

WRITE-UP
ANTSec
“GASIN AJA LAH”



CODE CHALLENGE
2025

Contents

Contents.....	2
Introduction Team.....	3
Detail Challenge Solved.....	4
A. Forensic.....	4
1. 1t's t0 d33p.....	4
2. A Brief Memory.....	5
B. Web Exploit.....	6
1. Si keras kepala.....	6
2. Feedback Dosa Lama: The Real Mystery.....	7
3. Jago Wan Tap Challenge.....	9
C. Reverse Engineering.....	10
1. cobabacaakudong.....	10

Introduction Team

Nama Team : ANTSec
Slogan : GASIN AJA LAH
Asal Kampus : Universitas Teknologi Yogyakarta
Ketua Team : Muhammad Mukhlis Robani

Detail Challenge Solved

A. Forensic

1. 1t's t0 d33p

Saat melakukan forensik pada sebuah server, tim kami menemukan image disk yang tampaknya kosong. Tidak ada file mencurigakan, namun informasi intelijen mengatakan ada sesuatu yang penting tersembunyi di dalamnya.

Dapatkan kamu menemukan flag yang disembunyikan dalam metadata file atau struktur file system-nya?

Penyelesaian :

Dari soal yang diberikan terdapat sebuah file bernama archive.img lalu saya mendownloadnya dan melakukan pengecekan terhadap metadata yang ada didalamnya dengan menggunakan comand strings. Setelah melihat isi metadatanya terdapat sebuah secret (rahasia) yang merupakan flag.

```
(root@kali)-[/home/kali/Desktop/code-chaallenge/foren]
# strings archive.img
/mnt/tmp
lost+found
notes.txt
83zt
secret
CTF{th1s_1s_d33p}
lost+found
notes.txt
/mnt/ctf
83zt
secret
CTF{th1s_1s_d33p}
/mnt/tmp
83DK
secret
CTF{th1s_1s_d33p}
4Rzt
secret
Q1RGe2QzM3BfaGlkZGVufQo=
4Rzt
secret
Q1RGe2QzM3BfaGlkZGVufQo=
try harder!
```

FLAG : CTF{th1s_1s_d33p}

2. A Brief Memory

Seorang analis SOC mendeteksi adanya anomali dalam aktivitas login di sistem internal. Beberapa menit sebelum sistem dimatikan, pengguna mencatat sesuatu yang tampaknya penting dalam base64.

Kami berhasil melakukan snapshot sistem dalam bentuk memory dump. Berdasarkan timeline aktivitas, ada indikasi bahwa informasi penting sempat muncul di layar, namun tidak ditemukan dalam file sistem.

file

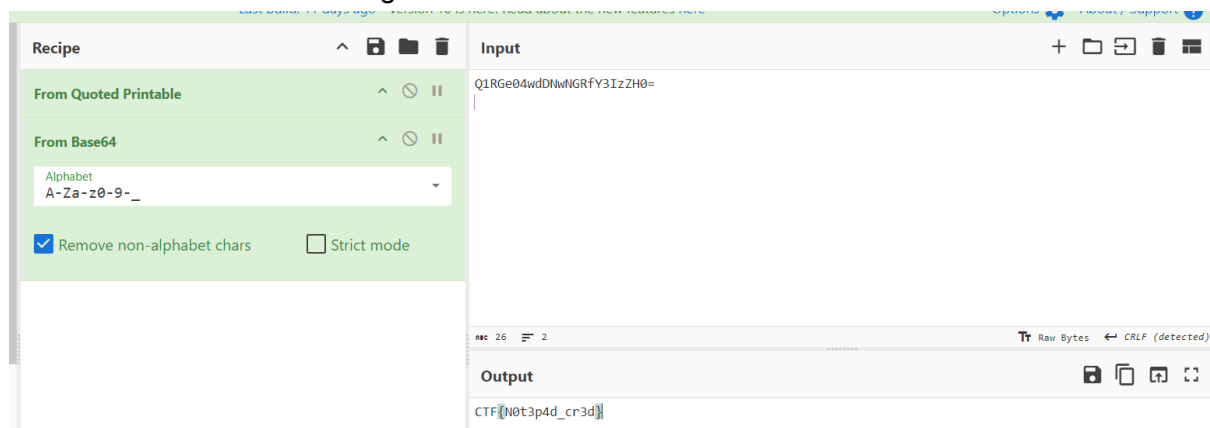
Flag CTF{...}

Penyelesaian :

Dari soal yang diberikan terdapat sebuah file. Pertama, download file tersebut. Lalu langkah selanjutnya adalah mengecek isi file tersebut dengan command strings. Akan tetapi karena isi yang keluar terlalu banyak dilakukan pengecekan dengan strings tertentu dengan menggunakan grep "flags". Ketika menggunakan grep "flags" ketemu sebuah encode base64 yang merupakan petunjuk seperti pada soal.

```
flags
iosflags@std@YA?AU?$_Smanip@H@1@H@Z
update-memoryprotectionflags
oflagsWWW
msft:rm/algorithm/flags/1.0
update-memoryprotectionflags
flags:Q1RGe04wdDNwNGRfY3IzZH0=
[PropCache %p]: Written '%s'='%s' (flags: %x), rc=%Rrc
[PropCache %p]: Deleted '%s'='%s' (flags: %x), rc=%Rrc
flags
client_cluster_flags_p1
client_cluster_flags_p2
?resetiosflags@std@YA?AU?$_Smanip@H@1@H@Z
flags in
```

Copy strings tersebut dan lakukan decode menggunakan cyberchef dengan operasi base64. Setelah dilakukan decode flag ketemu.



FLAG : CTF{N0t3p4d_cr3d}

B. Web Exploit

1. Si keras kepala

Di ruang admin katanya ada aturan main yang bikin kepala siapa pun jadi mikir dua kali. Nama admin harus diketik persis kayak aslinya—bahkan spasi, tanda baca, atau karakter kecil bisa bikin gagal total.

Pernah ada mahasiswa iseng, katanya cuma karena beda sedikit (ada yang bilang spasi, ada yang bilang typo), tiba-tiba berhasil duduk di kursi yang selama ini dibilang "cuma legenda".

Password-nya juga katanya gampang dihafal, pernah jadi password admin setahun terakhir.

Kalau login kamu berhasil, berarti kamu benar-bener paham aturan keras kepala di kampus ini. Tapi jangan buru-buru puas—kadang login "terlihat benar" pun belum tentu itu yang dicari oleh sistem!

Flag CTF{...}

<https://soal1-ctf-univ.himatisi-tus.com>

Penyelesaian :

Dari soal yang diberikan terdapat sebuah link. Pertama kunjungi link tersebut. Lalu cek source code dari file tersebut. Dari informasi tersebut didapatkan bahwa ada sebuah password untuk login dan mendapatkan informasi lebih lanjut. Akan tetapi ada sebuah rahasia untuk bisa login dengan mengubah sedikit pada username nya. Jadi pada username gunakan kata admin dan spasi satu kali "admin " dan gunakan password "admin123". Lalu login dan flag ketemu.

Si Keras Kepala

Di ruang admin katanya suka ada yang "keras kepala" login harus benar-bener **ngikutin aturan main** mereka. Nama admin kadang suka "ngambek" kalau nggak diketik persis sama kayak aslinya, apalagi kalo ada spasi nyelip di belakang, atau karakter aneh. *Password yang bener katanya sih gampang diinget, pernah dipake admin tahun lalu juga...* Ada mahasiswa pernah iseng, katanya berhasil duduk di kursi admin cuma gara-gara ngetik nama yang "sedikit beda" dari biasanya.

Ingat: flag cuma keluar kalau kamu benar-bener nemuin cara login admin yang "keras kepala".

🎉 Selamat, kamu berhasil duduk di kursi admin beneran 'keras kepala'!
Flag: CTF{login_penuh_trik_universitas}
CTF{login_penuh_trik_universitas}

FLAG : CTF{login_penuh_trik_universitas}

2. Feedback Dosa Lama: The Real Mystery

Kampus ini katanya punya lorong rahasia yang bahkan admin jarang masuk.

Konon, ada pesan-pesan lawas yang sengaja disebar di berbagai sudut database— mulai dari catatan admin, pesan dosen rahasia, sampai potongan yang acak tersembunyi di tabel lain.

Kabarnya, untuk mendapatkan flag utuh, kamu harus "ngacak-ngacak" isi kampus digital ini: explore semua tabel, kolom, bahkan mungkin kamu perlu gabungin beberapa potongan jadi satu kalimat.

Jangan terjebak di feedback doang—kadang fragment flag itu ngumpet di tabel aneh, atau malah dipecah jadi baris-baris kecil yang cuma bisa kamu dapat kalau benar-benar oprek schema.

Tapi hati-hati, sistem ini juga suka ngasih flag palsu ke mereka yang cuma main asal nebak.

Peta harta karun kadang harus kamu gambar sendiri. Potongan demi potongan, baru bisa lengkap jadi satu kalimat kemenangan.

Flag CTF{...}

<https://soal2-ctf-univ.himatisi-tus.com>

Penyelesaian :

Dari soal terdapat sebuah petunjuk bahwa link yang diberikan merupakan sebuah website yang rentan dengan sql injection. Akan tetapi pastikan dahulu versi database yang digunakan. Dari informasi yang didapat, database yang digunakan adalah sqlite. Setelah versi dan database diketahui langkah selanjutnya mencoba mencari nama tabel pada database dan didapatkan seperti dibawah ini.

- id: admin_note
- pengirim: 2
- pesan:
- id: dosen
- pengirim: 2
- pesan:
- id: dosen_rahasia
- pengirim: 2
- pesan:
- id: feedback
- pengirim: 3
- pesan:
- id: flagpiece
- pengirim: 2
- pesan:
- id: mahasiswa
- pengirim: 2
- pesan:
- id: nilai
- pengirim: 2
- pesan:

Setelah tabel diketahui, cek satu satu kolom yang ada pada setiap tabel dan cek isi pada setiap tabel. Setelah dicek ternyata pada tabel dosen_rahasia dan tabel flagpiece terdapat potongan sebuah flag. Satukan informasi dan gunakan format sesuai deskripsi soal.

Masukkan nama pengirim (misal: Andi)

Cek Data

- **id:** 1
- **pengirim:** tables_
- **pesan:**
- **id:** 2
- **pengirim:** univ}
- **pesan:**

Masukkan nama pengirim (misal: Andi)

Cek Data

- **id:** 1
- **pengirim:** Pak Toni
- **pesan:** Ini cuma rahasia kecil
- **id:** 2
- **pengirim:** Bu Rina
- **pesan:** explore_all_

FLAG : CTF{explore_all_tables_univ}

3. Jago Wan Tap Challenge

Ada seorang bocah yang pengen banget jadi gamer pro. Setiap kali المبار, bukannya naik rank malah makin turun. KDA-nya minus terus, kill-nya dua, death lima, assist cuma enam.

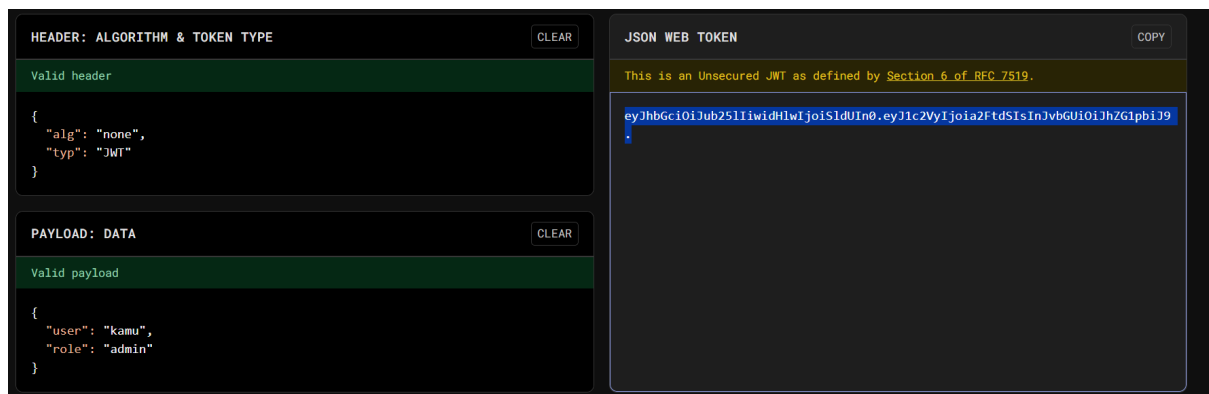
Temen-temennya pada ngatain cupu, soalnya hasilnya gitu-gitu aja padahal tiap hari latihan. Suatu hari, dia iseng cari-cari cara lain biar bisa auto naik kasta, siapa tau ada jalan pintas rahasia. Ada yang bilang, kadang buat jadi paling jago itu bukan cuma soal main, tapi juga soal ngerti celah yang gak semua orang lihat. Konon katanya, kadang kode penting suka kelewat, apalagi kalau udah lama nggak pernah diganti-ganti. Coba aja oprek, siapa tau kali ini bisa naik jadi MVP beneran.

Format: CTF{...}

<https://soal3-ctf-univ.himatisi-tus.com>

Penyelesaian :

Dari soal yang diberikan terdapat sebuah link. Ketika linknya di kunjungi terdapat sebuah JSON Web Token (JWT). Lalu cek isi tokennya di jwt.io . Lalu coba buat token baru dengan deskripsi seperti pada gambar dibawah ini. Salin Token dan masukkan kedalam inputan pada link website tadi.



The screenshot shows the JWT.io website interface. On the left, the 'HEADER: ALGORITHM & TOKEN TYPE' section is set to 'Valid header' with the JSON: { "alg": "none", "typ": "JWT" }. Below it, the 'PAYLOAD: DATA' section is set to 'Valid payload' with the JSON: { "user": "kamu", "role": "admin" }. On the right, the 'JSON WEB TOKEN' section shows the resulting token: eyJhbGciOiJub251IiwidHlwIjoiSldUIn0.eyJ1c2VyIjoia2FtdSIzInJvbGUiOiJhZG1pbiJ9. A warning message above the token states: 'This is an Unsecured JWT as defined by Section 6 of RFC 7519.'

Setelah token dimasukkan didapatkan flagnya.

Masukkan Apa Gitu:

eyJhbGciOiJub251IiwidHlwIjoiSldUIn0.eyJ1c2VyIjoia2FtdSIzInJvbGUiOiJhZG1pbiJ9.

Check Jawaban

Selamat, akses admin berhasil. Flag: CTF{JwT_fOrg3r}

CTF{JwT_fOrg3r}

FLAG : CTF{JwT_fOrg3r}

C. Reverse Engineering

1. cobabacaakudong

Di tengah malam, seorang developer misterius meninggalkan sebuah program aneh di server kami. Di dalamnya, hanya ada satu pesan: "Cek in ajah bray." Kami sangat khawatir program ini sangat berbahaya apakah kamu bisa mengeceknya dan menemukan anomali didalamnya

Flag CTF{...}

rev-ctf.himatisi-tus.com:1339

Penyelesaian :

Dari soal diberikan terdapat sebuah file dan link. Jadi pertama, cek isi file yang diberikan dan lakukan pengecekan isinya dengan comand strings. Setelah dicek terdapat sebuah hash seperti yang diblok. Ketika di hashing hasilnya adalah "sayangkamu". Jadi coba lakukan perintah untuk menjalankan file binarynya. Setelah dimasukkan hasil hashing tadi ternyata berhasil akan tetapi flagnya tidak muncul. Jadi dari soal tadi terdapat sebuah link yang diberikan. Jadi gunakan perintah nc (netcat) untuk mencari flagnya. "nc rev-ctf.himatisi-tus.com 1339"

```
-V8I
-o,y
@u5H
2ecdf565d44933226cc6709c761c0acd
| CEK IN AJAH BRAY!! |
[?] Cekin :
Berhasill Baray!
Hash mu:
Nyahh Flagg:
flag.txt
Salah Bray!
basic_string: construction from null is not valid
0123456789abcdef
;*3$"
zPLR
GCC: (GNU) 14.2.1 20250207
coba_baca_aku_dong.cpp
_ZNSt8__detail30__integer_to_chars_is_unsignedIjEE
_ZNSt8__detail30__integer_to_chars_is_unsignedImEE
```

Setelah dijalankan dan memasukkan string "sayangkamu" hasilnya mendapatkan flag.

```
(root@kali)-[/home/kali/Desktop/code-chaallenge/reverse]
# nc rev-ctf.himatisi-tus.com 1339
| CEK IN AJAH BRAY!! |
[?] Cekin : sayangkamu
Berhasill Baray!Hash mu:2ecdf565d44933226cc6709c761c0acd
Nyahh Flagg:CTF{K0kkkk_0310390293029420_l00_j4g00_br4yy}
```

FLAG : CTF{K0kkkk_0310390293029420_l00_j4g00_br4yy}