

Forum:[Hack Forums](#)

Thread: [what scanners do you use to scan sites for vuln?](#)

drneed - October 30, 2020, 11:45 am

OSINT probably..

10000days - October 30, 2020, 3:29 pm

I'd recommend checking out:

- sqlmap
- OpenDoor
- WPScan
- XSSStrike

G.P.D. - October 30, 2020, 5:25 pm

(Oct 30, 2020 03:29 PM)10000days Wrote: [\[CITE\]](#) I'd recommend checking out:

- sqlmap
- OpenDoor
- WPScan
- XSSStrike

Those are really good scanners, but I'd recommend Nikto and DNSDumpster as well :

<https://github.com/sullo/nikto>

<https://dnsdumpster.com/>

ButtermilkJesus - November 1, 2020, 7:12 am

(Oct 30, 2020 05:25 PM)Whait Wrote: [\[CITE\]](#) Those are really good scanners, but I'd recommend Nikto and DNSDumpster as well :

<https://github.com/sullo/nikto>

<https://dnsdumpster.com/>

Dns dumper is a top tier tool I totally agree, check it out OP

Money- - November 1, 2020, 7:19 am

(Oct 30, 2020 05:25 PM)Whait Wrote: [\[CITE\]](#) Those are really good scanners, but I'd recommend Nikto and DNSDumpster as well :

<https://github.com/sullo/nikto>

<https://dnsdumpster.com/>

Becareful with nikto tho , the user-agent gets detected easily etc.

Might wana randomize the user-agent while scanning. Won't be surprise 1 or 2 scan attempts ya got IP blacklisted.

Sides, manually fuzzing around web apps for exploits its even more fun than scanning which I know helps in saving time.

drneed - November 1, 2020, 11:12 am

(Nov 1, 2020 08:19 AM)Money- Wrote: [\[CITE\]](#) Becareful with nikto tho , the user-agent gets detected easily etc.

Might wana randomize the user-agent while scanning. Won't be surprise 1 or 2 scan attempts ya got

IP blacklisted.

Sides, manually fuzzing around web apps for exploits its even more fun than scanning which I know helps in saving time.

sometimes i don't know where to start, usually i go with a "Nmap scan vuln script" and random other tools like sqlmap, nosqli, are these even useful. if theres a method you follow, would like to know

ps: ofc if you dont mind.

G.P.D. - November 1, 2020, 11:56 am

(Nov 1, 2020 08:19 AM)Money- Wrote: [\[CITE\]](#) Becareful with nikto tho , the user-agent gets detected easily etc.

Might wana randomize the user-agent while scanning. Won't be surprise 1 or 2 scan attempts ya got IP blacklisted.

Sides, manually fuzzing around web apps for exploits its even more fun than scanning which I know helps in saving time.

True, manual fuzzing and checking is for me the best way of finding special vulns. I mainly use tools to find endpoints.

vorticalbox - November 3, 2020, 10:40 am

(Nov 1, 2020 12:56 PM)Whait Wrote: [\[CITE\]](#) True, manual fuzzing and checking is for me the best way of finding special vulns. I mainly use tools to find endpoints.

Tools are great for marking off or finding low hanging fruit or finding potential spots for your to focus on.