

Forum:[Hack Forums](#)

Thread: [\[GUIDE\] Automating Subdomain Enumeration for Bug Bounty Recon](#)

psycheuser - August 23, 2026, 5:27 am

When you start hunting on a wide-scope bug bounty program, manual mapping takes way too long. The fastest hunters use automated reconnaissance pipelines to discover exposed assets before anyone else. Mapping out subdomains is the foundational step for catching hidden targets or subdomain takeovers.

Here is a clean, multi-layered blueprint for setting up an automated passive and active subdomain discovery workflow:

1. Passive Enumeration (Gathering Historic Data)

Start by querying public threat intelligence and historic internet records. You can use tools like Amass or Subfinder to scrape data from search engines, certificate transparency logs (like crt.sh), and passive DNS repositories. Running these tools across multiple API keys ensures high coverage without generating direct traffic to the target.

2. Active Brute-Forcing (Finding Unlisted Assets)

Passive tools won't catch brand new or unindexed subdomains. To find these, run an active resolver like massdns or puredns using a high-quality wordlist (like Assetnote's commonspeak2). Ensure you use a validated list of public trusted resolvers to prevent wildcard false positives or poisoning your results.

3. Permutation and Alteration Scanning

Once you have an initial list, use a tool like alterx or dnsgen to generate smart permutations based on common naming patterns (such as adding "-dev", "-staging", or numerical suffixes like "api-01"). Resolving these newly generated patterns frequently uncovers hidden pre-production servers.

4. Filtering for Active HTTP/S Services

A discovered domain is only useful if it's actually running a service. Route your final compiled list through httpx to quickly verify which endpoints are alive, capturing the HTTP response status codes, page titles, and web server banners automatically.

Setting up a seamless, chained pipeline saves hours of repetitive tool launching and lets you focus straight on the vulnerability analysis stage. For the bounty hunters here, do you prefer orchestrating your recon using custom bash loops, or do you run full framework architectures like Axiom?