

Write-Up

KOLABIA CTF 2024



Presented By:

LastSeenIn2026

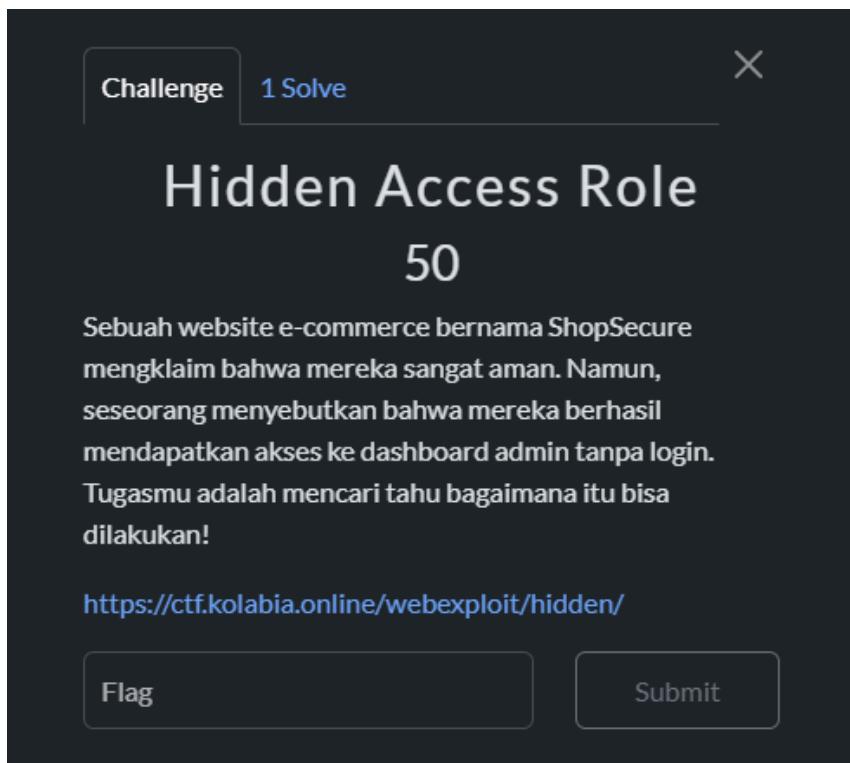
Sugeng Dwi Hermanto (SMKN 1 Cibinong)
Deffreus Theda (SMA Pradita Dirgantara)
Riduan (SMKN 2 Pangkalpinang)

[DAFTAR ISI]

[DAFTAR ISI].....	1
[WEB EXPLOITATION].....	1
1. Hidden Access Role.....	2
FLAG:.....	3
2. Ini website.....	4
FLAG:.....	5
3. Hard Nie Bang !!.....	6
FLAG:.....	7
4. Fortiness.....	8
FLAG:.....	11
[Cryptography].....	12
1. Kunci Rahasia.....	12
FLAG:.....	13
[Application].....	14
1. Petak Umpet Digital.....	14
FLAG:.....	21
2. History Ampera.....	22
FLAG:.....	24
[REVERSE ENGINEERING].....	25
1. Ini Reverse !!!.....	25
FLAG:.....	26
[PWN].....	27
1. Hai hai ini pwn yaa !!.....	27
FLAG:.....	30

[WEB EXPLOITATION]

1. Hidden Access Role

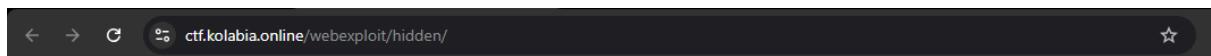


Overview:

Pada tantangan kali ini saya dikasih sebuah website yang dimana saya disuruh untuk memasuki dashboard admin pada website tersebut untuk menemukan flagnya.

Solution:

Berikut Tampilan awal web pada tantangan ini:

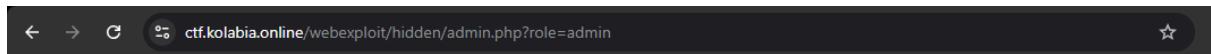


Welcome to ShopSecure

This is a secure e-commerce platform. Browse products safely!

Can you access the admin dashboard?

Pada tampilan awal web ini saya disuguhkan “Can You access the admin dashboard?” yang dimana saya disuruh untuk mengakses dashboard admin tersebut, dari clue ini saja kita bisa langsung mengakses file admin nya dengan cara “**/admin.php?role=admin**”.



Admin Dashboard

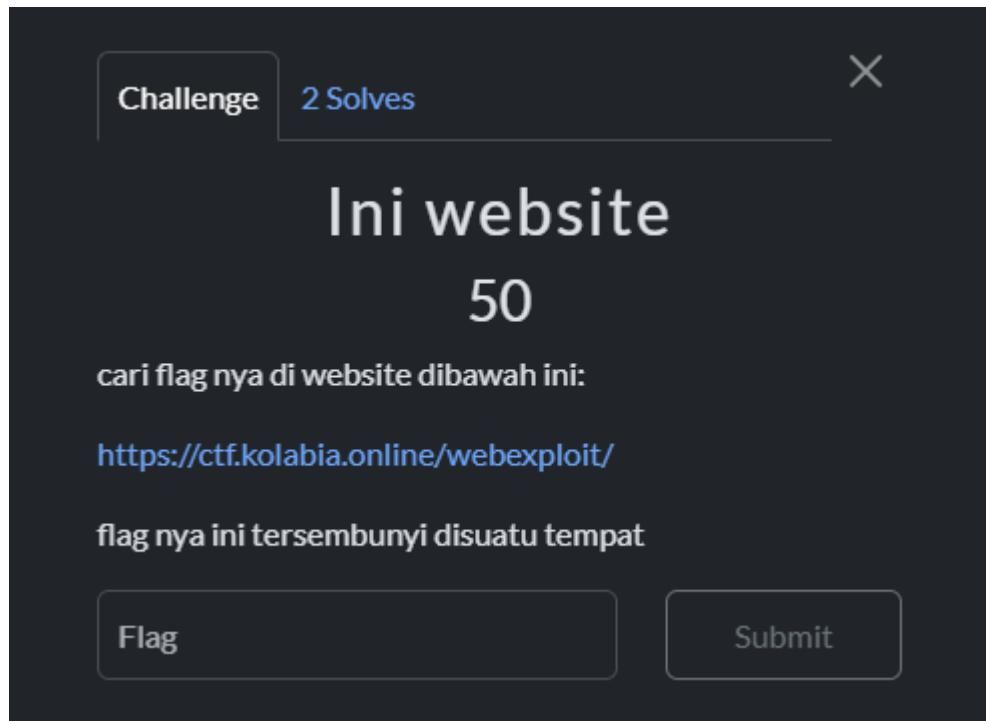
Flag: CTF{hidden_parameter_bypass}

nah voila kita berhasil mendapatkan flag pada tantangan ini !.

FLAG:

CTF{hidden_parameter_bypass}

2. Ini website

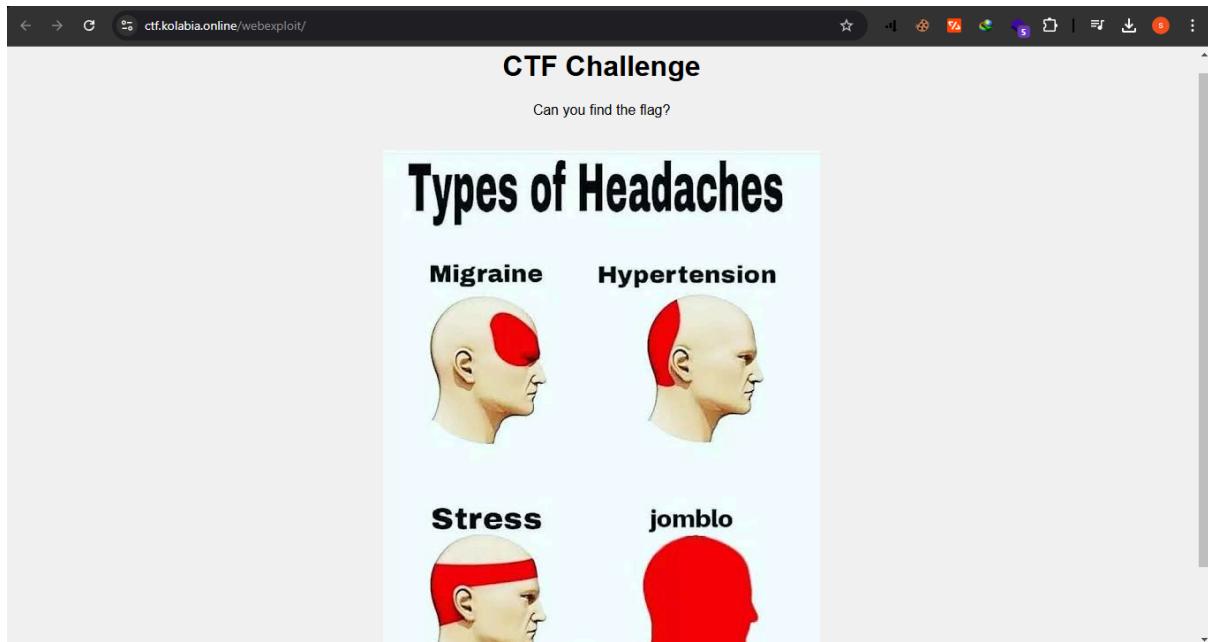


Overview:

Pada tantangan kali ini saya dikasih sebuah website yang dimana saya disuruh untuk menemukan flag yang terletak dalam source code web tersebut untuk menemukan flagnya.

Solution:

Berikut Tampilan awal web pada tantangan ini:



karena berdasarkan deskripsi soal “cari flagnya di website ini” saya langsung berinisiatif untuk melihat isi source code webnya, dan voila ketemu flagnya.

A screenshot of a browser's developer tools, specifically the 'View Source' tab. The page content is displayed in a monospaced font. A line of code containing a multi-line comment is highlighted in green: `<!-- Hint: CTF{You_Found_Me_In_The_Source} -->`. The rest of the code is in standard blue and black syntax highlighting.</div>

Nah voila ketemu flag pada tantangan ini, ternyata flag tersebut disisipkan pada source code webnya.

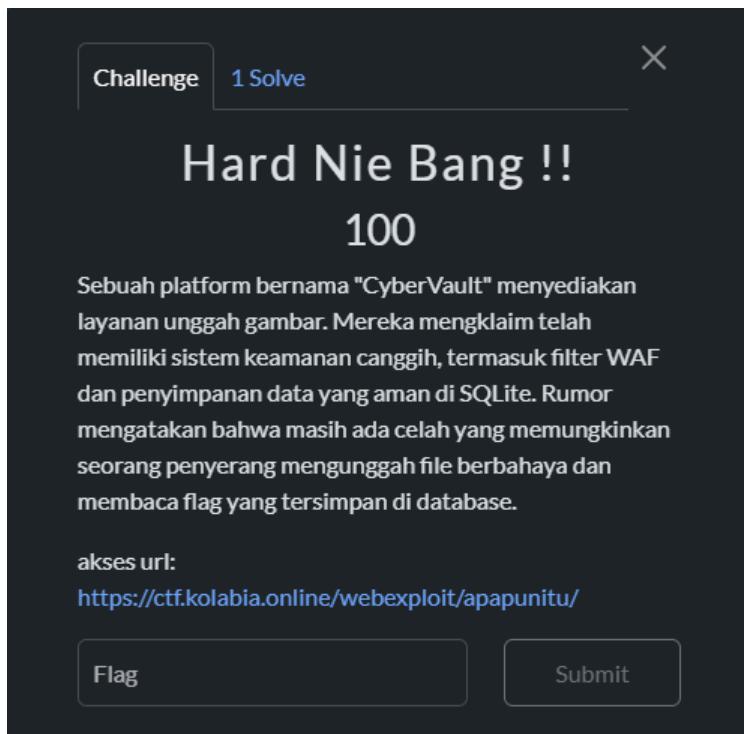
FLAG:

CTF{You_Found_Me_In_The_Source}

KOLABIA CTF 2024 | LastSeenIn2026

5

3. Hard Nie Bang !!



Overview:

Pada tantangan kali ini saya dikasih sebuah website upload file yang dimana saya disuruh untuk menemukan flag yang terletak dalam sebuah database pada SQL web tersebut, permasalahannya file upload yang diperbolehkan adalah bertipe jpeg/jpg.

Solution:

Berikut tampilan awal web pada tantangan ini:



File Upload Challenge

Upload your file here:

No file chosen

Berdasarkan deskripsi soal awalnya yaitu

“seorang penyerang mengunggah file berbahaya dan membaca flag yang tersimpan di database ”.

saya langsung berinisiatif untuk melihat isi shell pada web tersebut dengan menambah parameter “**shell.php?cmd=ls**” pada query ini tujuannya adalah untuk melihat isi direktori pada database web tersebut, dan voila saya menemukan file database flagnya “flags.db”



Baiklah tinggal lihat saya isi file flagnya dengan cara berikut:
“**?cmd=cat flags.db**”



Nah voila berhasil mendapatkan flag pada tantangan ini.

FLAG:

CTF{hidden_flag_in_db}

4. Fortress

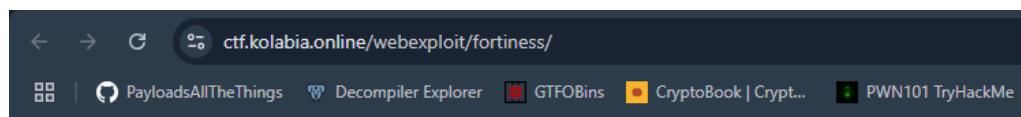
The screenshot shows a challenge card for a CTF competition. At the top left is a 'Challenge' button and a '0 Solves' counter. At the top right is a close button (X). The challenge title is 'Fortiness' and the points are '50'. The description reads: 'Perusahaan "CyberShield Inc." baru saja meluncurkan sistem keamanan terbaru mereka, lengkap dengan WAF berlapis dan mekanisme autentikasi berbasis cookies. Namun, seorang insider mengklaim bahwa terdapat kelemahan kritis yang bisa dimanfaatkan oleh seorang penyerang ahli.' Below the description is a section titled 'Tugas Anda:' with two bullet points: 'Menemukan cara masuk ke dashboard admin.' and 'Menemukan flag yang disembunyikan.' Below this is a section titled 'Akses URL berikut:' with a link [https://ctf.kolabia.online/webexploit/fortiness/]. At the bottom are two buttons: 'Flag' and 'Submit'.

Overview:

Pada tantangan kali ini saya dikasih sebuah website login yang dimana saya disuruh untuk login akun admin untuk mendapatkan flagnya, permasalahannya adalah tidak beritahu akun adminnya.

Solution:

Berikut tampilan awal web pada tantangan ini:



Welcome to CyberShield Inc.

Your ultimate security solution.

Login to continue:

Username:

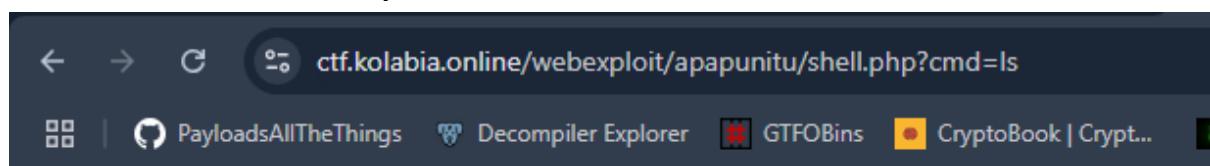
Password:

Ini adalah sebuah form login, kita disuruh login akun admin agar bisa mendapatkan flag yang berada di admin.php

Masalahnya karena ini challenge blackbox artinya tidak diberikan sebuah source code jadi sulit bagi kami menemukan vuln dari form login ini.

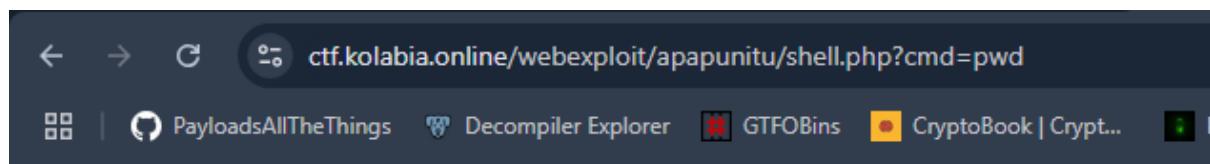
Lalu saya berpikir untuk menggunakan backdoor/shell yang ada di challenge “**Hard Nie Bang !!**”, karena setiap challengenya tidak menggunakan docker artinya kita bisa mengakses folder challenge lain.

Lalu saya mencoba pergi ke challenge “**Hard Nie Bang !!**” untuk memanfaatkan shell nya.



flags.db index.php setup_db.php shell.php upload.php waf.php

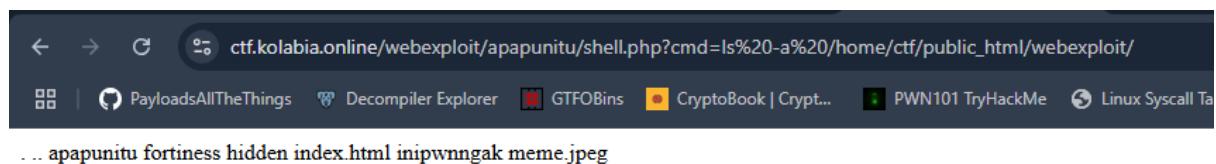
Selanjutnya saya menggunakan teknik path traversal, sebelumnya saya mencoba command **PWD** terlebih dahulu agar tau saya lagi di directory mana.



```
ctf.kolabia.online/webexploit/apapunitu/shell.php?cmd=pwd
```

/home/ctf/public_html/webexploit/apapunitu

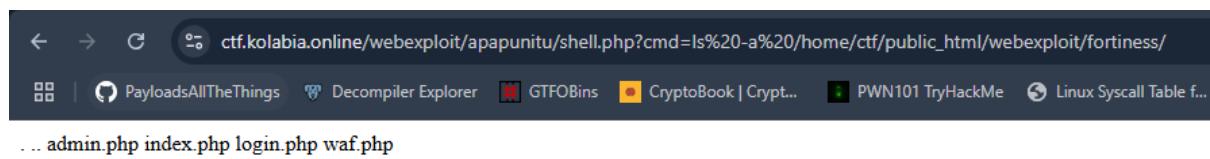
Lalu mundur 1 directory.



```
ctf.kolabia.online/webexploit/apapunitu/shell.php?cmd=ls%20-a%20/home/ctf/public_html/webexploit/
```

```
.. apapunitu fortiness hidden index.html inipwnngak meme.jpeg
```

dan boom benar saja, semua soal web berada di directory itu semua. sekarang saya focus challenge **fortiness** terlebih dahulu.



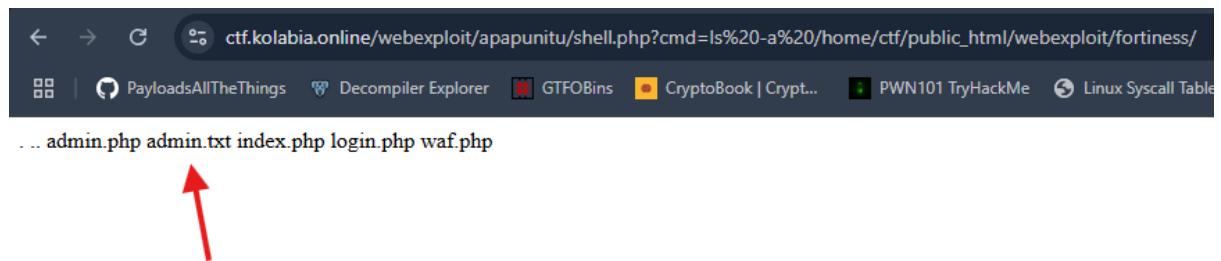
```
ctf.kolabia.online/webexploit/apapunitu/shell.php?cmd=ls%20-a%20/home/ctf/public_html/webexploit/fortiness/
```

```
.. admin.php index.php login.php waf.php
```

Dan disini terdapat sebuah file admin.php, kemungkinan flagnya berada dalam file tersebut, tapi permasalahannya adalah file .php source codenya tidak bisa dibaca begitu saja. jadi saya mencoba mengcopy file admin.php menjadi admin.txt agar bisa di baca.

berikut payloadnya:

https://ctf.kolabia.online/webexploit/apapunitu/shell.php?cmd=cp%20/home/ctf/public_html/webexploit/fortiness/admin.php%20/home/ctf/public_html/webexploit/fortiness/admin.txt



```
... admin.php admin.txt index.php login.php waf.php
```

Lihat saya berhasil mengcopynya menjadi admin.txt

Lalu jadi tinggal cat aja file admin.txt nya.



```
Admin Dashboard"; echo "  
Flag: CTF{fortified_bypass_success}  
"; } else { die("Access Denied: Unauthorized."); } } else { die("Access Denied: No valid authentication."); } ?>
```

Dan dapat flagnya.

Intinya disini adalah kita bisa menggunakan backdoor/shell challenge lain untuk mendapatkan flag nya.

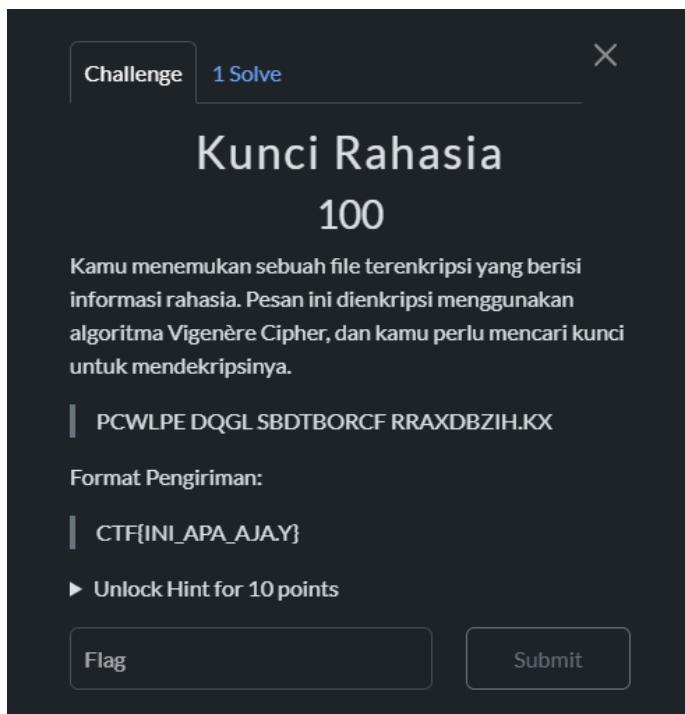
Disclaimer: tenang aja ini challenge tidak saya apa-apain hanya read saja, tidak ada file yang saya ubah / hapus dan file admin.txt juga sudah saya hapus.

FLAG:

CTF{fortified_bypass_success}

[Cryptography]

1. Kunci Rahasia



Overview:

Pada tantangan kali ini saya dikasih sebuah cipher Vigenere Cipher yang dimana saya dapat melakukan decode pada strings cipher tersebut saya akan mendapatkan flagnya, tantangan ini merupakan Classic Chall.

Solution:

1. Melakukan Decode Menggunakan Decoder Online

Baiklah disini saya akan mendecode strings cipher yang diberikan oleh soal CTF ini menggunakan tools **Cryptii**.

Ini Cipher yang perlu decode:

PCWLPE DQGL SBDTBORCF RRAXDBZIH.KX

Berikut Hasil Decodenya:

The screenshot shows a web-based cipher decoder. On the left, under 'Ciphertext', is the string 'PCWLPE DQGL SBDTBORCF RRAXDBZIH.KX'. In the center, the 'Decode' section is set to 'Vigenère cipher'. The 'Key' field contains 'KOLABIACTF'. The resulting 'Plaintext' on the right is 'FOLLOW DONG INSTAGRAM MHMDARIF.RS'.

Nah voila berhasil saya mendecode kode Vigenere cipher tersebut dengan key “**KOLABIACTF**” karena ini nama platform CTFnya saya asumsikan ini adalah secretkey/keynya.

Hasil dari decode tersebut adalah:

“**FOLLOW DONG INSTAGRAM MHMDARIF.RS**”

2. Mengubah Hasil Decode Sesuai Format Flag

jika kita mengikuti format flag pada deskripsi soal tersebut:

CTF{INI_APAPA_AJA.Y}

maka flagnya adalah:

“**CTF{FOLLOW_DONG_INSTAGRAM MHMDARIF.RS}**”

FLAG:

CTF{FOLLOW_DONG_INSTAGRAM MHMDARIF.RS}

[Application]

1. Petak Umpet Digital

The screenshot shows a challenge interface with the following details:

- Challenge**: 2 Solves
- Title**: Petak Umpet Digital
- Points**: 100
- Description**:

Selamat datang di tantangan Petak Umpet di Dunia Maya!
Tugas Anda adalah menggunakan logika dan kemampuan analisis untuk menemukan flag tersembunyi.
- Instructions**:

Perjalanan Anda dimulai di Twitter dengan akun berikut:
@mhmmdarifrs

Ikuti petunjuk di setiap cuitan untuk menemukan lokasi berikutnya. Cuitan terakhir akan memberikan Anda soal logika yang harus diselesaikan di website

Gunakan jawaban dari soal logika sebagai password untuk mendapatkan flag.

Jawaban hanya berupa angka.
- Flag Format**: CTF{...}
- Hint**: ▶ Unlock Hint for 30 points
- Buttons**: Flag, Submit

Overview:

Pada tantangan Application/Osint kali ini saya disuruh mencari informasi mengenai flag ini pada medsos sang author yaitu Twitternya username medsos author tersebut adalah “@mhmmdarifrs”.

Solution:

1. Petunjuk Pertama - Menuju Username Twitter

The image shows a screenshot of a Twitter profile for a user named Muhammad Arif (@mhmmdarifrs). The profile picture is a circular image of a person with grey hair. The bio reads: "Muhammad Arif @mhmmdarifrs Joined August 2024 2 Following 0 Followers Not followed by anyone you're following". Below the bio, there are three tabs: Posts (which is selected), Replies, and Media. A single tweet from Muhammad Arif is visible, posted 18 hours ago. The tweet content is: "HALLO PERJUANG KOLABIA CTF ! INI TANTANGAN PERTAMA DIMULAI DARI SINI. UNTUK MENEMUKAN PETUNJUK BERIKUTNYA ,PIKIRKANINI: "Tempat bersembunyi kedua mungkin adalah akun yang sedang mencari petak umpet." Selamat Mencoba! 🙌" The tweet has 8 likes and 1 reply.

Ketika saya menuju ke petunjuk pertama yaitu pada username Twitter author tersebut, saya disambut dengan pernyataan untuk mencari petunjuk selanjutnya untuk mengenai tantangan ini pada username lainnya pada twitter ini.

“Tempat bersembunyi kedua mungkin adalah akun yang sedang mencari petak umpet.”

Disini saya langsung berinisiatif untuk melihat daftar following akun author tersebut untuk mencari akun mengenai clue yang diberikan oleh akun pertama ini.

Ternyata ada 2 akun yang difollow oleh akun petunjuk pertama @mhmmdariftrs ini, yaitu “@ungmagnetism” dan “@FiersaBesari”.

Muhammad Arif
@mhmmdarifrs

Verified Followers Followers **Following**

 **unmag** ✓
@unmagnetism
I read you like a magazine wkwkwk

 **Fiersa Besari** ✓
@FiersaBesari
Manusia biasa yang senang menulis, bermusik, berkelana, dan suka iseng / 085282747109 (Ubay)

Disini saya langsung berinisiatif untuk mengecek 1 per 1 daftar follower pada kedua akun tersebut.

Tes An
@inipetakumpet

Verified Followers Followers **Following**

 **Fiersa Besari** ✓
@FiersaBesari
Manusia biasa yang senang menulis, bermusik, berkelana, dan suka iseng / 085282747109 (Ubay)

Singkatnya saya menemukan akun yang dimaksud pada clue di akun pertama tadi adalah “@inipetakumpet” sesuai dugaan saya

sebelumnya, bahwa diantara 2 akun following akun pertama itu pasti ada “akun yg dimaksud oleh clue tersebut”.

2. Langkah Kedua - Akun @inipetakumpet

The screenshot shows a social media profile for a user named 'Tes An' with the handle '@inipetakumpet'. The profile picture is a blue circle with a white letter 'T'. The bio reads: 'Not followed by anyone you're following'. Below the bio, there are three tabs: 'Posts' (which is selected), 'Replies', and 'Media'. A single post from 'Tes An' is visible, timestamped '21h' ago. The post content is:
Selamat ! kamu sudah menemukan akun kedua..
Untuk melanjutkan, gunakan logika sederhana ini !
"Akun yang terakhir adalah seorang bernama Fatih dengan angka acak di belakangnya"
Temukan Akun tersebut dan cari cuitan terbarunya ! Have a nice play !
The post has 2 likes and 6 comments.

Nah Voila berhasil menemukan akun keduanya, bahwa akun kedua tersebut adalah **@inipetakumpet**.

Pada akun kedua ini saya dikasih clue yang baru yaitu

“Akun yang terakhir adalah seorang bernama Fatih dengan angka acak di belakangnya”

Disini saya menemukan 2 akun, setelah saya cek untuk validasi mencari hint tambahan dari akun kedua tadi, saya menemukan akun yang dimaksud tersebut yaitu “**@FatihAj55618139**”.

“<https://x.com/FatihAj55618139>”

The screenshot shows a mobile interface for the X (Twitter) application. At the top, there is a search bar with the handle '@FatihAj55618139'. Below the search bar, there are five navigation tabs: 'Top' (underlined in blue), 'Latest', 'People', 'Media', and 'Lists'. The 'People' section is currently active, displaying two user profiles:

- Genta** (@Fatihaj40801207)
Hahaha
 [Follow](#)
- Fatih Aja** (@FatihAj55618139)
 [Follow](#)

At the bottom left, there is a link to 'View all'.

3. Langkah Ketiga - Akun @FatihAj55618139

Fatih Aja
@FatihAj55618139
Joined December 2024
0 Following 0 Followers
Not followed by anyone you're following

Posts Replies Media

Fatih Aja @FatihAj55618139 · 21h
kamu berhasil sampai disini !
Tantangan terakhir menunggumu di website:
ctf.kolabia.online/petakumpet

untuk masuk , jawab pertanyaan ini
"Aku adalah angka, Jika aku dikalikan dengan diriku sendiri,lalu dikurangin
10 , hasil nya adalah 8 kali aku.siapakah aku?"

1 4 1

Fatih Aja @FatihAj55618139 · 21h
Gunakan jawaban (hanya angka) sebagai password. SELAMAT BERPIKIR!!!

2 2

Pada akun ketiga ini saya dikasih informasi lagi untuk kelanjutan mendapatkan flagnya. disini saya dikasih sebuah pertanyaan dan url website untuk validasi jawaban tersebut, yang dimana jika saya dapat menginput jawaban tersebut akan mendapatkan flagnya.

"Aku adalah angka, Jika aku dikalikan dengan diriku sendiri,lalu dikurangin 10 , hasil nya adalah 8 kali aku.siapakah aku?"

Disini saya akan meminta bantuan **ChatGPT** untuk membantu saya menganalisa pertanyaan tersebut.

Langkah 3: Soal Logika

Di akun @FatihAj55618139, Anda diberikan soal matematika berikut:

"Aku adalah angka, jika aku dikalikan dengan diriku sendiri, lalu dikurangin 10, hasilnya adalah 8 kali aku. Siapakah aku?"

Langkah Penyelesaian Soal Logika:

Kita dapat mengubah soal ini menjadi persamaan matematika:

$$x^2 - 10 = 8x$$

Kemudian, kita pindahkan semua elemen ke satu sisi:

$$x^2 - 8x - 10 = 0$$

Ini adalah persamaan kuadrat yang dapat diselesaikan dengan rumus kuadrat:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Dengan substitusi nilai $a = 1$, $b = -8$, dan $c = -10$, kita mendapatkan dua solusi:

$$x = \frac{8 \pm \sqrt{64 + 40}}{2}$$

$$x = \frac{8 \pm \sqrt{104}}{2}$$

$$x = \frac{8 \pm 10.198}{2}$$

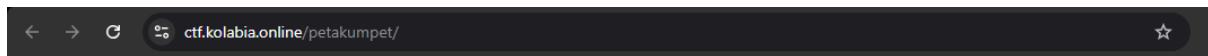
Ini memberi dua kemungkinan solusi:

- $x = \frac{8+10.198}{2} = 9.099$
- $x = \frac{8-10.198}{2} = -1.099$

Namun, karena jawaban yang diminta harus berupa angka bulat, kita memilih $x = 10$ sebagai jawaban yang paling sesuai.

Berkat analisa dari bantuan **ChatGPT** ini, bisa disimpulkan bahwa kita dapat memasukan angka 10 sebagai input pada website untuk validasi dan mendapatkan flagnya.

Berikut tampilan website untuk memvalidasi angka yang kita dapatkan tadi.



Selamat Datang di Tantangan Terakhir

Masukkan jawaban Anda:

Baiklah disini saya akan mencoba menginput angka yang saya dapatkan tadi, yaitu “**10**”.



Selamat Datang di Tantangan Terakhir

Masukkan jawaban Anda:

Selamat! Ini flagnya: CTF{Critical_Thinking_Master}

Nah voila berhasil mendapatkan flag pada tantangan ini.

FLAG:

CTF{Critical_Thinking_Master }

2. History Ampera

Challenge 1 Solve X

History Ampera

50

Peserta diminta untuk mencari informasi tersembunyi dalam artikel-artikel atau berita-berita yang sudah ada di internet mengenai Jembatan Ampera. Mereka harus mencari kode tersembunyi atau petunjuk dalam artikel tersebut yang mengarah pada flag.

Jembatan Ampera dan Sejarah Pembangunannya Telusuri artikel-artikel yang membahas sejarah Jembatan Ampera. Salah satu artikel yang bisa kamu temukan adalah tentang siapa yang terlibat dalam pembangunan jembatan tersebut dan tahun pembangunan jembatan. Cari tahu lebih banyak tentang peristiwa besar yang terjadi di sekitar tahun tersebut.

Renovasi Besar pada Tahun 2014 Cari artikel yang membahas renovasi besar pada Jembatan Ampera pada tahun 2014. Artikel-artikel ini sering menyebutkan penggunaan teknologi baru yang diterapkan selama renovasi. Ada kemungkinan bahwa angka-angka atau tanggal tertentu akan muncul di dalam artikel-artikel tersebut, yang akan menjadi bagian penting dari flag.

Mencari Kode Tersembunyi Setelah kamu menemukan artikel-artikel yang relevan, cari angka atau kombinasi angka yang tersembunyi dalam teks atau gambar yang ada di artikel tersebut. Angka ini bisa jadi bagian penting dari flag yang harus kamu gabungkan.

► Unlock Hint for 10 points

Flag Submit

Overview:

Pada tantangan Application/Osint kali ini saya disuruh mencari informasi mengenai History/Sejarah Mengenai tentang Jembatan Ampera palembang, dan flagnya berada pada artikel web yang memberitakan tentang sejarah pembangunan jembatan tersebut”.

Solution:

1. Sejarah Pembangunan Jembatan Ampera:

- **Tahun Pembangunan:** Pembangunan Jembatan Ampera dimulai pada April 1962 dan diresmikan pada 10 November 1965.
[Unsri Repository](#)
- **Pihak yang Terlibat:** Proyek ini didanai dari dana pampasan perang Jepang dan melibatkan tenaga ahli dari Jepang.
[Bams](#)
- **Peristiwa Besar di Sekitar Tahun Tersebut:** Pada tahun 1965, Indonesia mengalami peristiwa Gerakan 30 September (G30S) yang signifikan dalam sejarah politik negara.

2. Renovasi Besar pada Tahun 2014:

- Menurut informasi yang tersedia, tidak ada renovasi besar yang tercatat pada tahun 2014. Namun, terdapat rehabilitasi yang dilakukan oleh Kementerian PUPR yang mencakup perbaikan atap pylon, perkuatan struktur plat lantai, penggecatan rangka jembatan, dan penambahan tinggi pagar jembatan.
[Binamarga](#)
- **Teknologi Baru yang Diterapkan:** Salah satu teknologi yang diterapkan adalah pemasangan Structural Health Monitoring System (SHMS) untuk memantau kondisi kesehatan struktur jembatan.
[Binamarga](#)

3. Mencari Kode Tersembunyi:

- **Angka atau Kombinasi Angka:** Dari informasi di atas, beberapa angka penting yang dapat diperhatikan adalah:
 - Tahun pembangunan: 1962
 - Tahun peresmian: 1965
 - Tanggal peresmian: 10 November 1965
 - Berat bandul pemberat: masing-masing sekitar 500 ton
 - Kecepatan pengangkatan jembatan: sekitar 10 meter per menit
 - Waktu yang diperlukan untuk mengangkat penuh jembatan: 3 menit
 - Panjang jembatan: 1.177 meter
 - Lebar jembatan: 22 meter
 - Tinggi menara: 63 meter
 - Jarak antara menara: 75 meter
- **Menggabungkan Angka:** Perhatikan pola atau urutan angka yang mungkin membentuk kode. Misalnya, kombinasi tahun dan tanggal penting, atau angka yang sering muncul dalam konteks Jembatan Ampera.

4. Proyek Internasional yang Melibatkan Jembatan Ampera:

- Pembangunan Jembatan Ampera melibatkan kerja sama dengan Jepang, di mana dana pampasan perang Jepang digunakan dan tenaga ahli dari Jepang berperan dalam konstruksinya.

[Bams](#)

Setelah menganalisa dan berdiskusi dengan probset terkait membuat soal ini dan dengan data yang saya dapatkan, saya mendapatkan bahwa format flagnya adalah dalam bahasa inggris yaitu berikut:
“AmperaBridge2014Renovation”

Maaf disini saya hanya menampilkan teks dan url terkait artikel yang menyenggung tentang tantangan CTF ini saja.

FLAG:

CTF{AmperaBridge2014Renovation}

[REVERSE ENGINEERING]

1. Ini Reverse !!!



Overview:

Diberikan sebuah file elf bernama `reverse_program` yang dimana didalamnya terdapat sebuah flag, dan untuk mendapatkan flagnya kita hanya perlu melakukan static analysis.

Solution:

Pertama-tama saya menggunakan tools ida untuk static analysis. Lalu pergi ke **View > Open subviews > Generate Pseudocode** untuk nge decompile program.

```
1 int __fastcall main(int argc, const char **argv, const char **envp)
2 {
3     __int64 v3; // rsi
4     int i; // [rsp+Ch] [rbp-34h]
5     char s[24]; // [rsp+10h] [rbp-30h] BYREF
6     unsigned __int64 v7; // [rsp+28h] [rbp-18h]
7
8     v7 = __readfsword(0x28u);
9     strcpy(s, "CTF{ReverseXORisHard}");
10    checkDebugger(argc, argv);
11    obfuscateString(s);
12    v3 = (unsigned int)strlen(s);
13    xorEncryptDecrypt(s, v3, 171LL);
14    printf("Encrypted Flag (in bytes): ");
15    for ( i = 0; i < strlen(s); ++i )
16        printf("%d ", (unsigned __int8)s[i]);
17    putchar(10);
18    return 0;
19 }
```

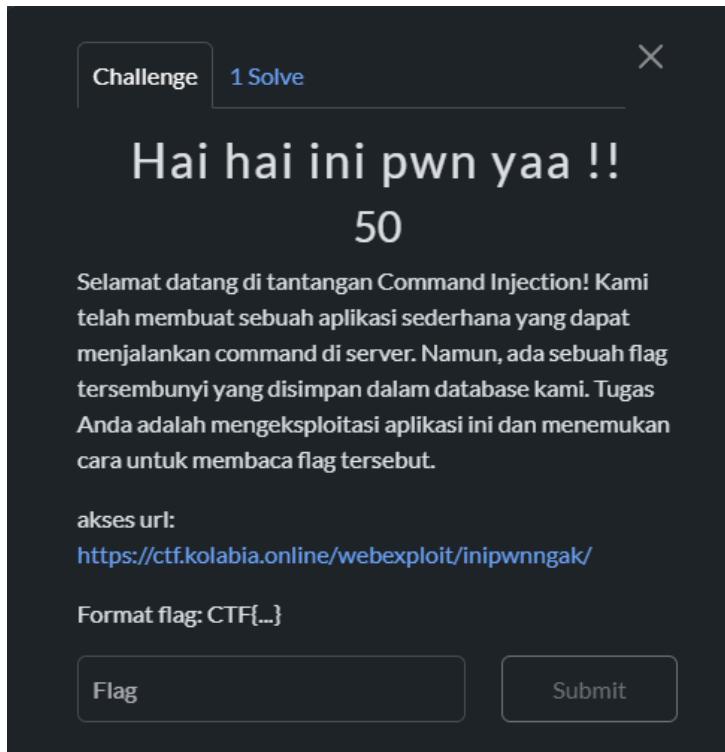
Dan yap flag berhasil ditemukan di dalam program.

FLAG:

CTF{ReverseXORisHard}

[PWN]

1. Hai hai ini pwn yaa !!

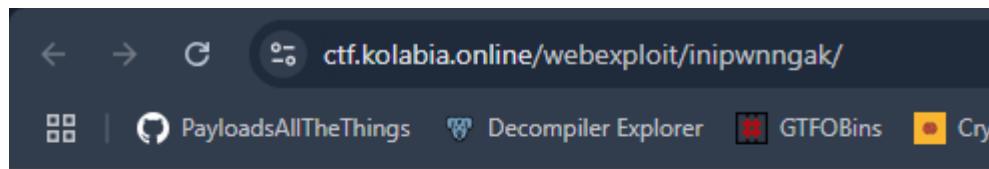


Overview:

Pada tantangan kali ini saya dikasih sebuah website yang dimana saya disuruh untuk memasukkan nama file yang mengandung flag untuk mendapatkan flagnya.

Solution:

Berikut tampilan awal web pada tantangan ini:



Command Injection Challenge

Masukkan nama file untuk membaca isinya:

Ini adalah sebuah form input, kita disuruh untuk memasukkan command injection untuk mendapatkan flagnya

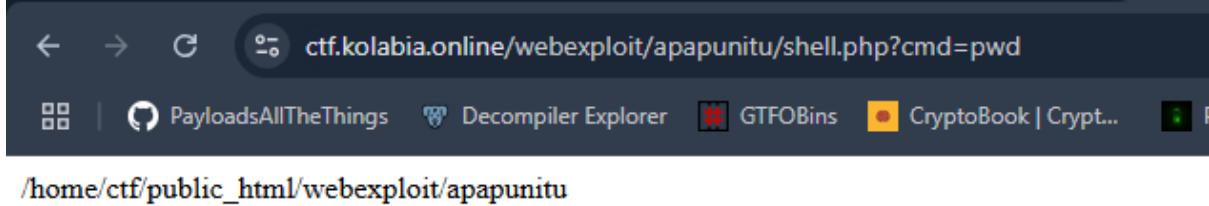
Masalahnya karena ini challenge blackbox artinya tidak diberikan sebuah source code jadi sulit bagi kami menemukan vuln dari form input ini.

Lalu saya berpikir untuk menggunakan backdoor/shell yang ada di challenge “**Hard Nie Bang !!**”, karena setiap challengenya tidak menggunakan docker artinya kita bisa mengakses folder challenge lain.

Lalu saya mencoba pergi ke challenge “**Hard Nie Bang !!**” untuk memanfaatkan shell nya.

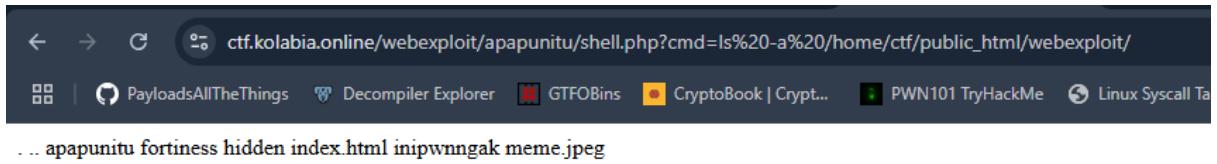


Selanjutnya saya menggunakan teknik path traversal, sebelumnya saya mencoba command **PWD** terlebih dahulu agar tau saya lagi di directory mana.



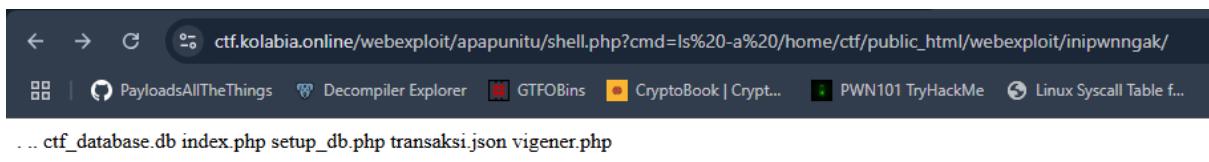
```
/home/ctf/public_html/webexploit/apapunitu
```

Lalu mundur 1 directory.



```
.. apapunitu fortiness hidden index.html inipwnngak meme.jpeg
```

dan boom benar saja, semua soal web berada di directory itu semua. sekarang saya focus challenge **inipwnngak** terlebih dahulu.



```
.. ctf_database.db index.php setup_db.php transaksi.json vigener.php
```

Dan disini terdapat sebuah file **ctf_database.db**, kemungkinan flagnya berada dalam file tersebut.

Lalu jadi tinggal cat aja file **ctf_database.db** nya.



```
SQLite format 3 @ .v0 L0ytableflagsCREATE TABLE flags (id INTEGER PRIMARY KEY, flag TEXT) $ OCTF {command_injection_db_success}
```

Dan dapat flagnya.

Intinya disini adalah kita bisa menggunakan backdoor/shell challenge lain untuk mendapatkan flag nya.

Disclaimer: tenang aja ini challenge tidak saya apa-apain hanya read saja, tidak ada file yang saya ubah / hapus.

FLAG:

CTF{command_injection_db_success}