

Forum:[Hack Forums](#)

Thread: [Good tools for finding FTP vulnerabilities](#)

Bshol - August 5, 2025, 12:04 am

Could you let me know the tools that make it easy to find FTP vulnerabilities? Thanks.

Money- - August 5, 2025, 12:14 am

Just look for CVEs on github. Or MSF scanners but i think those are outdated i guess..

Github look for interesting ftp CVEs and use those or read up new CVEs for FTP and try to write a scanner from the POC give on research articles.

Bshol - August 5, 2025, 12:29 am

(Aug 5, 2025 12:14 AM)Money- Wrote: [\[CITE\]](#) Just look for CVEs on github. Or MSF scanners but i think those are outdated i guess..

Github look for interesting ftp CVEs and use those or read up new CVEs for FTP and try to write a scanner from the POC give on research articles.

Thanks for your reply. Could you introduce some github links based on recent FTP CVEs?

???????????? - August 5, 2025, 12:33 am

(Aug 5, 2025 12:04 AM)Bshol Wrote: [\[CITE\]](#) Could you let me know the tools that make it easy to find FTP vulnerabilities? Thanks.1. Network Scanners & Script EnginesNmap (+ NSE scripts)ftp-anon: checks for anonymous login

ftp-brute: brute-forces credentials

ftp-vsftpd-backdoor: detects the infamous 2.3.4 backdoor

Masscan: Extremely fast host/port discovery; pair with Nmap NSE for deeper FTP checks.

2. Vulnerability ScannersOpenVAS (Greenbone): Full-blown CVE-driven scans—including FTP misconfigs and known CVEs.

Nessus: Commercial-grade checks for outdated FTP daemons, weak ciphers, permissive configs.

3. Brute-Forcing & Credential TestingHydra: Parallelized FTP login brute-forcing; supports username/password lists.

Medusa: Modular, large-scale credential testing.

Patator: Flexible brute-forcer, scriptable for FTP or multi-step auth flows.

4. Protocol Fuzzersboofuzz: Python-based, script custom FTP commands to spot crashes/vuln conditions.

SPIKE Proxy: Generic fuzzer adaptable for FTP to uncover buffer-overflows.

5. Pen-test Frameworks & ExploitationMetasploit: auxiliary/scanner/ftp/* (e.g. ftp_version, ftp_syst, ftp_banner) + exploit modules for vsftpd, ProFTPD, wu-ftp backdoors.

RouterSploit: Embedded-device exploits, includes FTP modules for weak creds and common flaws.

6. Compliance & Misconfiguration CheckersNikto: Scans FTP servers for default files, weak banners, outdated software.

Lynis: Audits Unix/Linux hosts (including FTP daemon configs) for hardening gaps.

DramaKing - August 5, 2025, 4:26 am

Anything with known FTP vulnerabilities has died by now.

K4RM4 - *August 5, 2025, 7:03 am*

Nmap and metasploit are two really good options.