



German
OWASP
Day 2025

THE SURPRISING COMPLEXITY OF FINDING KNOWN VULNERABILITIES

Dustin Born, Matthias Göhring

WE PROTECT
COMPANIES
AGAINST HACKERS
AND CRIMINALS.





01 QUALITY OF SECURITY ASSESSMENTS

THE CONTEXT

True Positive



True Negative

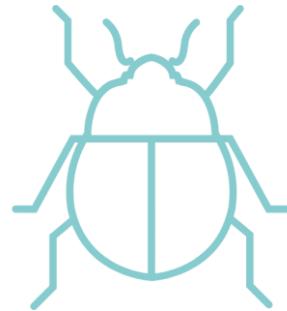


False Positive



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.



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

... in reality:

Pentests

CISA KEV NIST NVD MITRE ATT&CK
Red Teaming EPSS CPE CVSS Vulnerability Management
CWSS EUVD
CNA searchsploit
VULNERABILITIES endoflife.date
Code Reviews GHSA VulnCheck cve-search
OWASP Risk Rating VEX SBOM POC Snyk
Backports Exploit-DB GOOGLE OSV.DEV
Scans CWE Bug Bounty
Supply-Chain Security Databases
Scores
Tools & Misc

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>:  
<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>
```

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

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)

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

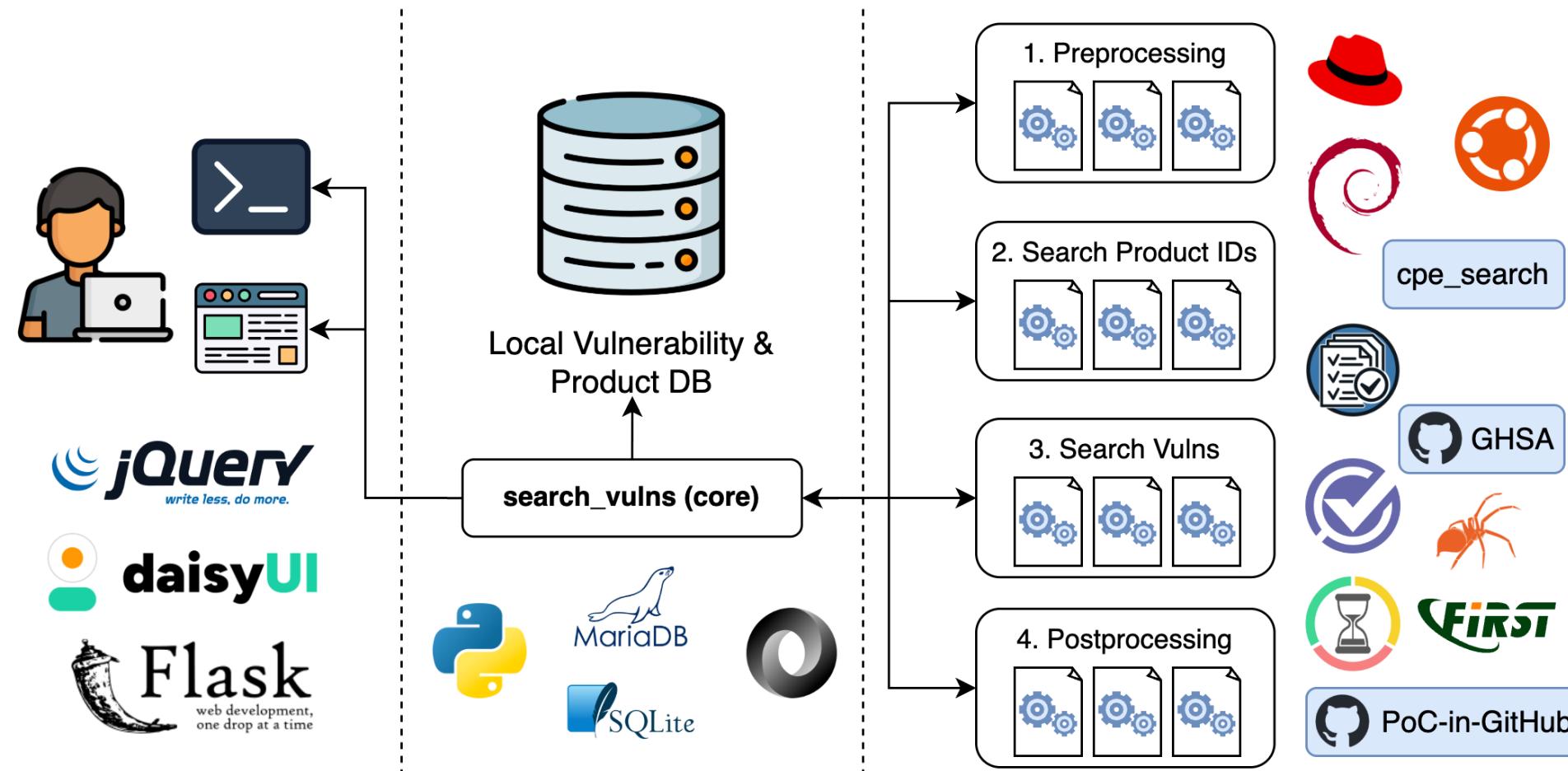


Rich and fine-
grained **export**



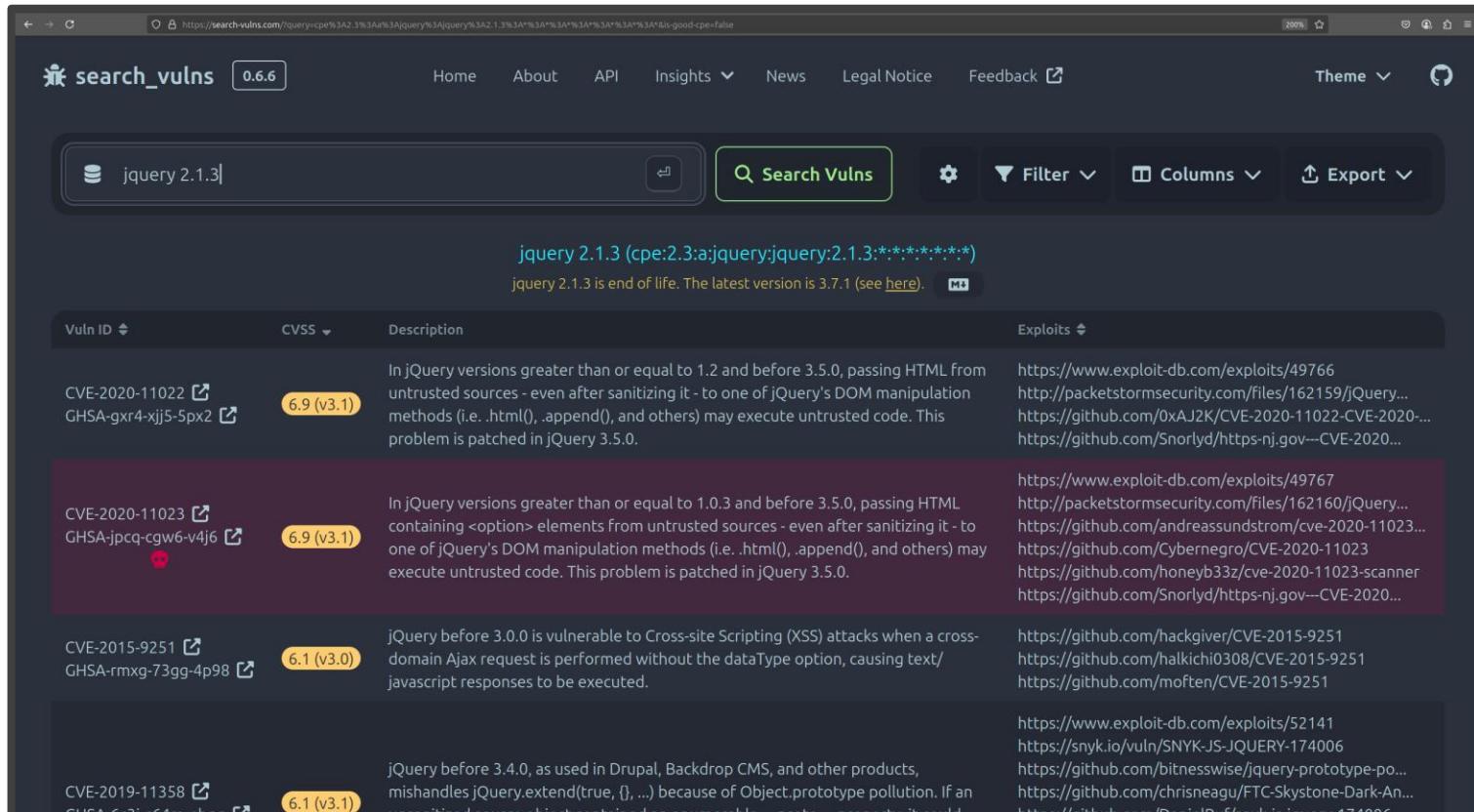
Offline database
and usage

Modular Architecture of search_vulns



Making It Simple – Introducing search_vulns

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



The screenshot shows the search_vulns website interface. The search bar at the top contains the query "jquery 2.1.3". Below the search bar, a message states "jquery 2.1.3 (cpe:2.3:a:jquery:jquery:2.1.3:***:***:***)" and "jquery 2.1.3 is end of life. The latest version is 3.7.1 (see [here](#)).". The main content area displays a table of vulnerabilities:

Vuln ID	CVSS	Description	Exploits
CVE-2020-11022	6.9 (v3.1)	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	https://www.exploit-db.com/exploits/49766 http://packetstormsecurity.com/files/162159/jQuery... https://github.com/0xAJ2K/CVE-2020-11022-CVE-2020... https://github.com/Snorlyd/https-nj.gov--CVE-2020...
CVE-2020-11023	6.9 (v3.1)	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	https://www.exploit-db.com/exploits/49767 http://packetstormsecurity.com/files/162160/jQuery... https://github.com/andreassundstrom/cve-2020-11023... https://github.com/Cybernegro/CVE-2020-11023 https://github.com/honeyb33z/cve-2020-11023-scanner https://github.com/Snorlyd/https-nj.gov--CVE-2020...
CVE-2015-9251	6.1 (v3.0)	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.	https://github.com/hackgiver/CVE-2015-9251 https://github.com/halkichi0308/CVE-2015-9251 https://github.com/moften/CVE-2015-9251
CVE-2019-11358	6.1 (v3.1)	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an	https://www.exploit-db.com/exploits/52141 https://snyk.io/vuln/SNYK-JS-JQUERY-174006 https://github.com/bitnesswise/jquery-prototype-po... https://github.com/chrisneagu/FTC-Skystone-Dark-An...

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

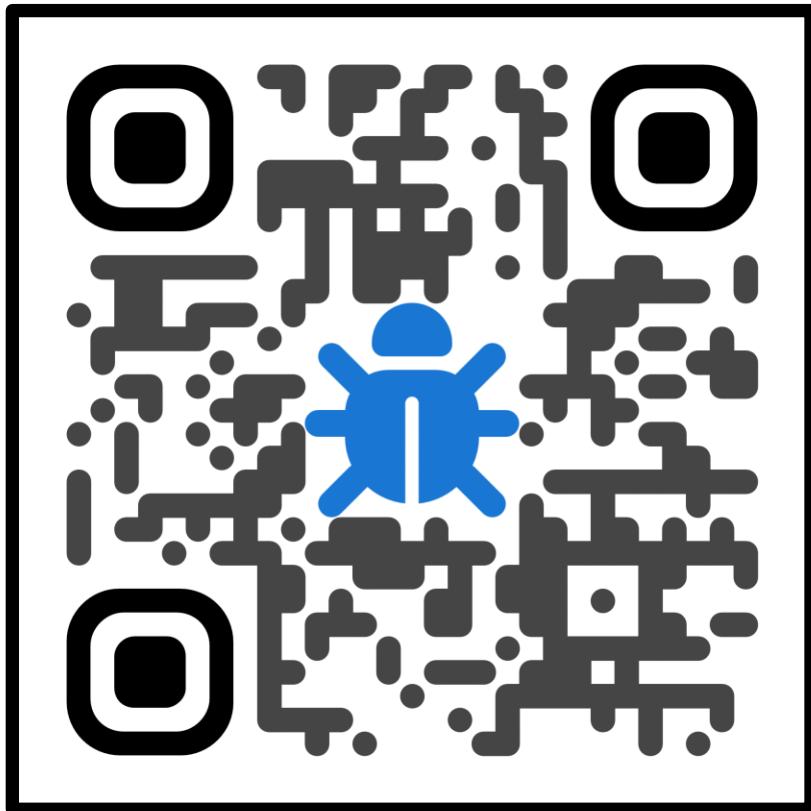




German
OWASP
Day 2025

THANK YOU!

Dustin Born, Matthias Göhring



<https://search-vulns.com>



https://github.com/ra1nb0rn/search_vulns



German
OWASP
Day 2025