

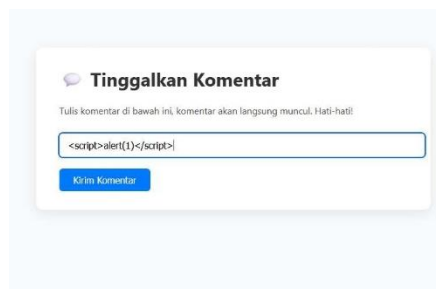
WRITE UP PESAWARAN CTF

Solve by **Vincent Aurigo Osnard, Muhamad Rizqi Wiransyah**

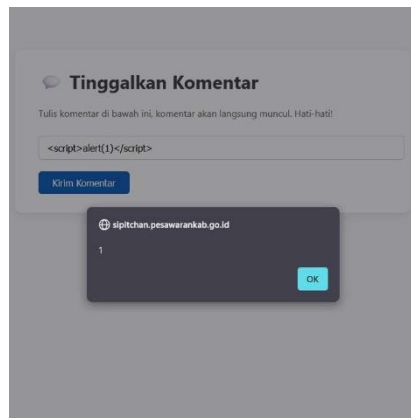
Solve 8/11 Challenge

WEB EXPLOITATION

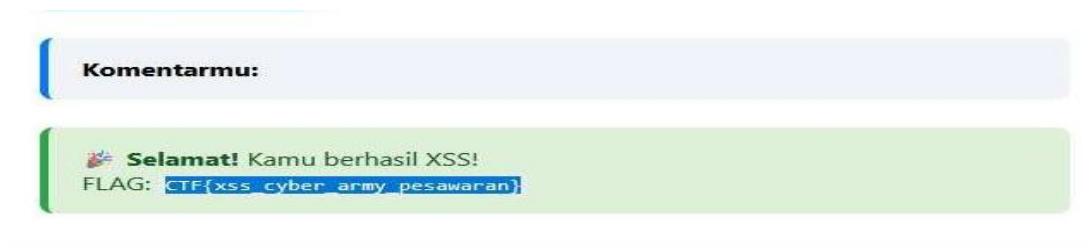
Challenge 1



Di berikan sebuah form comment yang tampaknya tidak disanitasi, sesuai dengan deskripsi. Kita bisa memasukkan payload uji coba “<script>alert(1)</script>” untuk memastikan apakah xss nya akan bekerja atau tidak



Injeksi berhasil klik “**ok**”. Dan lihat apakah ada yang terjadi.

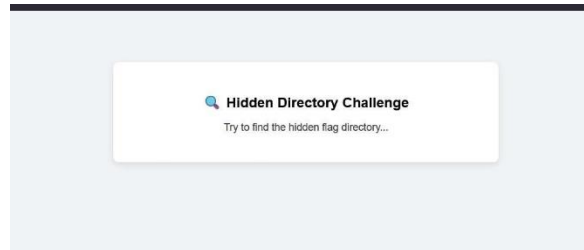


Flag:

CTF{xss_cyber_army_pesawaran}

Challenge 2:





Diberikan sebuah section **Hidden Direcotry Challenge** mencari sebuah file/dir tersembunyi yang ada di website.

```
<!-- Hint: hidden folder name: hidden -->
<!-- Hint: file name: flag.txt -->
/body>
```

ketika di cek source codenya terdapat sebuah hint . tertulis bahwa **Hidden Folder** bernama **hidden** dan ada file bernama **flag.txt**

```
https://sipitchan.pesawarankab.go.id/hidden_dir/hidden/flag.txt|
```

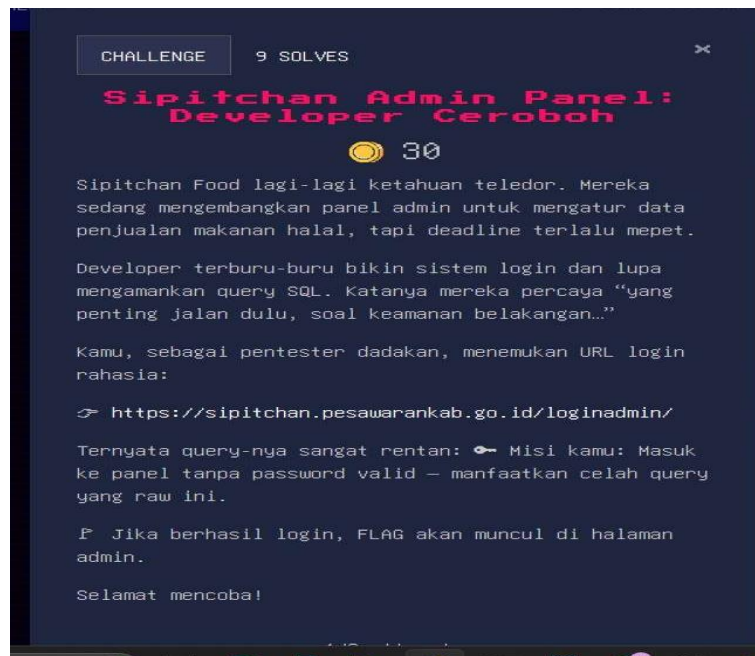
Saya membuka directory hidden tersebut.


```
Import bookmarks...
FLAG{hidden_directory_cyber}
```

Flag:

FLAG{hidden_directory_cyber}

Challenge 3:



 **Sipitchan Admin Panel**

"Yang penting jalan dulu, soal keamanan belakangan..."

Username

Password

Login

Disajikan sebuah login form. Disana terdapat kolom input username dan password. Ada statement **ternyata querynya sangat rentan** berarti bisa kita asumsikan kalau ini sql injection.

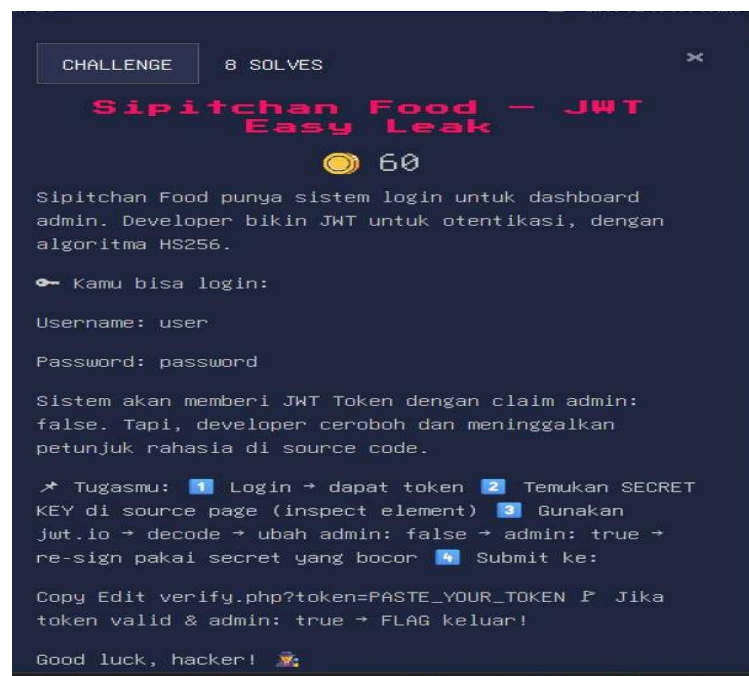
Kita bisa gunakan payload uji coba ' OR '1 pada kolom input username dan password

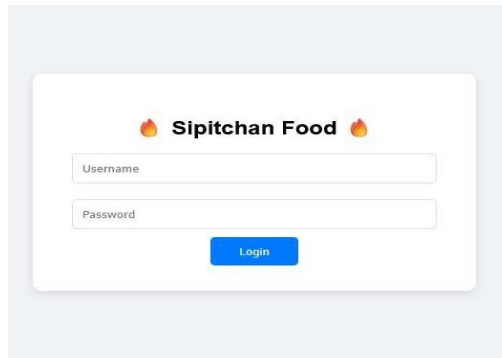


Flag:

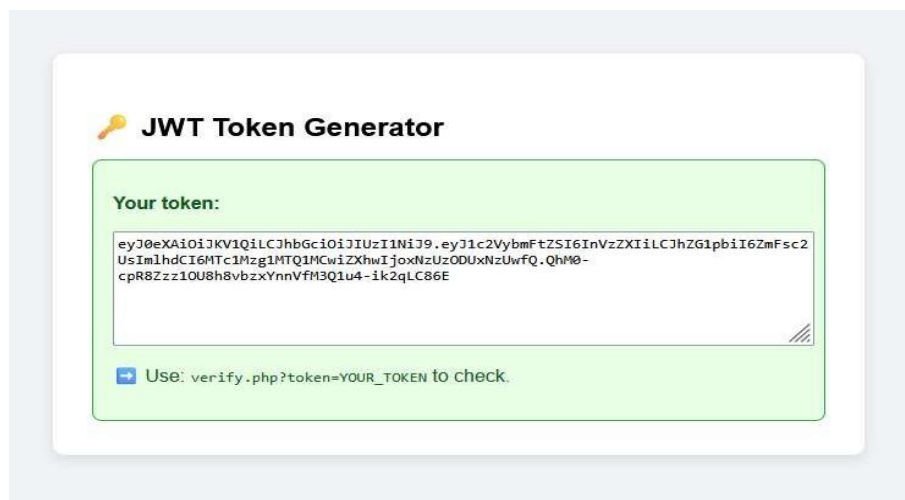
CTF{sql_injection_cyber_pesawaran}

Challenge 4:





Diberikan sebuah login form username dan password. Kita bisa login sebagai **user** dan pw **password**. Setelah login



```
JSON CLAIMS TABLE COPY ↗
{
  "username": "user",
  "admin": false,
  "iat": 1753849465,
  "exp": 1753849765
}
```

Jadi saya menggunakan **jwt.io** untuk melakukan decode dari token jwt yang di berikan. Setelah decode saya melihat bahwa **“admin”:”false”**. Jadi saya ubah menjadi true. Setelah itu ketika saya coba verifikasi menggunakan **verify.php?token=my_token**

Tapi ternyata saya mendapatkan error **invalid signature** saya pun mengecek kembali **jwt.io** dan ternyata



Saya pun menghabiskan banyak waktu untuk mencari dimanakah signature itu di letakan. Setelah pencarian yg cukup memakan waktu saya mendapatkan signaturenya pada source code **login.php**

```
<input type= submit value= login /  
</form>  
<!-- TODO: Hapus secret sebelum deploy: sipitchan-jualan-makanan-halal-sekali -->  
div>  
>
```

Saya dengan cepat langsung mengganti signature yang salah itu dengan yang benar dan melakukan verifikasi sekali lagi. Dan saya mendapatkan flagnya. Tetapi sayangnya saya lupa untuk melakukan ss 🤔

Flag:

CTF{Redacted}

Pesawaran CTF 2025 Flag WriteUp Cryptography

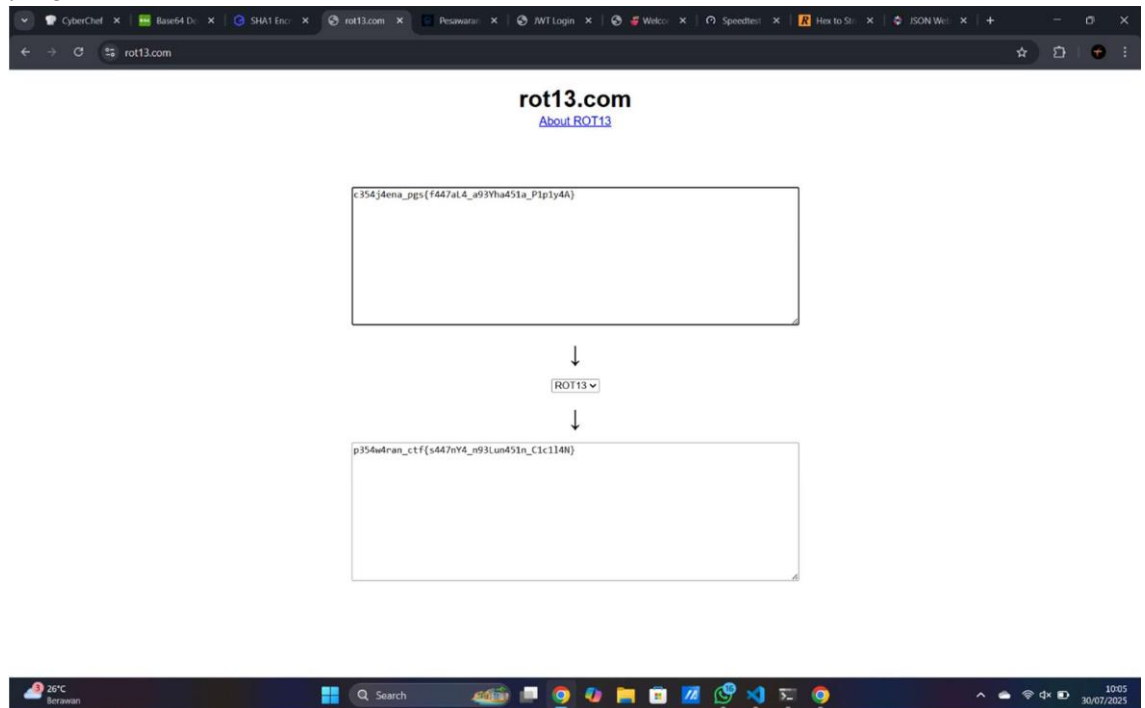
- Gaji Tiga Belas
 - Soal

Kamu hendak menarik gaji ketiga belas, di suatu bank pemerintah. Saat menarik struk transaksi kamu menemukan sebuah ciphertext rahasia:

c354j4ena_pgs{f447aL4_a93Yha451a_P1p1y4A}

- Solusi

Aku menggunakan tool online Bernama <https://rot13.com/> untuk mendecode flag yang terdecode karena rot13



dan bingo aku menemukan flagnya yaitu :
p354w4ran_ctf{s447nY4_n93Lun451n_C1c114N}

- Berpasang-pasangan
 - Soal

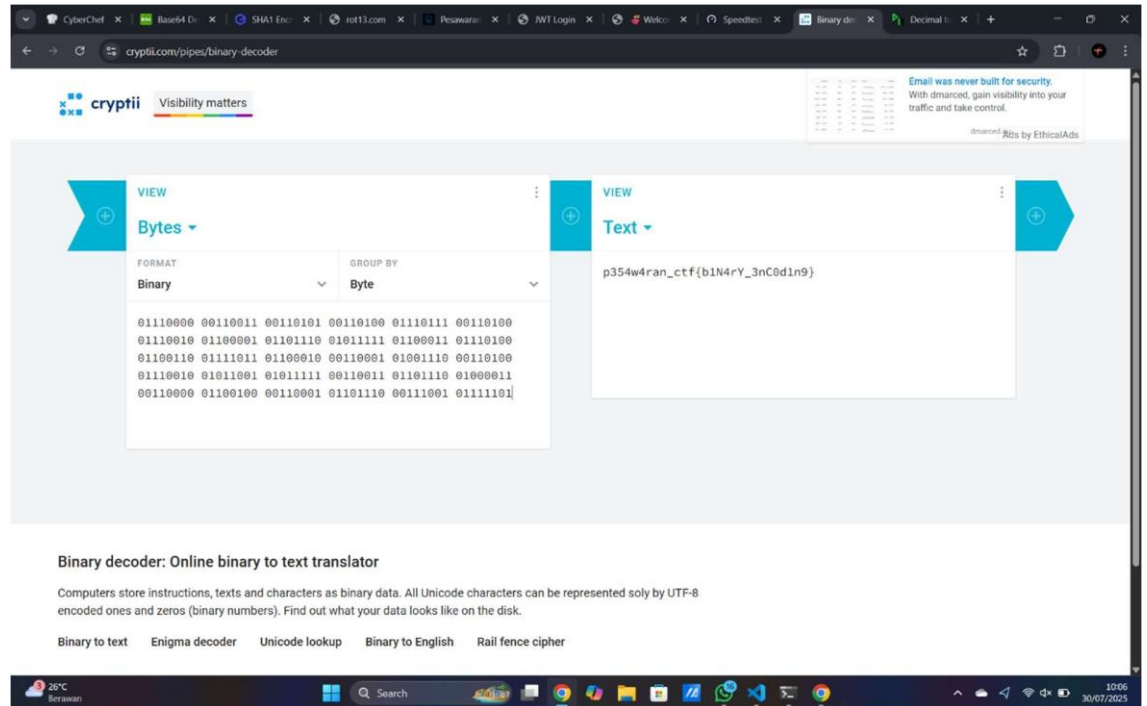
Bayangkan dirimu sekarang sedang ujian magang di instansi keamanan siber, terdapat kamu diminta untuk mengubah format ini menjadi karakter text:

*01110000 00110011 00110101 00110100 01110111 00110100 01110010 01100001
01101110 01011111 01100011 01110100 01100110 01111011 01100010 00110001
01001110 00110100 01110010 01011001 01011111 00110011 01101110 01000011
00110000 01100100 00110001 01101110 00111001 01111101*

- Solusi

Untuk soal ini aku juga menggunakan tool online yaitu

<https://cryptii.com/pipes/binary-decoder> dan aku berhasil mendapatkan flagnya



Dan aku mendapatkan flagnya p354w4ran_ctf{b1N4rY_3nC0d1n9}

- Perbatasan Distrik 16

• Soal

Anggap diri kamu seorang penugas keamanan siber magang di sebuah kantor pemerintahan, dikerahkan ke lokasi vandalisme di distrik 16 kota dalam, dan menemukan angka ini tertulis di lapangan. Divisi judi online, telah menyimpulkan ini tidak terkait judi apapun, tetapi cukup mencurigakan karena ditemukan di jalan tertulis dengan pilok putih, silahkan calon ahli cybersecurity pecahkan.

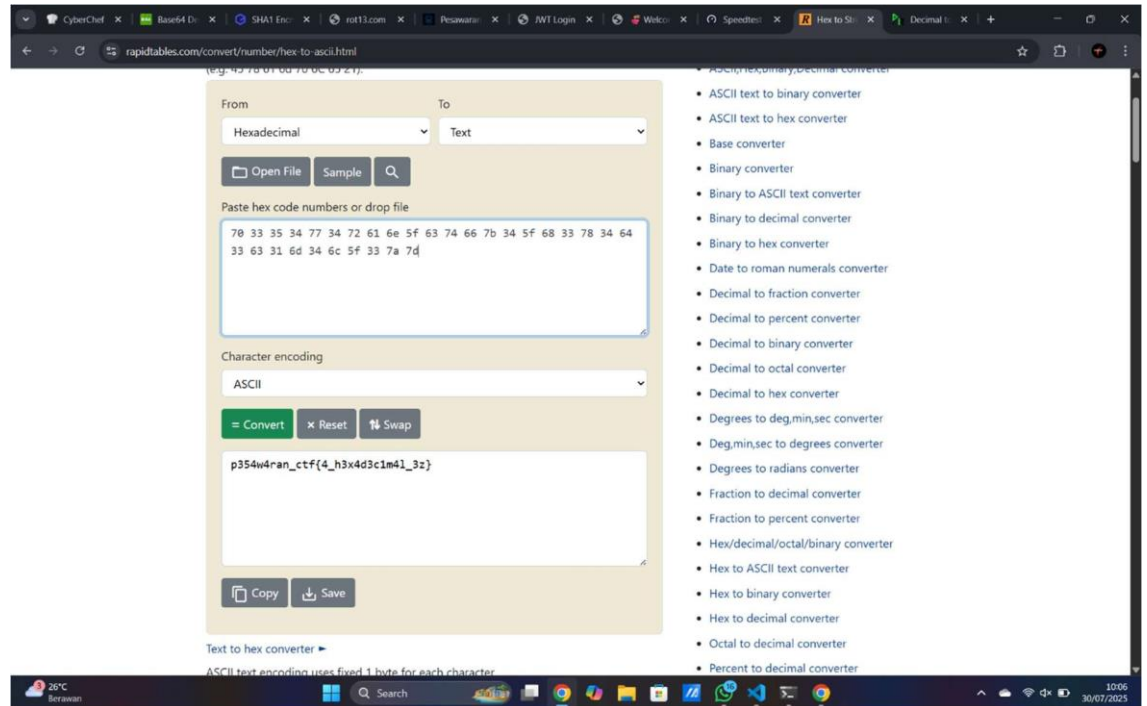
Berikut ini yang angka yang tertulis di jalan.

70 33 35 34 77 34 72 61 6e 5f 63 74 66 7b 34 5f 68 33 78 34 64 33 63 31 6d 34 6c
5f 33 7a 7d

• Solusi

Pada soal ini aku menggunakan tool online

<https://www.rapidtables.com/convert/number/hex-to-ascii.html> untuk mendecode hex



Dan aku berhasil mendapatkan flagnya p354w4ran_ctf{4_h3x4d3c1m4l_3z}

- Nomor Serial CD

• Soal

Kamu menemukan nomor mencurigakan dari balik kotak kemasan celana dalam yang kamu beli dari pedagang ikan disamping toko kue Sipitchan, walaupun bukan branded luar negeri, kita harus cintai produk lokal.

Ini adalah nomor serialnya:

112 51 53 52 119 52 114 97 110 95 99 116 102 123 99 51 108 52 78 52 95 100 52
76 52 77 95 117 78 49 99 48 100 51 125

• Solusi

Untuk soal ini aku menggunakan tool online untuk medeode decimal

<https://www.prepostseo.com/tool/decimal-to-ascii>

CyberChef x Base64 Di x SHA1 Enc x rot13.com x Pesawar x JWT Login x Welc x Speedtest x Hex to St x Decimal t x +

prepostseo.com/tool/decimal-to-ascii

REPOSTSEO Plagiarism Checker DA Checker Paraphrasing Summarizer Essay Writer Image To Text Humanizer new

Chat Premium Login

Decimal to ASCII Converter

To use prepost **Decimal to ASCII** Converter, Enter the Decimal Numbers below

Decimal To Ascii

Decimal To Binary Converter

Decimal To Hex

Decimal To Octal

Ascii To Decimal

Load sample data

112 51 53 52 119 52 114 97 110 95 99 116 102 123 99 51 108 52 78 52 95 100 52
76 52 77 95 117 78 49 99 48 100 51 125

Convert

☐ 0x/0b prefix

Number delimiter
Space

35

Hex (bytes)
70 33 35 34 77 34 72 61 6E 5F 63 74 66 7B 63 33 6C
34 4E 34 5F 64 34 4C 34 4D 5F 75 4E 31 63 30 64 33
7D

ASCII text
p354w4ran_ctf{c3l4N4_d4L4M_uN1c0d3}

28°C
Berawan

Search

1006
30/07/2025

Dan aku mendapatkan flagnya: *p354w4ran_ctf{c3l4N4_d4L4M_uN1c0d3}*