□□ Hacker Tools: ReNgine – Automatic recon

BY ANNA HAMMOND · AUGUST 24, 2021 · LAST UPDATED ON MARCH 6, 2025

Every bug bounty journey starts in the same way: Reconnaissance. We need to scope out our target. Find out what they are hosting, what services are running, what ports are open and so on. This can be extremely time-consuming when done manually, not to think of the nightmare to organise all these insights. Luckily ReNgine exists to help us with all of that. Let's take a look at this amazing tool!

> **"I am excited to announce reNgine 1.0! In a nutshell, a feature-packed major release that will potentially change the way you Recon!**
> **Here is the reNgine 1.0 trailer.https://t.co/EjQgXo812hhttps://t.co/qx8cJbDuDx#reconnaissance #recon #security**
> **1/16**
>
> **— Yogesh Ojha (@ojhayogesh11) August 15, 2021"**

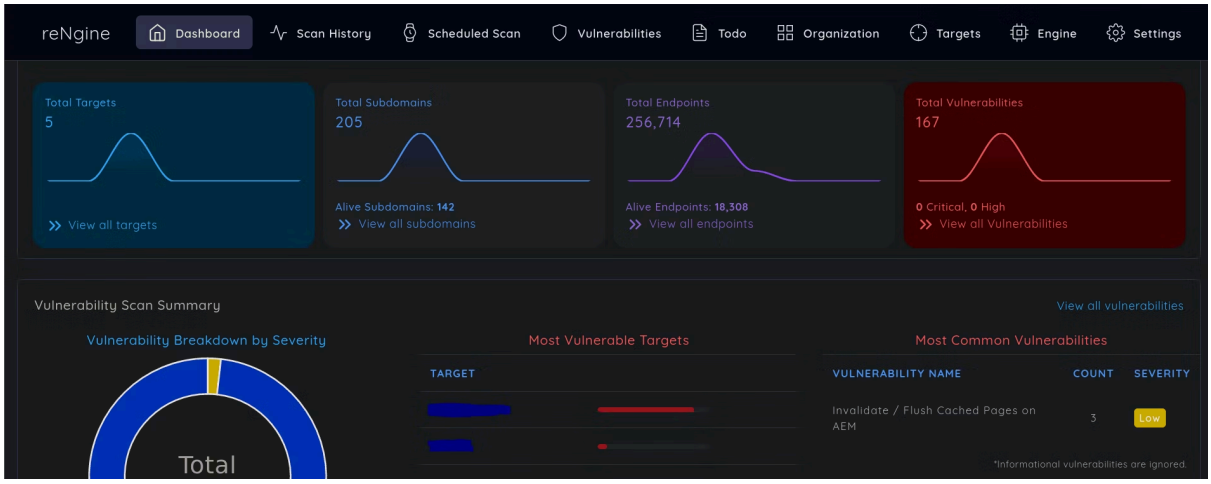
□□ What is ReNgine?

> **"An automated reconnaissance framework for web applications with focus on highly configurable streamlined recon process via Engines, recon data correlation and organization, continuous monitoring, backed by database and simple yet intuitive User Interface.**
>
> **https://github.com/yogeshojha/rengine"**

Time to disect this quote taken from the README. So ReNgine is an automated reconnaissance framework for web applications. Their focus lies within building a clear attack path or streamline for the recon process. This is done using engines, which are building blocks or sets of instructions that lead to a result such a an engine for enumerating subdomains.

All of this data is then organized for you and backed up in a database. This way, you can always access the results of scans you ran in the past. Additionally, you can enable the continuous monitoring of a target by running scans at set intervals. This combined with past data will allow you to quickly see changes in infrastructure. Things that change are things where new vulnerabilities can arise so now you know what to retest.

Lastly, all of this is wrapped in an intuitive UI that allows you to interact and parse all of the data.



ReNgine dashboard

⚒️ Setting up ReNgine

But this platform must be incredibly difficult to set up, right? Wrong! It's so easy, let's run through the steps.

- Clone the repository and cd into the newly created directory:
  `git clone https://github.com/yogeshojha/rengine && cd rengine`
- Edit the environment file:
  `nano .env`
  Note that the only thing that really requires changing is the password for postgresql because well security. Not using default passwords and all that, you know the drill
- Run the initialization script:
  `sudo ./install.sh`
  This script will install, set up and start all the required docker containers for ReNgine to run. Keep an eye out for the script requesting a username and password as you will need this to log into the UI.

Is that it? Yep! Head over to https://127.0.0.1 to access the UI!

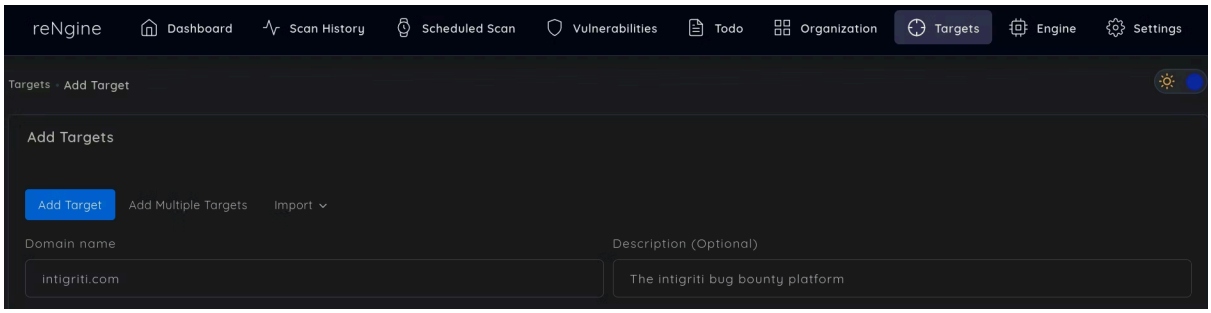
ReNgine pixel art

🚀 Our first scan

Let's perform our first ever scan!

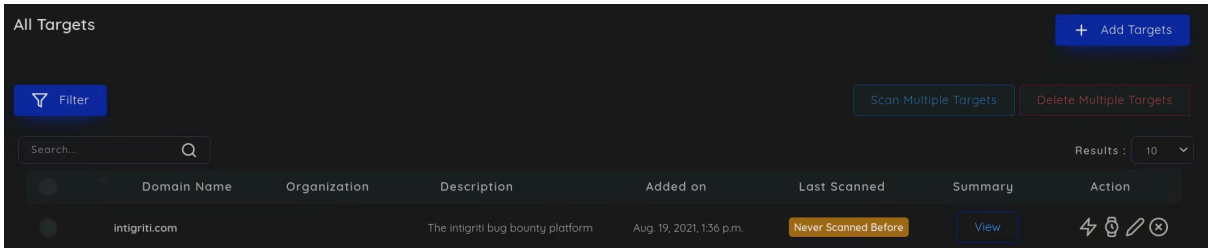
Step 1: Create a target

Go to the targets tab and add a new target. Enter the domain name and if wanted, a description.



Adding a target on ReNgine

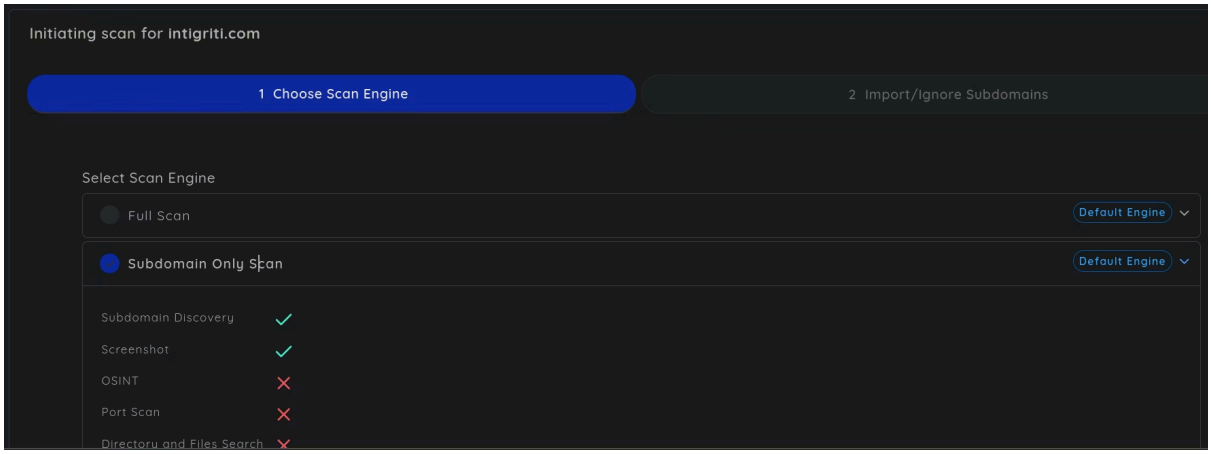
That will get you to the following view, where you can clearly see that we've never scanned this target before. Let's change that!



ReNgine target list

Step 2: Perform your first scan

Click the lightning icon next to your target to initiate a scan. You will be redirected to the a page where you can select the engine to be run on your target. In this case, I would like to perform a subdomain scan, so I select that one.



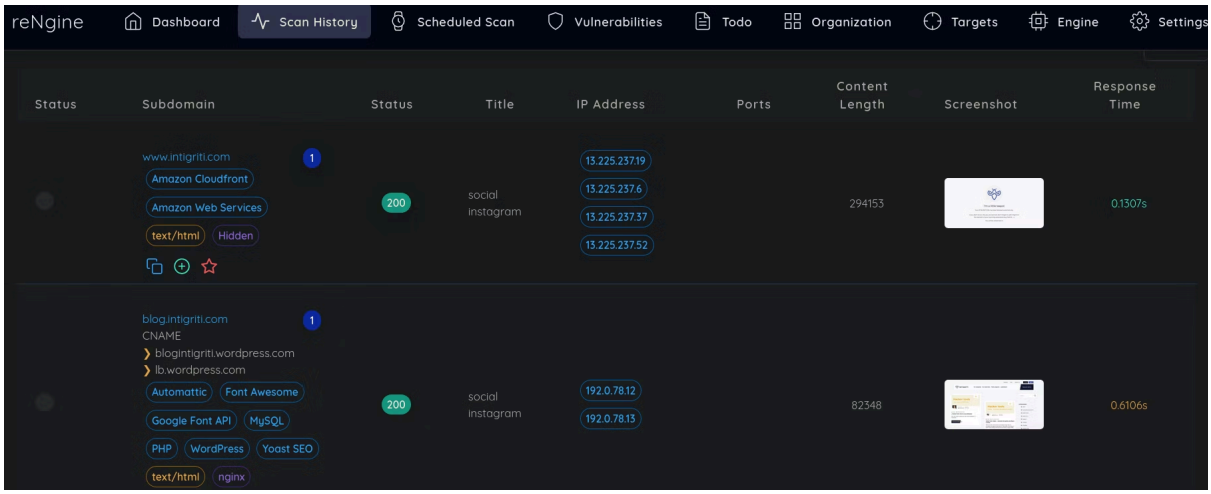
Starting a scan on ReNgine

I don’t have time to cover every feature in depth but this one is really, really cool. Is a subdomain out of scope? Don’t worry, just list them here and they will not be scanned!

Setting domains as out of scope in ReNgine

Step 3: Assessing the results

Once your scan finished, you can view all the results. Note that in this case, I only ran a subdomain scan however, this tool can do so much more!



Results ReNgine

Features

Let’s cover some more features that ReNgine has to offer

- Port discovery
- Endpoint discovery
- Directory busting
- Vulnerability scan using Nuclei (customizable)
- Parallel scanning

- Data visualization
- Configurable scan engines
- OSINT capabilities
- Alerting to Slack, Discord or Telegram
- To do lists
- Notes
- Proxy support
- And so, so much more

For a more extensive explanation check out the GitHub repository at https://github.com/yogeshojha/rengine.

Conclusion

ReNgine is a powerful service to help you level up your reconnaissance.

If you would like to recommend a tool for us to cover next week, then be sure to let us know down below. Also be sure to check out all the previous Hacker Tools articles, such as the last one on XSSHunter.

Did you know that there is a video accompanying this article? Check out the playlist!