WhoisXMLAPI

OWASP Amass and WhoisXML API Are Now Integration Partners

Posted on May 20, 2022

Access to relevant data is extremely valuable in today’s information-driven environment. That is especially true in the realm of attack surface mapping. By getting a sense of attack surfaces through asset discovery processes for vulnerability management, organizations can assess their security posture and better protect themselves against external attacks.

Attack surface mapping may seem like a lot of work, but cybersecurity experts don’t have to go at it alone. Many members of the cybersecurity community are linked through the Open Web Application Security Project® (OWASP) Foundation, a nonprofit organization that aims to improve software security. The OWASP Amass Project, meanwhile, embodies the community’s synergistic and collaborative effort.

What Is OWASP Amass?

The OWASP Amass Project led to the creation of an open-source tool that helps cybersecurity professionals map out their overall attack surface through Domain Name System (DNS) enumeration and external asset discovery.

Amass can do the above using active reconnaissance techniques and gathering open-source information. The tool can be installed either by compiling data from the source code or using third-party platforms like Docker.

Amass Data Collection Techniques

Amass uses innovative data-gathering methods and techniques. For instance, it scrapes data from different search engines and tools, such as Google, Baidu, Ask, Bing, DNSDumpster, Dogpile, and DNSTable.

Amass also obtains DNS data through basic enumeration methods, reverse DNS seeping, brute forcing, and subdomain permutation, among others.

Furthermore, the tool integrates with several API services, including WhoisXML API, which provides domain and IP intelligence. Other APIs within Amass are VirusTotal, URLScan, Twitter, CommonCrawl, HackerTarget, to name a few.

Amass also scrapes web archives, such as ArchiveToday, the Wayback Machine, and ArchiveIT, ensuring that even historical information is included.

OWASP is open to more people and organizations who wish to contribute to Amass, so more APIs and data sources could be added by using Amass Data Source (ADS) scripts, thus making the tool more comprehensive.

Who Can Use Amass?

OWASP Amass was developed for security professionals who need to perform attack surface mapping and external asset discovery. These users include IT managers, security researchers, chief information security officers (CISOs), penetration testers, and security auditors.

To date, more than 900 forks of the Amass code are available on GitHub, and its adoption continues to grow. In fact, the tool is increasingly being used in bug bounty hunting.

Amass Subcommands

Amass users can perform five subcommands—intel, enum, track, viz, and db. These are described in more detail below.

- **amass intel:** Searches for open-source intelligence related to a target.
- **amass enum:** Performs DNS enumerations and network mapping for Internet-facing systems.
- **amass track:** Compares enumeration results for a target with previously gathered data.
- **amass viz:** Visualizes enumeration results through force-directed link graphs.

- **amass db:** Investigate and manipulate the graph database.

Each of the subcommands has arguments that enable users to obtain more specific data. For example, the following subcommand and argument would return all domains from the reverse WHOIS search result of the target (example[.]com), separated by commas:

```
amass intel -whois -d example.com
```

A complete list of arguments for all subcommands can be found here.

With the OWASP Amass Project, security professionals can tap into multiple cybersecurity intelligence sources by using a single tool. That streamlines the process and gives them more power in their fight against cybercrime.

WhoisXML API contributes to the Amass project by providing domain and IP intelligence through API integration with a variety of plans and subscriptions available for individuals and businesses alike. WhoisXML API is a leading source of domain and IP intelligence, supplementing the capabilities of several cybersecurity systems, from threat intelligence platforms (TIP) to security information and event management (SIEM) systems.