Evaluating Information on the Internet

Internet Publishing Reality

- Anyone can publish content online.
- Information may appear as:
  - Blog posts
  - Articles
  - Social media posts
  - Edited public wiki pages
- Because publishing is open to everyone, unverified or unfounded claims can easily spread.
- Topics like cybersecurity practices, programming trends, or DevSecOps preparation may contain unreliable opinions.

Therefore, readers must critically evaluate online information.

Key Factors for Evaluating Information

Source (Authority Check)

- Identify who created or published the information.
- Check:
  - Author’s qualifications
  - Organization reputation
  - Expertise in the subject area
- Publishing content online does not automatically make someone an expert.

Evidence and Reasoning

- Verify whether claims are supported by:
  - Credible data
  - Research findings
  - Logical arguments
- Reliable information relies on:
  - Facts
  - Demonstrable evidence
  - Sound reasoning

Objectivity and Bias

- Determine whether information is:
  - Neutral and balanced
  - Rationally presented

- Watch for:
  - Hidden agendas
  - Product promotion
  - Attacks on competitors
- Prefer sources showing multiple viewpoints.

Corroboration and Consistency

- Cross-check information with multiple independent sources.
- Reliable claims are usually supported by:
  - Several reputable publications
  - Consistent expert agreement
- Avoid trusting a claim supported by only one source.

Advanced Internet Search Techniques

Exact Phrase Search (" ")

- Double quotation marks search for an exact word or phrase.
- Only pages containing the exact sequence are shown.
- Example:
  - "passive reconnaissance"

Site-Specific Search (site:)

- Limits search results to a specific website or domain.
- Example:
  - site:tryhackme.com success stories
  - (Searches only inside TryHackMe website)

Exclude Keyword (-)

- Removes unwanted words or topics from search results.
- Example:
  - pyramids -tourism
  - (Shows information about pyramids excluding tourism-related pages)

File Type Search (filetype:)

- Used to find specific document formats instead of web pages.
- Common file types:
  - PDF → Documents
  - DOC → Word files
  - XLS → Excel sheets
  - PPT → Presentations
- Example:
  - filetype:ppt cyber security
  - (Finds cybersecurity presentations)

Specialized Search Engines

Shodan

Search engine for Internet-connected devices.

What it searches:

- Servers
- Routers
- Networking equipment
- Industrial Control Systems (ICS)
- IoT devices (cameras, smart devices)

Key Capability:

Identifies devices based on software versions and service banners.

Example Search:

- apache 2.4.1
- (Finds servers running Apache version 2.4.1)

Censys

Search engine for Internet assets and hosts.

Difference from Shodan:

- Shodan → Devices & systems
- Censys → Hosts, websites, certificates, domains

Main Uses:

- Domain enumeration
- Open port auditing
- Service discovery
- Detecting unauthorized or rogue assets

VirusTotal

Online malware and virus scanning platform.

Features:

- Scan uploaded files
- Scan URLs
- Check file hashes
- Uses multiple antivirus engines simultaneously

Advantages:

- Combines results from many security vendors
- Provides community analysis and comments
- Helps verify suspicious files

A file flagged as malware may sometimes be a false positive.

Have I Been Pwned (HIBP)

Checks whether an email address appears in known data breaches.

It reveals:

- Exposure of personal data
- Possible password leaks

Security Importance:

- Many users reuse passwords.
- If one platform is breached, other accounts may also become vulnerable.

CVE and Exploit Resources

CVE (Common Vulnerabilities and Exposures)

- CVE is a standardized system used to identify security vulnerabilities in software and hardware.
- It acts like a dictionary or catalog of known vulnerabilities.
- Each vulnerability receives a unique identifier:
  - CVE-Year-Number

- Example:
  - CVE-2024-29988

- CVE-2014-0160 (Heartbleed)
  - Critical vulnerability in OpenSSL
  - Allowed attackers to read sensitive memory data

Exploit Database (Exploit-DB)

A public archive containing:

- Exploit codes
- Vulnerability demonstrations
- Security testing scripts

Used mainly for:

- Penetration testing
- Red team assessments
- Security research