

BroBot

发表于 2021-01-09 分类于 [Challenge](#) , [2020](#) , [CSICTF](#) , [Misc](#)
[Challenge](#) | [2020](#) | [CSICTF](#) | [Misc](#) | [BroBot](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

<https://dunsp4rce.github.io/csictf-2020/miscellaneous/2020/07/22/BroBot.html>

by vishalananth

题目描述

This BoT can speak, can you ask him the flag? https://telegram.me/csictf_brobot/

题目考点

解题思路

I opened the Telegram App in my mobile and started a conversation with the bot. I tested out all available commands and understood that the bot is a text2voice bot which will convert whatever text we give into an equivalent voice file. We get a github link for the bot's source code when we type /about command.

So, I went ahead and checked the source code of the bot.

```
1 def send_voice_msg(update, context):
2     text = update.message.text
3     fs = open(f"/home/ctf/{update.message.from_user.id}", "w")
4     fs.write(f"echo '{text}'")
5     fs.close()
6     os.system(
7         f"su ctf -c 'sh /home/ctf/{update.message.from_user.id} | espeak -w /home/ctf/{update.message.from_user.id}.wav --stdin'"
8     )
9     update.message.reply_audio(
10         open(f"/home/ctf/{update.message.from_user.id}.wav", "rb")
11     )
12     os.system(
13         f"rm /home/ctf/{update.message.from_user.id}; rm /home/ctf/{update.message.from_user.id}.wav"
14     )
15     return ConversationHandler.END
```

We see that the text we give is appended with the echo command and is run and converted to its equivalent audio file using espeak. Since the input is not sanitized, we can make echo execute whatever command we want. Trying '\$(cat flag.txt)' give us the following voice file with the flag.

[brobot.wav]({{site.baseurl}}/assets/BroBot/brobot.wav)

Flag

```
1 csictf{ai_will_take_over_the_world}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/CSICTF/Misc/icK71DRAXiG4BdwiDEYGzv.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge](#) [#2020](#) [#Misc](#) [#CSICTF](#)

[Escape Plan](#)

[Mafia](#)