BurpSuite

Pre

Most bug hunters open Burp Suite the moment they get a target. I wait.

Here are the 5 things I do before touching Burp Suite:

1. Google Dorking the target
   site:target.com ext:php OR ext:json OR ext:env \\You'd be surprised what's indexed that shouldn't be.
2. Subdomain enumeration \\subfinder + httpx pipeline.\\I'm looking for forgotten dev/staging subdomains.\\They're almost always less hardened than the main app.
3. JavaScript file hunting\\I run waybackurls + gf on every JS file.\\Devs leave API keys, internal routes, and hardcoded tokens here more than anywhere else.
4. Reading the job listings\\The company's open roles tell me their exact tech stack.\\“We use AWS Lambda, React, and PostgreSQL” = I know exactly what to test.
5. Checking old vulnerability disclosures\\Search HackerOne's disclosed reports for the same target or similar tech.\\Patterns repeat. Developers make the same mistakes twice.

Burp Suite is a powerful tool. But it's useless without knowing where to point it.

Recon is where 80% of my findings actually start.

Save this. You'll use it.

Which step surprised you the most? Drop it below

— @sheoraninfosec Bug Bounty Hunter · HackerOne & Intigriti Original post: https://www.linkedin.com/feed/update/urn:li:activity:7459437305418727424

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/tools/burpsuite

Last update: **2026/09/20 14:27**