Write Up CTF LKS LAMPUNG 2024

TIM SMKN 4 BANDAR LAMPUNG

ANGGOTA

1. DENIS SETIAWAN
2. FARREL ZATAR R

**1. Pemanasan**



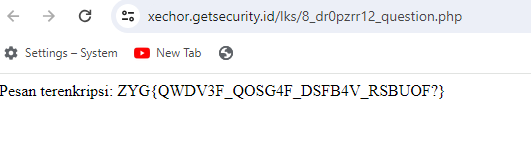
Diberikan format soal seperti di atas dan di berikan clue sebuah string yang berisi

“ }Ɐopɹǝq\_uh6uǝꓷ\_ƖhʅnW{Sꓘꓶ”. dari sini terlihat bahwa flagnya sudah tertera namun dalam posisi terbalik, maka kami menyusun ulang flag tersebut sehingga menjadi format yang benar.

**FLAG : LKS{Mul41\_den94n\_berdoA}**

**2. Yuk Mulai**

**Diberikan sebuah link : https://xechor.getsecurity.id/lks/8\_dr0pzrr12\_question.php**



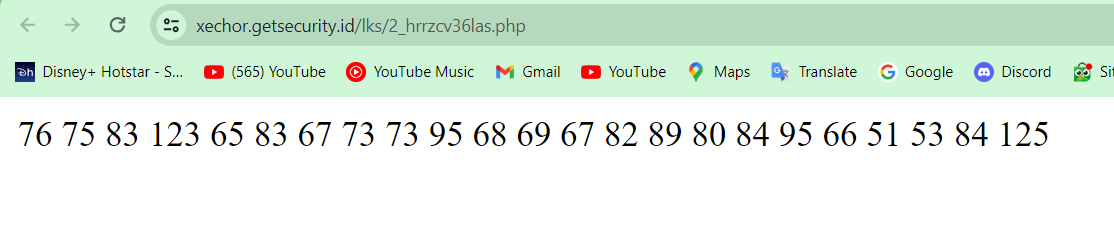
diberikan sebuah pesan terenkripsi, dan bisa dilihat bahwa ini menggunakan metode caesar cipher

**Flag: LKS{CIPH3R\_CAES4R\_PERN4H\_DENGAR?}**

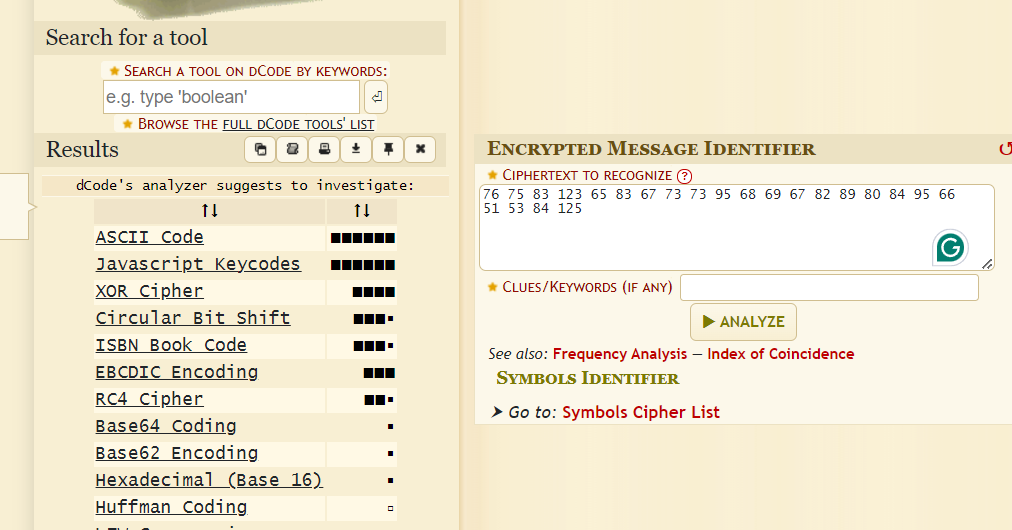
**3. Masih Oke yah ?**

****

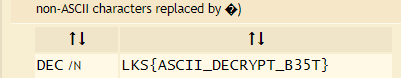
**diberikan sebuah link yang menuju sebuah site.**

****

**terdapat sebuah angka yang akan langsung kita coba analisis.**

****

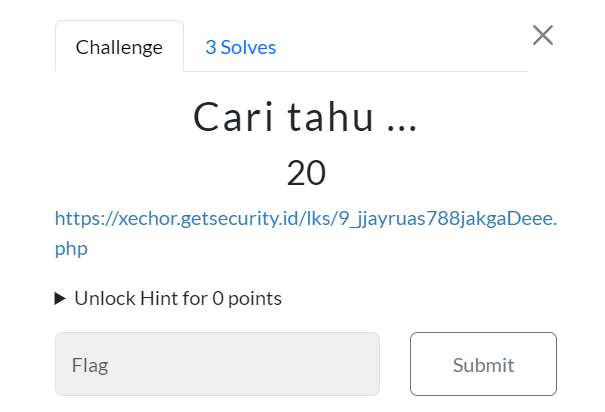
ternyata itu adalah ascii, mari kita jadikan itu sebuah cypher/plain text



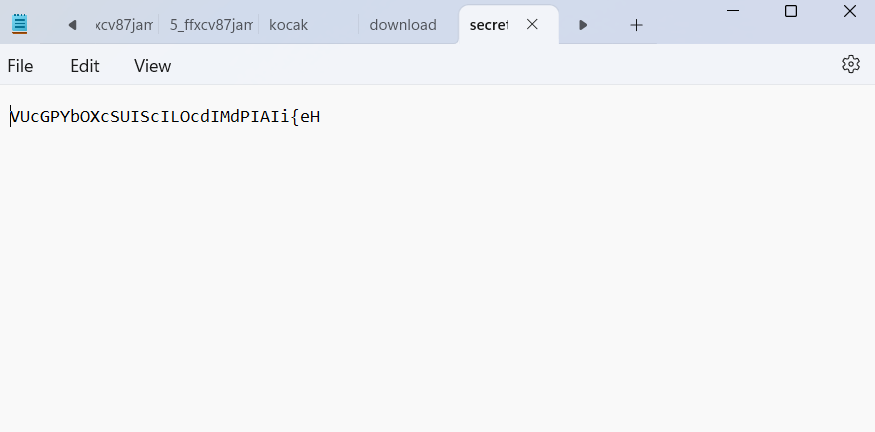
flag berhasil di temukan.

**FLAG : LKS{ASCII\_DECRYPT\_B35T}**

**4. Cari tahu …**

****

Diberikan sebuah link yang mengarahkan untuk mendownload sebuah file dengan nama “secret.txt.enc”, yang apabila kita buka dengan notepad maka akan menghasilkan sebuah string yang berisi sesuatu yang telah di enkripsi sebelumnya.



ini mencurigakan sekali

dibagian hint kita di berikan kode php seperti ini :

function decryptCaesarCipher($encrypted, $shift) { $decrypted = ''; $chiper = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789{}\_?';

for ($i = 0; $i < strlen($encrypted); $i--) {

$char = $encrypted[$i];

$pos = strpos($chiper, $char);

if ($pos !== false) {

$newPos = ($pos - $shift) % strlen($chiper);

if ($newPos < 0) {

$newPos += strlen($chiper);

}

$decrypted = $chiper[$newPos];

} else {

$decrypted = $char;

}

}

return $decrypted;

}

$encryptedMessage = file\_get\_contents('secret.txt.enc'); $shift = 10; $decryptedMessage = decryptCaesarCipher($encryptedMessage, $shift); echo $decryptedMessage;

dari kode php ini kita dapat memahami fungsi bagaimana proses file tersebut di enkripsi maka dengan melakukan sedikit perubahan kode kami membuat ini

<?php

function decryptCaesarCipher($encrypted, $shift) {

$decrypted = '';

$chiper = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789{}\_?';

for ($i = 0; $i < strlen($encrypted); $i++) {

$char = $encrypted[$i];

$pos = strpos($chiper, $char);

if ($pos !== false) {

$newPos = ($pos - $shift) % strlen($chiper);

if ($newPos < 0) {

$newPos += strlen($chiper);

}

$decrypted .= $chiper[$newPos];

} else {

$decrypted .= $char;

}

}

return $decrypted;

}

$encryptedMessage = "VUcGPYbOXcSUIScILOcdIMdPIAIi{eH";

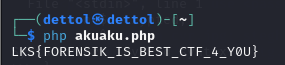
$shift = 10;

$decryptedMessage = decryptCaesarCipher($encryptedMessage, $shift);

echo $decryptedMessage;

?>

kami membuat file dengan ekstensi php di kali linux untuk dari kode yang telah di buat sebelumnya dengan perintah pico dan paste kode sebelumnya



setelah kami menjalankan file tersebut kami mendapatkan flagnya

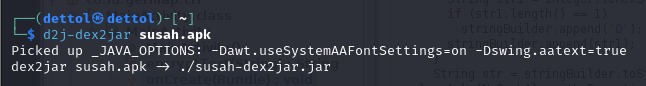
**FLAG : LKS{FORENSIK\_IS\_BEST\_CTF\_4\_Y0U}**

**5. Go... kamu bisa...**

****

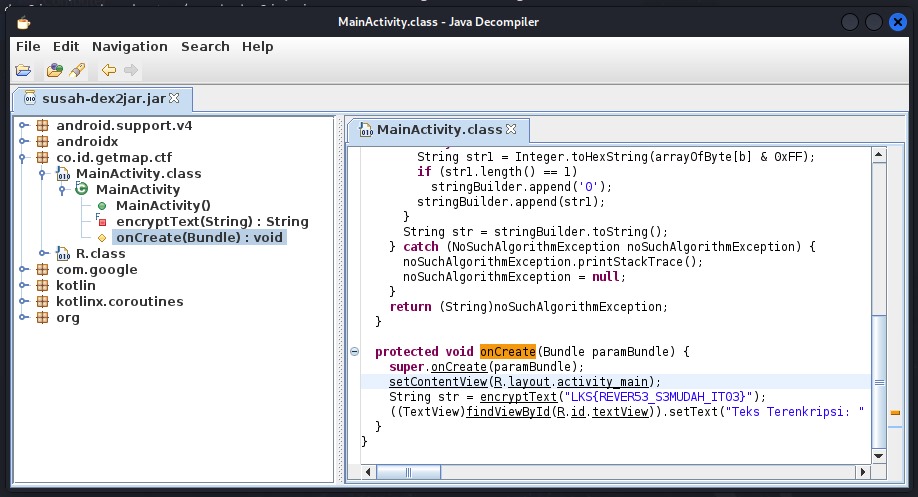
Diberikan sebuah file yang berekstensi .apk hal pertama yang kami lakukan adalah mendownloadnya melalui perintah wget di kali linux.

Selanjutnya kami mengubah ekstensi filenya menjadi jar dengan dex2jar



selanjutnya kami menggunakan jd-gui untuk membuka file jar tersebut.

pada paket getmap.ctf kamu membuka folder class MainActivity.class dan menemukan flag tersimpan di dalam String str

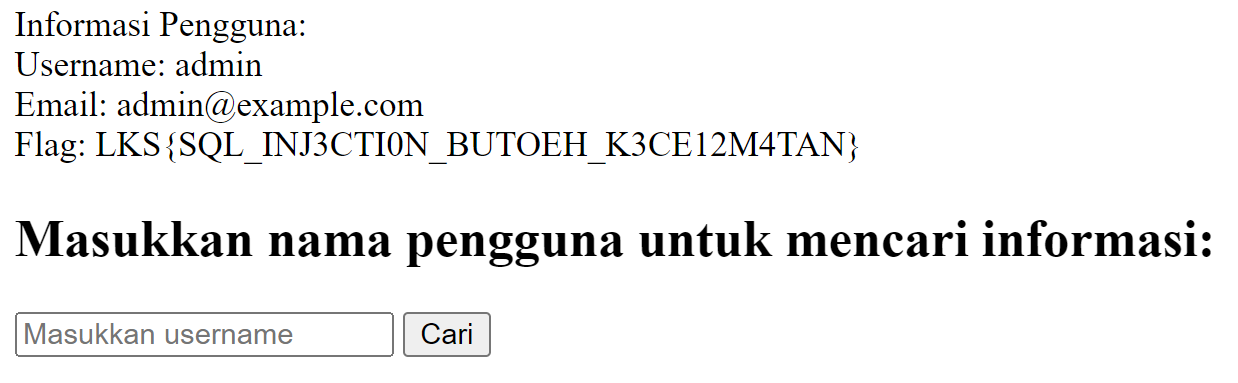


**FLAG : LKS{REVER53\_S3MUDAH\_IT03}**

**6. Atur Nafas dulu ...**

****

diberikan sebuah link yang menuju ke sebuah login form



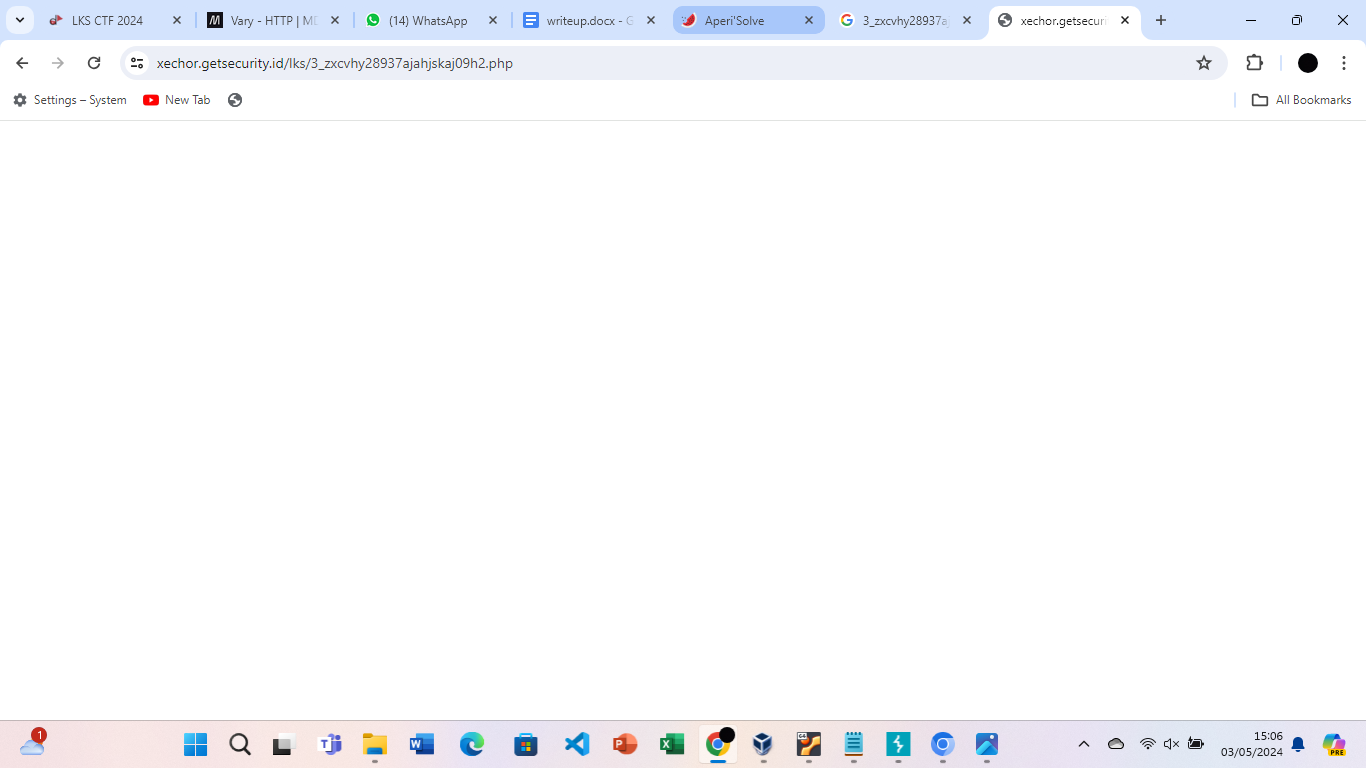
dengan memasukan username admin maka flagnya akan di dapatkan

**FLAG : LKS{SQL\_INJ3CTI0N\_BUTOEH\_K3CE12M4TAN}**

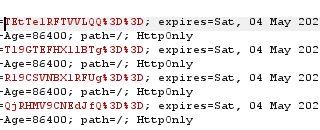
**7.Blank !!  
  
diberikan sebuah link 3\_zxcvhy28937ajahjskaj09h2.php**

**merupakan url link yang belum lengkap jadi dibentuk menjadi url flu :** [**https://xechor.getsecurity.id/lks/3\_zxcvhy28937ajahjskaj09h2.php**](https://xechor.getsecurity.id/lks/3_zxcvhy28937ajahjskaj09h2.php)

**setelah itu**

****

**kita cari di burp suite dan ketemu :**

****

**kemudian saya decode menggunakan base64**

**dan menemukan hasil   
  
Flag:LKS{TEMUKAN\_FLAG\_YANG\_BISA\_TERB4G1\_B4GI}**

**8.Lanjut yah !!**

**setelah menginspect inspect web yang tertera saya melihat cookies ;**

****

**kemudian saya dekode menggunakan base 64:**

****

**FLAG:LKS{INI\_D3CRYPT\_4YOU}**