

Not executed branch!?

☑ CTFd	☑
🕒 Created	@June 14, 2021 3:08 PM
Σ Done	☑
▼ Hint	
👤 author	👤 信一郎 工藤 🐼 baby blue
☰ field	Reversing
▼ placement	no need
▼ progress	Completed
▼ value(50-200)	150
☑ writeup	☑

概要

分岐で一方しか通らないようにプログラムされた実行ファイルがある。

もう一方の分岐へ処理を移行させることでフラグを表示させられる。

デバッガでIPをいじる方法と、バイナリエディタで jmp系命令をいじる方法がある。

問題文

タチコマからデータが送られてきた。何やらデータは中にあるようだが、暗号化されている上に分岐に関するバグがありうまく出力できないらしい。解析開始だイシカワ!!!

問題ファイル

D&Dでupload可能

このファイルもCTFdにおくファイル

```
https://s3-us-west-2.amazonaws.com/secure.notion-static.com/d51f1270-ec33-4047-80a5-49aed37735d3/Not_executed_branch.txt
```

備考：このファイルはELFバイナリなので拡張子消してください

Flag

これを入れるとAcceptする文字列

```
http-ctf{TachikomaIsSoCute}
```

解法ざっくり

詳細はWriteUpで