

Forum:[Hack Forums](#)

Thread: [Website vulnerabilities](#)

Nightmare _1 - June 1, 2023, 10:26 am

What methods are used to see the vulnerabilities of a website?

Omniscient - June 1, 2023, 10:37 am

(Jun 1, 2023 10:26 AM)Nightmare _1 Wrote: [\[CITE\]](#) What methods are used to see the vulnerabilities of a website?

Most use scanners that you run towards the target which hunts for them. Good scanners allow you to customize the scans. Most capable pentesters will have the newest vulns as part of the scan.

Nightmare _1 - June 1, 2023, 10:42 am

(Jun 1, 2023 10:37 AM)Omniscient Wrote: [\[CITE\]](#) Most use scanners that you run towards the target which hunts for them. Good scanners allow you to customize the scans. Most capable pentesters will have the newest vulns as part of the scan.

Can you tell me what scanner is good?

Omniscient - June 1, 2023, 10:55 am

This is a list of common tools at Owasp.

https://owasp.org/www-community/Vulnerability_Scanning_Tools

ALEDIO - June 1, 2023, 12:27 pm

(Jun 1, 2023 10:26 AM)Nightmare _1 Wrote: [\[CITE\]](#) What methods are used to see the vulnerabilities of a website?

There are several methods to find vulnerabilities within a website, after all the vulnerabilities and the methods to find them are almost infinite. Online you can find several global scanners to take a first look and identify the most obvious and most dangerous vulnerabilities, for more in-depth investigations you can go and look for different tools, each of them for a different function. Or in the more advanced cases you can hire a pentester who will be able to thoroughly probe everything you need (obviously he must be competent and prepared for your needs). Obviously, the investigation on what to do is up to you, if you need more in-depth advice on this topic, feel free to come here to ask for help.

Nightmare _1 - June 2, 2023, 9:04 am

(Jun 1, 2023 10:55 AM)Omniscient Wrote: [\[CITE\]](#) This is a list of common tools at Owasp.

https://owasp.org/www-community/Vulnerability_Scanning_Tools

Ok thanks, I'll study it

(Jun 1, 2023 12:27 PM)ALEDIO Wrote: [\[CITE\]](#) There are several methods to find vulnerabilities within a website, after all the vulnerabilities and the methods to find them are almost infinite. Online you can find several global scanners to take a first look and identify the most obvious and most dangerous vulnerabilities, for more in-depth investigations you can go and look for different tools, each of them for a different function. Or in the more advanced cases you can hire a pentester who will be able to thoroughly probe everything you need (obviously he must be competent and prepared for your needs). Obviously, the investigation on what to do is up to you, if you need more in-depth advice on this topic, feel free to come here to ask for help.

Is it free? Ha ha

Bombmen - *June 22, 2023, 11:28 am*

Acunetix web vulnerability scanner is good

ArialFont - *June 26, 2023, 9:46 am*

The first steps is doing Information Gathering before you even start to scan a website or web application.

After collecting some information you can start slowly to scan.

I'll would say to start with simple port scanning only (with nmap for as example) before running a full vuln scanner for example Acunetix or other which are super noisy for scanning and could flag you automatically as threat.

Maybe you wont get any results if you will be detected as threat in the beginning if you don't start simple with small steps.