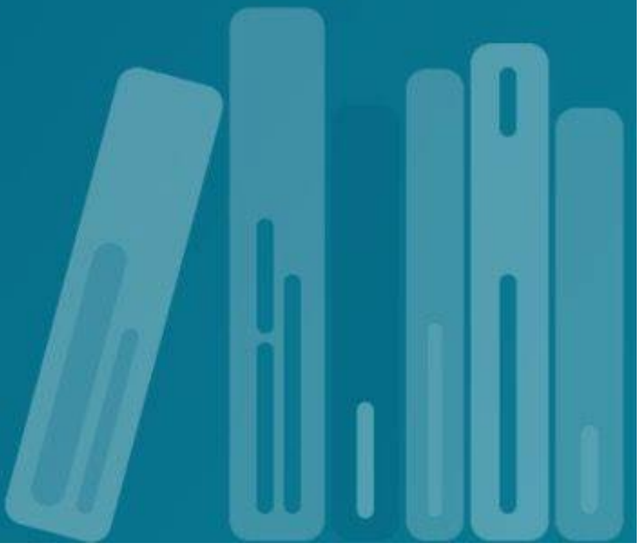
Overview of Real-World Breaches



APISEC UNIVERSITY

coinbase	Unauthorized trading
UNITED STATES POSTAL SERVICE	Account data harvesting
venmo	Excess data exposure
Instagram	Account takeover
bumble	Account tampering
T-Mobile	SEC reporting
OPTUS	Ransom
experian	3rd party exposure

APISEC UNIVERSITY

coinbase

ZDNET

Home / Finance / Blockchain

Coinbase pays out largest bug bounty ever for trading interface flaw

The researcher who discovered the issue was paid $250,000.

Tree of Alpha @Tree_of_Alpha · Feb 19

I just used 0.0243 ETH to sell 0.0243 BTC on the BTC-USD pair, a pair I do not have access to, without holding any BTC.
Hoping this is a UI bug, I check the fills on the order, and they match the API: those trades really happened, on the live order book.

What happened:

- User scraped API calls from web UI
- Identified 4 key parameters for any Coinbase transaction
- Manipulated the parameters via API calls
- Sold crypto they DID NOT own

OWASP API #1
Broken Object Level Authorization

UNITED STATES POSTAL SERVICE


KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

USPS Site Exposed Data on 60 Million Users

November 21, 2018 54 Comments

U.S. Postal Service just fixed a security weakness that allowed anyone who has an account at **usps.com** to view account details for some 60 million other users, and in some cases to modify account details on their behalf.

OWASP API #1
Broken Object Level Authorization

What happened:

- USPS relied on traditional code and web scanners
- Found missing API authentication
- USPS added authentication
- Left out authorization
- User A able to access User B details (any of 60M accounts)

PELOTON

Featured Article

Peloton's leaky API let anyone grab riders' private account data

But the company won't say if it has evidence of malicious exploitation

Zack Whittaker @zackwhittaker / 4:00 AM PDT • May 5, 2021 Comment

OWASP API #1
Broken Object Level Authorization

OWASP API #2
Broken Authentication

What happened:

- Open API allowed requests for user details with NO authentication
- 4M user account details exposed (including Joe Biden)
- Including accounts marked private
- Researcher reported to Peloton
- No response after 90 days
- "Fixed" vulnerability by adding authentication
- But hackers could still access all records, just needed to authenticate

venmo

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

DAN SALMON SECURITY JUN 26, 2019 9:00 AM

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

Opinion: Venmo makes sending and receiving money a social affair. But those emoji-laden payment descriptions leave you exposed to cyberattacks.

"There's truly no reason to have this API open to unauthenticated requests," he told TechCrunch. "The API only exists to provide like a scrolling feed of public transactions for the home page of the app, but if that's your goal then you should require a token with each request to verify that the user is logged in."

What happened:

- Venmo homepage presented live feed of transactions
- Hacker sniffed traffic and identified API calls
- Wrote 20-line script, using 2 IPs
- Pulled 115K transactions/day – even with rate limiting in place
- API returned ALL transaction details
- 207M transactions harvested

OWASP API #2
Broken Authentication

OWASP API #3
Broken Object Property Level Authorization

OWASP API #4
Unrestricted Resource Consumption

Instagram

TIME SUBSCRIBE

TECH • INSTAGRAM

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

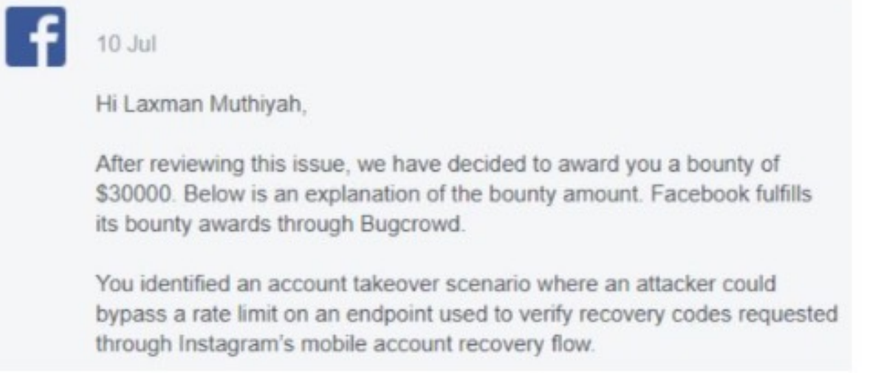
"We recently discovered that one or more individuals obtained unlawful access to a number of high-profile Instagram users' contact information — specifically email address and phone number — by exploiting a bug in an Instagram API," a spokesperson for Instagram said in a statement to TIME.

OWASP API #1
Broken Object Level Authorization

OWASP API #2
Broken Authentication

What happened:

- Account reset requires 6-digit code
- Researcher found API to submit reset code guesses
- Guesses limited to 200 per IP
- Researcher demonstrated could rotate through 5,000 IPs in seconds
- Enables takeover of ANY account



10 Jul

Hi Laxman Muthiyah,

After reviewing this issue, we have decided to award you a bounty of $30000. Below is an explanation of the bounty amount. Facebook fulfills its bounty awards through Bugcrowd.

You identified an account takeover scenario where an attacker could bypass a rate limit on an endpoint used to verify recovery codes requested through Instagram's mobile account recovery flow.

bumble

threatpost Podcasts / Malware / Vulnerabilities / InfoSec Insiders

Dating Site Bumble Leaves Swipes Unsecured for 100M Users

What happened:

- API permitted access to 95M user account details w/o authentication
- Incremental IDs allowed easy scraping of entire database
- Enabled calculation of users' exact location via triangulation
- API allowed paid features to be enabled without proper privileges

OWASP API #1
Broken Object Level Authorization

OWASP API #2
Broken Authentication

OWASP API #5
Broken Function Level Authorization

T-Mobile™

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of report (Date of earliest event reported): January 19, 2023

T-Mobile

T-MOBILE US, INC.

(Exact Name of Registrant as Specified in Charter)

What happened:

> "The preliminary result from our investigation indicates that the bad actor(s) obtained data from this API for approximately 37 million current postpaid and prepaid customer accounts."

On January 5, 2023, I-Mobile US, Inc. (the "Company," "we," or "our") identified that a bad actor was obtaining data through a single Application Programming Interface ("API) without authorization. We promptly commenced an investigation with external cybersecurity experts and within a day of learning of the malicious activity, we were able to trace the source of the malicious activity and stop it. Our investigation is still ongoing, but the malicious activity appears to be fully contained at this time, and there is currently no evidence that the bad actor was able to breach or compromise our systems or our network.

OPTUS

What happened:

- API endpoint required no authentication to access
- Attacker harvested 9.8M user details and threatened $1M ransom
- Data included driver's license, Medicare IDs, name, phone, email

OWASP API #1
Broken Object Level Authorization

OWASP API #3
Broken Object Property Level Authorization

OWASP API #4
Unrestricted Resource Consumption

What happened:

- Experian partner site offered loan eligibility feature
- Feature used Experian API for lenders to automate credit score lookup
- Attacker sniffed API calls
- API accessible with no authentication
- Results delivered with name, address and *any* value for date of birth

OWASP API #1
Broken Object Level Authorization

OWASP API #3
Broken Object Parameter Level Authorization

OWASP API #9
Improper Inventory Management