☰ Menu

CVE-2022-35142, CVE-2022-35143, CVE-2022-35144 – DoS, XSS and Weak Password Policy in Renato a Markdown powered knowledge base

gainsec

August 4, 2022

Another day, another few CVEs!

I was working with the same friend (Tyler Fryxell) from CVE-2022-34009 which I posted about HERE

We were testing another open source project called Renato! It can be found HERE

Although we didn't spend too much time, we ran into a few issues affecting Renato version 0.17.0.

The simplest was the password policy. We found (obviously) quickly that the default password was “password”. Which is extremely weak again dictionary attacks! We also found that there were no password requirements when replacing this password so with passwords like “p” allowed, it makes brute force attacks trivial. This ended up being CVE-2022-35143

The next finding was another lower risk finding even though it was a stored cross-site scripting (XSS). This finding was an attacker with local access, like an administrator can upload a markdown file with malicious JavaScript which can be accessed and then executed by unauthenticated targets. Since this was the default way to add files to your Renato instance it was a concern. This is actually a pretty common issue when applications support markdown so it’s definitely something to look out for when testing application in the future! This ended up being CVE-2022-35144

Payload used:

```
<script>alert(document.domain)</script>
```

Lastly we found a Denial of Service (DoS) which in my opinion was the most interesting! This DoS affected the “Search” GET parameter and caused the application to crash by just searching a specific payload. The best part was unauthenticated attackers can exploit this vulnerability! This ended up being CVE-2022-35142

Payload used:

```
'%22--%3E%3C%2fstyle%3E%3C%2fscript%3E%3Cscript%3Eshadowlabs(0x000045)%3C%2fscript%3E
```

As you can see nothing special but the basics are still useful!

Anyway, I reached out to the developers HERE (especially Ryan Lelek) who were more then helpful and professional.

They published a fix HERE and gave me credit which I'm super grateful for!

Renato version 0.17.1 was released HERE and they gave me credit again which I'm even more super grateful for!

Perhaps I'll have to go back to confirm their fixes!

Until next time!

END TRANSMISSION

‹ CVE-2022-34613, CVE-2022-34618, CVE-2022-34619 – Multiple XSS (And more) in Mealie

CVE-2022-37857, CVE-2022-37163, CVE-2022-37164 Hardcoded Credentials/Weak Password Policies ›

Leave a Reply

Enter your comment here...

Search …

Twitter Feed

Jon G Retweeted

Robo… · Nov 24

Replying to @GergelyOrosz

I wonder how long it'll take Twitter to develop a company culture around managing Elon.

13 402

@gain_sec

Cyber Security, Privacy, Psychology, Piracy and Law
Gain Awareness. Gain Peace of mind. Gain Security™
NO SECURITY = NO LIFE
#gainsec

Follow on Instagram

Load More Posts

Follow Us