

Forum:[Hack Forums](#)

Thread: [RuFi - The Pentesters Wet Dream \[COMING SOON\]](#)

outlaw - March 16, 2022, 2:33 pm

RuFi (RustFinder) is a reconnaissance tool written in RUST. It is currently in development and I thought I'd share with you my current progress. Once completed, RuFi will be completely open source and free for anyone to use or develop (yes, it will be on github)! The end goal is to be a Swiss Army Knife of web recon tools to aid pentesters in their endeavor to keep us all safe from the spookies!

Let me know what you guys think, or if you have any suggestions. This is only the beginning, I have a lot of ideas on what to do with this tool already.

What's To Come?Command line args

DNS Resolver

Custom wordlists

Common Port Test (theoretically should be faster than nmap for most common ports)

Domain Whois

Crawler/Spider

And Much Much More!..

IP GeoLocation

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

Directory Enumeration

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

Subdomain Enumeration

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

Bare in mind this is in development and is no where near finished, just thought I'd share the current state and see what everyone thinks.

Let me know!

-Outlaw ?

wtf - March 16, 2022, 2:34 pm

WTF, i don't know what this is but i really want it

MavenGradle - March 16, 2022, 3:02 pm

It's nice to see a Rust project being worked on, on HackForums. Goes to show how popular the language has become and how useful it is!

outlaw - March 16, 2022, 3:02 pm

(Mar 16, 2022 02:34 PM)wtf Wrote: [\[CITE\]](#) WTF, i don't know what this is but i really want it
It's a recon tool. A tool for providing information about domains/networks.

BL4CK98 - March 16, 2022, 3:28 pm

I am really excited to see this tool launched it will help alot. Good job Outlaw!

outlaw - March 16, 2022, 4:40 pm

(Mar 16, 2022 03:02 PM)MavenGradle Wrote: [\[CITE\]](#) It's nice to see a Rust project being worked on, on HackForums. Goes to show how popular the language has become and how useful it is!

I'm new to RUST itself but not programming and I must say, I haven't enjoyed learning a language this much since my first language VB6!

(Mar 16, 2022 03:28 PM)BL4CK98 Wrote: [\[CITE\]](#) I am really excited to see this tool launched it will help alot. Good job Outlaw!

Hopefully I'll have an alpha out within a week :)

I have IRL work to do, so working on this in my spare time.

SUI-3183372 - March 16, 2022, 4:46 pm

Cool share, dude. Keep up the good work :)

flyingduck - March 16, 2022, 6:19 pm

i still dont understand it but

BL4CK98 - March 17, 2022, 1:04 am

(Mar 16, 2022 04:40 PM)outlaw Wrote: [\[CITE\]](#) I'm new to RUST itself but not programming and I must say, I haven't enjoyed learning a language this much since my first language VB6!

Hopefully I'll have an alpha out within a week :)

I have IRL work to do, so working on this in my spare time.

I will surely use it! Good luck!

outlaw - March 17, 2022, 3:38 am

(Mar 16, 2022 04:46 PM)BV1 Wrote: [\[CITE\]](#) Cool share, dude. Keep up the good work :)

Thanks bud :) it's going to take a while to finish as I'm only working on it in my spare time but it's getting there slowly. I should hopefully have an alpha ready within a week.

(Mar 16, 2022 06:19 PM)flyingduck Wrote: [\[CITE\]](#) i still dont understand it but

Spoiler ([Click to View](#))

Haha, what don't you understand bro?

Polymath - March 17, 2022, 3:56 am

This looks really cool, is there an expected date for when development and testing is done?

MavenGradle - March 17, 2022, 11:16 am

(Mar 17, 2022 08:32 AM)xadamxk Wrote: [\[CITE\]](#) Somehow, somewhere, [MavenGradle](#) just creamed his pants.

Only if and when he releases it, and if he doesn't, I'll do it for him.

#NoPressure

MavenGradle - March 17, 2022, 12:53 pm

(Mar 17, 2022 11:28 AM)forfeit Wrote: [\[CITE\]](#) ...

I'm interested to see the speed of the port test, since you can use aggressive methods for nmap and masscan especially for externally facing assets and spider and crawler is built into Burp Pro, but I am otherwise interested in seeing it.

I still think the work being done is quality and I don't want to discourage you, just curious what the use case is over the other tools in the public repos already.

I'm not entirely convinced to be honest. I see him using an API (a public one, I presume) to do most of the work, but that kind of makes using Rust a bit pointless. You might as well make this in JavaScript and it would have about the same performance; the performance of the API would be the bottleneck.

Feel free to correct me OP. But these are just my observations.

outlaw - March 21, 2022, 11:42 am

(Mar 17, 2022 11:16 AM)MavenGradle Wrote: [\[CITE\]](#) Only if and when he releases it, and if he doesn't, I'll do it for him.

#NoPressure

What do you mean you'll do it for me ;_ ;

Give me time haha, I'm really busy with IRL work too

(Mar 17, 2022 11:28 AM)forfeit Wrote: [\[CITE\]](#) Not to be overly cynical, but curious what your tool offers that others do not.

For instance, <https://github.com/ffuf/ffuf>, can do very intense fuzzing. whois is built in native to most unix distributions.

For custom wordlists, are you implementing the tool to generate it and if so, how and how will it be better than - LINKS REDACTED

I'm interested to see the speed of the port test, since you can use aggressive methods for nmap and masscan especially for externally facing assets and spider and crawler is built into Burp Pro, but I am otherwise interested in seeing it.

I still think the work being done is quality and I don't want to discourage you, just curious what the use case is over the other tools in the public repos already.

(Mar 17, 2022 01:04 PM)forfeit Wrote: [\[CITE\]](#) My observations is that he's learning RUST for knowledge and piecing together some features that he probably uses everyday at work and even if it's not optimized as the best tool out there, at least he got some development knowledge in the works, which is honestly pretty commendable and better than anything I see in the marketplace here. ?

It won't offer anything that others wont, that's not my intention here. Ngl I really hate it when people say that because hardly anyone programs completely unique tools etc haha. The port test will essentially ping the most common ports and rust being as fast as it is I believe it'll be faster than a basic nmap scan, although admittedly not as productive or anywhere near as good. I'm actually intrigued to see the speed difference myself so I'll get back to you on that one. The wordlists will take from input via command line, so you can use any wordlist you like. Something like

```
Code ./rufi -u https:///what.ever --dirs -w /home/user/Desktop/wordlists.txt
```

What you said in your last post was completely correct lol. Apart from the work part, I don't work in the tech industry. This tool is just for me to learn/gain more rust knowledge, it's not going to be the best tool in the world and I'm sure Maven could do a much better job and faster lol. It's just a project I'm working on for my own benefit really and with sharing it open source it could maybe help someone else too.

(Mar 17, 2022 12:53 PM)MavenGradle Wrote: [\[CITE\]](#) I'm not entirely convinced to be honest. I see him using an API (a public one, I presume) to do most of the work, but that kind of makes using Rust a bit pointless. You might as well make this in JavaScript and it would have about the same performance; the performance of the API would be the bottleneck.

Feel free to correct me OP. But these are just my observations.

The only API being used currently is for the geolocation :P

outlaw - March 24, 2022, 4:08 am

To give you guys some confidence and to show it's being actively worked on (as I can, IRL work hours have gone crazy again)

Here's the DNS Resolver in development

Spoiler ([Click to View](#))