Merkle Fence

10 of the worst **API security breaches** in 2023

www.merklefence.com

SWIPE LEFT

An estimated **83% of all internet traffic comes from APIs**(1). API breaches have a major impact, while being less frequently publicly revealed. API-related security breaches affected over **16 million records** in 2022. However, by 2023, the average impact per API-related data breach would be approximately **6 million records**(2). API breaches are projected to cost the world **$75 billion** in financial losses each year(3).

Merkle Fence

SWIPE LEFT

83% Internet Traffic comes from APIs

16 Records in 2022

MILLION

6 In 2023 **MILLION** Records

This report examines the top API Security events of 2023 against the backdrop of the OWASP API Security Top 10 vulnerabilities, as well as related Common Weakness Enumerations (CWEs) and Common Vulnerabilities and Exposures (CVEs).

Merkle Fence

SWIPE LEFT

1. Imagine if a stranger could unlock your car...

On January 3, 2023, Sam Curry and his team, uncovered a major API vulnerability impacting top automotive brands like **Toyota, Mercedes, BMW, Ferrari, Rolls Royce, and Reviver.** This flaw put car owners' personal information at risk. Attackers could potentially unlock, start, track vehicles, or even falsely report them as stolen, posing a serious security threat[4].

The attack exploited two common vulnerabilities listed in the OWASP API Security Top 10: **Broken Authentication** and **Broken Object Property Level Authorization.** The related Common Weakness Enumerations (CWEs) are CWE-213, CWE-287
and CWE-915

Merkle Fence

SWIPE LEFT

2. Toyota's Supply Chain Vulnerabilities

On February 6, 2023, security researcher Eaton discovered a huge flaw in Toyota's Global Supplier Preparation Information Management System (GSPIMS). This critical web tool oversees Toyota's global supply chain relationships. Surprisingly, Eaton discovered that only having a valid Toyota employee email address was enough to gain access. Using Open-Source Intelligence (OSINT) techniques, he found employee emails, resulting in unlawful access to over 14,000 user accounts and critical information(5).

This attack primarily exploited two OWASP API Security Top 10 vulnerabilities: API2 (Broken Authentication) and API6 (Unrestricted Access to Sensitive Business Flows). This attack's linked Common Weakness Enumerations (CWEs) are CWE-287 and CWE-204.

Merkle Fence

SWIPE LEFT

3. This API's Flaw Exposed Confidential Raid Coordination Data Among U.S. Law Enforcement

SweepWizard, a US law enforcement raid coordinating tool, leaked confidential information. This compromise allowed unauthorized access to sensitive data without login credentials. This vulnerability could reveal law enforcement operation timing and suspect and official PII. The breach affected roughly **6000 people.**

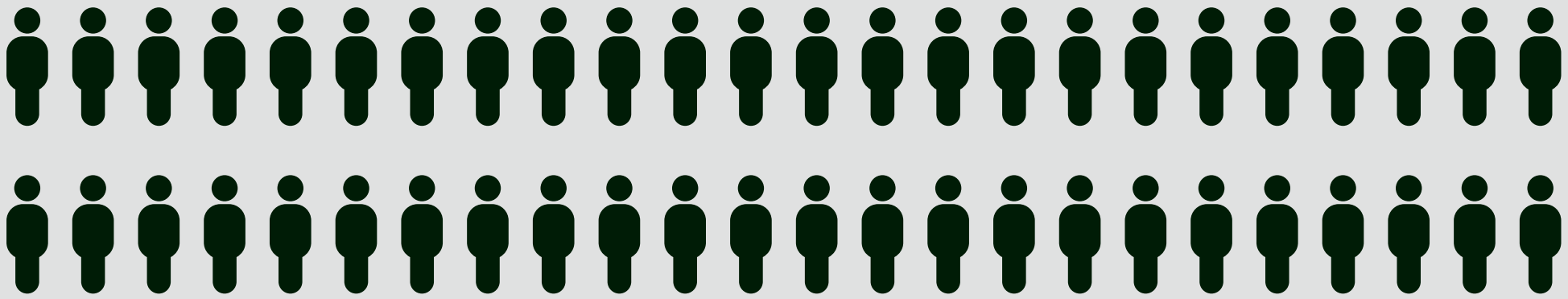
Merkle Fence

SWIPE LEFT

After receiving a tip on SweepWizard's API vulnerability, WIRED Magazine responsibly informed the LAPD. WIRED Magazine documented this incident on January 11, 2023[6].

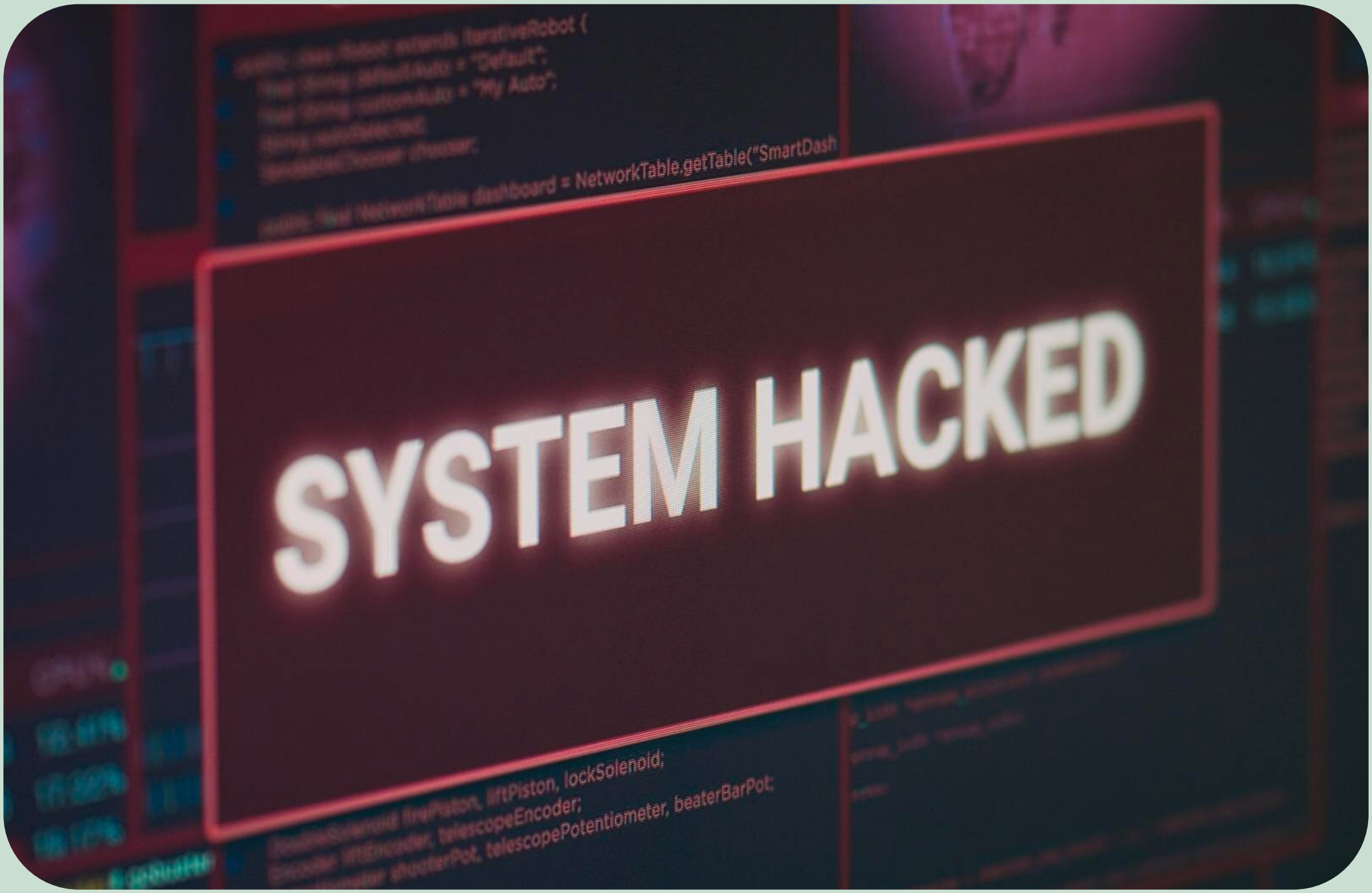
6,000

Pepople Affected



Merkle Fence

SWIPE LEFT



This attack involves CWE-285, 287, and 213. The breach exploited OWASP API Security Top 10 vulnerabilities API1 (Broken Object Level Authorization), API2 (Broken Authentication), API3 (Broken Object Property Level Authorization), and API8 (Security Misconfiguration).

Merkle Fence

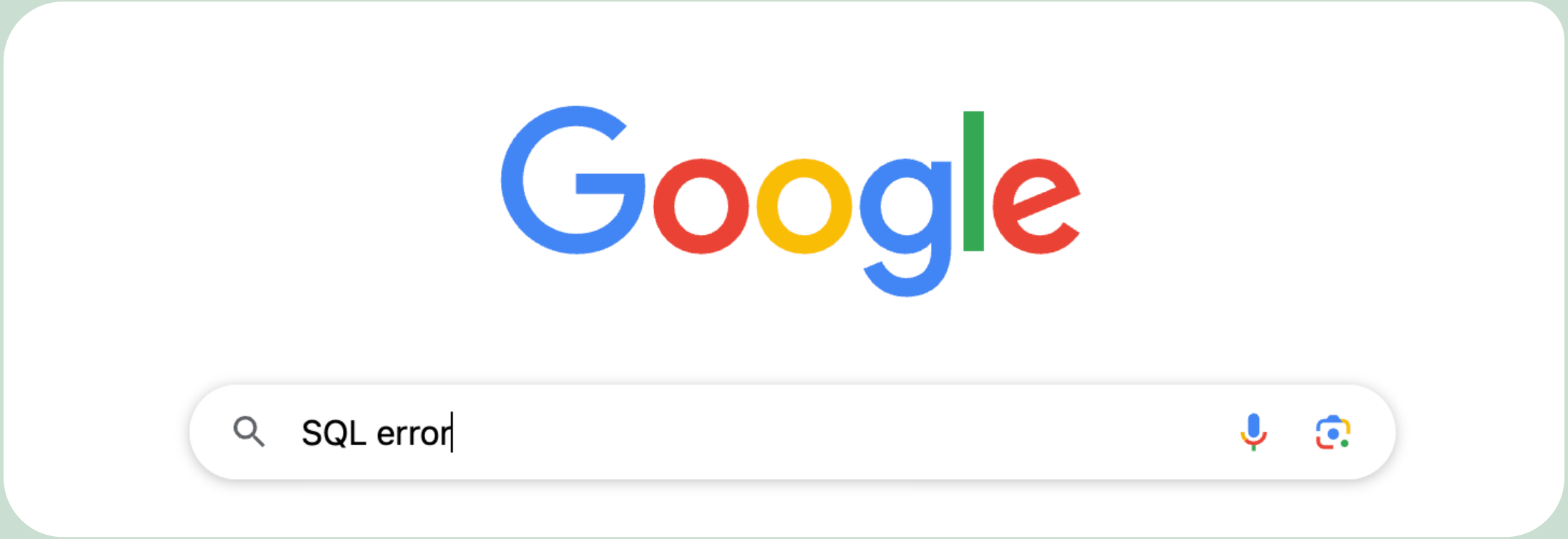
SWIPE LEFT

4. A Google Search Result Turned Out To Be An API Leaking Bangladeshi Citizens Data

An API address on a Bangladeshi government website that let people's Personally Identifiable Information (PII) be seen was found by Viktor Markopoulos from Bitcrack Cybersecurity on June 27, 2023. According to TechCrunch, Markopoulos's discovery was a happy accident.

He said, “It just appeared as a Google result and I wasn’t even intending on finding it. I was Googling an SQL error and it just popped up as the second result" (7)

A huge 50,000,000 Bangladeshi individuals' email addresses, phone numbers, and national ID card numbers were found.



Merkle Fence

SWIPE LEFT

The CWEs that go with this attack are CWE-285 and CWE-213. The breach took advantage of flaws listed in the OWASP API Security Top 10, such as API1 (Broken Object Level Authorization) and API3 (Broken Object Property Level Authorization).

Merkle Fence

SWIPE LEFT

5. Major Flaw in Indian Government Site, Risked 17 million Records

Sourajeet Majumder discovered a bug on an Indian government website that let people see their Aadhaar numbers, ID cards, and fingerprints. An Aadhaar number is a 12-digit personal identification number that can be used anywhere in India to prove who you are and where you live.

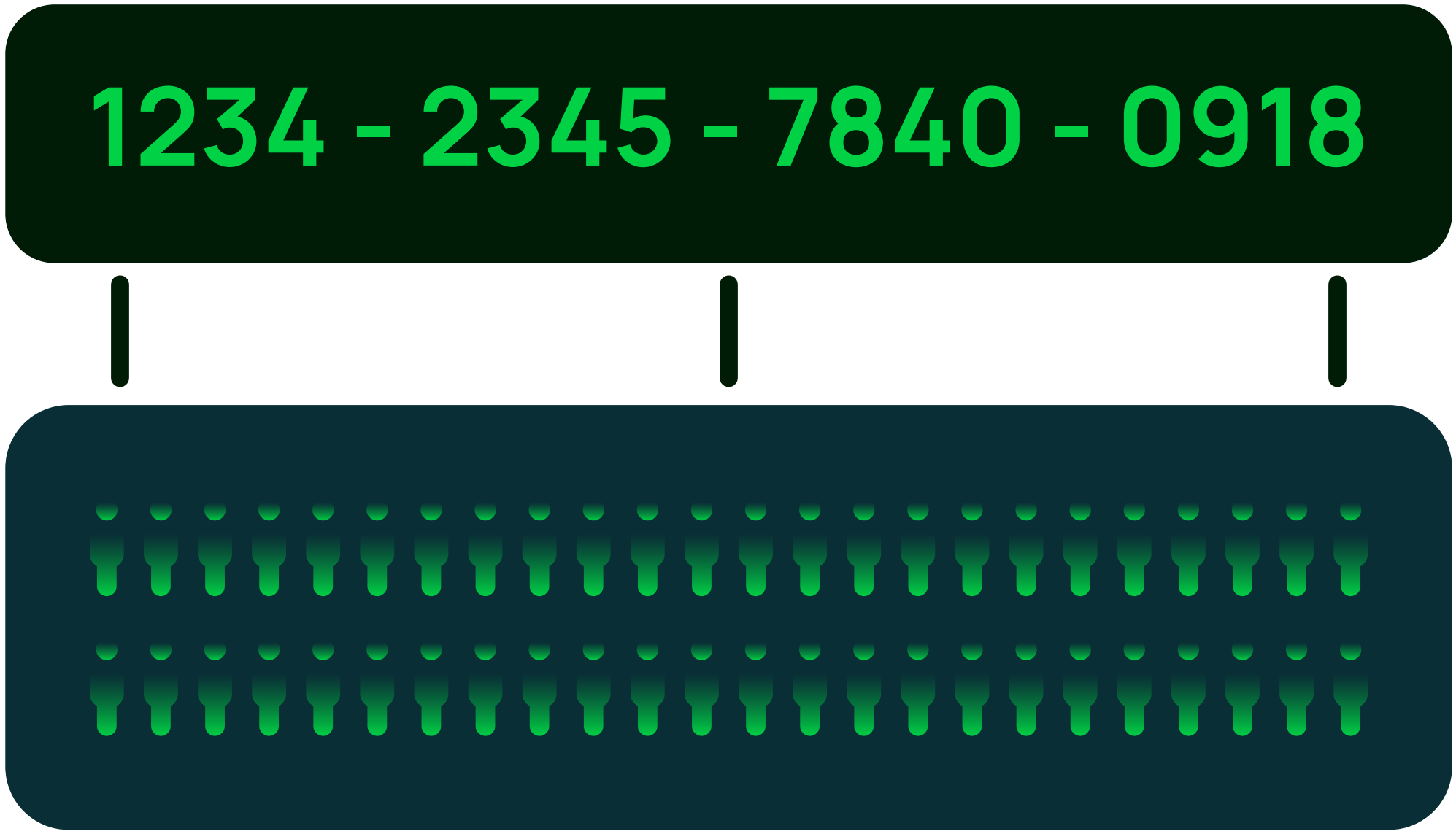
Merkle Fence

SWIPE LEFT

The website where this bug was found was processing 17,000,000 records at the time it was found, so there is a chance that 17,000,000 records have been stolen(8).

These three CWEs are linked to this attack: CWE-285, CWE-213, and CWE-319. The attack took advantage of flaws listed in the OWASP API Security Top 10, such as API1 (Broken Object Level Authorization), API3 (Broken Object Property Level Authorization), and API8 (Security Misconfiguration).

Aadhaar number



17 MILLION

Records Have been stolen

Merkle Fence

SWIPE LEFT

6. T-Mobile's Security Breach Exposes 37 Million Customer Records via Vulnerable API

T-Mobile discovered a security incident on January 5, 2023, in which a hacker exploited a vulnerable API to obtain customer information. A total of **37,000,000** active T-Mobile customer records were acquired(9). Due to the gravity of the circumstances, T-Mobile formally announced the occurrence in a filing with the United States Securities and Exchange Commission on January 19, 2023(10).

CWE-285 is the associated CWE for this attack. Vulnerabilities detailed in the OWASP API Security Top 10 were exploited during the incident, including API1 (Broken Object Level Authorization) and API5 (Broken Function Level Authorization)

Merkle Fence

SWIPE LEFT

7. A Network Breach At A Golf Equipment Manufacturer Led To More...

Topgolf Callaway Brands Corp., an American golf equipment manufacturer, found suspicious system activity on their networks on August 1, 2023, resulting in a massive breach. The personal information of **1,114,954 people** was compromised, including their names, addresses, emails, phone numbers, order histories, passwords, and security question answers.

Merkle Fence

SWIPE LEFT

The records could be accessed by both authenticated and unauthorized users[11].

Merkle Fence

SWIPE LEFT

This incident is classified under CWE-285 and CWE-287. The breach exploited vulnerabilities outlined in the OWASP API Security Top 10 which includes API1 (Broken Object Level Authorization), and API2 (Broken Authentication).

Merkle Fence

SWIPE LEFT

8. Research Uncovers High-Risk Flaws in QuickBlox, Putting Over 1 Million Users At Risk

Team82 and Check Point Research (CPR) security researchers worked to examine the security of the widely used QuickBlox software development kit (SDK) and application programming interface (API). The analysis uncovered serious flaws in QuickBlox's infrastructure,

which supports chat and video services in important industries such as finance and medical.

Merkle Fence

SWIPE LEFT

These flaws put the personal information of over **1,000,000 users** at danger. The researchers demonstrated possible dangers, such as accessing smart intercoms and remotely unlocking doors, or stealing patient data from telemedicine apps, with proof-of-concept vulnerabilities(12). CVE-2023-31184 has been assigned to the identified vulnerability, which has a CWE of CWE-798.

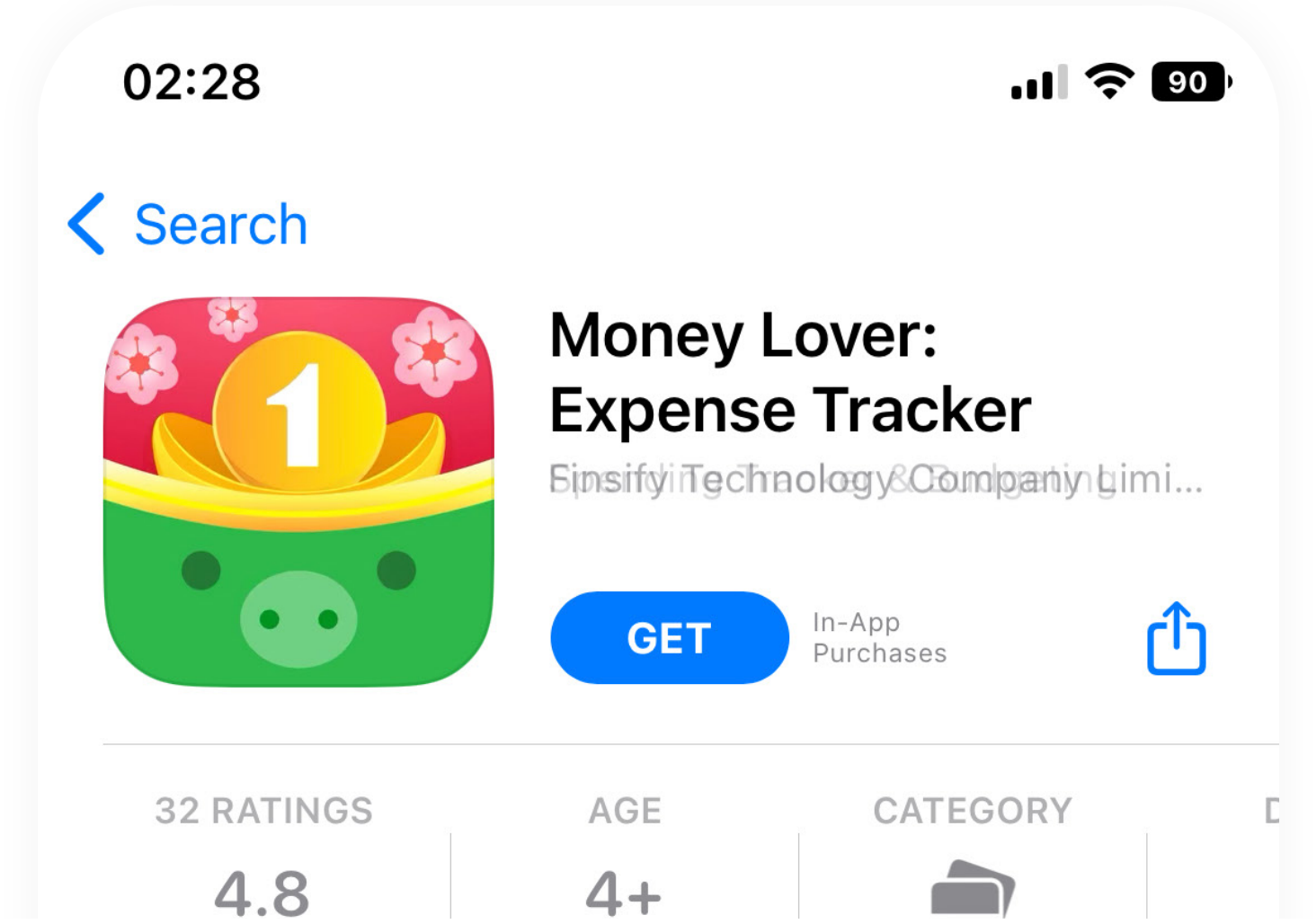
Merkle Fence

SWIPE LEFT

9. Security Flaw in 'Money Lover' App Risks 5 Million User Emails

The finance tracking app 'Money Lover' was found to have an Excessive Data Exposure vulnerability, notably in its "Shared Wallets" capability. Authenticated users could get unauthorized access to live transactions, revealing the emails of around **5,000,000 users.** Troy Driver discovered this vulnerability and responsibly disclosed it to Money Lover developers[13].

5 MILLION



This vulnerability is classified as CWE-213. The attack took advantage of an OWASP API Security Top 10 vulnerability, notably API3 (Broken Object Property Level Authorization).

Merkle Fence

SWIPE LEFT

10. Duolingo API Hack Compromises 2.6 Million User Accounts

By submitting a valid email, a malicious hacker was able to obtain generic account information such as names, email addresses, and languages of study by exploiting a vulnerability in the Duolingo API. The malevolent hacker successfully extracted the personal data of 2,600,000 Duolingo users and offered it for sale on a hacking forum(14).

2 MILLION

The breach exploited a vulnerability outlined in the OWASP API Security Top 10, API2 (Broken Authentication) and the associated CWE is CWE-287.

Merkle Fence

SWIPE LEFT

Additional Reading

1. https://www.akamai.com/site/it/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf
2. https://www.firetail.io/api-data-breach-tracker
3. https://www.imperva.com/company/press_releases/vulnerable-apis-costing-businesses-up-to-75-billion-annually
4. https://samcurry.net/web-hackers-vs-the-auto-industry
5. https://eaton-works.com/2023/02/06/toyota-gspims-hack
6. https://www.wired.com/story/sweepwizard-police-raids-data-exposure
7. https://techcrunch.com/2023/07/07/bangladesh-government-website-leaks-citizens-personal-data
8. https://techcrunch.com/2023/10/12/india-aadhaar-fingerprints-west-bengal
9. https://edition.cnn.com/2023/01/19/tech/tmobile-hack/index.html
10. https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000119312523010949/d641142d8k.htm
11. https://www.bleepingcomputer.com/news/security/golf-gear-giant-callaway-data-breach-exposes-info-of-11-million
12. https://claroty.com/team82/research/major-security-flaws-in-popular-quickblox-chat-and-video-framework-expose-sensitive-data-of-millions
13. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/money-lover-app-vulnerability-exposes-personal-info
14. https://www.bleepingcomputer.com/news/security/scraped-data-of-26-million-duolingo-users-released-on-hacking-forum

Merkle Fence

SWIPE LEFT

Additional Reading

CWE-213 https://cwe.mitre.org/data/definitions/213.html
CWE-287 https://cwe.mitre.org/data/definitions/287.html
CWE-915 https://cwe.mitre.org/data/definitions/915.html
CWE-204 https://cwe.mitre.org/data/definitions/204.html
CWE-285 https://cwe.mitre.org/data/definitions/285.html
CWE-319 https://cwe.mitre.org/data/definitions/319.html
CWE-798 https://cwe.mitre.org/data/definitions/798.html
CVE-2023-31184 https://nvd.nist.gov/vuln/detail/CVE-2023-31184
API1 (Broken Object Level Authorization)
https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorizatio
n
API2 (Broken Authentication)
https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authenticatio
API3 (Broken Object Property Level Authorization)
https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-au
thorization
API5 (Broken Function Level Authorization)
https://owasp.org/API-Security/editions/2023/en/0xa5-broken-function-level-authoriza
tion
API8 (Security Misconfiguration)
https://owasp.org/API-Security/editions/2023/en/0xa8-security-misconfiguration

Merkle Fence

SWIPE LEFT

Merkle Fence

Ready to raise the bar for your application security?

Take the Leap with MerkleFence

TO GET STARTED, VISIT:

www.merklefence.com