

Forum:[Hack Forums](#)

Thread: [Mass Vulnerability Scanner?](#)

Yorkiebar15 - September 13, 2014, 5:58 am

Before I start and get flamed for using tools, I'd like to state that if vulnerabilities are found, I would of course attempt to exploit them manually.

The problem I'm facing is that I have scanned a website for other websites hosted on the same server and there's almost 300 - scanning each one for a vulnerability one at a time would take way too long, and I can't seem to find any half-decent tools which accepts multiple URLs as a list to scan for vulnerabilities on.

If anyone has any suggestions, that would be great. Window or Linux is fine ?

Da? ?ae - September 13, 2014, 6:09 am

I haven't heard of such things program wise. I'm almost positive there would be command lines for Linux,

I don't think your stupid, and I'm sure you've googled the topic, but I'd try to search for a Linux based command line that you can just add a text file of lists,

OR you could do this on windows too.

There's probably a program that could be made to do this, taking the resources from a vuln scanner, and adding a little bit of code that would make it do-able with a .txt file of all websites listed, I'm not quite sure though. I'll EDIT this if I find anything

Niely - September 13, 2014, 6:28 am

Burp Suite

SQLmap

W3Af

Nikto

Wikto

Vega

Web-scarab

...

Are all tools for finding vulnerabilities in websites.

Kali Linux have most of them I think. :)

You can also get some Firefox add-ons like SQL Me and XSS Me but those don't work that excellent. ;)

Good luck!

0x03a8 - September 13, 2014, 6:41 am

Nessus is good too :)

but sadly nessus isn't completely free

Best Healer EU - September 13, 2014, 7:00 am

(Sep 13, 2014 06:28 AM)?Niely Wrote: [\[CITE\]](#) SQLmapStop right there please, He asked for a

program to scan for web vulnerabilities, Not just SQL vulnerability.

OP w3af is good, But learn how to information gather with NMAP, Not really that hard to learn.

Yorkiebar15 - September 13, 2014, 7:36 am

(Sep 13, 2014 06:28 AM)?Niely Wrote: [\[CITE\]](#) Burp Suite

SQLmap

W3Af

Nikto

Wikto

Vega

Web-scarab

...

Are all tools for finding vulnerabilities in websites.

Kali Linux have most of them I think. :)

You can also get some Firefox add-ons like SQL Me and XSS Me but those don't work that excellent. ;)

Good luck!

Thanks for the list. I've used Vega a lot in the past but recently it's stopped working on my Kali machine - it says 5 Cross Site Scripting vulnerabilities for literally every site I scan, even sites I've scanned before where it's shown many more vulnerabilities.

Do any of the tools on your list support URL list importing? That's what I'm mainly asking for.

How bout using your brain - September 13, 2014, 7:43 am

(Sep 13, 2014 07:00 AM)Best Healer EU Wrote: [\[CITE\]](#) Stop right there please, He asked for a program to scan for web vulnerabilities, Not just SQL vulnerability.

OP w3af is good, But learn how to information gather with NMAP, Not really that hard to learn. Well SQLi is a vulnerability, so why not list any tools to find/exploit them?

I could argue the same: Stop suggesting nmap because it will not find SQLi vulnerabilities....

Niely - September 13, 2014, 9:58 am

(Sep 13, 2014 07:00 AM)Best Healer EU Wrote: [\[CITE\]](#) Stop right there please, He asked for a program to scan for web vulnerabilities, Not just SQL vulnerability.

OP w3af is good, But learn how to information gather with NMAP, Not really that hard to learn. I agree with SirRootALot, SQLi is much for common and SQLmap a powerful and often used tool to find/do SQLi, so why should it hurt to mention it?

grady - September 13, 2014, 10:02 am

(Sep 13, 2014 07:00 AM)Best Healer EU Wrote: [\[CITE\]](#) Stop right there please, He asked for a program to scan for web vulnerabilities, Not just SQL vulnerability.

OP w3af is good, But learn how to information gather with NMAP, Not really that hard to learn. He's not attempting to gather information, he's attempting to scan it for vulnerabilities.

If you're going to criticize him and turn around do something extremely hypocritical, you'll fit in fine here at HackForums.

Best Healer EU - September 13, 2014, 11:48 am

(Sep 13, 2014 07:43 AM)SirRootALot Wrote: [\[CITE\]](#) Well SQLi is a vulnerability, so why not list any tools to find/exploit them?

I could argue the same: Stop suggesting nmap because it will not find SQLi vulnerabilities....
Not the skid crew!

He asked for a web vulnerability scanner, SQL is just one. And ofc nmap wont find sql vulnerabilites, Did i say that? Re read the op's post.

Your name is SirRootAlot, But you probably havent ever gone anywhere near to getting root access over a server, Better yet, even exploited anything. Good day!

Niely - September 13, 2014, 11:59 am

(Sep 13, 2014 11:48 AM)Best Healer EU Wrote: [\[CITE\]](#) Not the skid crew!

He asked for a web vulnerability scanner, SQL is just one. And ofc nmap wont find sql vulnerabilites, Did i say that? Re read the op's post.

Your name is SirRootAlot, But you probably havent ever gone anywhere near to getting root access over a server, Better yet, even exploited anything. Good day!

I personally think SirRootALot is more skilled as you, also, like I stated, SQLmap does find SQLi and helps you to exploit it easy. So it never hurts to mention especially not because SQLi is extremely much for common.

Best Healer EU - September 13, 2014, 1:00 pm

(Sep 13, 2014 11:59 AM)?Niely Wrote: [\[CITE\]](#) I personally think SirRootALot is more skilled as youl had a few giggles at that, Then i facepalmed 8 times.

Yorkiebar15 - September 13, 2014, 1:33 pm

I love how the simplest of questions can break out in to a full-blown argument on HF.

Anyways, thanks for the tools and stuff people ^_^

Niely - September 13, 2014, 1:40 pm

(Sep 13, 2014 01:00 PM)Best Healer EU Wrote: [\[CITE\]](#) I had a few giggles at that, Then i facepalmed 8 times.

I'm really wondering if you're just a multi-account of an idiot who's targeting me the whole time, or if you're really such a new idiot I can add on my list...

Best Healer EU - September 13, 2014, 2:28 pm

(Sep 13, 2014 01:40 PM)?Niely Wrote: [\[CITE\]](#) I'm really wondering if you're just a multi-account of an idiot who's targeting me the whole time, or if you're really such a new idiot I can add on my list...I will let you figure that out. You joined this year dude, why the hell would i want to target a legion kid? Or did you not know about the old shit legion back in 2013?

Niely - September 13, 2014, 2:37 pm

(Sep 13, 2014 02:28 PM)Best Healer EU Wrote: [\[CITE\]](#) I will let you figure that out. You joined this year dude, why the hell would i want to target a legion kid? Or did you not know about the old shit legion back in 2013?

You actually joined later then me and yes I've heard about the old Legion but now it's changed.

Best Healer EU - September 13, 2014, 2:38 pm

(Sep 13, 2014 02:37 PM)?Niely Wrote: [\[CITE\]](#) You actually joined later then me and yes I've heard about the old Legion but now it's changed.

Ok, bb, rofl, You really are an impersonator, Not hard tot tell.

Niely - *September 13, 2014, 2:42 pm*

(Sep 13, 2014 02:38 PM)Best Healer EU Wrote: [\[CITE\]](#) I only come on here to troll and make the impersonators look stupid;)

Uhm, okay, everyone got his own interests and pursuits in life...

Because I don't want to let this thread go off-topic and you probably won't say anything useful I've added you on my ignore-list.