

Forum:[Hack Forums](#)

Thread: [Manually Scan A Website With Thousands Of Urls For Vulns](#)

Redshadow - February 25, 2016, 8:08 am

Hello everyone

I am new here. Don't be mad by my question. I need tips to manually scan a website with thousands of urls for vulns

Leave a comment below. Thanks for reading!

Armada - February 25, 2016, 8:26 am

Use a vulnerability scanner... they are literally designed to do this for you.

Vellichor - February 25, 2016, 8:40 am

Continue learning until you know.

Redshadow - February 25, 2016, 9:01 am

Thanks Armada, which is the best scanner with less positive scan results and less negative scan results?

zdpooman - February 25, 2016, 9:03 am

I've found that using a mix of different tools to automate this process works well. The only real tips I could provide are try segmented scanning.

Perform scans one part at a time, sometimes vulnerabilities are reproducible throughout the entire website that are duplicated through every page, and thus not needing to scan every single dynamic page.

sdsdsdsdsd - February 25, 2016, 9:03 am

I would suggest you also get a proxy tool such as fiddler or burpsuite and start to understand how HTTP protocol work and then look for a vulnerability scanner to automate some of the tests

Armada - February 25, 2016, 9:26 am

(Feb 25, 2016 10:01 AM)Redshadow Wrote: [\[CITE\]](#) Thanks Armada, which is the best scanner with less positive scan results and less negative scan results?

Scanning using a variety of scanners is best for results.

The false positives need to be worked out after, but vulns that appear across multiple scanning platforms tend to be accurate, or really prominent false positives.

Always use a series of proxies and relays for these scans to avoid being bricked from the servers firewall.

Intriguer - February 25, 2016, 10:24 am

Use a vulnerability scanners like Armada said. with a quick search in google you can find what are u looking for.

And u can try Acunetix if u running windows.

basuraza - February 25, 2016, 12:33 pm

Is there any tool to scan + get access like a exploiter toolkit?
Something that detect the vuln and allow to inject code/sqli/xss/crfs...

It would be great if there is such tool. Thanks :D

Redshadow - February 27, 2016, 5:19 am

Thanks Nixxo, I am running Windows 7 64bit and I just installed Acunetix Web Vulnerability Scanner V8 (Free Edition). Is there any big difference between Acunetix Web Vulnerability Scanner V8 and V9.5 and V10?

Thanks Armada, using multiple vulnerability scanners to verify vulnerability on a website is a good idea but will you recommend top 5 website vulnerability scanners.

Seraum - February 28, 2016, 6:57 am

Take a look at Nikto, skipfish, w3af... Choose a cheap linux VPS for one month (< \$5), install Debian, and test all of this tools. Look at sectools and owasp. Another solution : download Kali Linux (backtrack), create a vm (virtual box) and have fun

Redshadow - February 29, 2016, 10:42 pm

Thanks Seraum, I have kali 2.0 installed already. I have played with w3af but the scan is very shallow and poor. I have played with Owasp zap too in kali but am not impressed too by it scans. I will look into Nikto and skipfish. Are Nikto and skipfish for windows or linux os? I need a scanner that can scan very deep into a website.

SIM-1241186 - March 1, 2016, 9:20 pm

(Feb 25, 2016 09:26 AM)Armada Wrote: [\[CITE\]](#) Use a vulnerability scanner... they are literally designed to do this for you.

Worst piece of advice ever. Most if not all vulnerability scanners are garbage. They leave thousands of requests to the server and logs everywhere. Any decent site is going to block your requests or become painfully aware that someone is scanning. Any shit site that you actually can scan because it's a piece of garbage isn't worth getting into the bad habit of scanning websites over.

OP, I'll just give you a simple tip.

Step 1: Go to Google

Step 2: type the following - site:yoursitename.com ext:php

If the site is running asp or aspx then change ext:php to ext:asp or whatever.

Now you'll be given an indexing of URL's from your site which contain php extension assuming they are running php (or whatever other filetype you specified).

Now you can check parameters and see if you can find anything.

Though, do note this is just one common trick and by far the simplest thing to do. There's more advanced methods but I gave you a quick easy solution.

Redshadow - March 2, 2016, 1:28 am

Thank you hackforumspang, I will give it a try today!

Armada - March 2, 2016, 4:04 am

(Mar 1, 2016 10:20 PM)hackforumspang Wrote: [\[CITE\]](#) Worst piece of advice ever. Most if not all vulnerability scanners are garbage. They leave thousands of requests to the server and logs everywhere. Any decent site is going to block your requests or become painfully aware that someone is scanning. Any shit site that you actually can scan because it's a piece of garbage isn't

worth getting into the bad habit of scanning websites over.

OP, I'll just give you a simple tip.

Step 1: Go to Google

Step 2: type the following - site:yoursitename.com ext:php

If the site is running asp or aspx then change ext:php to ext:asp or whatever.

Now you'll be given an indexing of URL's from your site which contain php extension assuming they are running php (or whatever other filetype you specified).

Now you can check parameters and see if you can find anything.

Though, do note this is just one common trick and by far the simplest thing to do. There's more advanced methods but I gave you a quick easy solution.

So all those fortune 500 companies, Enterprise businesses, banking and financial systems and governments are just total idiots for using commercial pen testing software then , right?

They are better to just use google for searching out .php extensions? ?

GTFO of here please, dont give stupid advice like that.

Redshadow - March 3, 2016, 12:41 am

Armada, which is the best commercial pen testing software will you advise me to get? Don't be angry at my question, I am new here. Thanks for reading!