

Forum:[Hack Forums](#)

Thread: [exploit a vulnerable onion site](#)

n00bmaster420 - May 16, 2025, 8:14 am

i found a vulnerable onion website and i want to exploit it but metasploit doesn't work is there any way to exploit it

Bastille - May 16, 2025, 8:18 am

How did you manage to find a vulnerability ? with tools or manually ?

You need to pass the traffic through Tor network, with tools such as Tornado or Torsocks

Interesting thread on this topic : <https://hackforums.net/showthread.php?tid=6282527>

It seems that Tor also start a proxy when you run the command "tor" in cli, never tried it tho, feel free to share a feedback

n00bmaster420 - May 16, 2025, 8:24 am

i used proxychains with nmap

Skorp - May 16, 2025, 12:04 pm

Metasploit does work, the exploit you are utilizing may be ineffective. How are you trying to enter the site?

DramaKing - May 16, 2025, 2:13 pm

Funny that you ask how to exploit a random, generic Tor site after supposedly having found a vulnerability.

vetbesim - May 16, 2025, 2:26 pm

A lot of metasploit exploits require you to listen for a connection, im guessing you have to port forward for it to work but i never portforwarded to use metasploit

If its an exploit based on something that the site is using, like an old version of wordpress with a vulnerability, then look up for code on exploitdb or github.

listen on a port using netcat or what you like, then use a service like portmap or ngrok to make it so the website can connect to your port

after thats done just modify parts of the exploit code so it connects to the forwarded ip and port

And also listen to what bastille told you he is giving good info too

DramaKing - May 16, 2025, 6:35 pm

The site needs to be exploited before receiving a reverse connection, so that's unlikely to be the problem.