German OWASP Day 2025

# THE SURPRISING COMPLEXITY OF FINDING KNOWN VULNERABILITIES

Dustin Born, Matthias Göhring

more security. usd

# WE PROTECT COMPANIES AGAINST HACKERS AND CRIMINALS.

German OWASP Day 2025

# 01 QUALITY OF SECURITY ASSESSMENTS

**THE CONTEXT**

German OWASP Day 2025

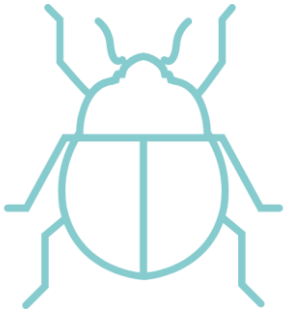
# THE SURPRISING COMPLEXITY OF FINDING KNOWN VULNERABILITIES

## True Positive


## True Negative


## False Positive


## False Negative



## Known Vulnerabilities

Publicly documented security issues, catalogued in databases (e.g. NIST NVD)

→ Research / database lookup

## Unknown Vulnerabilities

Undocumented security issues, incl. zero-day or application-specific vulnerabilities

→ Active test methods, such as pentesting

# Let’s focus on known vulnerabilities.

German OWASP Day 2025

# 02 VULNERABILITY MANAGEMENT CHALLENGES

**THE PROBLEM**

# In an ideal world...

Search for Software Version

*Example: Fortinet FortiWeb 8*

List of Vulnerabilities

- Single, authoritative source & unique IDs
- Meaningful severity & risk scoring for prioritization
- Detailed information & remediation advice (IoCs, PoC)
- Machine-readable access using API

German OWASP Day 2025

# ... in reality:

Let’s focus on known vulnerabilities.

**If a vulnerability is known, why is finding information so hard?**

# The Foundation: CVE, CPE and CVSS

**Common Vulnerabilities and Exposures** (CVE): Unique ID, issued by CVE Numbering Authority (CNA) to collect vulnerability information.

**Challenges with CVE Data:**
Inconsistencies and analysis delay limit CVE's reliability as a sole data source.

## NVD Dashboard

### CVEs Received and Processed

| Time Period | New CVEs Received by NVD | New CVEs Analyzed by NVD | Modified CVEs Received by NVD | Modified CVEs Re-analyzed by NVD |
|---|---|---|---|---|
| **Today** | 92 | 147 | 0 | 11 |
| **This Week** | 202 | 248 | 0 | 12 |
| **This Month** | 2831 | 2929 | 0 | 433 |
| **Last Month** | 4386 | 4156 | 0 | 931 |
| **This Year** | 43971 | 37842 | 0 | 4006 |

### CVE Status Count

| | |
|---|---|
| Total | 319355 |
| Received | 281 |
| Awaiting Analysis | 26194 |
| Undergoing Analysis | 484 |
| Modified | 138940 |
| Deferred | 94583 |
| Rejected | 16179 |

### NVD Contains

| | |
|---|---|
| CVE Vulnerabilities | 319355 |
| Checklists | 847 |
| US-CERT Alerts | 249 |
| US-CERT Vuln Notes | 4486 |
| OVAL Queries | 0 |
| CPE Names | 1513487 |

# The Foundation: CVE, CPE and CVSS

**Common Vulnerabilities and Exposures (CVE):** Unique ID, issued by CVE Numbering Authority (CNA) to collect vulnerability information.

**Common Platform Enumeration (CPE):** Structured naming scheme to address systems, software and its versions.

# Common Platform Enumeration (CPE)

```
cpe:2.3:<part>:<vendor>:<product>:<version>:<update>:                STRUCTURE
<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>
```

```
cpe:2.3:a:fortinet:fortiweb:8:*:*:*:*:*:*:*                          EXAMPLE
```

The CPE structure is great for automation, but mapping simple text search is nontrivial. The central CPE database is maintained by NVD, which is struggling to keep up the pace, leading to inconsistencies and missing CPEs.

# The Foundation: CVE, CPE and CVSS

**Common Vulnerabilities and Exposures (CVE):** Unique ID, issued by CVE Numbering Authority (CNA) to collect vulnerability information.

**Common Platform Enumeration** (CPE): Structured naming scheme to address systems, software and its versions.

**Common Vulnerability Scoring System (CVSS):** Unified severity score from 0 to 10 based on exploitability and impact metrics.

## Data Sources

Beyond CVE & NVD: GitHub Security Advisories (GHSA), CISA Known Exploited Vulnerabilities (KEV), European Union Vulnerability Database (EUVD)

## Software Identification

Improving on CPE accuracy, alternative identifiers in closed ecosystems (package repositories)

## Scoring

From technical severity to risk-based scoring, e.g. with Exploit Prediction Scoring System (EPSS)

German OWASP Day 2025

# 03 FINDING KNOWN VULNERABILITIES MADE EASY

**(A CONTRIBUTION TO) THE SOLUTION**

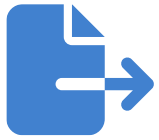
# Design Principles of search_vulns

**Accuracy**: find all that's relevant

**Consolidating** information across data sources

**All-in-one**, easy access, automation using API

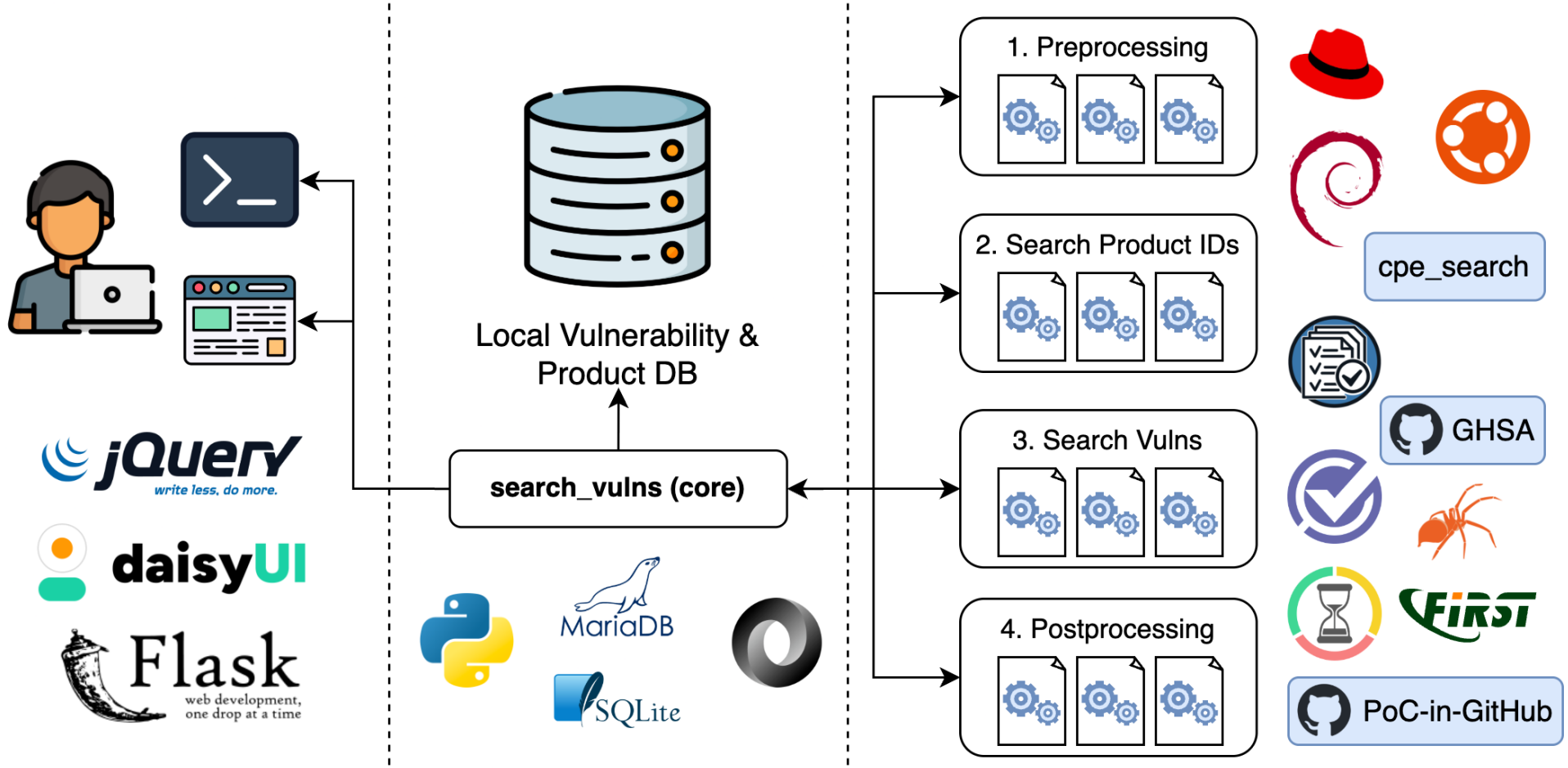
**Up-to-date** & beyond



Rich and fine-grained **export**

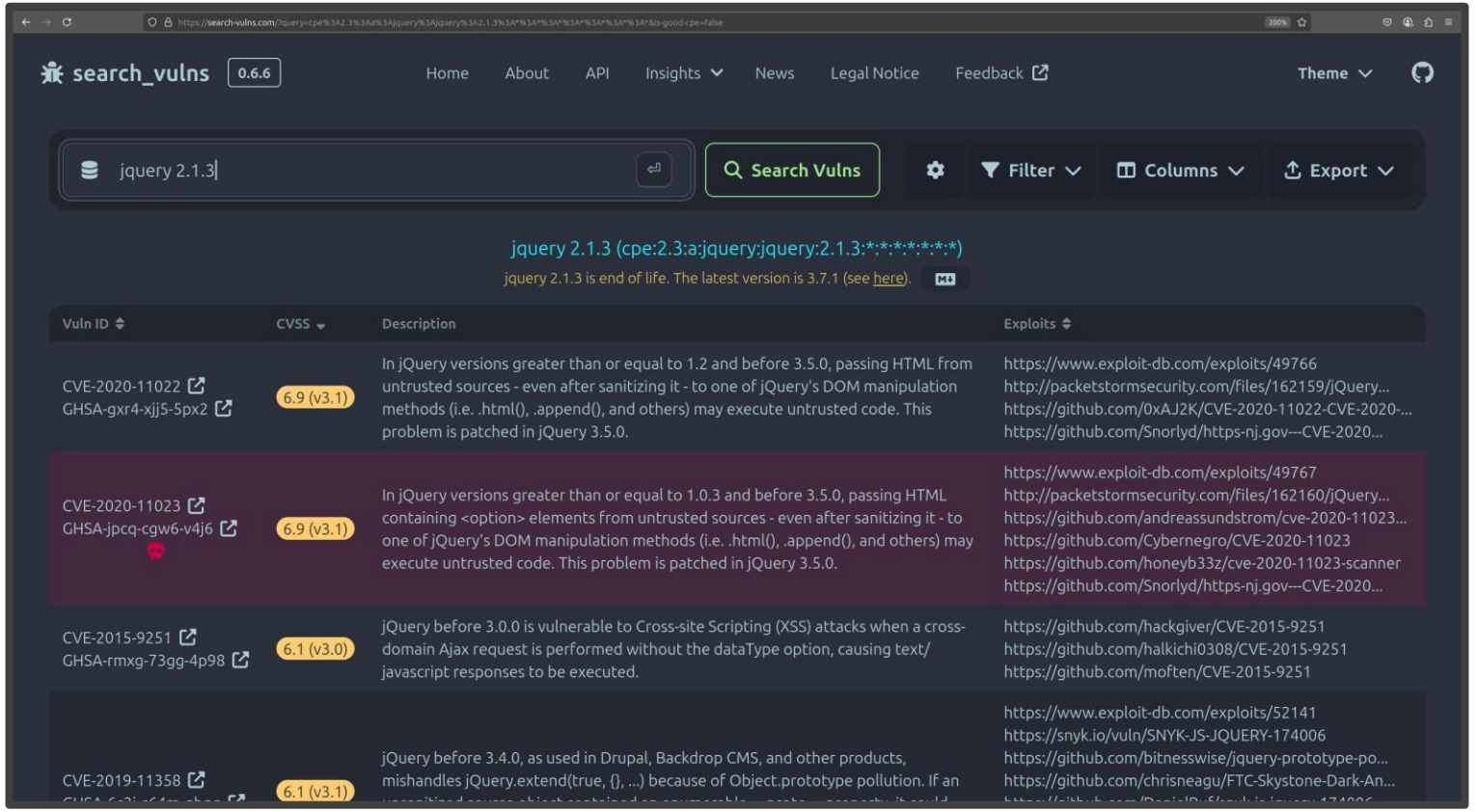
**Offline** database and usage

# Modular Architecture of search_vulns



# Making It Simple – Introducing search_vulns

Demo: https://search-vulns.com/



German OWASP Day 2025

# THE SURPRISING COMPLEXITY OF FINDING KNOWN VULNERABILITIES

Quality means
**finding all vulnerabilities**

Funding issues & analysis
delays with CVE & NVD

search_vulns can make
information more accessible

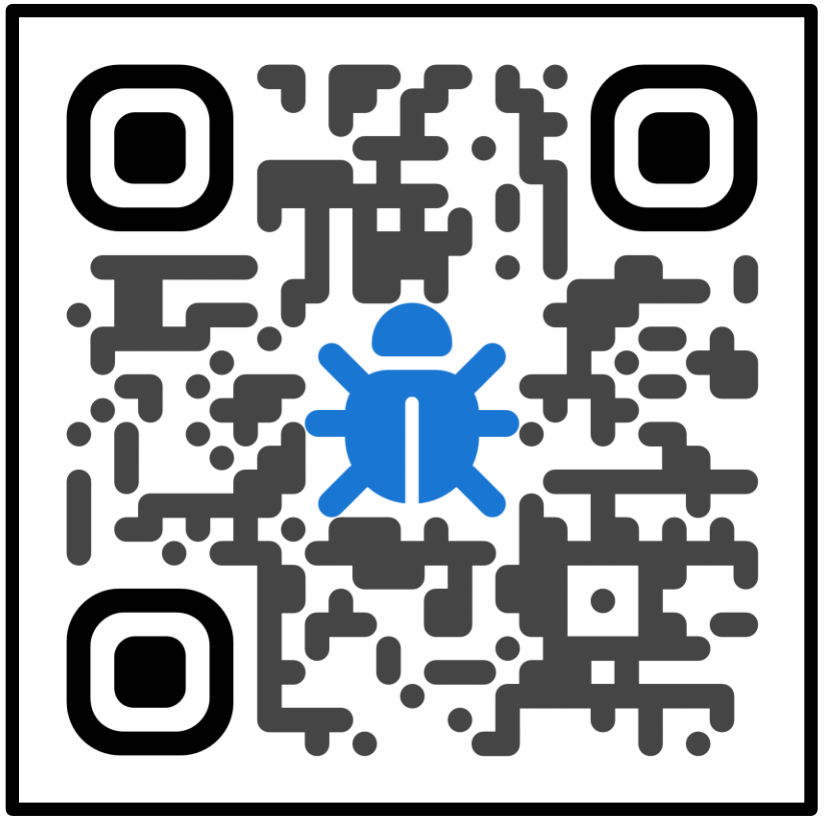
Finding details on known
vulnerabilities is hard

Defenders need modern standards
& tools for risk-based prioritization

German
OWASP
Day 2025

# THANK YOU!

Dustin Born, Matthias Göhring



https://search-vulns.com

https://github.com/ra1nb0rn/search_vulns

German

# OWASP

Day 2025