

Forum: [Hack Forums](#)

Thread: [\[Help\]Anyone know a better scanner then Exploit scanner?](#)

Wopecy - January 5, 2013, 4:20 pm

I'm trying to use exploits scanner right now and keep getting an error saying "Found 0 Sites For Testing". Do you guys know how to fix that or is there a better version.

I really don't like looking for sites manually so I try to use these.

Thanks

amus3d - January 5, 2013, 4:23 pm

You won't learn anything, but meh.

<https://hackforums.net/showthread.php?tid=2336527>

Jae? - January 5, 2013, 4:23 pm

Why would you hack random websites anyway? That's going to get you nowhere.

Wopecy - January 5, 2013, 4:30 pm

(Jan 5, 2013 05:23 PM)amus3d Wrote: [\[CITE\]](#) You won't learn anything, but meh.

<https://hackforums.net/showthread.php?tid=2336527>

Thanks a lot brother, I really needed it. ?

°ZAHLEIRE™ - January 5, 2013, 5:21 pm

(Jan 5, 2013 05:23 PM)Jae? Wrote: [\[CITE\]](#) Why would you hack random websites anyway? That's going to get you nowhere.

Could be for practice or to upload a shell.

puremindd - January 5, 2013, 6:12 pm

(Jan 5, 2013 05:23 PM)amus3d Wrote: [\[CITE\]](#) You won't learn anything, but meh.

<https://hackforums.net/showthread.php?tid=2336527>

You couldn't at least recommended Nessus, w3af, Core Impact, or shitunentix..all better than wtf that was p sure.

(Jan 5, 2013 05:23 PM)Jae? Wrote: [\[CITE\]](#) Why would you hack random websites anyway? That's going to get you nowhere.

Although he probably isn't trying to learn, it is better than posting botnet sources and going to porn websites to find xss instead of watching porn (cough cough). "Hacking" random sites, granted they are not honeypots are meh for gaining some burner boxes..

|-_-_-_-| - January 5, 2013, 11:24 pm

@amus3d

he's looking for a tool to populate a list of sites from google dorks the only think he could learn from using such a tool would be pressing the search button.

@Jae?

maybe he wants to practice hacking some sites, he could learn quite a lot of things from doing so, although the same could be achieved from creating his own environment with his servers, it wouldn't

prove as useful as having a 3rd party to enforce security measures like in the wild. im not saying this is what he is going to do he may just want to hack a random website but that would be an example of it being useful

@puremint

this is not what he's looking for he's looking for a Dork scanner from what i can see in the OP. and the post you are criticising is exactly something the OP would be looking for

Noah™ - January 6, 2013, 3:25 am

I would reccomend SQL pozion v1.1 its pretty good but I would advise you not to hack and deface dorks sites. Makes you look like a skid

alexmkd1 - January 6, 2013, 4:27 am

SQL Poizon would be good, yes, but, why would you even hack some random websites? It's noobish thing.

kevin_n - January 6, 2013, 4:49 am

(Jan 5, 2013 05:23 PM)amus3d Wrote: [\[CITE\]](#) You won't learn anything, but meh.

<https://hackforums.net/showthread.php?tid=2336527>

hello sir,

well wot do you suggest as best scanner for a planned target ?

i have target and searched it by acunetix and found nothin'.

would you mind tell me what should i use as a scanner to find bugs?

i now that for being best i should go manually but im not an expert.

thanks for your time readyin' my post anyway

Empire--dumps - January 6, 2013, 4:50 am

Wow, if you haven't ever used a exploit scanner in your life raise your hand. Geezzus ^_^ For dorks I use SQL Poizon. For specfic I've been jumping between Nessus and OpenVAS. Can't seem to rule out one or the other.

puremindd - January 6, 2013, 12:10 pm

(Jan 6, 2013 05:50 AM)Empire--dumps Wrote: [\[CITE\]](#) Wow, if you haven't ever used a exploit scanner in your life raise your hand. Geezzus ^_^ For dorks I use SQL Poizon. For specfic I've been jumping between Nessus and OpenVAS. Can't seem to rule out one or the other.

Nessus is usually better than OpenVAS, granted you know what you're doing, seeing that openvas is like an updated fork of Nessus. Some people also like to use Nexpose; but meh manual pentesting + nmap is fine for most people..

kevin_n - January 8, 2013, 1:26 am

(Jan 6, 2013 01:10 PM)puremint Wrote: [\[CITE\]](#) Nessus is usually better than OpenVAS, granted you know what you're doing, seeing that openvas is like an updated fork of Nessus. Some people also like to use Nexpose; but meh manual pentesting + nmap is fine for most people..

is openVas better than acunetix vulnerability scanner?

Empire--dumps - January 8, 2013, 8:48 am

(Jan 8, 2013 02:26 AM)kevin_n Wrote: [\[CITE\]](#) is openVas better than acunetix vulnerability scanner? Comparing apples to oranges. They're different things, web app & platform scanners.

Burp Suite vs Acunetix. Acunetix is the better option. But I'd be happy with the results of either. Kinda comes down to OS and ease of access. There are better paid options, but they're not even reasonably priced for general consumer use.

kevin_n - January 8, 2013, 9:23 am

(Jan 8, 2013 09:48 AM)Empire--dumps Wrote: [\[CITE\]](#) Comparing apples to oranges. They're different things, web app & platform scanners.

Burp Suite vs Acunetix. Acunetix is the better option. But I'd be happy with the results of either. Kinda comes down to OS and ease of access. There are better paid options, but they're not even reasonably priced for general consumer use.

well good answer and i thank you so much, by the way how can we identify some one else website-wordpress-version? so we can search some exploits for that.

thanks in advance

Empire--dumps - January 9, 2013, 6:40 pm

(Jan 8, 2013 10:23 AM)kevin_n Wrote: [\[CITE\]](#) well good answer and i thank you so much, by the way how can we identify some one else website-wordpress-version? so we can search some exploits for that.

thanks in advance

Right click on the wordpress site>view source

Crtl+F "find"> enter "meta name="

You should see something like "<meta name="generator" content="WordPress 3.2.1" />"

kevin_n - January 11, 2013, 3:03 am

(Jan 9, 2013 07:40 PM)Empire--dumps Wrote: [\[CITE\]](#) Right click on the wordpress site>view source

Crtl+F "find"> enter "meta name="

You should see something like "<meta name="generator" content="WordPress 3.2.1" />"

wow this is rock&roll tip, great and awesome.

big thanks buddy