

Forum:[Hack Forums](#)

Thread: [Automatic quote "white label" penetration test.](#)

Mr. Robot - July 12, 2023, 4:55 am

So the goal is to create something that can do a nice overview of a website into a PDF output from simply entering in the target URL/domain.

I've been reworking my old code to make it more streamlined and so far it's coming out great. I am mainly making this thread to find someone who wants to work on it with me via voice and convo.

Monetization options:

1. Sell it as a white label so people can throw their own logo on it and offer penetration test overviews for companies.
2. Create a website that users can enter their URL and email address and it will run the scan (provided they have a proof.txt file on their domain) and email them the PDF output.
3. Fiverr/Other style services.

It uses dynamic paragraphing based on the output so let's say it identifies port "22" or another "SSH" port, then we will add in a paragraph using the variable of the domain/IP that exposed that port and what information is related to that.

I also have a number of extra pieces of information being attached such as OMG cables, MiTM attacks, Insider threats etc to help companies identify weak points to investigate with more being added.

I've made it in such a way that it's extremely edit to work on intentionally so we can expand it handle any errors appropriately so that EVERY pdf file will look good regardless.

Database lookups are also implemented using the leak-lookup API wherein we can do a count of all the identified breaches for a domain and add in discussion about those breaches and how credential reuse in different website platforms leave them vulnerable etc etc.

This is not a full deep dive, simply a cost-effective quick overview. I've also found it extremely useful for scanning scam Chinese sites so there's that too.

I am open to all suggestions and ideas.

Here is how it is currently looking. All generated from simply entering the domain "hackforums.net". (I have disabled a few subdomain identifiers for this run)

Spoiler [\(Click to View\)](#)

Most recent updates:

Added in some images/paragraphing

Added in Port scan results for domains not behind cloudflare

Added in Confidentiality notice on Title page

Spoiler [\(Click to View\)](#)

#Most recent updates now:

Added in categories for explaining LFI, RFI, XSS, SQLi, and a bunch of other shit.

Fixed the password/database lookup and count

Lukasi - July 12, 2023, 5:15 am

Can it run on Windows?

Mr. Robot - July 12, 2023, 5:19 am

(Jul 12, 2023 05:15 AM)Lukasi Wrote: [\[CITE\]](#) Can it run on Windows?

Of course. Working hard on it.

Stanley - July 13, 2023, 5:39 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

vexiata - July 13, 2023, 10:42 am

This looks sick, how long did it take to make if you don't mind me asking?

CentryAgo - July 13, 2023, 10:03 pm

(Jul 13, 2023 10:42 AM)vexiata Wrote: [\[CITE\]](#) This looks sick, how long did it take to make if you don't mind me asking?

im guessing 3 months

Mr. Robot - July 13, 2023, 10:44 pm

(Jul 13, 2023 10:03 PM)CentryAgo Wrote: [\[CITE\]](#) im guessing 3 months

Lmao nah like around a week or so.

CentryAgo - July 15, 2023, 9:43 pm

(Jul 13, 2023 10:44 PM)Mr. Robot Wrote: [\[CITE\]](#) Lmao nah like around a week or so.

my boyyyyy ?

Mr. Robot - July 15, 2023, 11:36 pm

(Jul 15, 2023 09:43 PM)CentryAgo Wrote: [\[CITE\]](#) my boyyyyy ?

Working hard on it. Almost done.

Hackers - July 16, 2023, 5:36 am

Nice, looks like a great tool and the PDF deliverable can make this software a pretty powerful funnel if people pay for reports or have subscriptions to access a certain # of reports per mo.

Mr. Robot - July 16, 2023, 5:41 am

(Jul 16, 2023 05:36 AM)nodes Wrote: [\[CITE\]](#) Nice, looks like a great tool and the PDF deliverable can make this software a pretty powerful funnel if people pay for reports or have subscriptions to access a certain # of reports per mo.

Yeah definitely that's a good thought.

CtlAltAnon - July 22, 2023, 8:21 am

This is really cool. What re you looking for help with it on? This is a really cool project that interests e but I am unsur e of what I could bring to the table. It looks like you have it all down 100%

Mr. Robot - July 22, 2023, 10:38 am

(Jul 22, 2023 08:21 AM)CtlAltAnon Wrote: [\[CITE\]](#) This is really cool. What re you looking for help with it on? This is a really cool project that interests e but I am unsur e of what I could bring to the table.

It looks like you have it all down 100%

Still lots too do, also inspired by my avatar or came up with it 7 years too late? :D

CtlAltAnon - July 22, 2023, 10:54 am

(Jul 22, 2023 10:38 AM)Mr. Robot Wrote: [\[CITE\]](#) Still lots too do, also inspired by my avatar or came up with it 7 years too late? :D

No yours is way cooler than mine! I didn't even see it was the masks I have. I googled guy fawkes mr robot mask, downloaded, cropped and uploaded. I asked someone on here about remaking it.

On the subject of your project I definitely think you have a great product here and it would make a great subscription service. As far as pricing I would try and get a good idea of what your target market makes off of their jobs and try to find a sweet spot that would fit into their budget while offering them the ease of use with your service. That way you don't make the price too high or too low but you can try to focus it in. Because something like this in that industry would probably have a nice monthly price tag.

Mr. Robot - July 22, 2023, 11:03 am

(Jul 22, 2023 10:54 AM)CtlAltAnon Wrote: [\[CITE\]](#) No yours is way cooler than mine! I didn't even see it was the masks I have. I googled guy fawkes mr robot mask, downloaded, cropped and uploaded. I asked someone on here about remaking it.

On the subject of your project I definitely think you have a great product here and it would make a great subscription service. As far as pricing I would try and get a good idea of what your target market makes off of their jobs and try to find a sweet spot that would fit into their budget while offering them the ease of use with your service. That way you don't make the price too high or too low but you can try to focus it in. Because something like this in that industry would probably have a nice monthly price tag.

I am currently coding up a part for parameter extraction to add on which is slowly coming along. Crawls the initial website page for parameters and then will generate a burpsuite request you can paste right in for testing if it recognizes a login form. All the other endpoints can then be tested for LFI/RFI/XSS etc etc