Remote Code TeXecution

TSJ CTF 2022

February 27, 2022

1 The Bot

I made a Discord bot that renders your LaTeX files for you. Since that's a pretty unsafe feature, I have taken extreme security measures to prevent you from doing anything nasty. You can find the vulnerable bot in the TSJ CTF Discord server. The bot has 2 available commands:

1. `/upload <file>`
   You can select a file from your device and upload it to the bot. The filename must end with `.tex`.

2. `/render`
   You will be given two options: white background with black text, or transparent background with white text. After choosing an option, the bot renders your most recently uploaded file to PDF, and then sends it to you as an image.

You can use the commands in the bot's direct messages or in the TSJ CTF server – don't worry, no one else can see your command invocations.

Because command attachments are ephemeral, the bot also provides another way to upload files: Whenever you send a file ending with `.tex` to the bot as a direct message, it will ask you whether or not to upload the file. Pressing the "Yes" button has the same effect as using the `/upload` command on the same file. **Warning: Send a direct message, don't send your file to the server directly – otherwise everyone else can see your payload!**

To use commands in Discord, type the slash character `/` into the chat, and a helpful menu will show up.

2 Some Details

- Your file can be at most 1024 bytes large. If you upload a file larger than that, only the first 1024 bytes will be processed.

- You file contents will be put between `\begin{document}` and `\end{document}` before rendering. If it contains a preamble, documentclass, etc., you will get a compilation error.
- If the bot thinks your file is unsafe, it may refuse to show you its output.

3 Flags

There are two flags in this challenge:

1. The first flag is written as a comment in the bot's source code. Leak the main source file to find the flag.
2. The second flag must be obtained by executing `/readflag`. This executable prints the flag to its standard output.

4 Additional Info

- The bot is running in a `python:3.10` Docker container and uses the Python package `py-cord==2.0.0b4` to interact with Discord.
- The bot uses TEX Live 2020.20210202-3. The command used to build your file is `pdflatex -no-shell-escape -jobname output <input-file>`.
- There is rate-limiting: The bot can only build your file at most 15 times per 10 minutes.