

Forum:[Hack Forums](#)

Thread: [Web Recon](#)

Shutzhacker - February 23, 2025, 2:25 am

best and effective way of doing a Web Application recon. Is it just by looking up on google with some dorks or shodan or scanning for some subdomains and also ips related to the target domain or is it beyond that.

I will love to hear your thoughts and how you engage doing your recon also do you enjoy the process or it's boring ?

s0lo - February 23, 2025, 7:18 am

dont know if its the best or close to that, but i enjoy using rengine for doing recon on web

Shutzhacker - February 23, 2025, 1:51 pm

(Feb 23, 2025 08:18 AM)s0lo Wrote: [\[CITE\]](#) dont know if its the best or close to that, but i enjoy using rengine for doing recon on web

It works for you ?

s0lo - February 24, 2025, 11:44 pm

(Feb 23, 2025 02:51 PM)Shutzhacker Wrote: [\[CITE\]](#) It works for you ?

love it, look it up, it just combines multiple tools, APIs, LLMs, automates the process and then you just dig through and act on the findings

Shutzhacker - February 27, 2025, 9:18 pm

(Feb 25, 2025 01:33 PM)Virulent Wrote: [\[CITE\]](#) Start with passive techniques, such as domain and subdomain discovery (using tools like WHOIS, Sublist3r, or Amass), Google dorking, and OSINT analysis via social media and search engines. Next, conduct active reconnaissance with tools like Nmap to scan ports, Burp Suite to analyze HTTP headers, and Nikto for vulnerability scanning. Advanced techniques include brute-forcing login forms, fuzzing for input validation flaws, and testing for common vulnerabilities like SQL injection and XSS.

Nice thanks for sharing your thoughts with everyone