


WhoisXML API Data Is Now Available on ProjectDiscovery Subfinder

Posted on July 16, 2024

 ProjectDiscovery
WhoisXMLAPI

WhoisXML API is excited to announce a new integration with [ProjectDiscovery](#), an open-source-led security company that specializes in the detection of new, exploitable vulnerabilities.

This new collaboration brings WhoisXML API's comprehensive [subdomain data](#) to ProjectDiscover's [Subfinder](#), a tool designed to discover valid subdomains for any domain name through passive enumeration.

This integration further expands Subfinder's data coverage, enabling users to use WhoisXML API intelligence to perform thorough and accurate subdomain enumeration for asset discovery, penetration testing, bug bounty hunting, security assessments, threat detection, and other critical security processes.

WhoisXML API provides Subfinder users with various advantages through this integration, including:

- **Extensive and increasing subdomain data coverage:** The integration gives users access to a massive repository of subdomain data comprising billions of subdomains, with more than 1 million added every day.
- **Widely compatible data formats:** WhoisXML API's subdomain data is well-parsed and comes in consistent data formats compatible with commonly used systems and other intelligence sources.
- **Accurate and up-to-date intelligence:** WhoisXML API's long-standing relationships with major data aggregators, such as domain registries, registrars, and ISPs, grant it direct access to high-quality and accurate raw data. That helps ensure the freshness and reliability of the data the company delivers.

To learn more about the integration, please visit this [installation page](#).

About ProjectDiscovery

ProjectDiscovery is a globally distributed startup on a mission to democratize cybersecurity. We are an open-source-powered security company specializing in preemptive identification of new, exploitable vulnerabilities and misconfigurations. Our cloud platform integrates asset management, vulnerability detection, and cloud security tooling with unique remediation capabilities to provide an

end-to-end solution that continuously secures enterprises' external perimeters and prioritizes protection against attackers over auditors.