Classifying and Recording Vulnerabilities

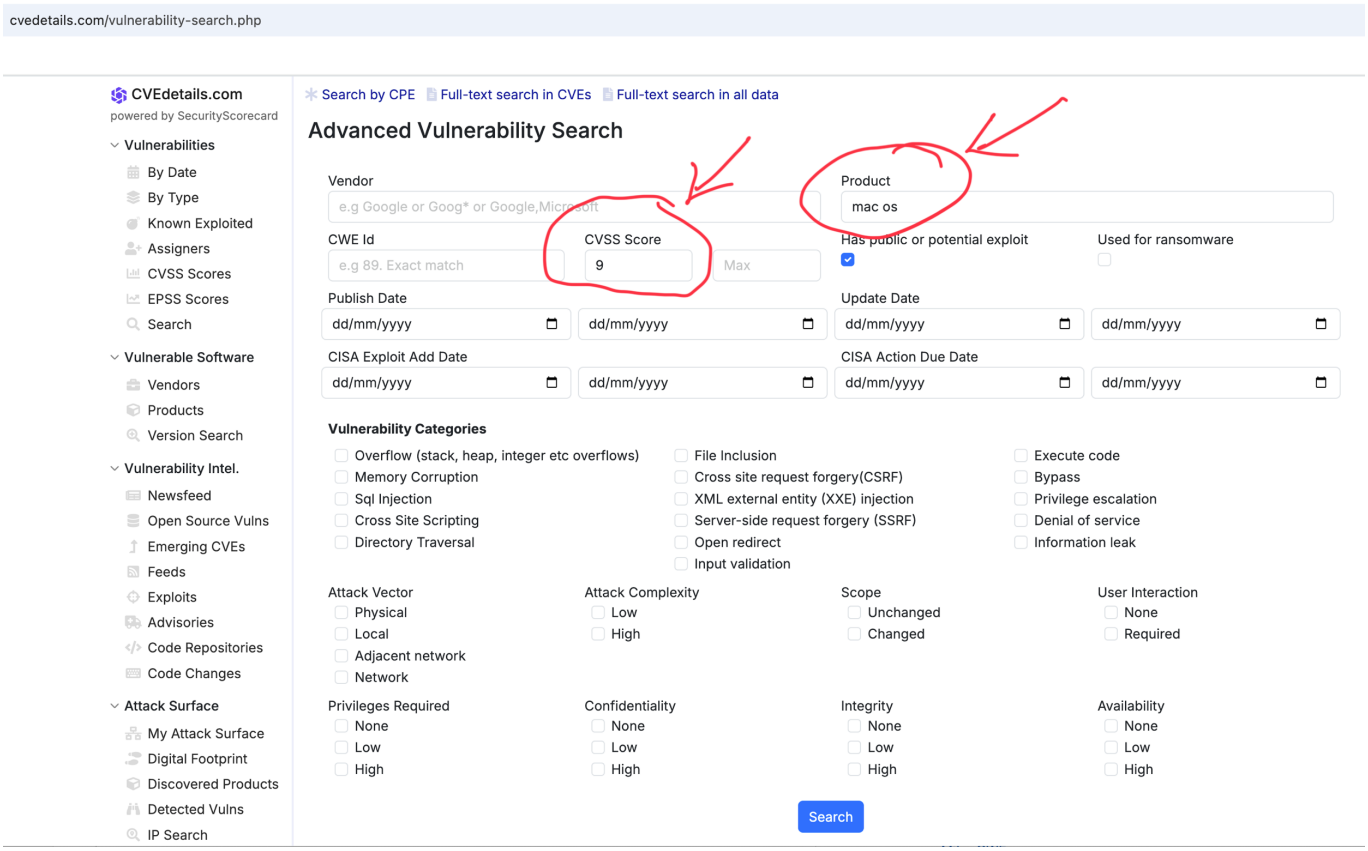
Weakness vs. Exploit

- **Vulnerability:** an exploitable instance of a weakness that can be exploited by an attacker.
- **Weakness:** classes of vulnerabilities, e.g., a bug/flaw (e.g., buffer overflow, injection) that could lead to a vulnerability.
- **Exposure:** mistake or configuration issue than can be used as an entry point.
- **Exploit:** piece of code, software, or a set of commands that takes advantage of a vulnerability or flaw .
- Useful: classify both **weakenesses** and **vulnerability** instances.

CVE (Common Vulnerabilities and Exposures)

- Mitre CVE List
- NVD - National Vulnerability Database
- CVE Details

CVE Details



CVE Entries

- CVSS score: 0-10, it measures the technical severity of a vulnerability.
- EPSS score: 0-10, it measures how likely is the vulnerability to be exploited within the next 30 days.

CVE (Common Vulnerabilities and Exposures)

- Standardized vulnerability IDs, hosted by MITRE.
- Format: CVE-YYYY-NNNN (changed in 2014 to support more digits).
- CVEs link vendor advisories and **proof-of-concepts**.

CWE (Common Weakness Enumeration)

- MITRE-hosted list of known software flaws.
  - Mitre CWE
- Provides identification, examples, mitigation.
- CWEs can be hierarchical: e.g.,
  - 120 (classic buffer overflow),
  - 121 (stack),
  - 122 (heap).

CVE Entries

- Steps: Report → ID assignment → Disclosure → Listing.
- Example: CVE-2018-7600 (Drupal remote code execution).
- NIST's NVD provides CVSS scores and analysis.
- **Impact**: e.g. Confidentiality, Integrity, Availability, Non-Repudiation.
- Relationship with other CWEs
- Mitigation strategies

CWE - (Common Weakness Enumeration)

Examples:

CWE-807 Reliance on Untrusted Inputs in a Security Decision

CWE-22 Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)

CWE-134 Uncontrolled Format String

CWE-190 Integer Overflow or Wraparound

CAPEC (Common Attack Pattern Enumeration & Classification)

- Describes attack steps in detail.
- Maps to CWEs (e.g., attack targets specific weakness).
- Not limited to software—includes hardware, physical, and social engineering attacks.
- Steps that an attacker would take to exploit a vulnerability.
- Capec Mitre

Some Representative Exploits

Chromium Upgrade (v66 → v67)

- 24 CVEs addressed:
  - 6 out-of-bounds access
  - 2 heap buffer overflows
  - 2 use-after-free
  - 2 bypasses

Chromium vs Chrome

Feature	Chromium	Google Chrome
Open source?	✅ 100% open-source	❌ Contains proprietary components
Maintained by	Google + community	Google
Includes Google branding?	❌ No logos, no auto-updates	✅ Yes (logos, auto-update, crash reports)
Built-in Flash/PDF	❌ May not be included	✅ Included
Sync with Google	❌ No	✅ Yes

Meltdown & Spectre

Vulnerabilities in the Picture

- Exploit out-of-order/speculative execution.
- Break memory isolation in modern CPUs.
- Require kernel and hardware updates.

YouTube: Meltdown and Spectre

Detecting and Reporting Vulnerabilities

The Business of Bugs

- Zero-day vulnerabilities = valuable assets.
- Markets:
  - **White market**: responsible disclosure.
  - **Grey market**: gov/law enforcement buyers.
  - **Black market**: underground economy.

Disclosure Models

- **Responsible disclosure**: coordinate with vendor.
- **Full disclosure**: public info forces faster fixes.
- **Non-disclosure**: private use or NDA-bound sharing.

Bug Bounty Programs

- Encourage ethical reporting, offer rewards.
- Examples:
  - **Zero-Day Initiative**
  - **Bugcrowd** (400+ programs)

Risks of Full Disclosure

- Image: HP Cyber Risk Report 2016.
- Pressures vendors, but may expose users before patching.
