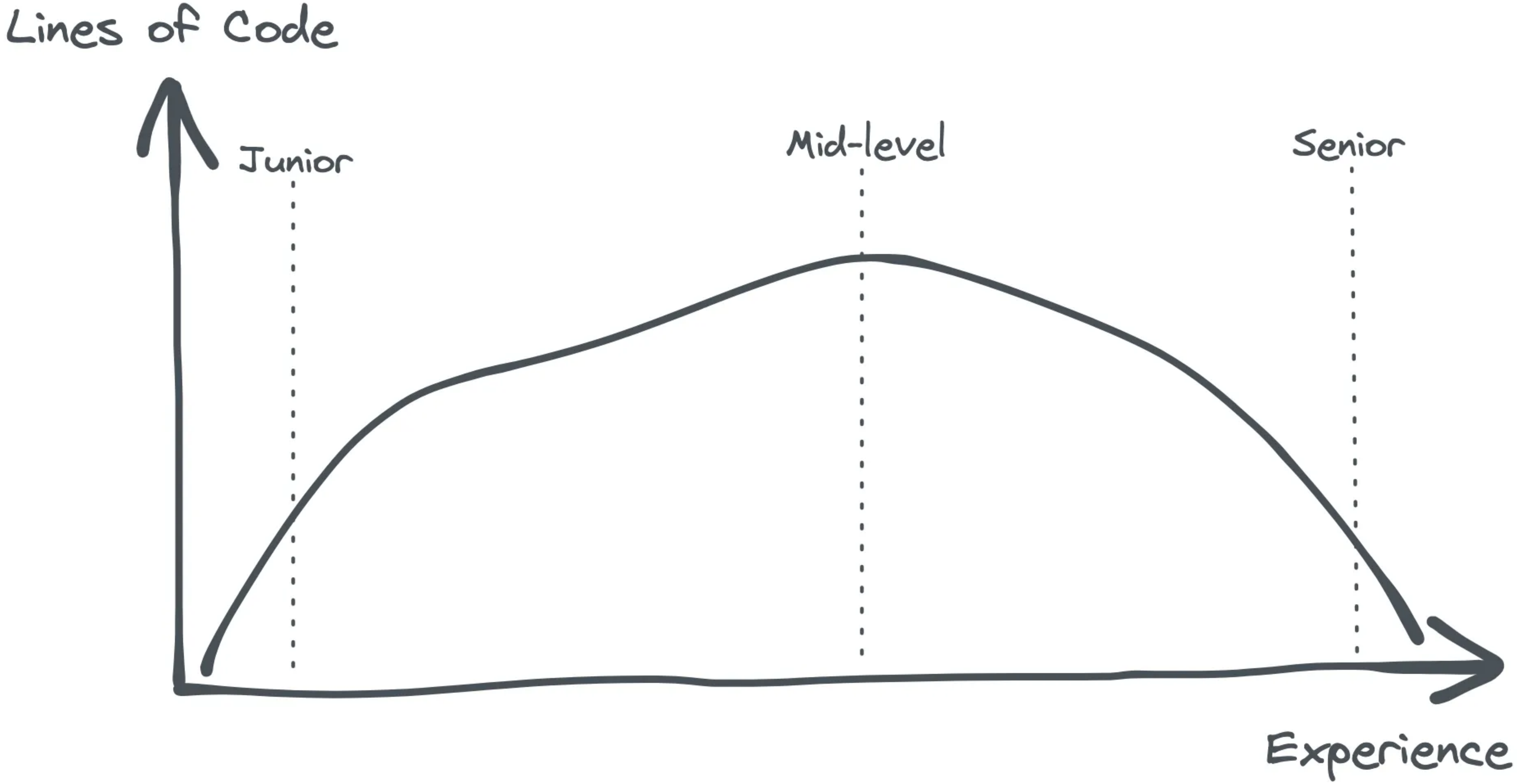
Codename D.D.S.

Marcin Baranowski

Who thinks his application is 100% secure?

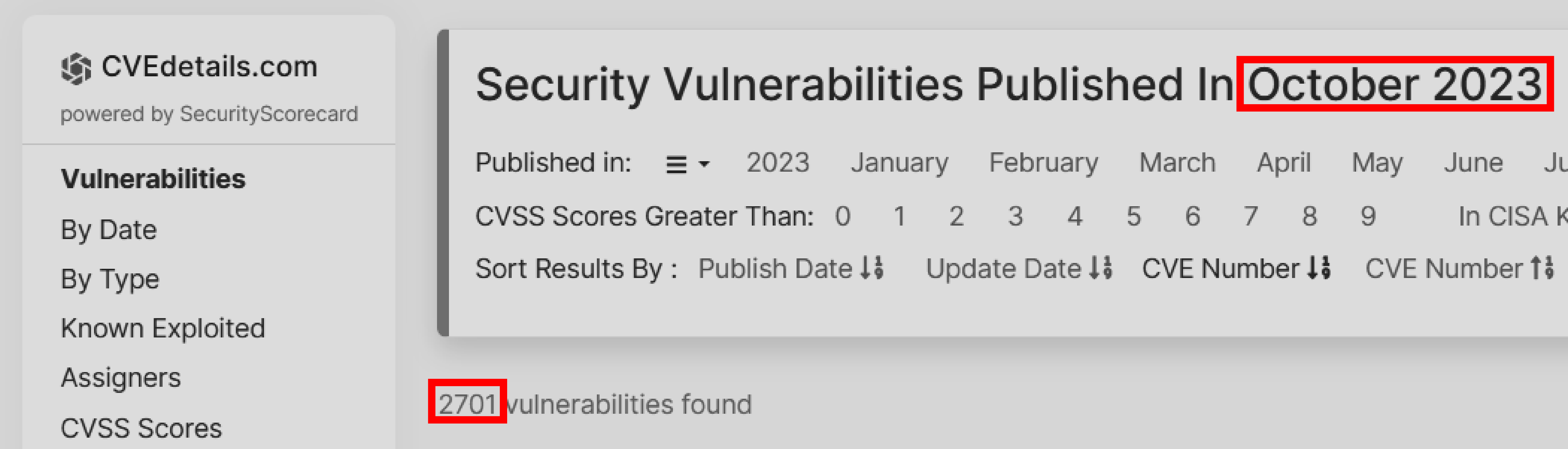
Marcin Baranowski

- Senior Software Engineer
- Security Partner



Source: medium.com

How many new vulnerabilities are revealed every day?



CVEdetails.com

powered by SecurityScorecard

Vulnerabilities

By Date

By Type

Known Exploited

Assigners

CVSS Scores

Security Vulnerabilities Published In October 2023

Published in: ≡ ▾ 2023 January February March April May June Ju

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA K

Sort Results By : Publish Date ↓ Update Date ↓ CVE Number ↓ CVE Number ↑

2701 vulnerabilities found

How many new vulnerabilities are revealed every day?

~69

Mean based on 2022 findings

OWASP
®

Top 1 – Broken Access Control

Top 1 – Broken Access Control

ℹ

- No access control
  - Missing RBAC
  - No permissions defined
- Incorrectly defined access control

!

- Unprivileged access to pages by modification of url
- Admin access from regular user
- Unauthorized access witout sign in

✓

- Deny by default
- Rate limit
- RBAC
- Access lists
- Server side session invalidation on log out
- Short-lived tokens

Top 2 – Cryptographic failures

Top 2 – Cryptographic failures

ℹ

- Sending data by plain text
- Keeping data by plain text
- Outdated encrypting algorithms

!

- Leaked db is readable with no/small effort
- Network traffic can be hijacked
- … and used in malicious way

✓

- Identify sensitive data
- Encrypt all kept/transfered sensitive data
- Use only safe protocols
- Disable cache for response of sensitive data

Top 3 - Injection

ℹ

- Inproper validation of user input
- Concatenation of strings containing user input
- Using unsafe operations like *exec()*

!

- Sql on username input
- Sql in rest query

✓

- Validate user input
- Use frameworks/parametrization to create sql queries
- Use *limit* to avoid mass db records leakage
- Avoid „running” any user input
- … and if You really must use well known, safe sandboxes