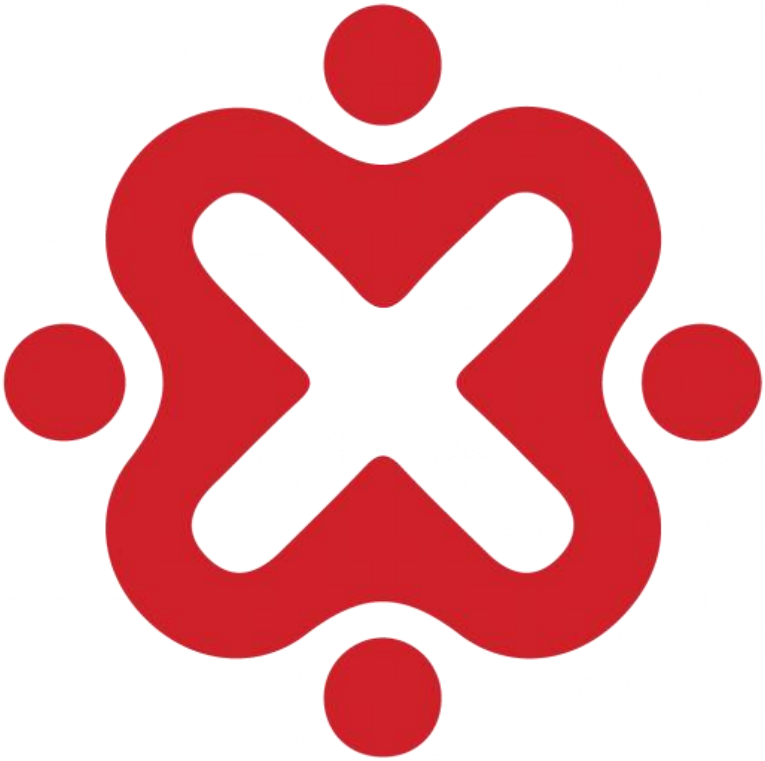
ZeroDay
(Celah yang belum terdeteksi)



ID-Networkers
Indonesian IT Expert Factory

Introduction Team

Nama Team : ZeroDay
Anggota : Muhammad Rizki Maulana, farrel, (づ￣ 3￣)づbRizzzY (rizaldisakims@gmail.com)

Members

User Name	Score
Muhamad Rizki Maulana Captain	100
farrel	270
(づ￣ 3￣)づbRizzzY	180

Point : 550

Summary Findings Each Category

Category	Soal Selesai / Dari Soal yang ada	Point
Web Exploit	13/13	130
Other	1/2	10
Welcome Flag	1/1	10
Web 303	7/7	70
Cryptography	6/7	60
Log Analysis	9/9	90
USB Forensic	6/8	60
Browser Forensic	10/10	100
Windows Forensic	0/15	0
Forensic	2/2	20

Pengurangan Nilai : 0 Point

Detail Challenge Solved

Welcome Flag

Forgot Encode

Deskripsi :

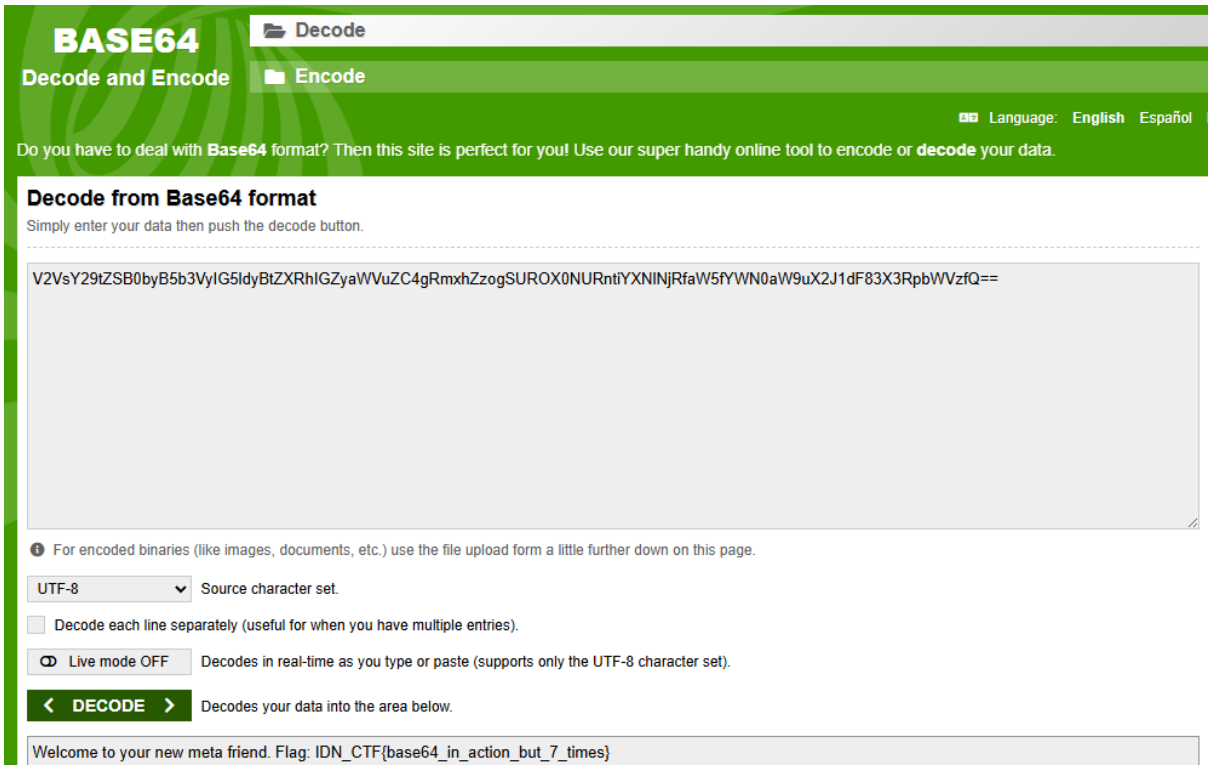
sesorang menggunakan encoding untuk menyimpan rahasianya tapi dia melakukanya sambil berbincang dengan orang lain sehingga dia lupa.

bantu orang tersebut untuk menemukan rahasianya:

Vm0wd2VHUXhUWGhYV0d4VlYwZG9iMVJVU2pSVlZsbDNWMnQwYUZKc2NGWlZWM1IzWVRBeFdHVkVSbHBoTVZwUVZrUkdXbVF5U2tWWGJHUnBWa1phTmxaVVNqUlRNRFZ6VjI1V1ZXSlZXbFZWYWs1dlVsWmtjbFp0Um10TlYxSllWbTAxVTJGR1NsbFJiRkpWVm0xb1ExUldXbXRXTVdSMFpFWmtUbUpGY0ZsWFZFSlhWVEZSZUZOWWJGWmlSa3BoV1d0a2IyUnNiSEZTYlhSclZqQTFTbFl5TVVkVWJGcFZWbXhvVjJKSFVqWlViRnByVm1zeFZsZHJPVmRpU0VKWVYxZDRVMVp0VVhoaVJtUllZbXMxV1ZadGVFdE5SbkJXVmxSV2FGSXdjRWRaTUdoVFYwWmFjMk5JUmxWV2JIQXpXWHBLUzFJeVJrZFdiV2hvVFVoQ01sWnRNREZrTWsxM1RWWmtZVkpXV2xWWlZFNVRWREZhY1ZKcmRGUlNiRVl6Vmxkek5WZEdXbFZSYWxKV1RXcFdjbFl5TVV0VFJsWnpZVWRHVjJWcldtOVdiR1EwVVRGYVZrMVZWazVTUkVFNQ==

Author: Rafly Permana

Lampiran :



Solusi :
" Terlihat dari Deskripsi bahwa ini adalah pesan encoding, dan dia lupa sampai berapa dia encoding.. terlihat bahwa yang dia gunakan juga base64 dengan ciri "==", maka dari itu saya mencoba untuk melakukan decoding beberapa kali"

Flag : IDN_CTF{base64_in_action_but_7_times}

Forensic

QRIS

Deskripsi:
2 kali
Author : Mohamad Fattyr

Lampiran: forensic.jpeg

Langkah yang dilakukan:
1.Scan QR
pertama Ketika QR code discan pertama kali menggunakan QR scanner biasa menggunakan hp, hasilnya bukan flag, melainkan code yang di encode seperti berikut:

1VST1gwWk1RVWQ3VmpOU04xOWxORk0zWDFJaE9VaFVmUT09

2. decode

Kami decode menggunakan base64

```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo U1VST1gwWk1RVWQ3VmpOU04xOWxORk0zWDFJaE9VaFVmUT09 | base64 -d
```

Outputnya: **SUROX0ZMQUd7VjNSN19lNFM3X1IhOUhUfQ==**

Dan hasilnya masih code encode , sesuai dengan deskripsi yaitu harus 2 kali di decodenya.kita decode yang ke-2 kalinya.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo SUROX0ZMQUd7VjNSN19lNFM3X1IhOUhUfQ==  | base64 -d
```

Dan flag finalnya yaitu:

IDN_FLAG{V3R7_e4S7_R!9HT}

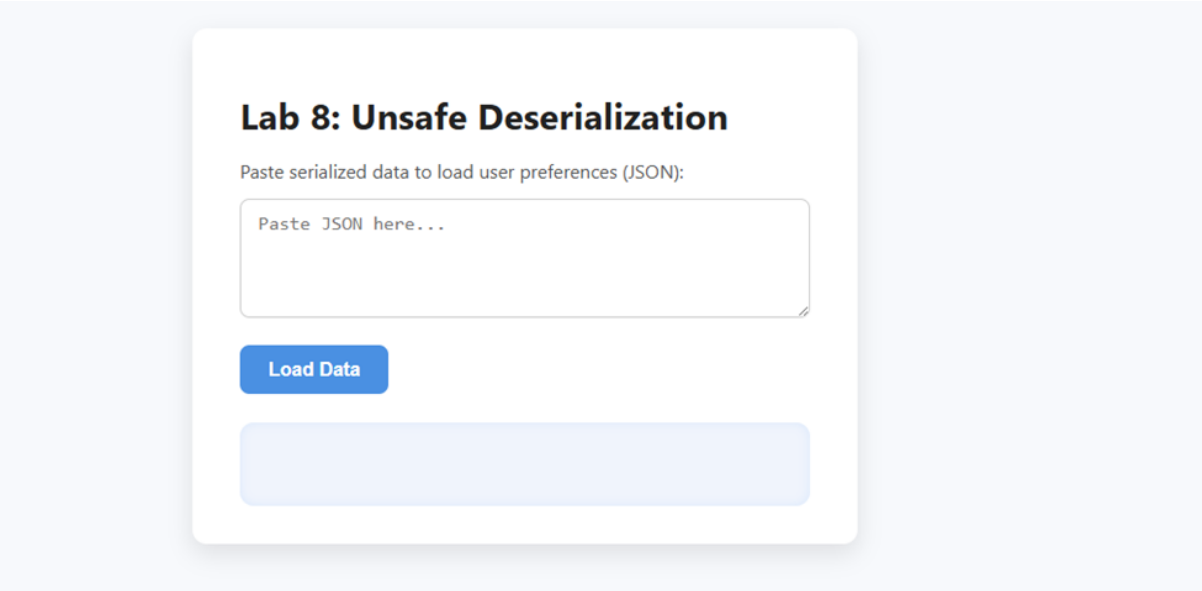
Web 303

Unsafe Deserialization

Deskripsi:
- Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran: https://ctf.solusiber.com/web_101/lab8/
Langkah yang dilakukan:

1. analisis halaman web

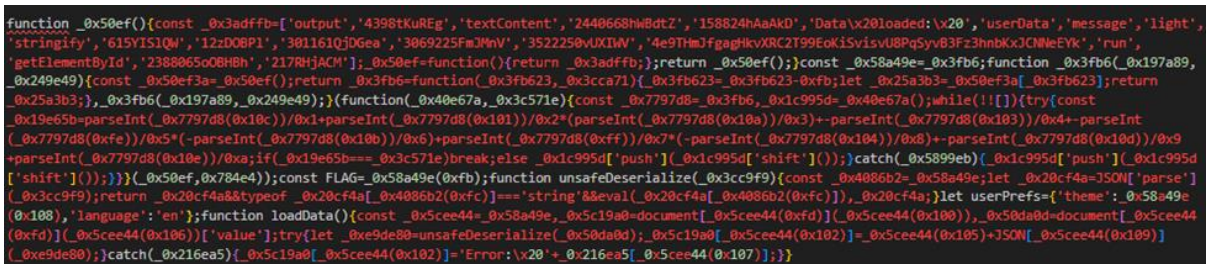


tampilan utama berupa form input bertuliskan:

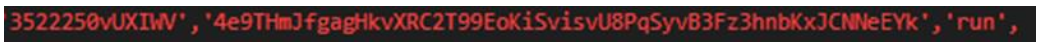
Paste serialized data to load user preferences (JSON):

Terdapat kotak teks dan tombol "Load Data". Hal ini mengindikasikan bahwa data dalam bentuk JSON akan diproses dan ditampilkan.

2. Lihat Source Code / Inspect



Pada bagaian javascript saya menemukan code acak mencurigakan yaitu:



4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk

Karena disebutkan flag di-encode menggunakan metode sama seperti Bitcoin & Solana, kita coba menggunakan python3 untuk mendecodenya :

Dan flag akhirnya yaitu:

IDN_CTF{unsafe_deserialization_executed}

JWT Token Manipulation

Deskripsi:

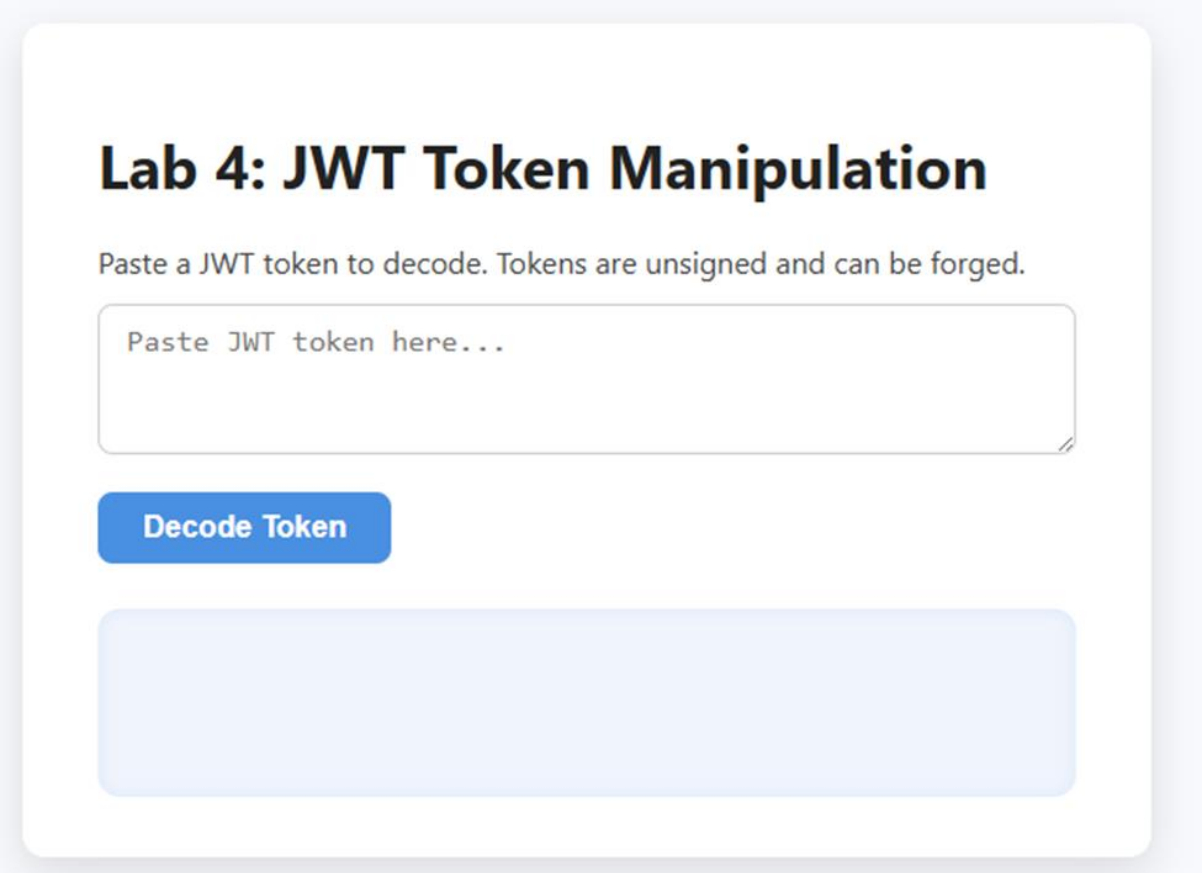
Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Author: Rafly Permana

Lampiran: https://ctf.solusiber.com/web_101/lab4/

Langkah yang dilakukan:

1. Analisis halaman web



Tampilan awal menampilkan form input dengan petunjuk:

“Paste a JWT token to decode. Tokens are unsigned and can be forged.”

Terdapat textarea dan tombol "Decode Token".

2. Inspect Element dan cari ‘javascriptnya’

Ditemukan kode obfuscated, namun setelah diperhatikan, terdapat variabel:

Ini menandakan bahwa flag-nya sudah hardcoded dalam script, hanya di-encode.

3. decode

Berdasarkan deskripsi challenge, disebutkan bahwa flag di-encode menggunakan metode yang sama seperti Bitcoin dan Solana. Saya menggunakan python3 lagi untuk mendapatkan hasil akhirnya, seperti:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -c "import base58; print(base58.b58decode('FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY').decode())"
```

Dan flag nya yaitu:

IDN_CTF{jwt_token_manipulated}

Prototype Pollution Demo

Deskripsi:

Flagnya Di Encode Dengan Encoder yang sama dengan Bitcoin dan Solana

Author: Rafly Permana

Lampiran: https://ctf.solusiber.com/web_101/lab3/

Langkah yang dilakukan:

1. Analisis halaman web

Halaman menampilkan form input untuk memasukkan JSON data dengan label:

"Submit JSON data to update the app config (e.g. {"theme":"dark"})"

Terdapat tombol "Update Config" yang mengindikasikan bahwa data JSON akan dimasukkan ke dalam objek konfigurasi.

2. Inspect elemen

Analisis code nya

```
const _0x323d89=_0x47df;(function(_0x10a409,_0x292dfc){const _0x1839df=_0x47df,_0x4e904d=_0x10a409();while(!![]){try{const _0x36f012=-parseInt(_0x1839df(0x83))/0x1*(parseInt(_0x1839df(0x8b))/0x2)+-parseInt(_0x1839df(0x88))/0x3*(parseInt(_0x1839df(0x96))/0x4)+-parseInt(_0x1839df(0x97))/0x5*(parseInt(_0x1839df(0x89))/0x6)+parseInt(_0x1839df(0x91))/0x7*(-parseInt(_0x1839df(0x93))/0x8)+parseInt(_0x1839df(0x90))/0x9*(parseInt(_0x1839df(0x8f))/0xa)+-parseInt(_0x1839df(0x82))/0xb+parseInt(_0x1839df(0x99))/0xc;if(_0x36f012===_0x292dfc)break;else _0x4e904d['push'](_0x4e904d['shift']());}catch(_0x5e4db2){_0x4e904d['push'](_0x4e904d['shift']());}}(_0xccee,0xb1890));const FLAG=_0x323d89(0x86);let appConfig={'theme':_0x323d89(0x94),'secure':![],'admin':![]};function merge(_0x8f18ef,_0x51be34){const _0x4b608d=_0x323d89;for(let _0x4ff426 in _0x51be34){if(typeof _0x51be34[_0x4ff426]===_0x4b608d(0x84)&&_0x51be34[_0x4ff426]!==null){if(!_0x8f18ef[_0x4ff426])_0x8f18ef[_0x4ff426]={};merge(_0x8f18ef[_0x4ff426],_0x51be34[_0x4ff426]);}else _0x8f18ef[_0x4ff426]=_0x51be34[_0x4ff426];}}function _0x47df(_0x206659,_0x26dc78){const _0xccee7d=_0xccee();return _0x47df=function(_0x47df86,_0xd69584){_0x47df86=_0x47df86-0x82;let _0x38ea1f=_0xccee7d[_0x47df86];return _0x38ea1f;},_0x47df(_0x206659,_0x26dc78);}function _0xccee(){const _0x5c4a91=['ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS','message','3EBrghy','6564dbeISw','output','38qOFssj','Invalid\x20JSON\x20or\x20error:\x20','No\x20admin\x20rights\x20detected.','Config\x20updated:\x20','201MjOup','2616849eVVcvL','63QVALqW','value','949448hBgiJA','light','admin','1513956VyvDeo','480qNMqYS','getElementById','27831936JkNoun','textContent','904365sHjsom','28411RqLoaZ','object','Admin\x20privilege\x20escalated!\x20Flag:\x20'];_0xccee=function(){return _0x5c4a91;};return _0xccee();}function updateConfig(){const _0xa00427=_0x323d89,_0x3aac91=document['getElementById'](_0xa00427(0x8a));try{const _0xfa20a1=JSON['parse'](document[_0xa00427(0x98)]('jsonInput')[_0xa00427(0x92)]);merge(appConfig,_0xfa20a1);let _0x3c731d=_0xa00427(0x8e)+JSON['stringify'](appConfig)+'\x5cn';({}[_0xa00427(0x95)]===!![]||appConfig['admin']===!![]?_0x3c731d+=_0xa00427(0x85)+FLAG:_0x3c731d+=_0xa00427(0x8d),_0x3aac91[_0xa00427(0x9a)]=_0x3c731d);}catch(_0x5cdbd2){_0x3aac91['textContent']=_0xa00427(0x8c)+_0x5cdbd2[_0xa00427(0x87)];}}
```

ditemukan kode JavaScript dengan nama variabel dan fungsi yang di-obfuscate. Namun, terdapat bagian penting seperti:

```
['ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS','
```

Dan kemungkinan code acak tersebut adalah flag yang di encode

3. Decode flag

Berdasarkan deskripsi challenge, disebutkan bahwa flag di-encode menggunakan metode yang sama dengan Bitcoin dan Solana. Berarti kita menggunakan python3 lagi untuk mendecodenya.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -c "import base58; print(base58.b58decode('ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS').decode())"
```

Dan untuk flag finalnya yaitu:

IDN_CTF{prototype_pollution_success}

Unsafe eval()

Deskripsi:

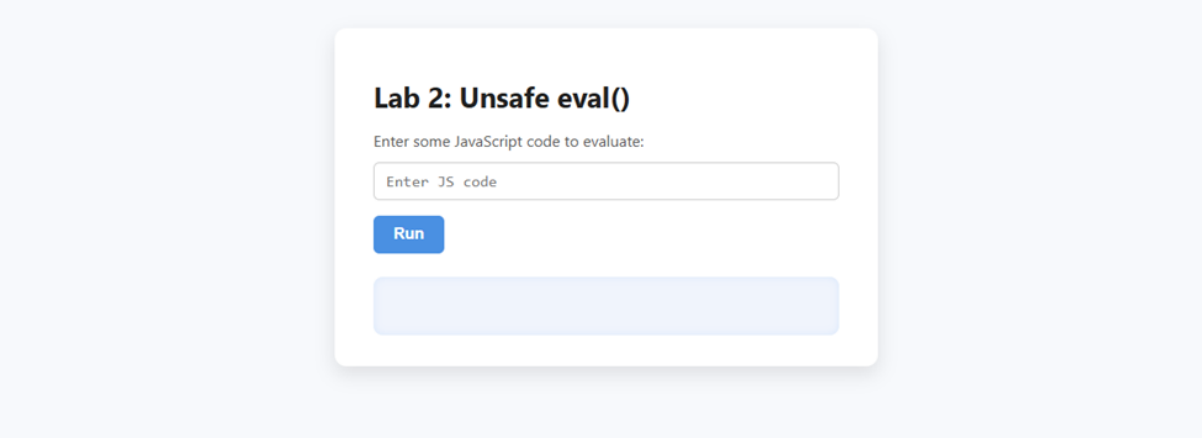
Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Author: Rafly Permana

Lampiran: https://ctf.solusiber.com/web_101/lab2/

Langkah yang dilakukan:

1. Analisis halaman web



Tampilan web memperlihatkan:

- Sebuah textbox dengan placeholder: Enter JS code

- Tombol Run

- Fungsi JavaScript runCode() akan mengeksekusi isi input menggunakan eval().

- Ini indikasi klasik dari unsafe eval(), yang biasanya rawan disalahgunakan.

2. Inspect element

Ditemukan baris penting yang besar kemungkinan adalah flagnya , yaitu

```
FLAG='8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc';function runCode()
```

3. Decode flag

Berdasarkan deskripsi bahwa encoding-nya sama dengan Bitcoin dan Solana.jadi kita mengguanakn python3 lagi

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -c "import base58; print(base58.b58decode('8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTj
Ec').decode())"
```

Dan flag finalnya yaitu:

IDN_CTF{you_used_eval_successfully}

DOM-Based XSS

Deskripsi:

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Author: Rafly Permana

Lampiran: https://ctf.solusiber.com/web_101/lab1/

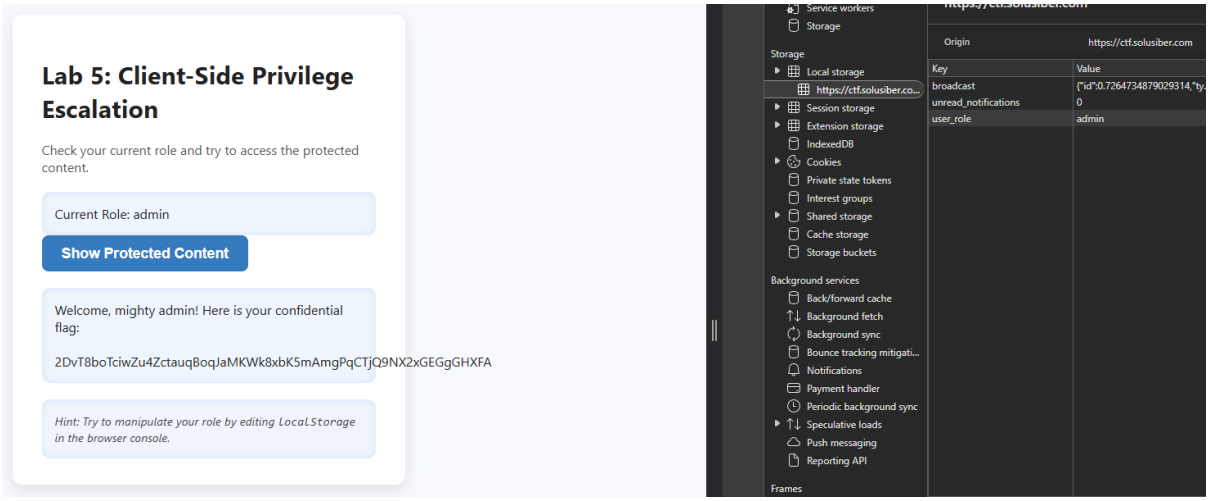
Client-Side Privilege Escalation

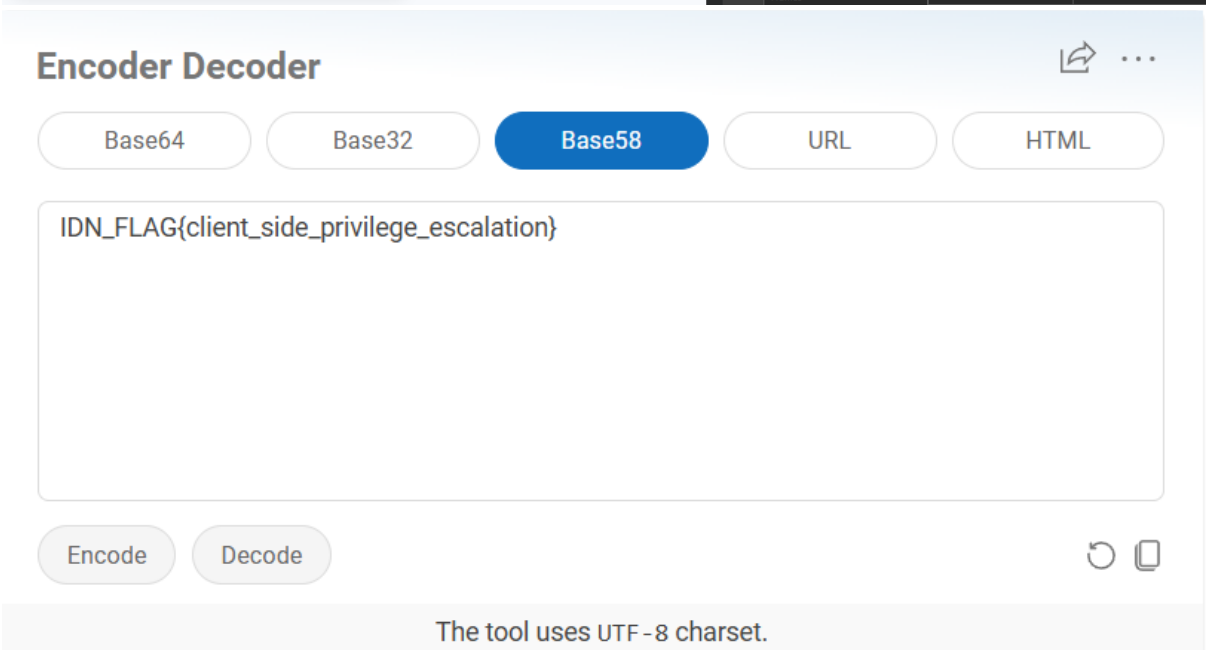
Deskripsi :

Website Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

**Author: Rafly Permana **

Lampiran : https://ctf.solusiber.com/web_101/lab5/





Solusi :
Mengubah User Role lalu melakukan decode

Flag : IDN_FLAG{client_side_privilege_escalation}

Web Exploit

Code Analysis

Deskripsi:
Tanjiro terus berlatih tanpa henti untuk menguasai Hinokami Kagura demi mengalahkan iblis Bulan Atas. Bantu dia membuka kekuatan sejatinya dengan menganalisis kode yang diberikan. Kunci untuk tingkat kekuatan berikutnya terletak pada pemahaman alur kerjanya kode.

Lampiran: https://ctf.solusiber.com/tanjiro_code/

```php
$input = $_GET["secret"] ?? "";
$clean_input = strtolower(str_replace(" ", "", $input));
$result = preg_replace("/".preg_quote($keyword, '/')."/", "", $clean_input, 1);

if ($result === "tanjiro") {
    echo $flag;
}
```

Langkah yang dilakukan:

Tools : VsCode

1.Analisis:

- Input dibersihkan: lowercase dan hapus semua spasi.

- Fungsi preg_replace() hanya menghapus 1 kali keyword dari string.

- Flag hanya akan keluar jika $result === "tanjiro" setelah 1 kali hapus.

2.Identifikasi Masalah:

Supaya $result bisa menjadi tanjiro, kita harus memastikan setelah penghapusan keyword pertama, sisa string tetap tanjiro.

Dengan clue yang ada dan hasil praktis yang ditemukan (tanjirotanjiro berhasil), kita asumsikan bahwa ‘$keyword’ = "tanjiro".

Jadi , Payload yang dipakai:

?secret=tanjirotanjiro

Proses:

1.Input tanjirotanjiro dimasukkan.

2.Setelah dibersihkan jadi:

Tanjirotanjiro -> (lowercase + hapus spasi tetap tanjirotanjiro).

3.Jalankan preg_replace() satu kali:

preg_replace('/tanjiro/', '', 'tanjirotanjiro', 1) -> hasilnya: tanjiro.

Karena hasil akhirnya tanjiro, flag keluar.

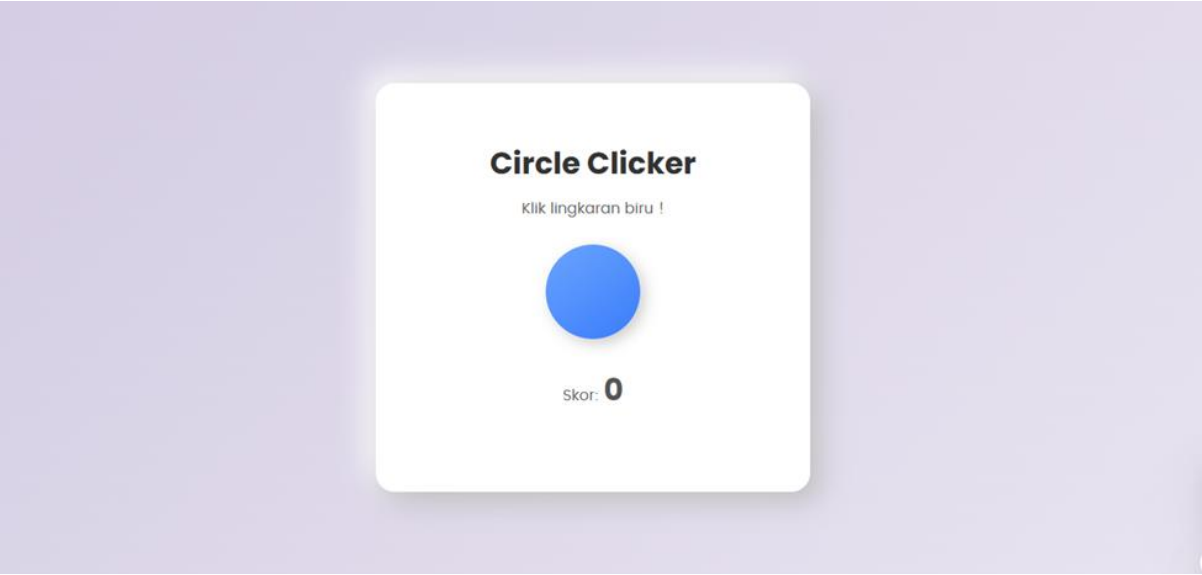
Flagnya:

IDN_CTF(d0ub!e_t4njiro_m4ke_u_H4ppy?}

Circle Clicker

Deskripsi:
- Click Sampai 1000 kali!

Lampiran: https://ctf.solusiber.com/circle_clicker/



Langkah yang dilakukan:

Tools : VsCode ,python3

1. Menganalisis code ‘javascript’ yang ada di dalam inspect elemen

Didalm code ini , ada beberapa hal yang menarik ya.

Kode ini menunjukan ada clue di console setelah jumlah klik tertentu, yaitu:

```
clickCount === 0x5 && !secretUnlocked && console.log('Hmm, ini hanya permainan klik biasa?');
clickCount === 0xa && !secretUnlocked && console.log('Atau mungkin ada sesuatu yang tersembunyi... 🤔');
clickCount === 0xf && !secretUnlocked && console.log('Petunjuk: coba ketik revealSecret() di console');
```

Nah di bagian ketiga ada petunjuk ‘ketik revealSecret()’ di console. Setelah kita mengklik ‘revealSecret’ akan muncul seperti ini:

Dari gambar tersebut kita menemukan flag pertama yaitu:

5WJoJxz5CCVWDSE---

Setelah itu kami menemukan flag keduanya di code javascript:

```
](‘%cLuar\x20biasa!\x20Kamu\x20mendapatkan\x20bagian\x20kedua\x20flag:\x20master}’,_0x1faaef(0x18b)),
```

Flag kedua:

Master

Setelah semua flag terkumpul , mari kita gabungkan dari flag pertama dan kedua:

5WJoJxz5CCVWDSEmaster

Ini belum selesai, karena deskripsi menyebutkan bahwaa "Di Encode Dengan Encoder yang sama dengan bitcoin dan solana", maka saya menggunakan python3 untuk mendecode nya.

Dan flag final nya yaitu:

IDN_CTF{click_master}

ID-Networkers

Deskripsi :

Sebuah situs publik baru saja diluncurkan ID-Networkers. Tampilannya sederhana dan tidak mencurigakan—hanya halaman beranda dengan ucapan “Selamat Datang di ID-Networkers” dan beberapa tamabahan lainya.

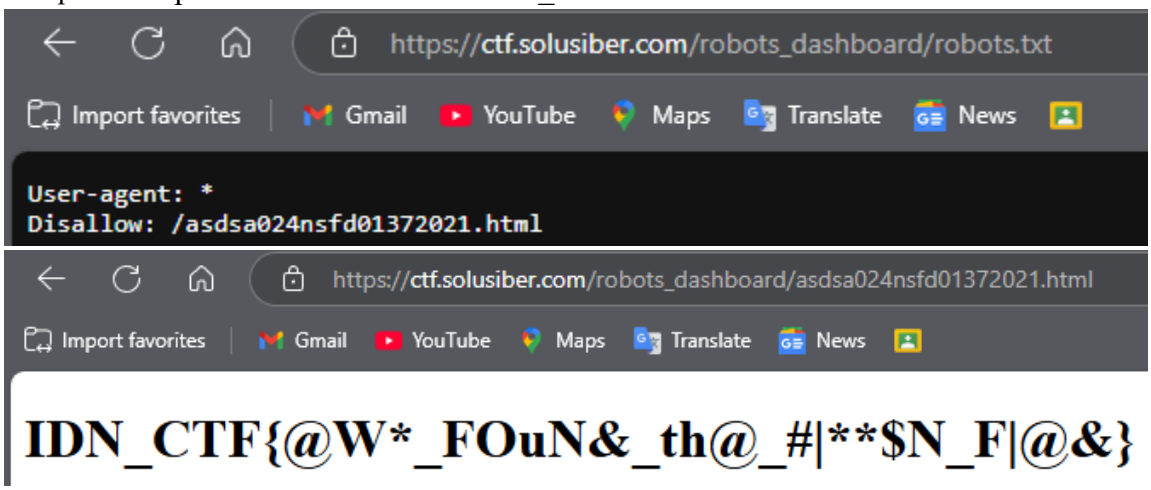
Namun, informasi mengatakan bahwa developer situs ini terlalu percaya pada "aturan" yang ditulis untuk mesin pencari. Mereka menyembunyikan direktori rahasia dengan harapan crawler tidak akan melihatnya...

Tapi kamu bukan crawler, kamu seorang penyusup yang teliti.

Website

Author: Rafly Permana

Lampiran : https://ctf.solusiber.com/robots_dashboard/



Solusi :
Membaca robots.txt lalu mengikuti path yang ada

Flag : IDN_CTF{@W*_FOuN&_th@_#|**$N_F|@&}

Konoha Breach

Deskripsi :

Desa Konoha baru saja meluncurkan sistem data tabel internal untuk para ninja tingkat tinggi. Sistem ini hanya bisa diakses setelah login dengan kredensial resmi admin.

Namun, rumor menyebutkan bahwa sistem ini dibangun tergesa-gesa oleh seorang Chuunin yang baru belajar PHP. Konon, ada celah klasik yang memungkinkan siapa pun melewati sistem login dan mengakses dashboard rahasia tanpa kredensial!

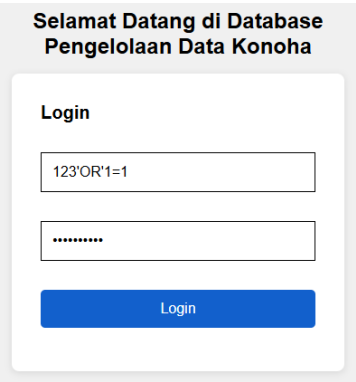
Bocoran pertama yang muncul berisi daftar shinobi aktif dan lokasi markas Anbu. Keamanan Konoha kini dalam bahaya…

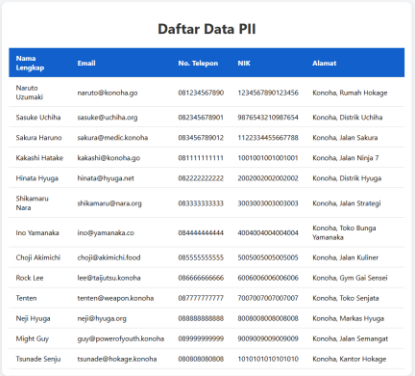
Bisakah kamu menyusup ke sistem tanpa login dan menemukan yang tersembunyi?

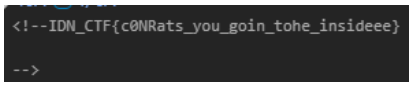
Website

Author: Rafly Permana

Lampiran : https://ctf.solusiber.com/login_bypass/







Solusi :
SQL Injection

Flag : IDN_CTF{c0NRats_you_goin_tohe_insideee}

Support Force

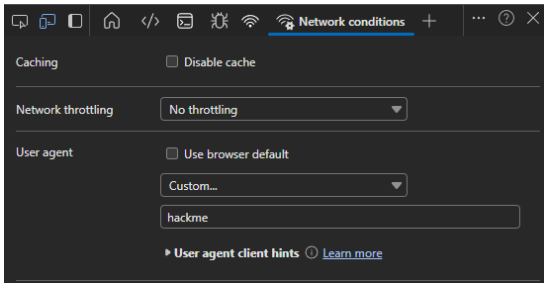
Deskripsi :

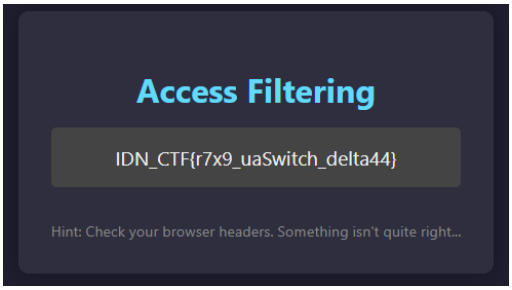
Ini klub eksklusif buat agen rahasia. Browser biasa? Maaf, Anda tidak terdaftar. Tapi kalau kamu bisa pura-pura jadi "Agent hackme", pintu rahasia mungkin bakal terbuka buatmu.

Website

Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/support_force/





Solusi :
Menangani User Agent

Flag : IDN_CTF{r7x9_uaSwitch_delta44}

IDN Education

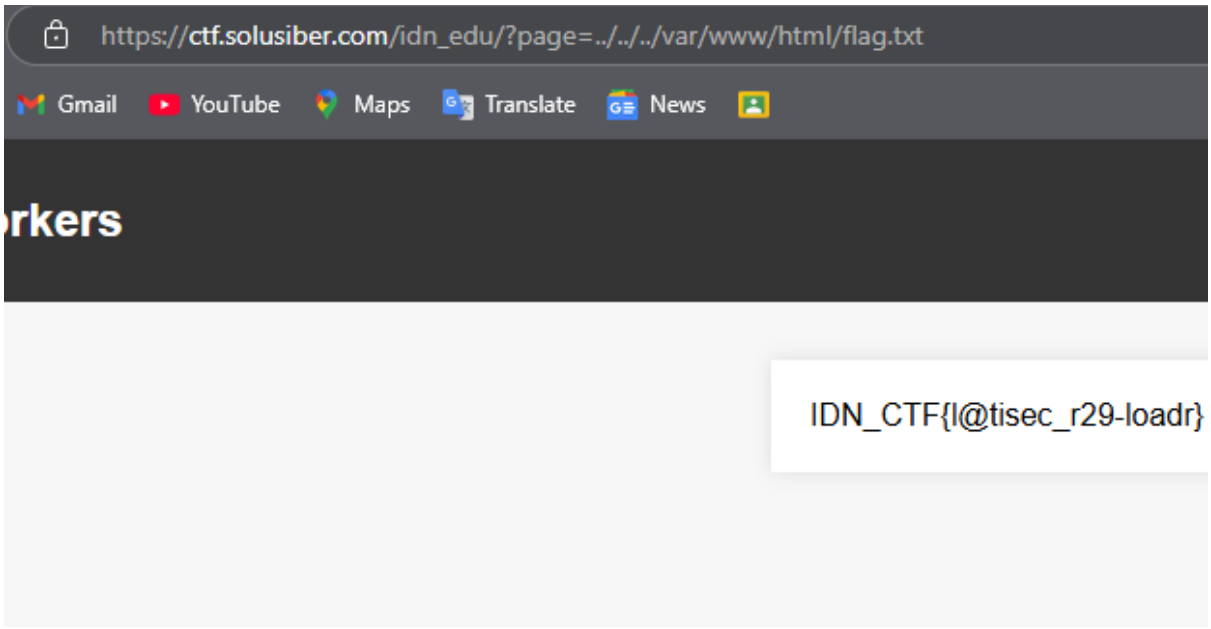
Deskripsi :

Siapa sangka file-file tersembunyi di balik input sederhana? Coba kamu buka celahnya, biar file yang terpendam itu bisa keluar. Siapa tahu ada kejutan!

Website

Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/idn_edu/



Solusi :
Menemukan flag dengan payload ../../../var/www/html/flag.txt

Flag : IDN_CTF{l@tisec_r29-loadr}

Beyond Way

Deskripsi :

Mungkin kamu nggak pernah diajari buat berjalan keluar dari jalan yang benar... tapi kalau kamu bisa, kamu bakal dapetin sesuatu yang terlarang. Ayo jalanin manipulasi path-nya! 🏃‍♂️🔮 Website Author : Rafly Permana

Lampiran : https://ctf.solusiber.com/search_free/

Solusi :
Mencari file flag.txt

Flag : IDN_CTF{tvec-resolver_41}

Other

User Guide

Deskripsi:
FLAG

Lampiran : User Guide CTFd IDN Cyber Security.pdf

Solusi: diakhir lampiran ada flagnya , cuman disamarkan dengan warna putih
Flag: IDN_FLAG{makasih_sudah_baca_guide}

Log Analysis

Log Analysis 1

Deskripsi :

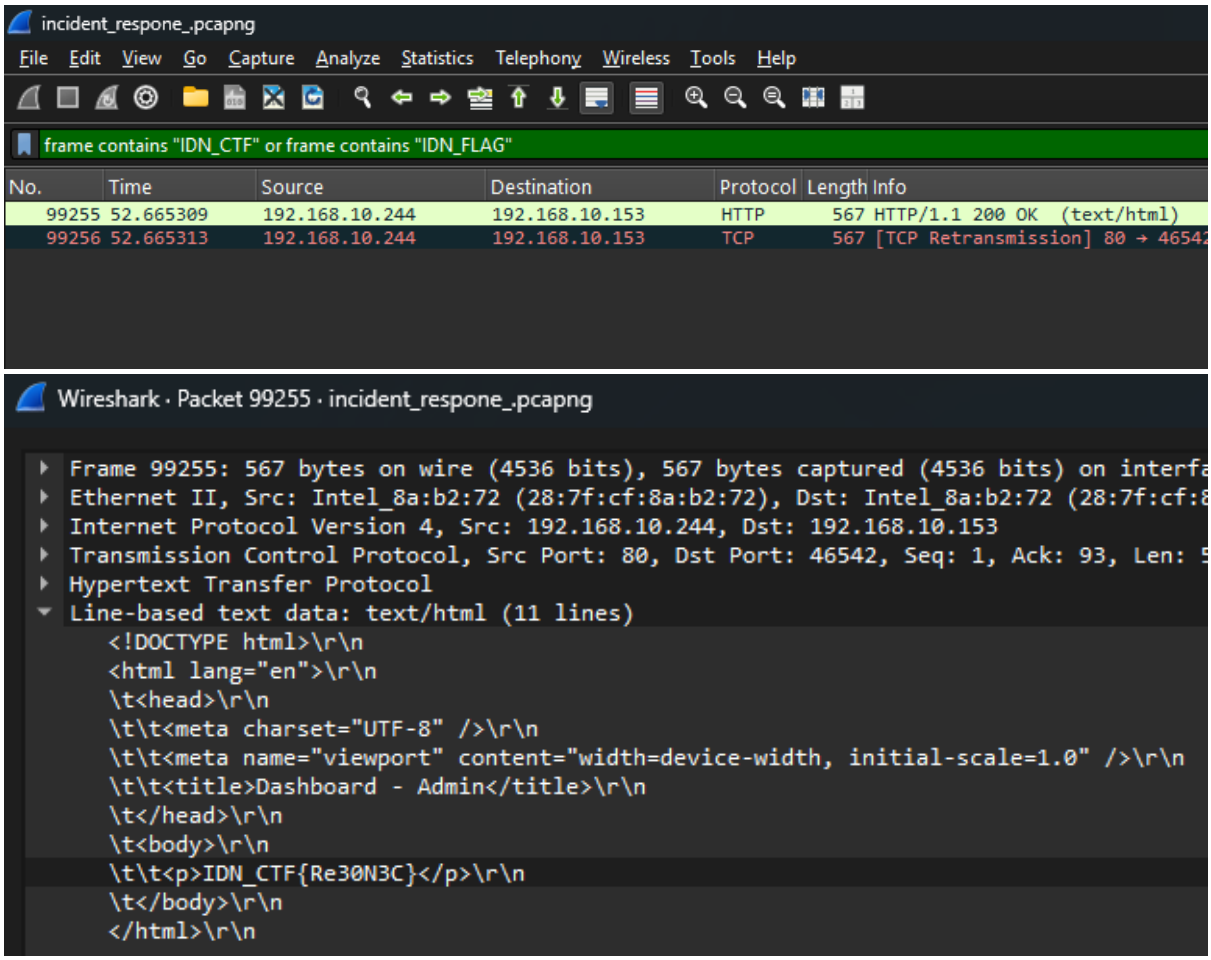
pada file pcap dibawah, hacker mencoba untuk melakukan sesuatu yang berhubungan dengan recon

pada service, silahkan cari...

Format Flag : IDN_CTF{jawaban}

Author : Aditya Firman Nugroho

Lampiran : incident_response_.pcapng



Solusi :
Melakukan filter kata

Flag : IDN_CTF{Re30N3C}

Log Analysis 2

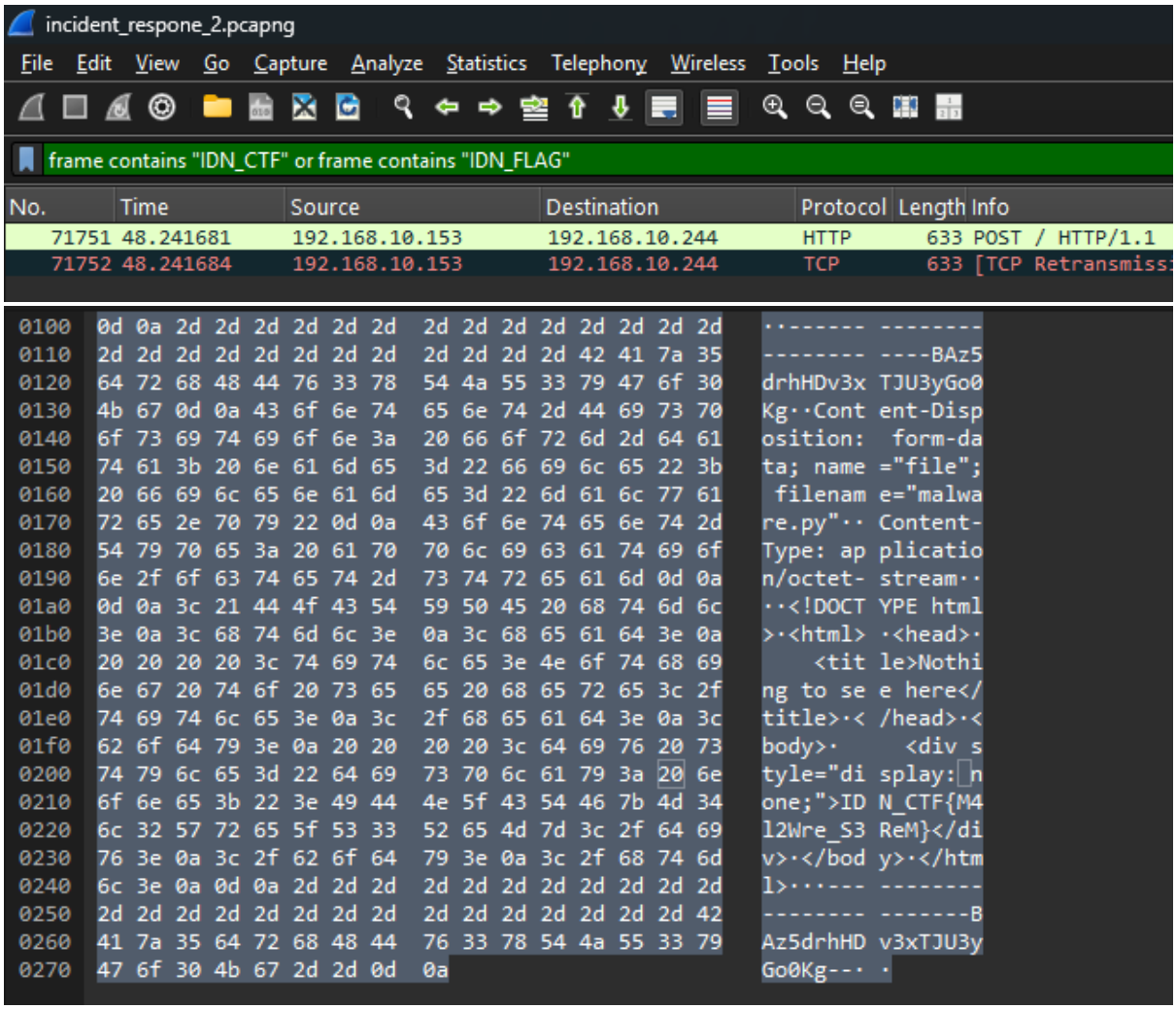
Deskripsi :

awas, hati-hati, pelan-pelan, ada .....

Format Flag : IDN_CTF{jawaban}

Author : Aditya Firman Nugroho

Lampiran : incident_response_2.pcapng



Solusi :
Melakukan filter kata

Flag : IDN_CTF{M4lWre_S3ReM}

Log Analysis 3

Deskripsi :

analisis log acces.log ini, file ip yang dimasukan pada system ?

Format Flag : IDN_CTF{jawaban}

Author : Aditya Firman Nugroho

Lampiran : access.log

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charge HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MS
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charges HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; M
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chart HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charts HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MS
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chat HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chats HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /check HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checking HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible;
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible;
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout_iclear HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compa
192.168.18.6 - - [27/Apr/2025:12:55:31 +0000] "POST /upload/malware.py HTTP/1.1" 200 4313 "-" "curl/8.12.1"
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /randomfile1 HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatibl
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /frand2 HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MS
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bash_history HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compati
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bashrc HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; M
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cache HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MS
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.config HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; M
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cvs HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cvsignore HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.forward HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible;
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.git/HEAD HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.history HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible;
```

Solusi :
POST merupakan suatu perintah untuk mengirim file, oleh karena itu mecari keyword POST

Flag : IDN_CTF{malware.py}

Log Analysis 4

Deskripsi :

analis log auth.log, user apa yang sukses masuk ke dalam system ?

Format Flag : IDN_CTF{user}

Author : Aditya Firman Nugroho

Lampiran : auth.log

```
Apr 27 13:05:10 test sshd[19014]: Accepted password for ghxyss from 192.168.18.6 port 52320 ssh2
Apr 27 13:05:10 test sshd[19014]: pam_unix(sshd:session): session opened for user ghxyss(uid=1000) by (uid=0)
Apr 27 13:05:10 test systemd-logind[872]: New session 4 of user ghxyss.
```

Solusi :
Mencari kata kunci yang menandakan user berhasil login

Flag : IDN_CTF{ghxyss}

Log Analysis 5

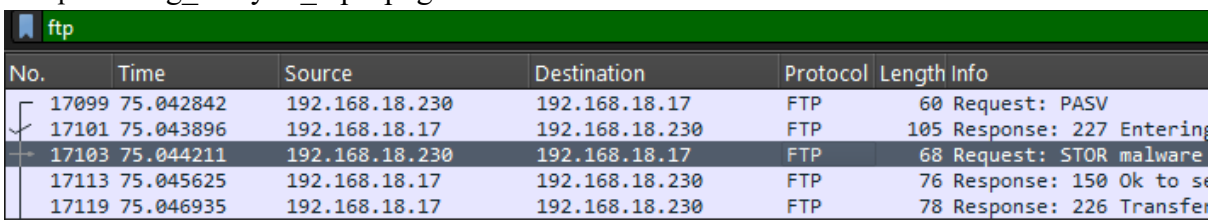
Deskripsi :

"dengan service ... file ... di dalam server " - administrator

Format Flag : IDN_CTF{service:file}

Author : Aditya Firman Nugroho

Lampiran : log_analysis_5.pcapng



Solusi :
Melakukan filtering pada protocol dan menemukan request pada file malware

Flag : IDN_CTF{ftp:malware}

Log Analysis 6

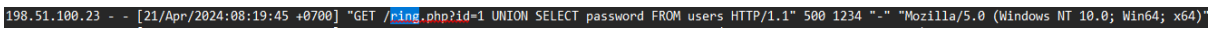
Deskripsi :

Seseorang mencoba mengeksploitasi endpoint dengan teknik SQL Injection, menghasilkan internal server error. Apa nama file yang ditargetkan dalam eksploitasi tersebut?

IDN_CTF{jawaban}

Author: Rafly Permana

Lampiran : log1.txt



Solusi :
Menemukan log yang berisi meminta akses kepada file ring.php

Flag : IDN_CTF{ring.php}

Log Analysis 8

Deskripsi :

Pada tanggal 22 April, salah satu user berhasil mendapatkan akses root melalui SSH. Berdasarkan log, berikan IP address asli dari user tersebut.

IDN_CTF{jawaban}

Author: Rafly Permana

Lampiran : log3.txt

```
Apr 22 12:01:40 server1 sshd[2347]: Accepted password for user1 from 198.51.100.23 port 51432 ssh2
Apr 22 12:01:42 server1 sshd[2347]: pam_unix(sshd:session): session opened for user user1 by (uid=0)
Apr 22 12:02:01 server1 sudo:    user1 : TTY=pts/1 ; PWD=/home/user1 ; USER=root ; COMMAND=/bin/cat /etc/passwd
Apr 22 12:02:05 server1 sudo: pam_unix(sudo:session): session opened for user root by user1(uid=0)
Apr 22 12:02:07 server1 sudo: pam_unix(sudo:session): session closed for user root
Apr 22 12:02:10 server1 kernel: [UFW BLOCK] IN=eth0 OUT= MAC=00:0c:29:68:22:db:00:50:56:c0:00:01:08:00 SRC=192.0
URGP=0
```

Solusi :
Mencari keyword yang mengindikasikan login

Flag : IDN_CTF{192.51.100.23}

Log Analysis 9

Deskripsi :

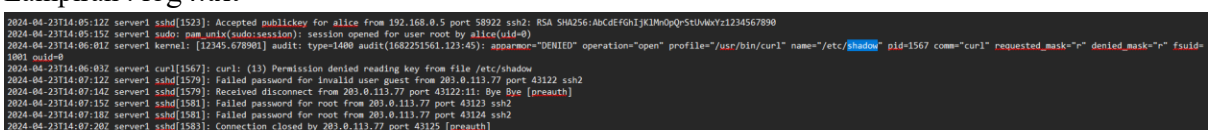
Pengguna manakah yang berhasil mendapatkan akses root, mencoba membaca file shadow menggunakan curl, namun ditolak oleh AppArmor? Sebutkan IP-nya dan hash publik RSA yang digunakan saat login.

pisahkan jawaban dengan koma (,) Contoh: user,10.10.10.9,BASE64:Jinasidn023nnandd

IDN_CTF{jawaban}

Author: Rafly Permana

Lampiran : log4.txt



Solusi :
Menemukan bahwa user alice membuka session root dan melakukan curl pada /etc/shadow namun akses ditolak

Flag : IDN_CTF{alice,192.168.0.5,BASE64:AbCdEfGhIjKlMnOpQrStUvWxYz1234567890}

Browser Forensic

Tools : DB Browser SQLite

Browser Forensic 1

Deskripsi :

> Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!
>
> Tools apa yang di cari oleh user ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip

```
github.com/ParrotSec/mimikatz
```

Solusi :
Melihat user mengunjungi repositori github pada file History

Flag : IDN_FLAG{mimikatz}

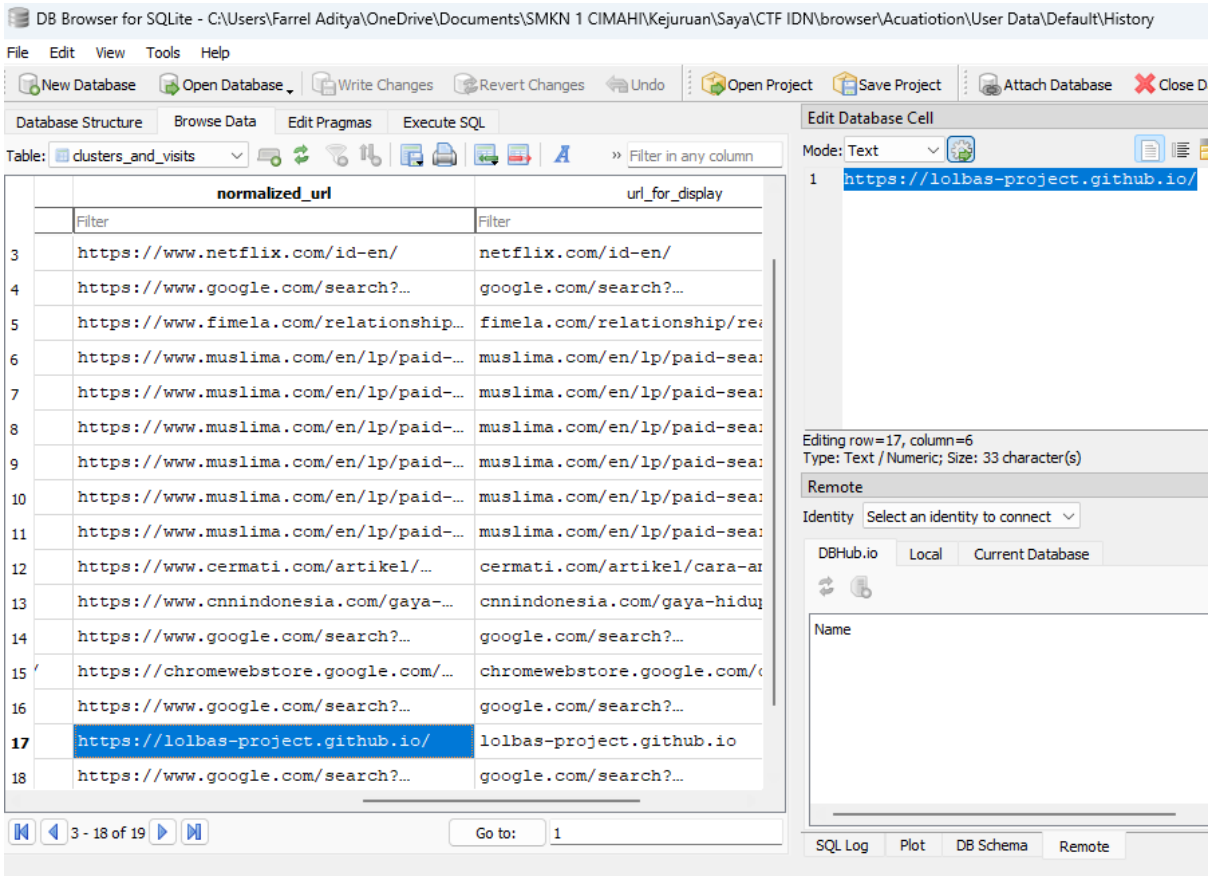
Browser Forensic 2

Deskripsi :

> Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!
>
> (Filenya ada di pertanyaan pertama)
>
> Website apa yang dicari oleh user berkaitan dengan Teknik Persistence, Privilage Escalation, DLL Injection etc ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :
Melihat user mengunjungi repositori github pada file History

Flag : IDN_FLAG{https://lolbas-project.github.io/}

Browser Forensic 3

Deskripsi :

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!

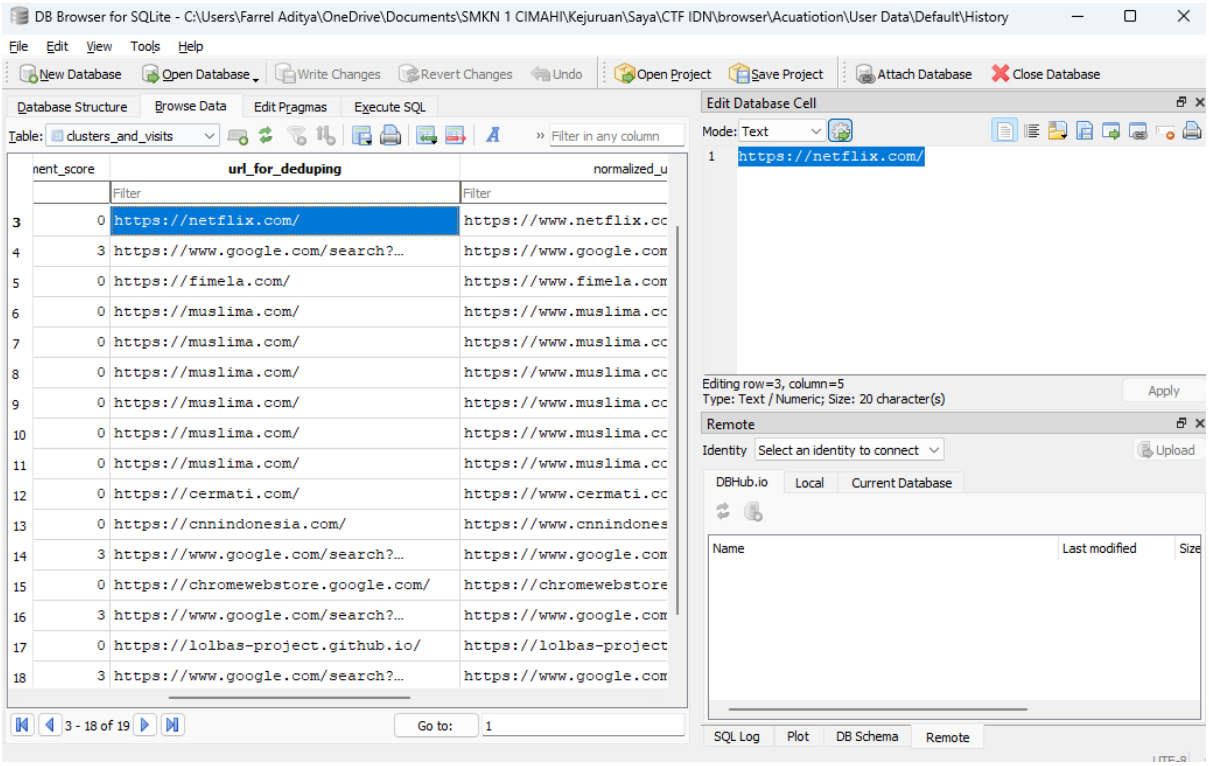
(Filenya ada di pertanyaan pertama)

Streaming Website yang ditonton oleh user ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :
Melihat user mengunjungi web streaming pada file History

Flag : IDN_FLAG{https://netflix.com/}

Browser Forensic 4

Deskripsi :

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!

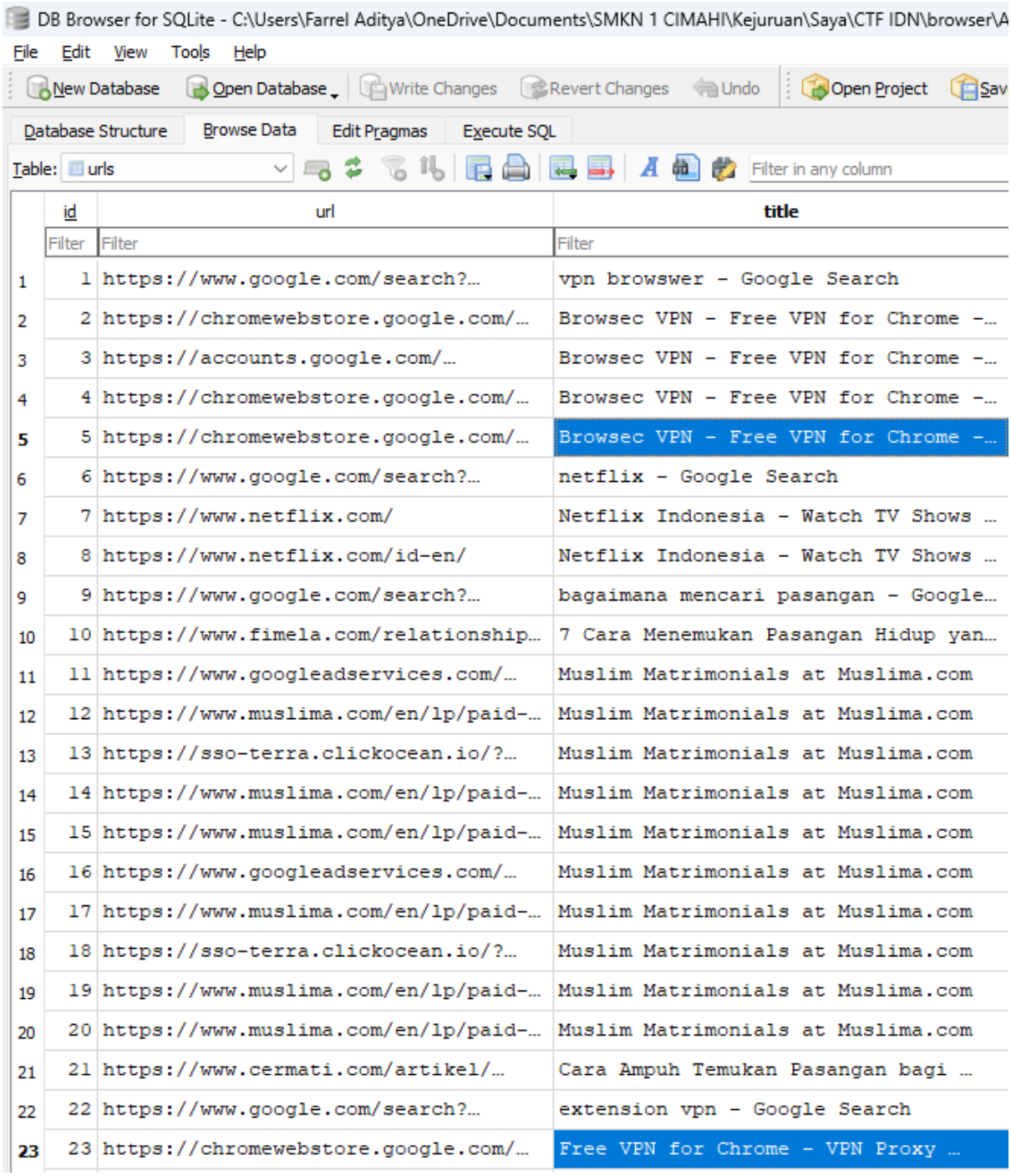
(Filenya ada di pertanyaan pertama)

Vpn apa saja yang diinstal oleh user ?

format flag : IDN_FLAG{VPN_1-VPN_2} example : IDN_FLAG{IPSEC_SECURITY-L2TP_SECURITY}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip


DB Browser for SQLite - C:\Users\Farrel Aditya\OneDrive\Documents\SMKN 1 CIMAHI\Kejuruan\Saya\CTF IDN\browser\A

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Undo | Open Project | Sav

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: urls | Filter in any column

	id	url	title
	Filter	Filter	Filter
1	1	https://www.google.com/search?…	vpn browswer - Google Search
2	2	https://chromewebstore.google.com/…	Browsec VPN - Free VPN for Chrome -…
3	3	https://accounts.google.com/…	Browsec VPN - Free VPN for Chrome -…
4	4	https://chromewebstore.google.com/…	Browsec VPN - Free VPN for Chrome -…
5	5	https://chromewebstore.google.com/…	Browsec VPN - Free VPN for Chrome -…
6	6	https://www.google.com/search?…	netflix - Google Search
7	7	https://www.netflix.com/	Netflix Indonesia - Watch TV Shows …
8	8	https://www.netflix.com/id-en/	Netflix Indonesia - Watch TV Shows …
9	9	https://www.google.com/search?…	bagaimana mencari pasangan - Google…
10	10	https://www.fimela.com/relationship…	7 Cara Menemukan Pasangan Hidup yan…
11	11	https://www.googleadservices.com/…	Muslim Matrimonials at Muslima.com
12	12	https://www.muslima.com/en/lp/paid-…	Muslim Matrimonials at Muslima.com
13	13	https://sso-terra.clickocean.io/?…	Muslim Matrimonials at Muslima.com
14	14	https://www.muslima.com/en/lp/paid-…	Muslim Matrimonials at Muslima.com
15	15	https://www.muslima.com/en/lp/paid-…	Muslim Matrimonials at Muslima.com
16	16	https://www.googleadservices.com/…	Muslim Matrimonials at Muslima.com
17	17	https://www.muslima.com/en/lp/paid-…	Muslim Matrimonials at Muslima.com
18	18	https://sso-terra.clickocean.io/?…	Muslim Matrimonials at Muslima.com
19	19	https://www.muslima.com/en/lp/paid-…	Muslim Matrimonials at Muslima.com
20	20	https://www.muslima.com/en/lp/paid-…	Muslim Matrimonials at Muslima.com
21	21	https://www.cermati.com/artikel/…	Cara Ampuh Temukan Pasangan bagi …
22	22	https://www.google.com/search?…	extension vpn - Google Search
23	23	https://chromewebstore.google.com/…	Free VPN for Chrome - VPN Proxy …

Solusi :
Melihat user melakukan pencarian tools VPN pada file History

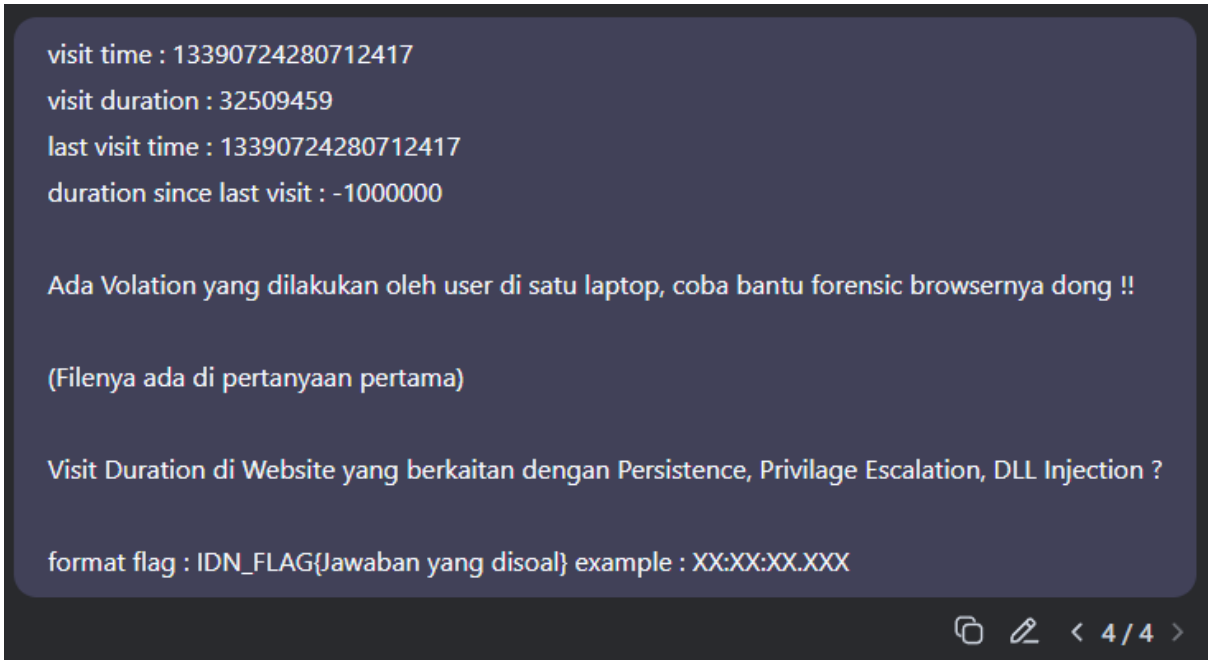
Flag : IDN_FLAG{BROWSEC_VPN-VPN_PROXY_VEEPN}

Browser Forensic 5

Deskripsi :

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !! (Filenya ada di pertanyaan pertama) Visit Duration di Website yang berkaitan dengan Persistence, Privilage Escalation, DLL Injection ? format flag : IDN_FLAG{Jawaban yang disoal} example : XX:XX:XX.XXX Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :
Mencari data yang diperlukan seperti berikut pada SQLite, lalu melakukan konversi waktu

Flag : IDN_FLAG{00:00:32.509}

Browser Forensic 6

Deskripsi :

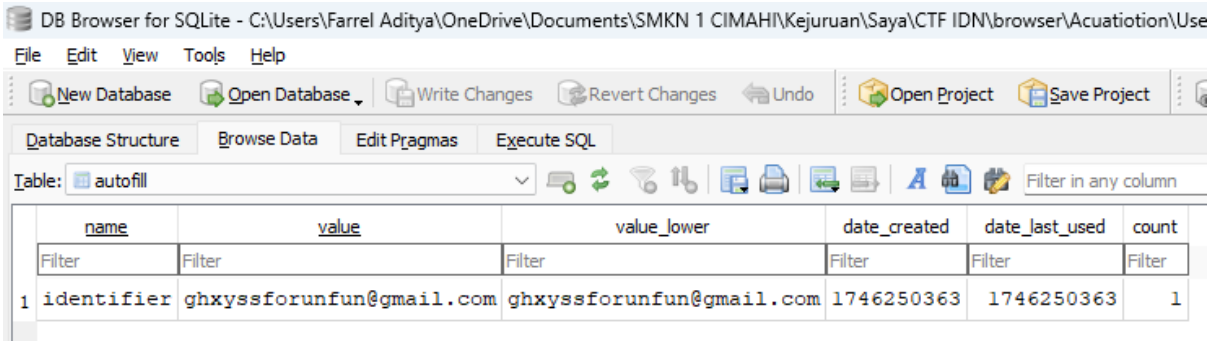
Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!
(Filenya ada di pertanyaan pertama)

Email yang digunakan pada browser ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :
Menemukan email pada file Web Data menggunakan SQLite

Flag : IDN_FLAG{ghxyssforunfun@gmail.com}

Browser Forensic 7

Deskripsi :

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!

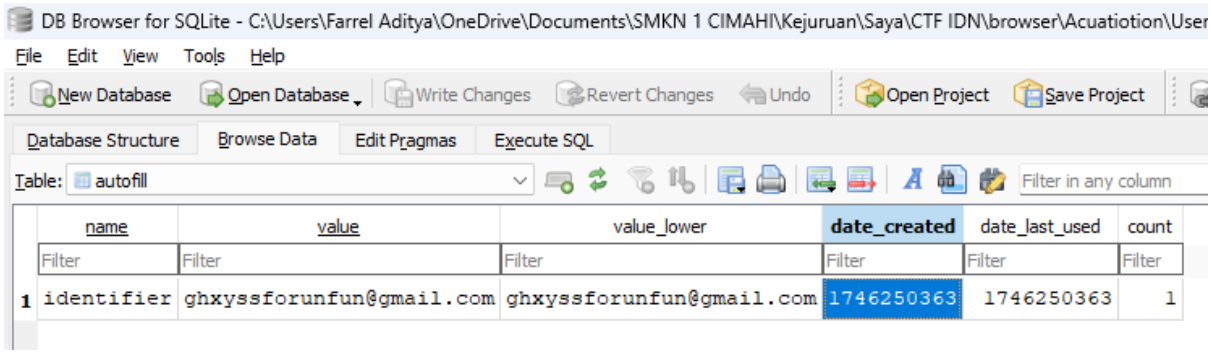
(Filenya ada di pertanyaan pertama)

date_created pada email menggunakan tools DB Browser SQLite ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :
Menemukan email beserta tanggal pembuatan pada file Web Data menggunakan SQLite

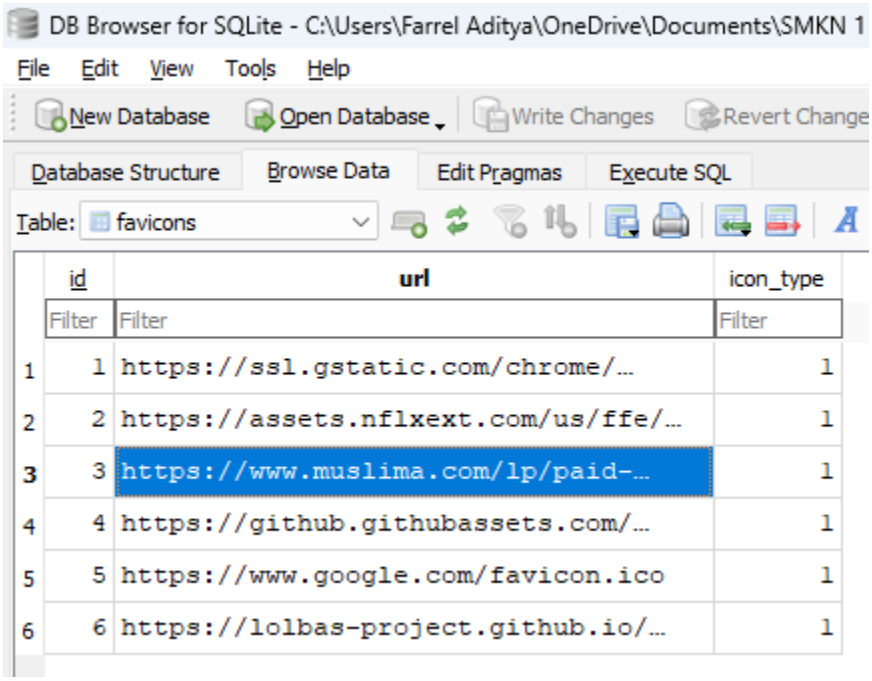
Flag : IDN_FLAG{1746250363}

Browser Forensic 8

Deskripsi :

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!
(Filenya ada di pertanyaan pertama)
url favicon, di website yang dicari oleh user ? (tidak berkaitan dengan hacker !!!)
format flag : IDN_FLAG{Jawaban yang disoal}
Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



	id	url	icon_type
	Filter	Filter	Filter
1	1	https://ssl.gstatic.com/chrome/...	1
2	2	https://assets.nflxext.com/us/ffe/...	1
3	3	https://www.muslima.com/lp/paid-...	1
4	4	https://github.githubassets.com/...	1
5	5	https://www.google.com/favicon.ico	1
6	6	https://lolbas-project.github.io/...	1

Solusi :
Menemukan data berisi situs favicon yang dikunjungi pada file Favicons

Flag : IDN_FLAG{ https://www.muslima.com/lp/paid-search/terra-assets/images/favicon-8b7d9ccfa1-3.ico}

Browser Forensic 9

Deskripsi :

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!

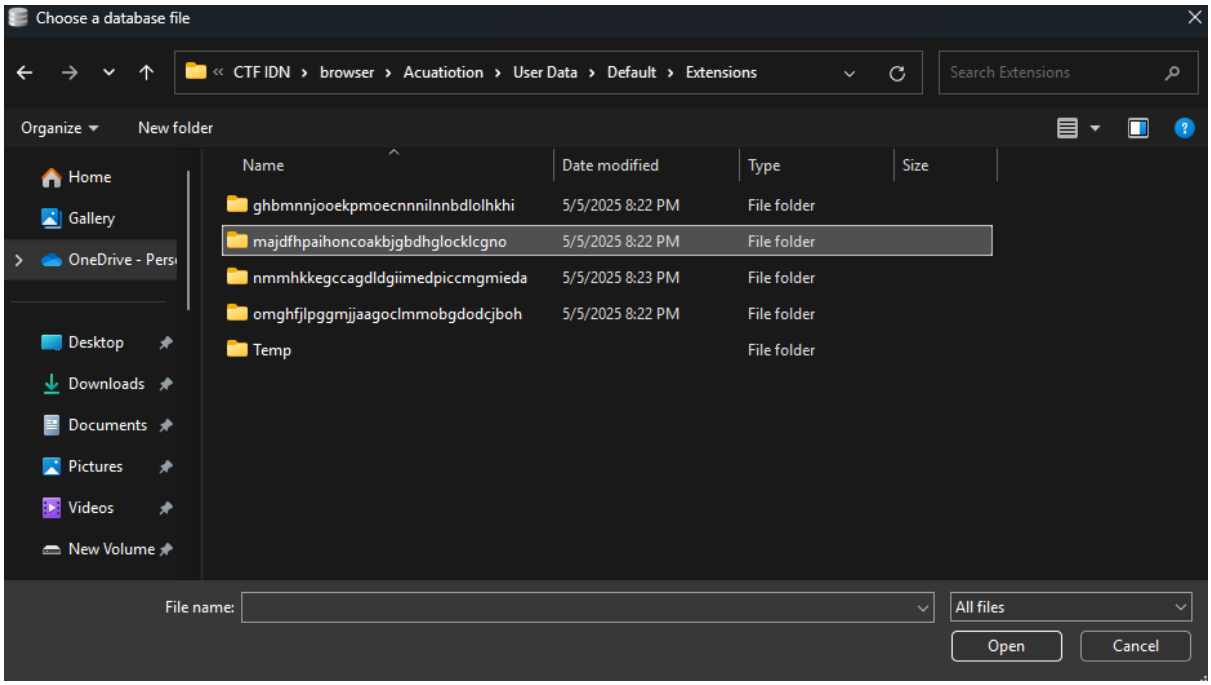
(Filenya ada di pertanyaan pertama)

extension id dengan icon salah satu vpn yang diinstal V.. !

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :
Mencoba ID Extensions yang ada

Flag : IDN_FLAG{majdfhpaihoncoakbjgbdhglocklcgno}

Browser Forensic 10

Deskripsi :

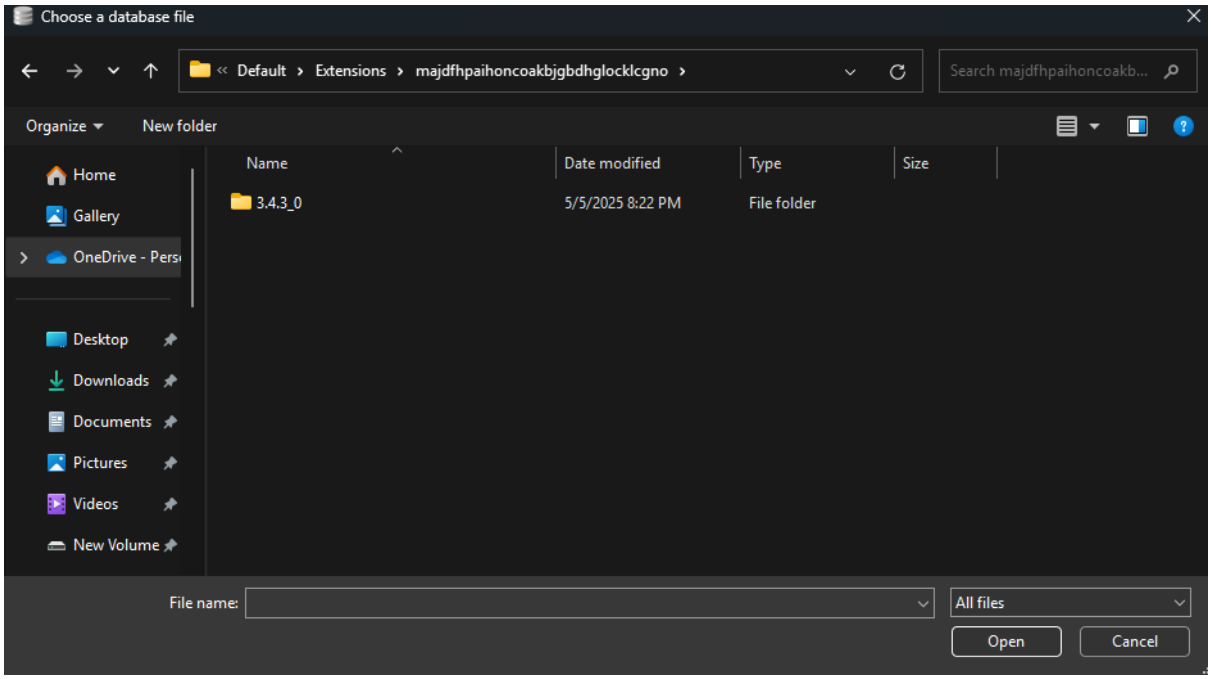
Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !! (Filenya ada di pertanyaan pertama)

Version vpn V.. yang diinstal oleh user ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :
Memasukan versi ekstensi yang sebelumnya

Flag : IDN_FLAG{3.4.3_0}

Usb Forensic

Cyptography

jadi gini lgi...

Deskripsi:
mau coba-coba aja terus, coba maen dino

Author: Aditya Firman Nugroho

Lampiran: jhlzhy.zip
Tools: Stegseek

```
┌──(kali㉿kali)-[~/Downloads]
└─$ stegseek jhlzhy.jpg /usr/share/wordlists/rockyou.txt
```

Ouputnya :

```
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "jhlzhy"
[i] Original filename: "flag.txt".
[i] Extracting to "jhlzhy.jpg.out".
```

Setelah menemukan passphrase, file diekstrak lagi menggunakan `steghide`

```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf jhlzhy.jpg
```

Masukkan passphrase yang sudah ditemukan, lalu dapat file `flag.txt`.

Isi file `flag.txt`:

PKU_JAM{ZalNhU0_Jv0sly}

Flag hasil ekstraksi ini ternyata masih dalam bentuk encode menggunakan cipher tertentu, dan setelah didekode, flag akhirnya adalah:

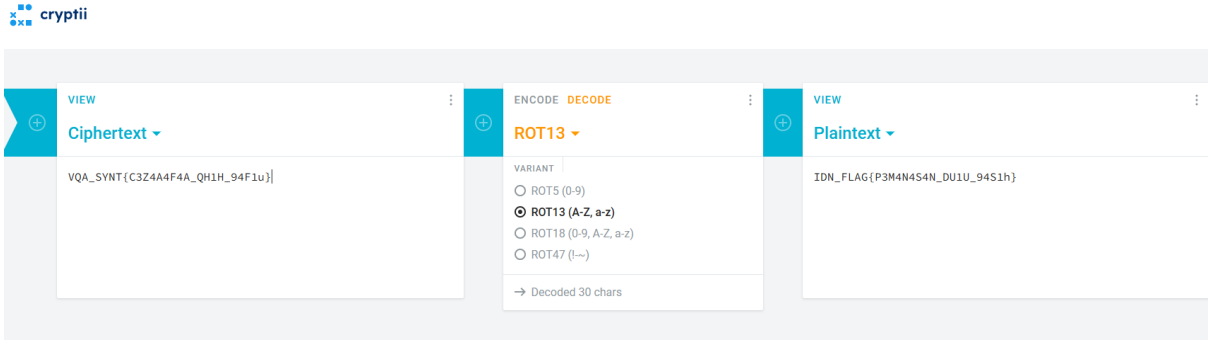
IDN_CTF{SteGaN0_Co0ler}

Rot1Aoka

Deskripsi :

Clue nya udah jelas kan? VQA_SYNT{C3Z4A4F4A_QH1H_94F1u} Author : Mohamad Fattyr

Lampiran :



Solusi :

“ Terlihat dari Deskripsi bahwa ini adalah pesan encoding, dan dia lupa sampai berapa dia encoding.. terlihat bahwa yang dia gunakan juga base64 dengan ciri “==”, maka dari itu saya mencoba untuk melakukan decoding beberapa kali”

Flag : IDN_FLAG{P3M4N4S4N_DU1U_94S1h}

Might Guy’s Secret

Deskripsi :

Suatu hari, Might Guy mengirimkan sebuah pesan rahasia ke Konoha HQ. Namun, pesan tersebut dicegat di tengah jalan.

Ini isi pesannya: QGA_OTS{v067j1723qk40f5v33z656afwse60kdf67u9606}

Bersama dengan pesan itu, kamu menemukan secarik kertas bertuliskan: "Giovan Battista Bellaso: 1553M: idnmantab"

Tampaknya Might Guy menggunakan teknik enkripsi klasik namun ampuh

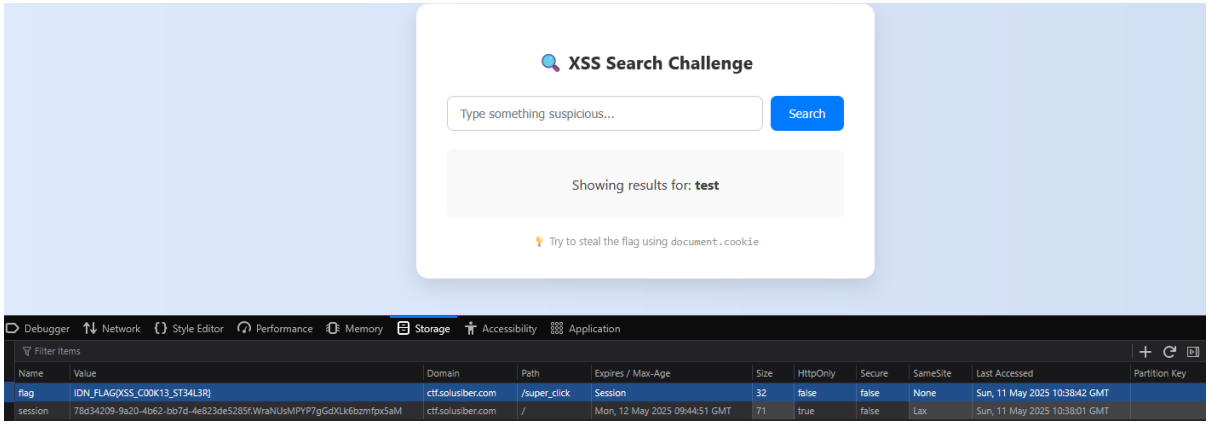
Authtor: Nur Cholis Majid

Lampiran :

Solusi :
Vigenere Cipher dari GPT

Flag : IDN_CTF{c067j1723pc40c5i33n656asdsd60cas67i9606}

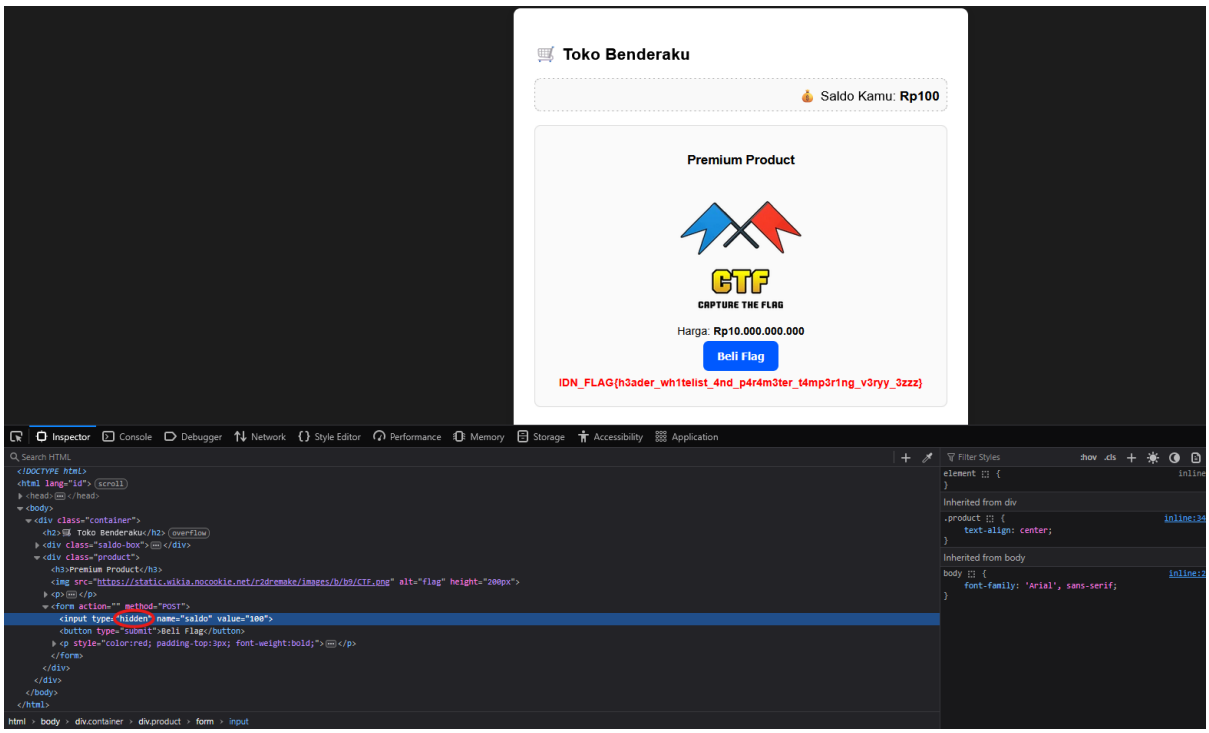
XSS



Solusi :
Input kata apa saja, lalu cek flag di Cookies melalui Inspect yang terdapat flag langsung.

Flag : IDN_FLAG{XSS_C00K13_ST34L3R}

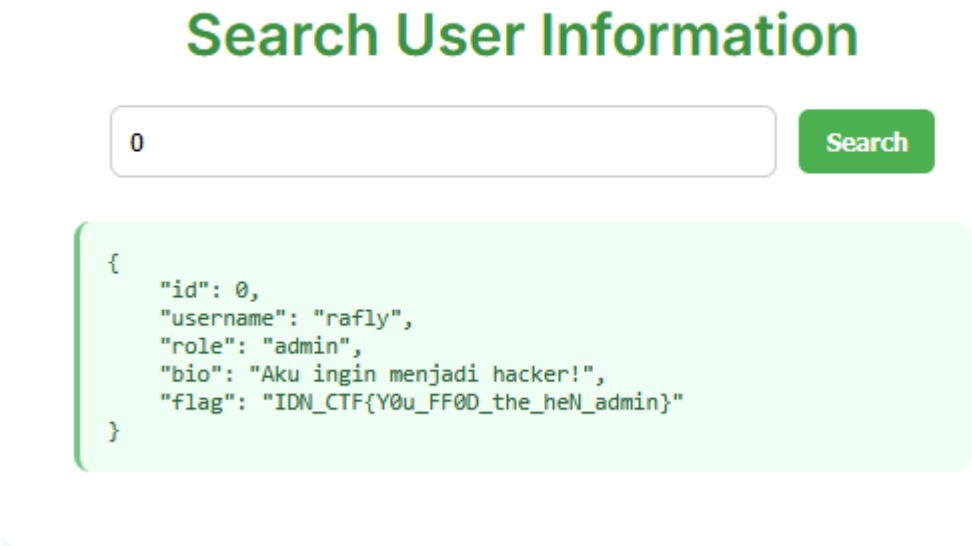
Hidden Buy Flag



Solusi:
Inspect di bagian type=”hidden”, lalu menggantikannya dengan “show”. Maka, flag akan muncul.

Flag: IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3r1ng_v3ryy_3zzz}

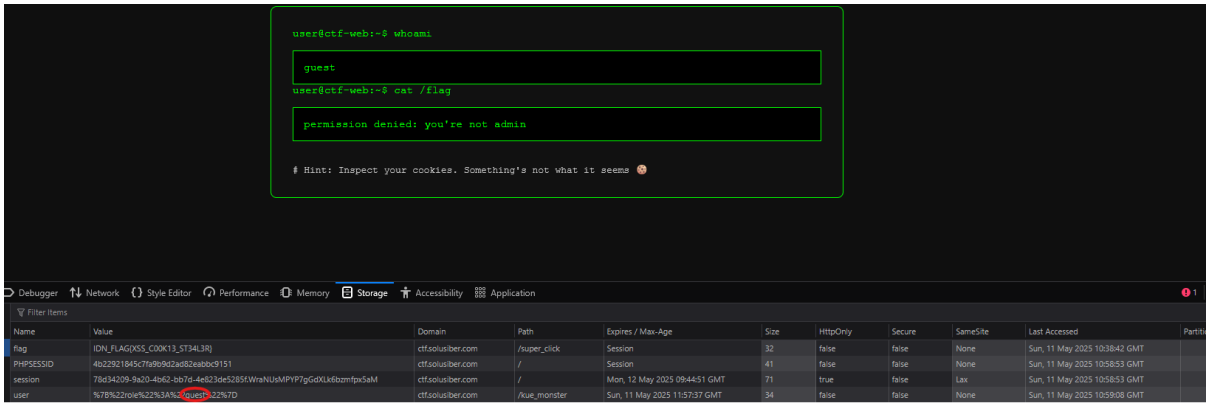
I’m Not Me, You Are Me

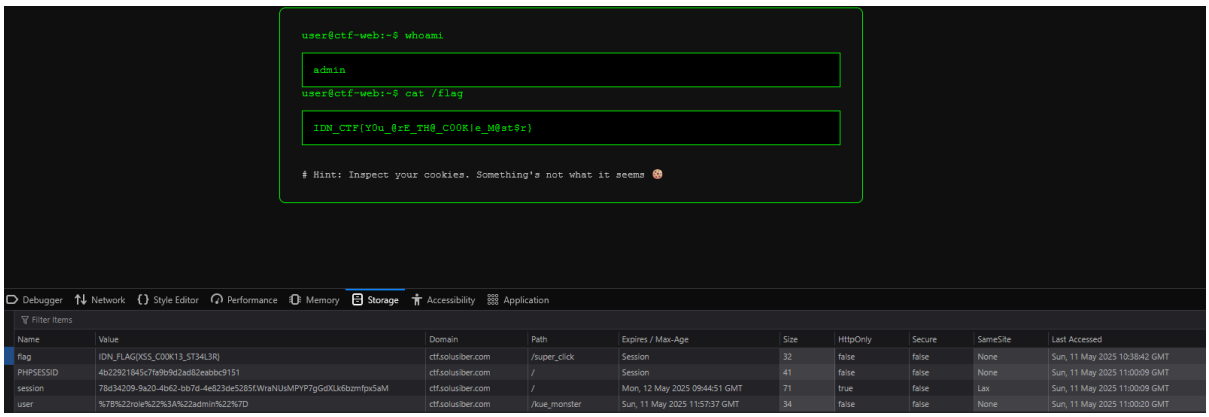


Solusi:
Dikarenakan id tidak dapat ditemukan dalam bentuk String, maka saya coba menggunakan angka dimulai dari 1 hingga 5, lalu diinput dengan 0.

Flag: IDN_CTF{Y0u_FF0D_the_heN_admin}

Kue Monster

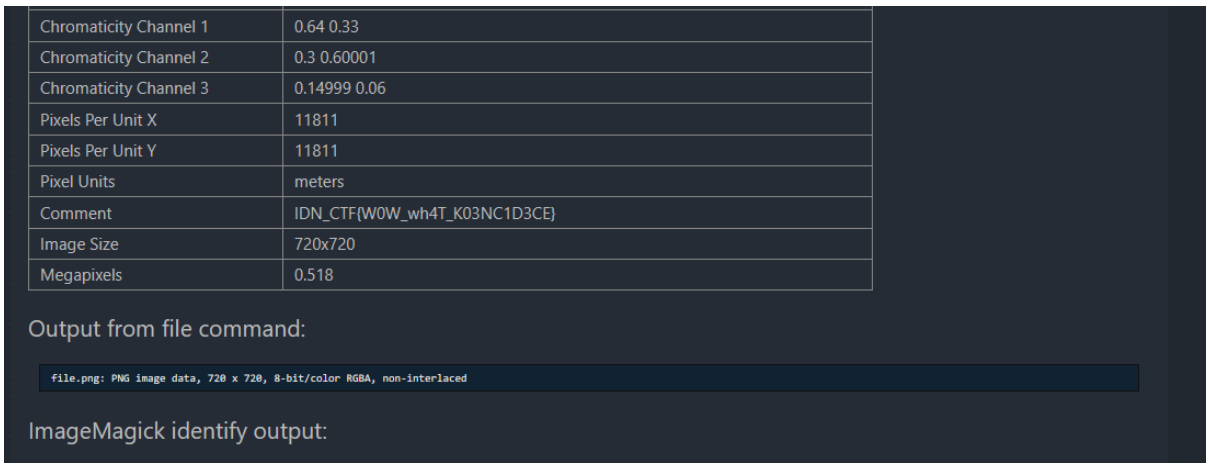




Solusi:
Memeriksa melalui Inspect pada tab Cookies, lalu di tabel “user” terdapat nilai %7B%22role%22%3A%22**guest**%22%7D, diganti dengan %7B%22role%22%3A%22**admin**%22%7D, lalu refresh ulang halaman tersebut.

Flag: IDN_CTF{Y0u_@rE_TH@_C00K|e_M@st$r}

jadi gini...



Solusi:
Data pada gambar material.png diekstrak menggunakan EXIF dan flag bisa ditemukan di bagian Comment.

Flag: IDN_CTF{W0W_wh4T_K03NC1D3CE}

Simple Substitution Cipher

ORF_EZY{ziol_ol_g_yqsx_wxz_lg_tq_ln}

Solusi:

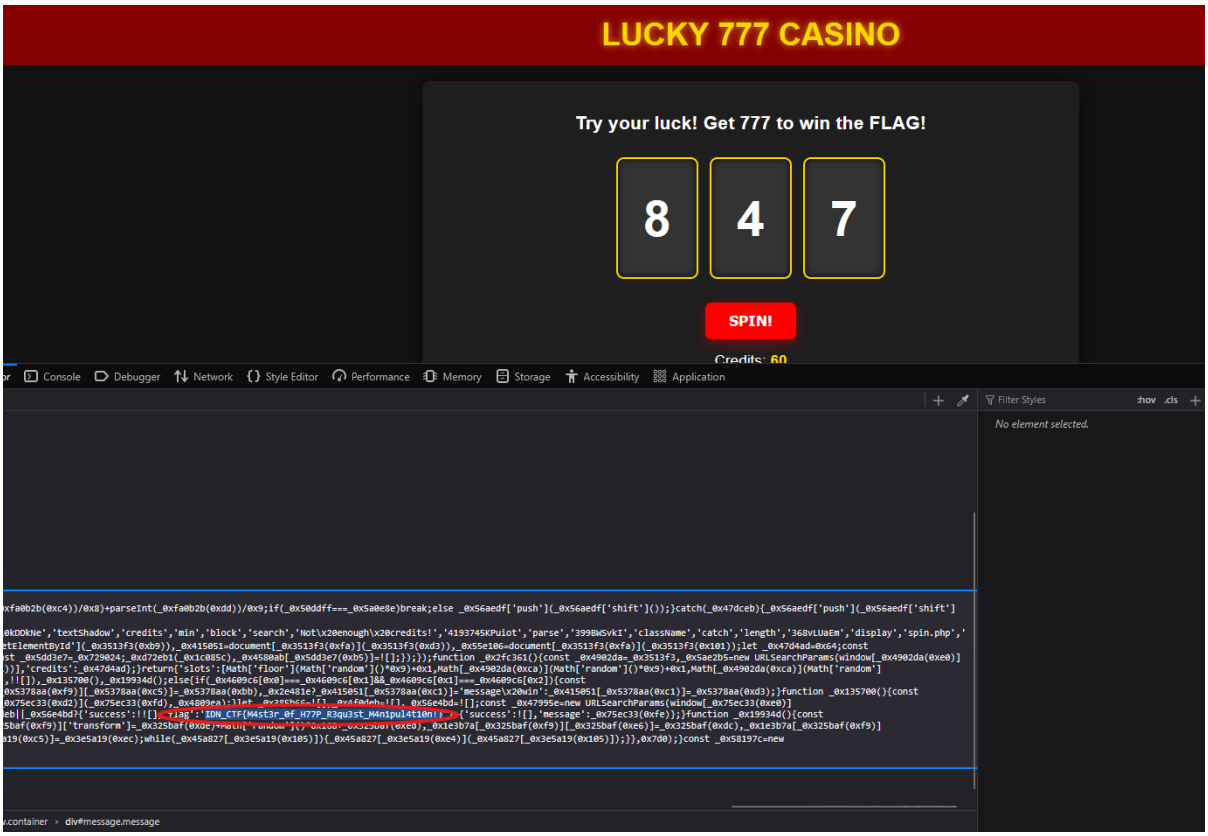
```
mathematica                                                    Copy  Edit

Plain : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
```

Mengganti soal tersebut mengikuti sesuai urutan cipher ke plain di setiap huruf.

Flag: IDN_CTF{this_is_falu_but_so_ea_sy}

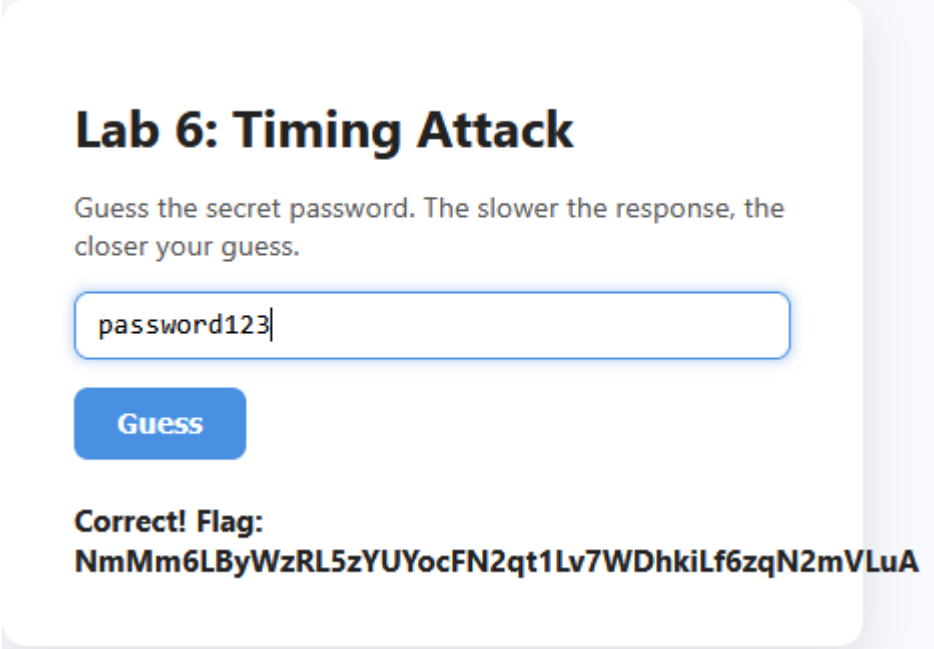
Casino 777



Solusi:
Setelah memanipulasi nilai menjadi angkat di setiap slot, tetap sama saja gagal. Maka saya mencari flagnya langsung di Inspect dan menemukan script flag.

Flag: IDN_CTF{M4st3r_0f_H77P_R3qu3st_M4n1pul4t10n!}

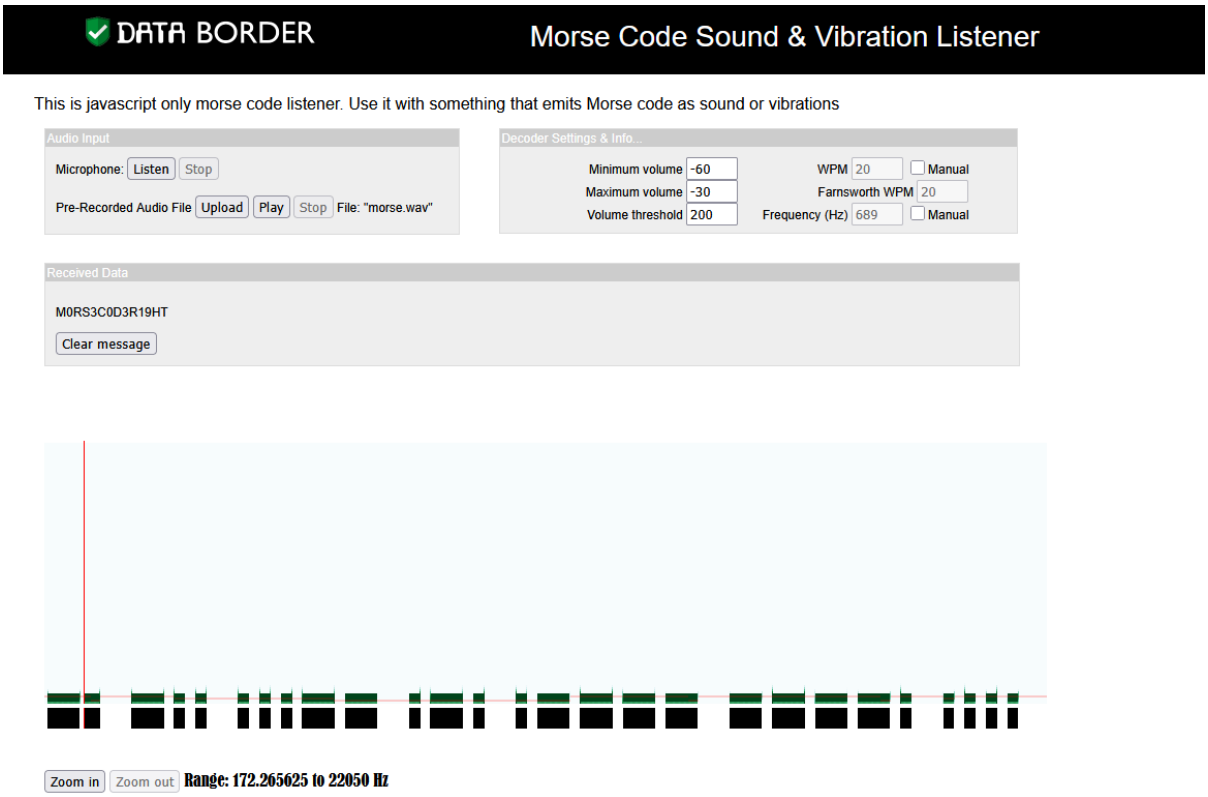
Timing Attack



Solusi:
Mencoba bentuk password yang paling umun digunakan, mengikuti lamanya waktu proses. Semakin lama waktu, maka semakin dekat kita menemukan hasil password yang sesuai.

Flag: IDN_FLAG{NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA}

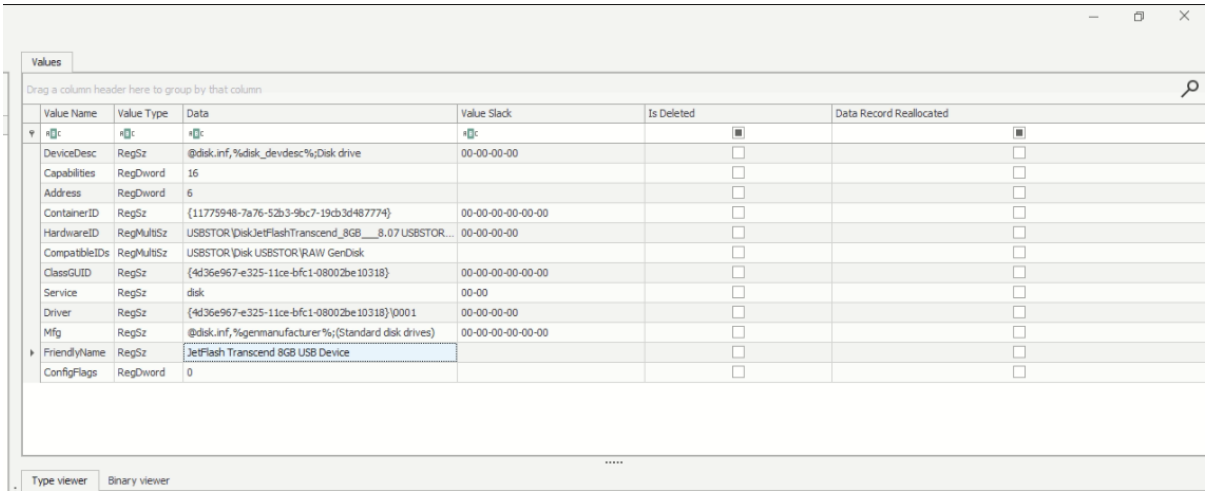
Pramuka



Solusi:
Mengunduh file morse.wav dan upload file tersebut ke website https://databorder.com/transfer/morse-sound-receiver/ . Setelah itu, maka isi flag akan muncul.

Flag: IDN_CTF{M0RS3_C0D3_R19HT}

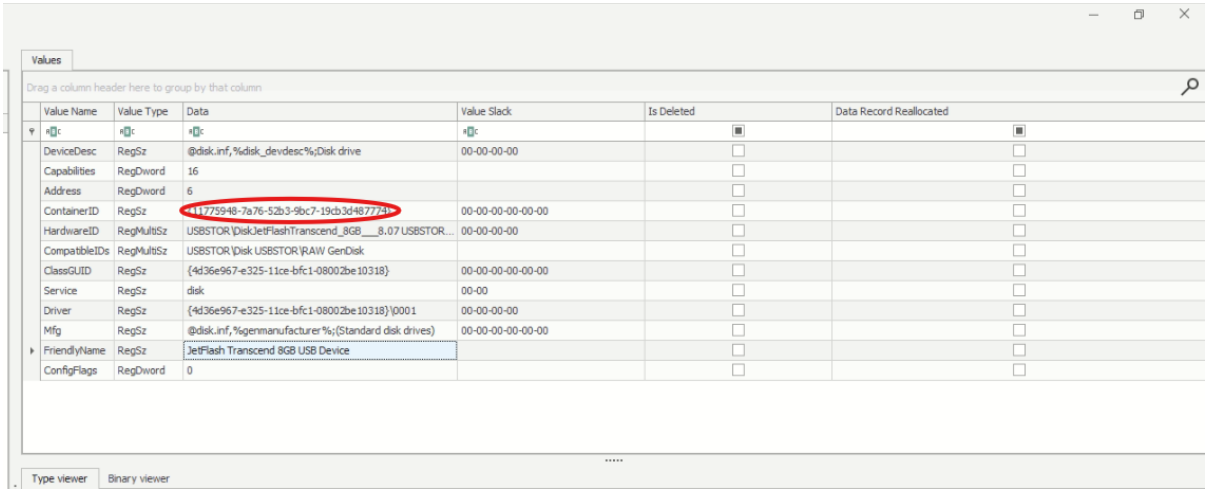
USB Forensic 2



Solusi:
Menggunakan tool Registry Explorer untuk ektrak data file HIV dan load file USBSTOR.hiv, lalu di bagian direktori XRVZQBFR&0, terdapat di tabel Value Name yang memiliki data sesuai.

Flag: IDN_FLAG{4d36e967-e325-11ce-bfc1-08002be10318}

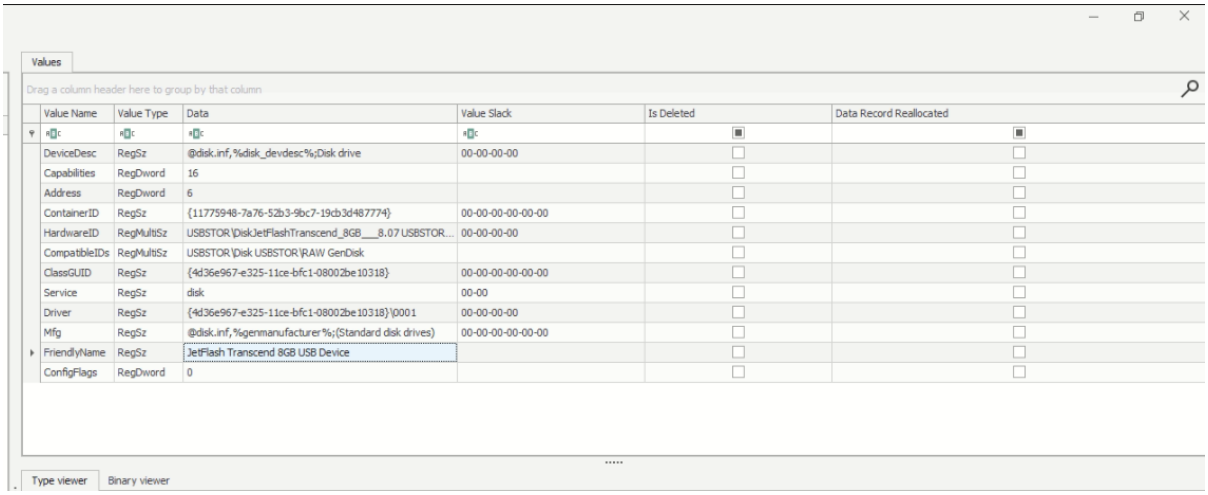
USB Forensic 3



Solusi:
Masih menggunakan tabel dari direktori XRVZQBFR&0, identitas kontainer dapat ditemukan.

Flag: IDN_FLAG{11775948-7a76-52b3-9bc7-19cb3d487774}

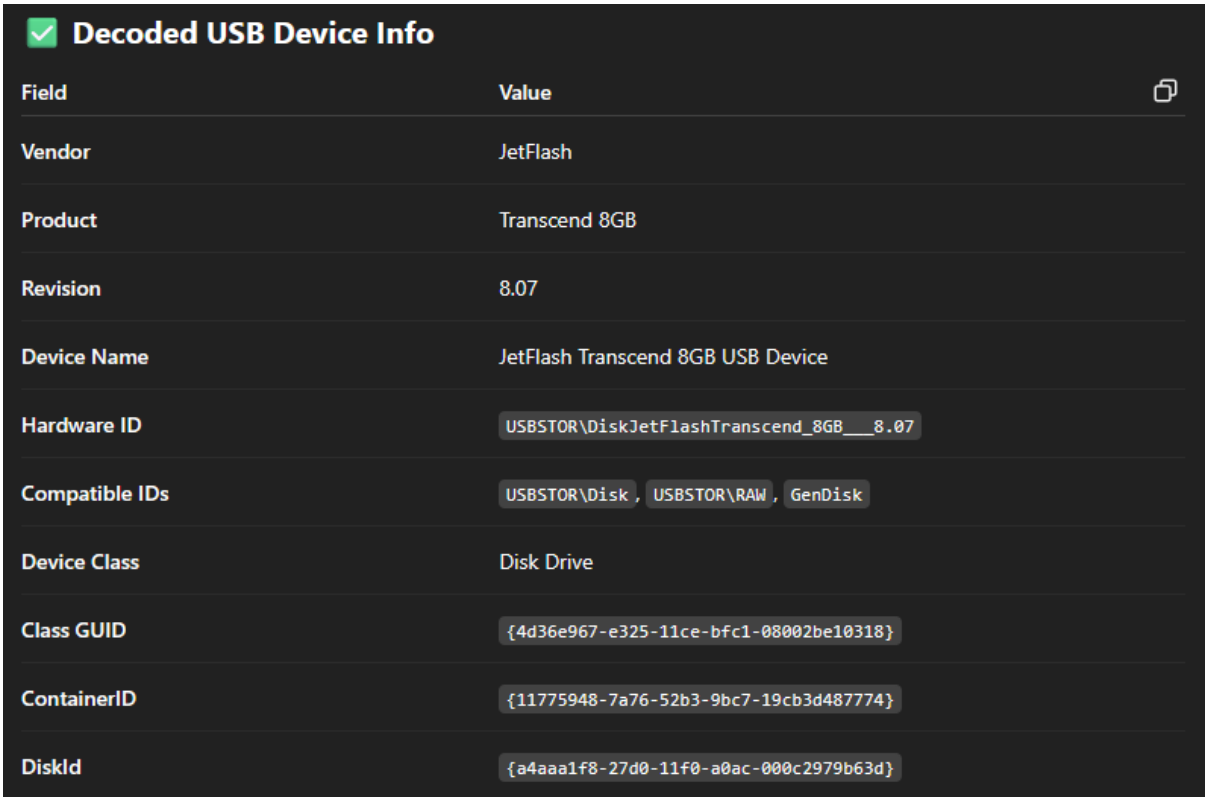
USB Forensic 1



Solusi:
Masih menggunakan tabel dari direktori XRVZQBFR&0, nama device dapat ditemukan di bagian value Friendly Name.

Flag: IDN_FLAG{JetFlash_Transcend_8GB_USB_Device}

USB Forensic 4



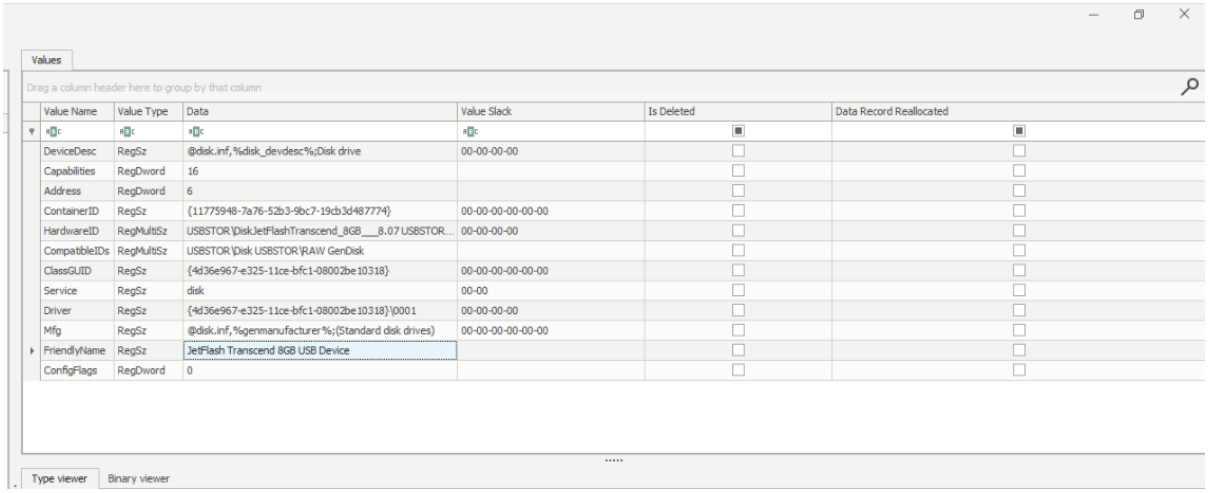
Decoded USB Device Info

Field	Value
Vendor	JetFlash
Product	Transcend 8GB
Revision	8.07
Device Name	JetFlash Transcend 8GB USB Device
Hardware ID	`USBSTOR\DiskJetFlashTranscend_8GB___8.07`
Compatible IDs	`USBSTOR\Disk` , `USBSTOR\RAW` , `GenDisk`
Device Class	Disk Drive
Class GUID	`{4d36e967-e325-11ce-bfc1-08002be10318}`
ContainerID	`{11775948-7a76-52b3-9bc7-19cb3d487774}`
DiskId	`{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}`

Solusi:
Mengkopi isi hex code dari USBTOR.hiv dan prompt di ChatGPT.

Flag: IDN_FLAG{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}

USB Forensic 5



Solusi:
Masih menggunakan tabel dari direktori XRVZQBFR&0, tetapi ini sudah menunjukkan ID serial.

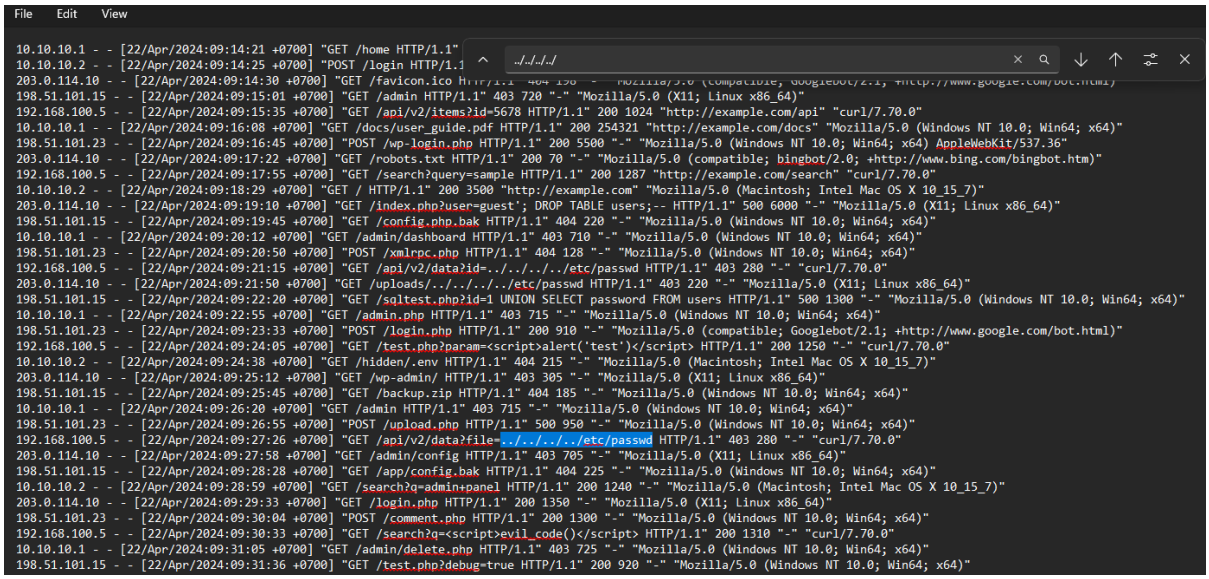
Flag: IDN_FLAG{XRVZQBFR&0}

USB Forensic 6

Solusi:
Menggunakan file NTUSER.dat lalu mengekstrakkan datanya menggunakan ChatGPT. Sehingga hasilnya adalah sebagai berikut.

Flag: IDN_FLAG{4fu284428u5984-8308848.txt}

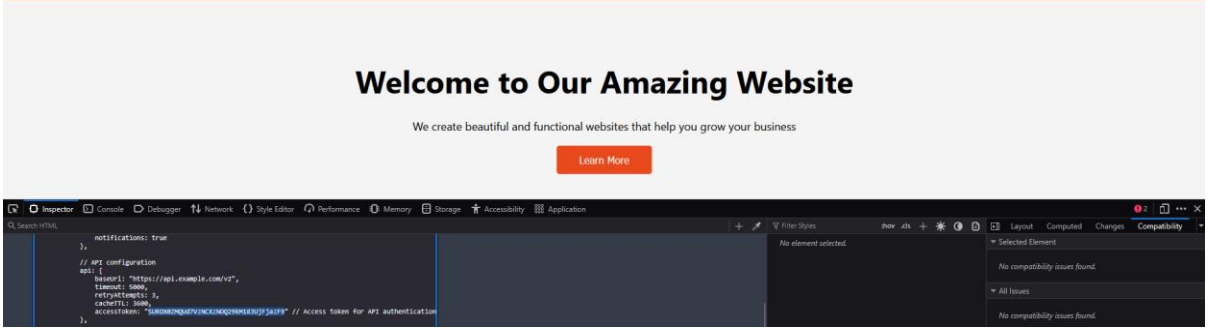
Log Analysis 7



Solusi:
Unduh file log2.txt dan cari serangan path traversal pada log dan mencari salah satu parameter lengkap yang memenuhi kriteria dalam permintaan ke endpoint API.

Flag: IDN_CTF{../../../../etc/passwd}

Awesome Website



Solusi:
Mengakses website “Awesome Website” dan flag dapat ditemukan pada script token API.

Flag: IDN_FLAG{SUROX0ZMQUd7VzNCXzNOQ29kM183UjFjazF9}