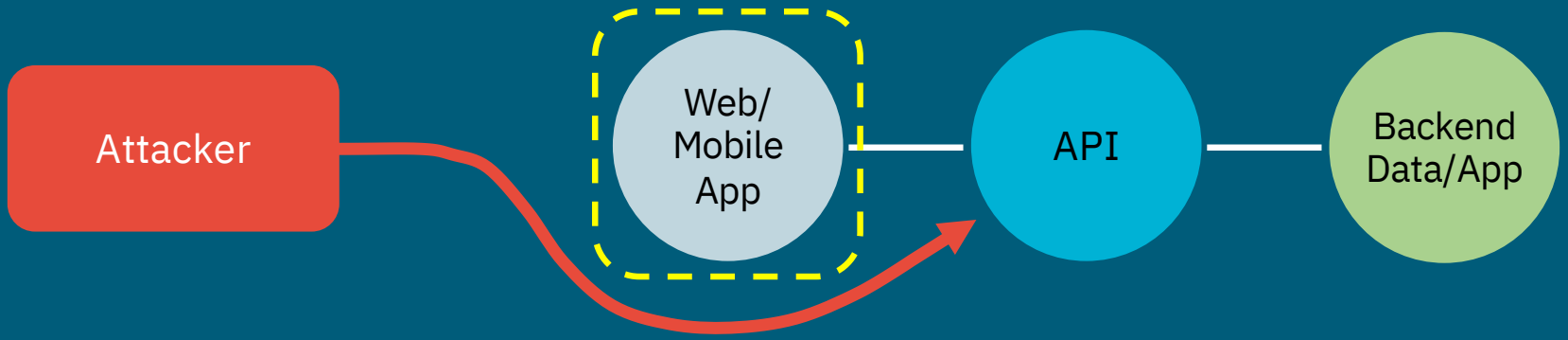
APIs:

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

APIs Hiding in Plain Sight



How APIs Get Attacked



Attackers look for APIs that are:

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

PCI DSS COMPLIANT

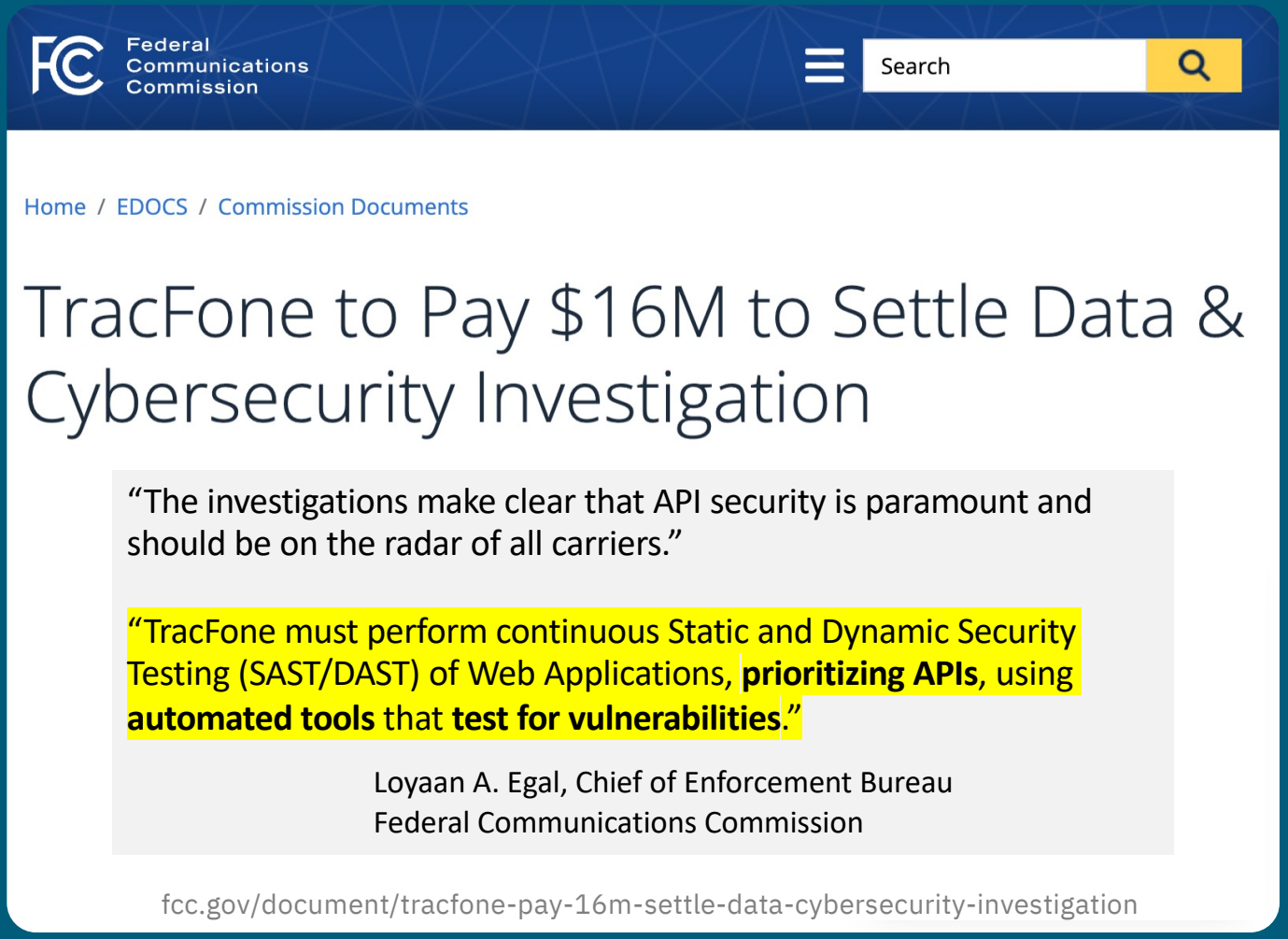
GDPR
European Commission
General Data Protection Regulation

HIPAA

U.S. SECURITIES AND EXCHANGE COMMISSION

UNECE r155

FedRAMP



What’s Happening in the Real World?

API Breaches

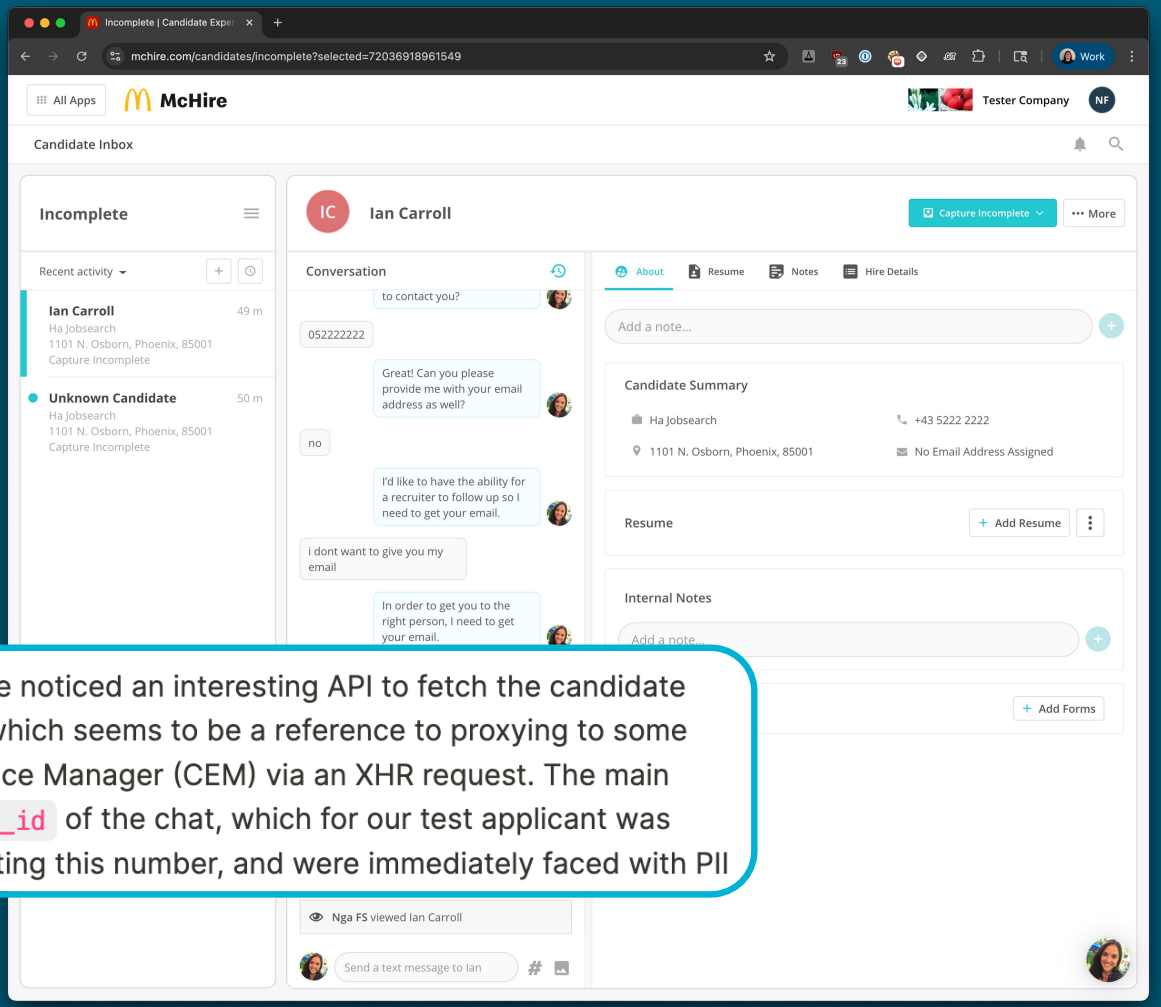
Target	Impact
USPS	60M records
Coinbase	Fraudulent transactions
Experian	10s of millions
Instagram	Account takeover
Optus	10M records
T-Mobile	30M records
Dell	49M records
Parler	70TB data harvested
Peloton	4M records
Bumble	95M records
Zoom	Unauthorized access

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

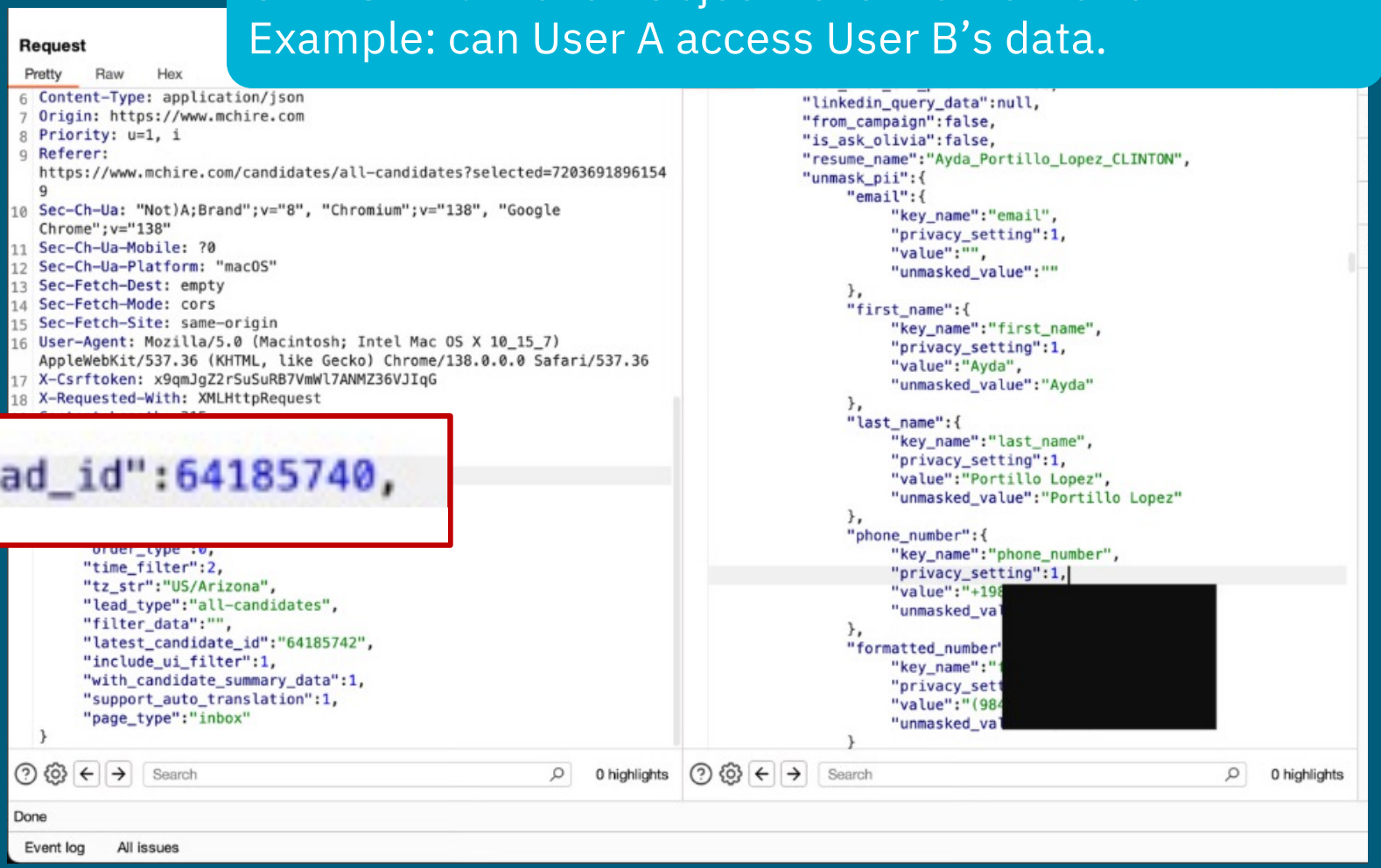
2023 OWASP API Security Top 10

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



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.

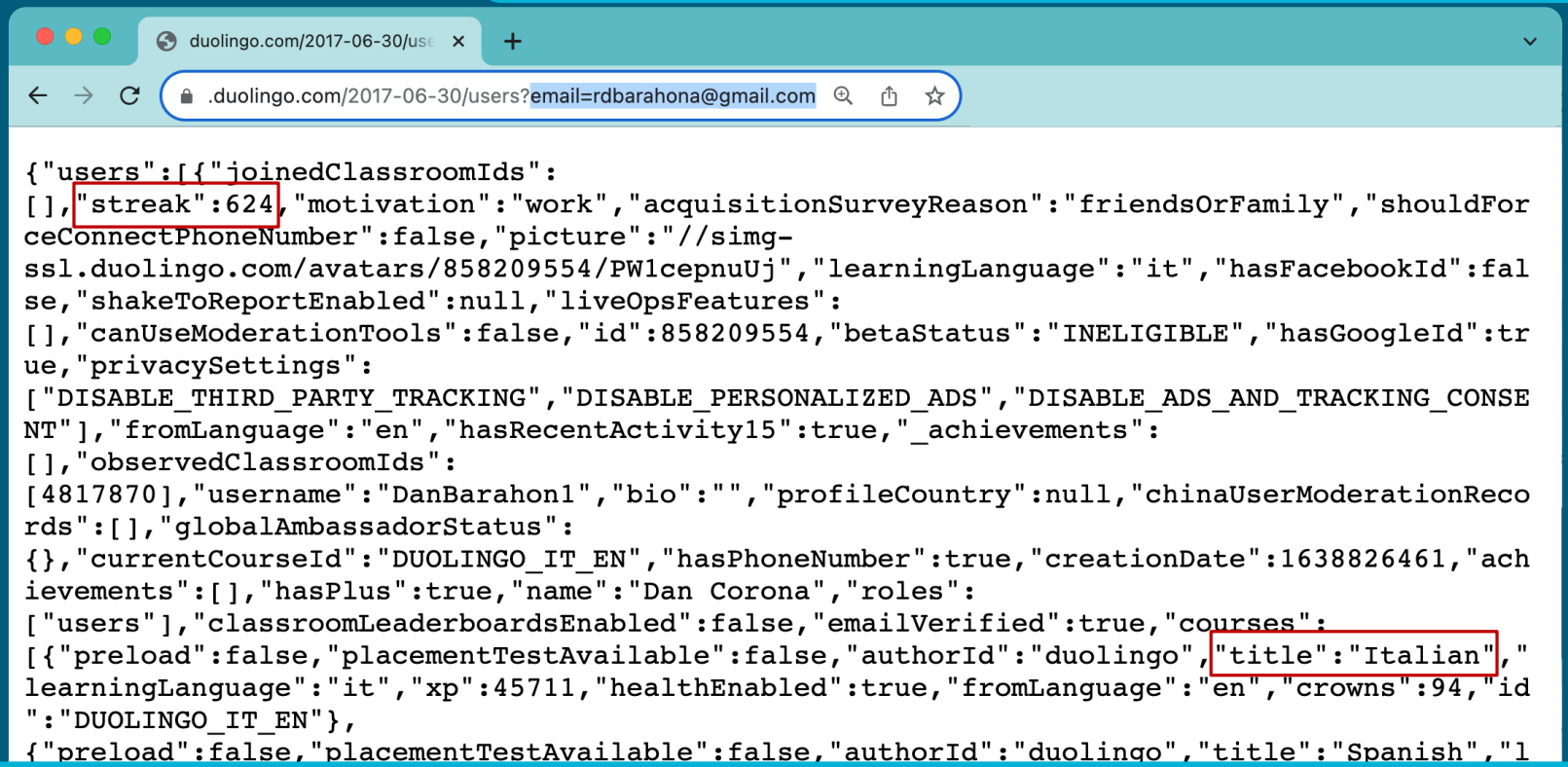


API Misuse: Hacker Exposes 2.6M Duolingo Users' Emails & Names

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

duolingo

OWASP-2: Broken Authentication
Weak/poor authentication. Often NO authentication.



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

venmo

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 Scraped 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

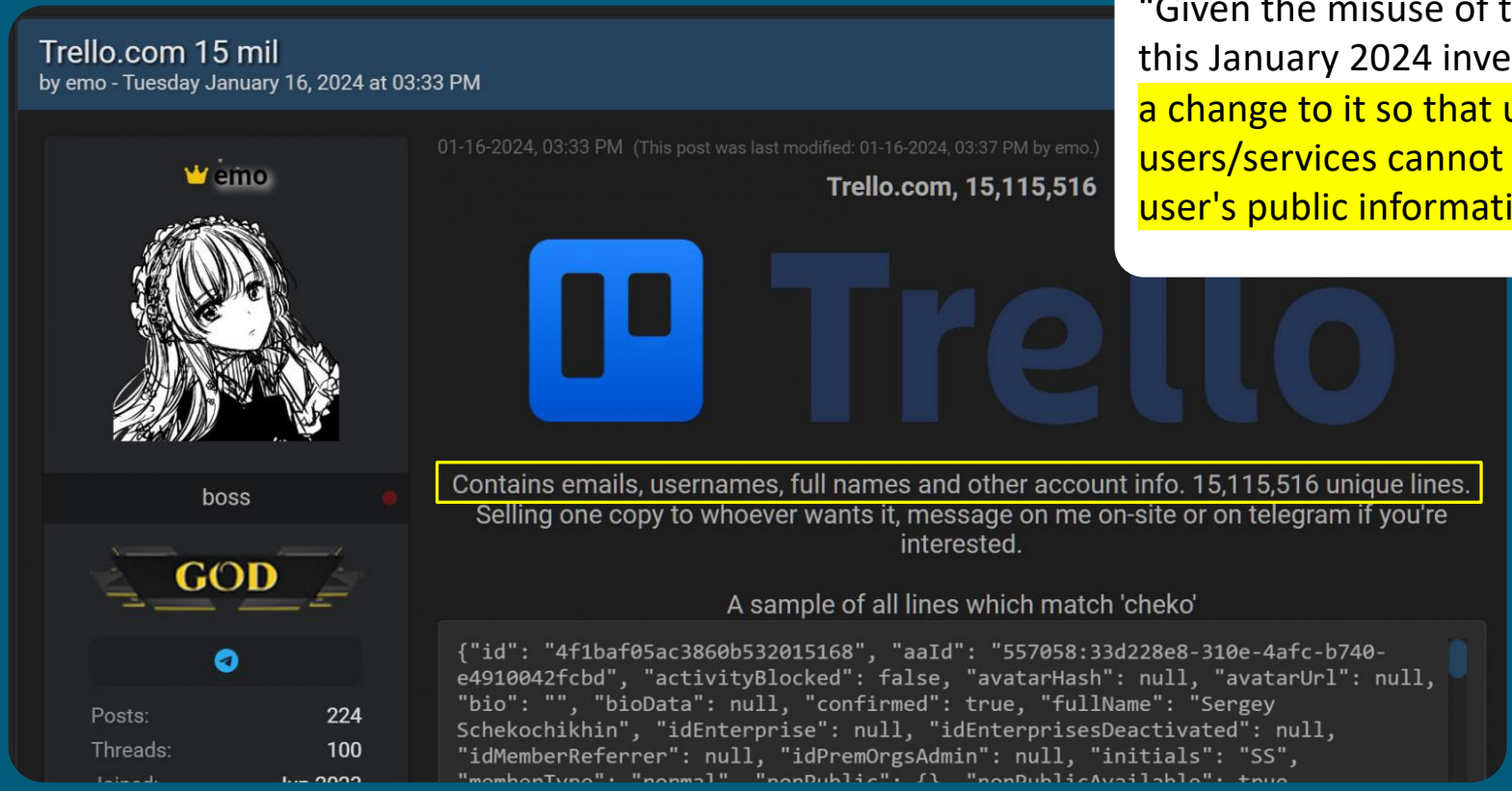
Venmo has no good reason to make user transactions public by default

"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

Trello

OWASP-4: Unrestricted Resource Consumption
Rate Limiting won't prevent determined attackers.



"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."

bumble

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

Instagram

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

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?

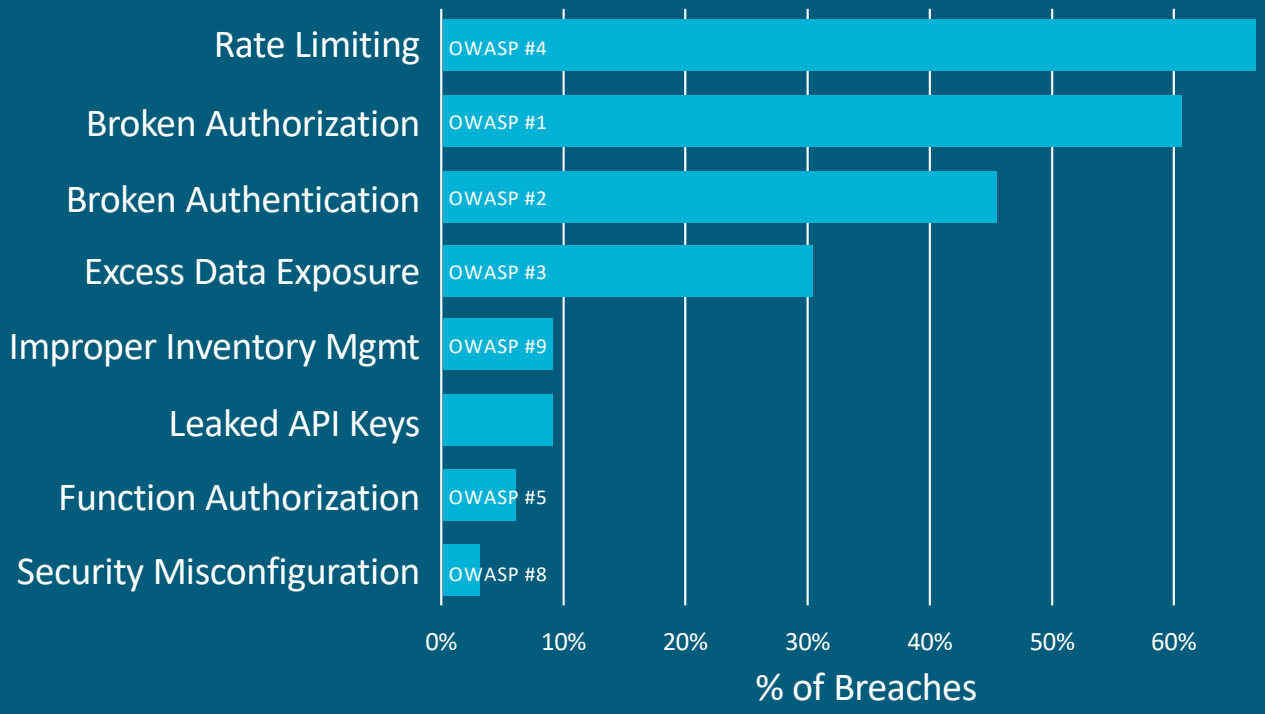
API Breaches

Target	Impact
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

Breach Analysis



Not the root cause.
Shows limits of runtime defenses.

The BIG 3:
Responsible for 90% of API breaches.

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

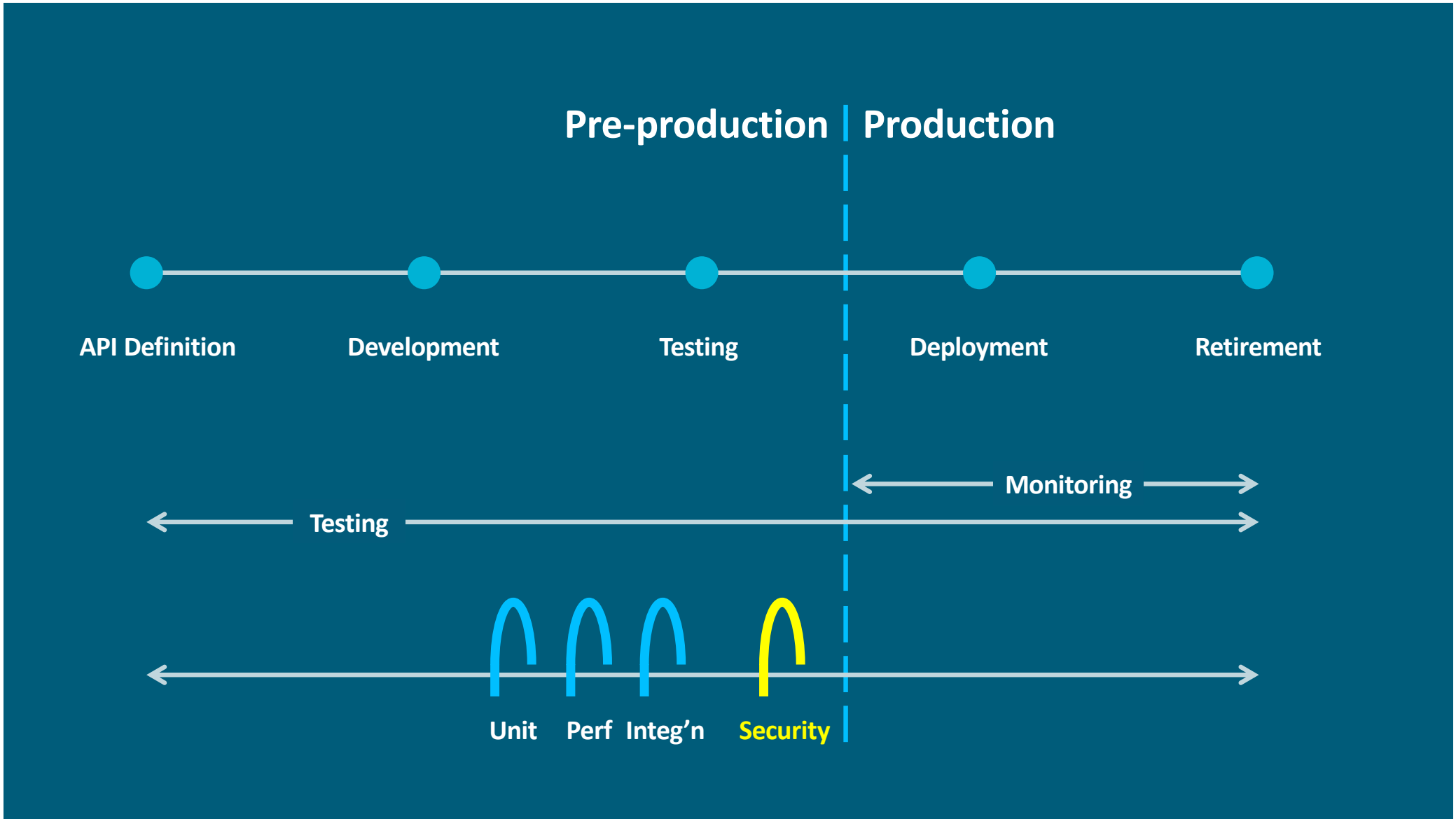
- Unsecured Endpoints
- Incremental IDs
- Injection, XSS
- Fuzzing, input validation
- Error handling

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 Definition
Development
Testing
Deployment
Retirement
Monitoring
Testing
Unit
Perf
Integ'n
Security

API Testing Approaches

Option 1:

Do nothing

Option 2:

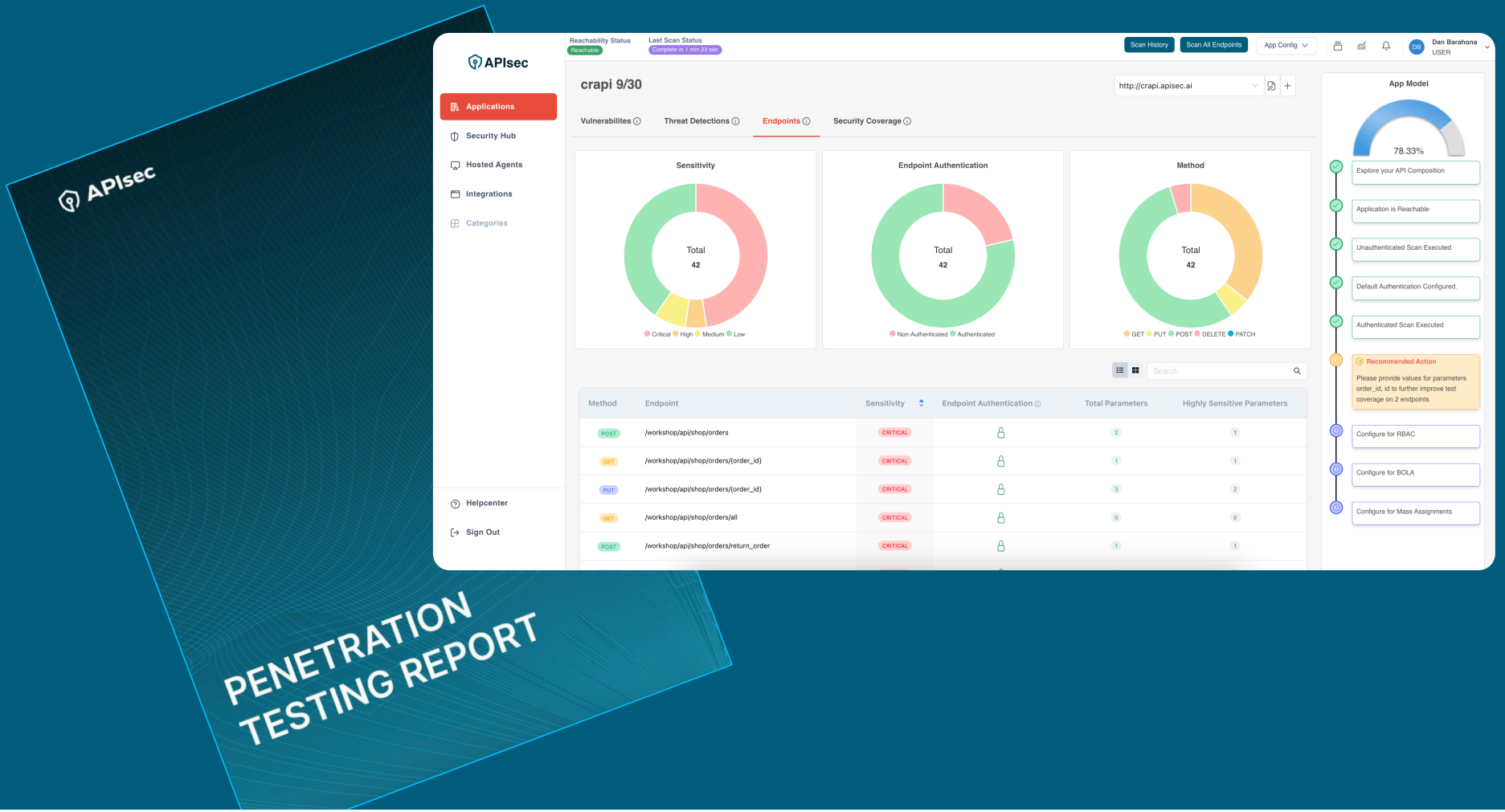
Do it yourself

Option 3:

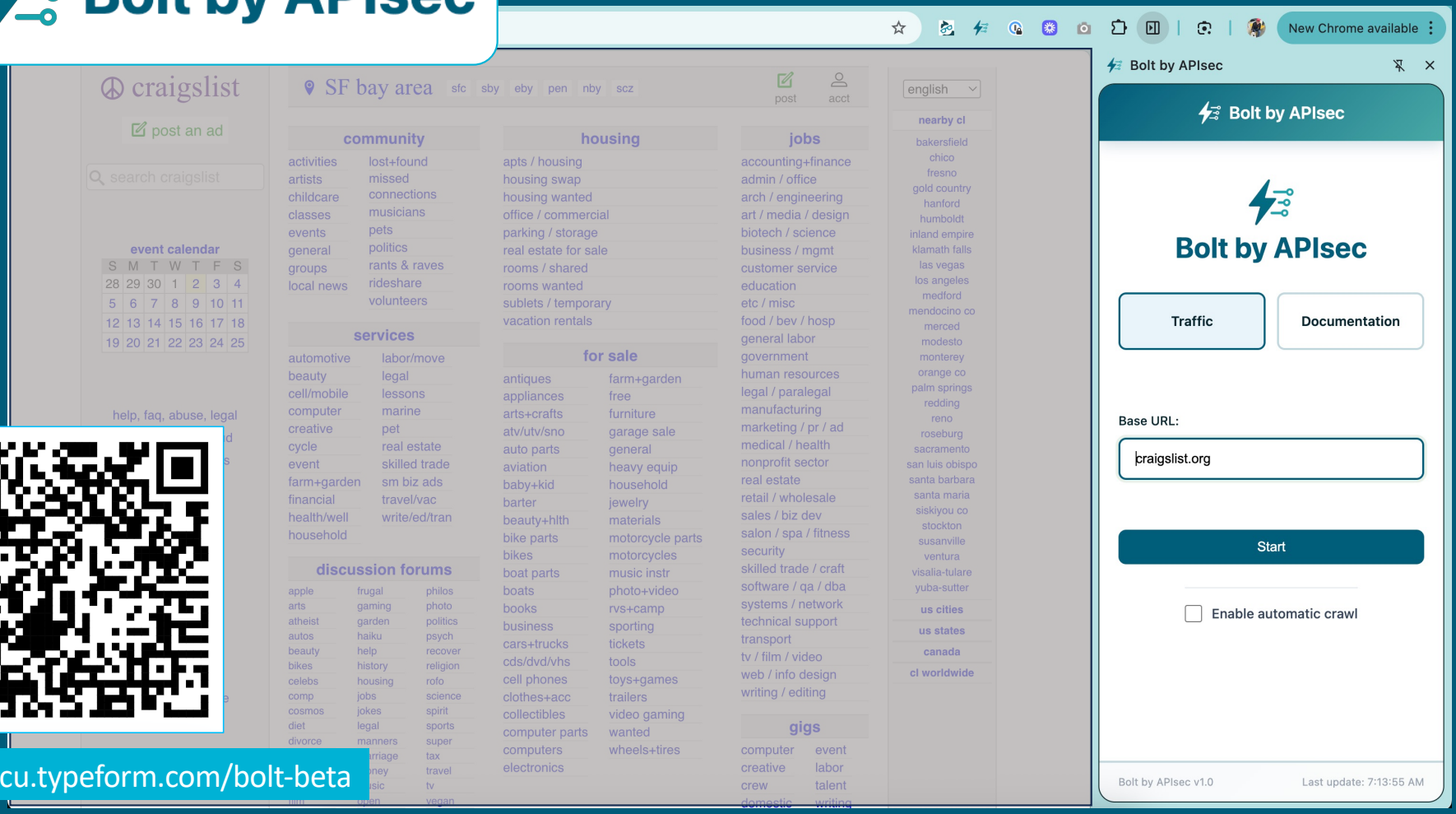
Pay someone else to do it

Pen-Testing

Automated API Security Testing



Bolt by APIsec



apisecu.typeform.com/bolt-beta

API Security Checklist

Authorization	❑ Do applications restrict cross account data access? ❑ Do applications restrict functional access to appropriate roles? ❑ Are RBAC and multi-tenant permissions tested continuously?
Authentication	❑ Are all sensitive API endpoints appropriately authenticated? ❑ Are API keys, tokens, sessions properly secured? ❑ Are all API endpoints tested to validate authentication is enforced?
Data Exposure	❑ Are all inputs sanitized and validated before processed? ❑ Is there PII, sensitive data, IP in API responses? Is it appropriate? ❑ Are injection, mass assignment, input validation controls tested?
API Inventory	❑ Is there a complete inventory of internal and 3rd party APIs? ❑ Are APIs properly retired when required?
Governance & Risk	❑ Are API dev/ops process standardized and documented? ❑ Are APIs documented and managed in a central platform? ❑ Are API security programs applied to internal and external APIs? ❑ Are APIs comprehensively security tested before every release?
Training	❑ Are Security & Engineering teams trained on API risks, best practices?

Thank you!

Dan Barahona
dan@apisecuniversity.com

Need CPEs?

apisecuniversity.com/workshop-cert