

Forum:[Hack Forums](#)

Thread: [Vulnerability Scanner or Reconnaissance Tool](#)

Raaz - May 28, 2017, 3:55 am

I had used it once but don't remember its name, all I want is a tool which can tell what software is website running, for example ASP.Net or Wordpress.

Can you name a few scanners which have this feature ? Thanks.

Profit ? - May 28, 2017, 9:09 am

Netcraft is a website that can do this. Nikto,Uniscan.

Key Punch - May 28, 2017, 1:04 pm

In addition to the reply above. Malgeto has a module.

Personally I would recommend trying to detect what a website is running passively first. Either craft a dork to find specific extensions:

site:target-site.com ext:php OR ext:asp

and to see if the website is using wordpress either try:

navigating to the /wp-content or /wp-includes

or view the source of the webpage and see if there are any links referencing a wordpress directory.

Lastly you could try using netcraft

Sp4ry - May 28, 2017, 9:41 pm

awvs is it and you can download now

Raaz - May 29, 2017, 4:28 am

(May 28, 2017 09:09 AM)Verifie? ? Wrote: [\[CITE\]](#) Netcraft is a website that can do this.

Nikto,Uniscan.

Thank you.

(May 28, 2017 01:04 PM)Dildo Shwaggins Wrote: [\[CITE\]](#) In addition to the reply above. Malgeto has a module.

Personally I would recommend trying to detect what a website is running passively first. Either craft a dork to find specific extensions:

site:target-site.com ext:php OR ext:asp

and to see if the website is using wordpress either try:

navigating to the /wp-content or /wp-includes

or view the source of the webpage and see if there are any links referencing a wordpress directory.

Lastly you could try using netcraft

Will take a look at netcraft, ASP.Net webforms may be detected using dorks but ASP.Net MVC is the real challenge, as it doesn't use .aspx or .ashx extensions. Thanks.

(May 28, 2017 09:41 PM)Sp4ry Wrote: [\[CITE\]](#) awvs is it and you can download now

Thank you too, I remember using Acunetix as well.

[BLANK] - May 29, 2017, 7:34 pm

Maybe the tool you are remembering is "httprecon".