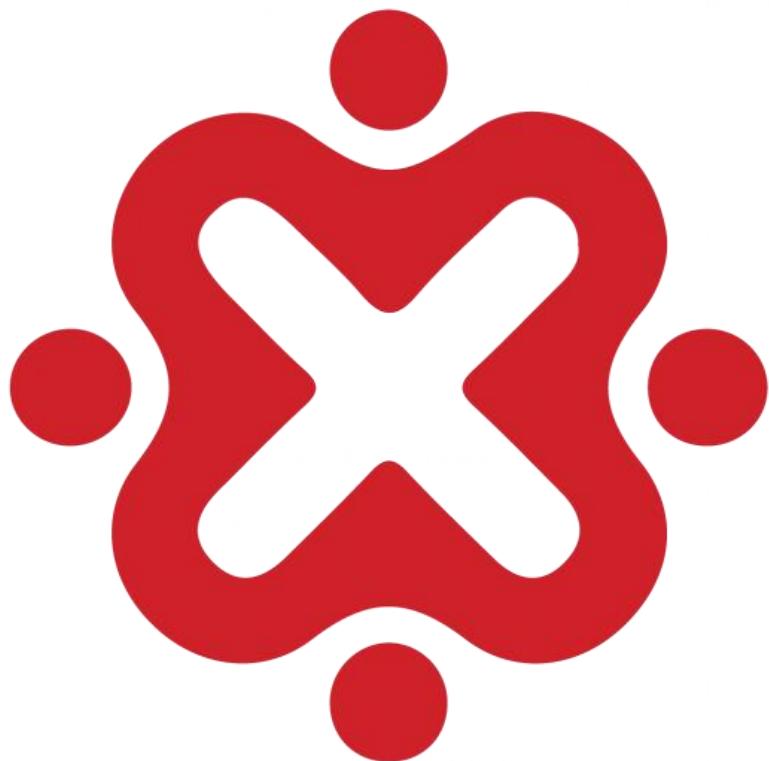




ZeroDay

(Celah yang belum terdeteksi)



ID-Networkers
Indonesian IT Expert Factory



Introduction Team	5
Detail Challenge Solved	7
Welcome Flag	7
Forgot Encode	7
Forensic	9
jadi gini...	9
QRIS	10
Web 303	11
DOM-Based XSS	11
Unsafe eval()	12
Prototype Pollution Demo	13
JWT Token Manipulation	14
Client-side Privilage Escalation	15
Timing Attack	16
Unsafe Deserialization	17
Web Exploit	18
Hidden Buy Flag	18
Konoha Breach	19
ID-Networkers	21
Support Force	22
Kue Monster	23
IDN Education	24
Beyond Way	26
Circle Clicker	27
Awesome Website	29
Casino 777	31
Other	32
User Guide	32
Web Exploit	33
I'm Not Me, You Are Me	33
XSS	34
Code Analysis	35
Log Analysis	36
Log Analysis 1	36
Log Analysis 2	37
Log Analysis 3	38
Log Analysis 4	39
Log Analysis 5	40
Log Analysis 6	41
Log Analysis 7	42



Log Analysis 8	43
Log Analysis 9	44
Browser Forensic	45
Browser Forensic 1	45
Browser Forensic 2	46
Browser Forensic 3	47
Browser Forensic 3	48
Browser Forensic 5	49
Browser Forensic 6	50
Browser Forensic 7	51
Browser Forensic 8	52
Browser Forensic 9	53
Browser Forensic 10	54
USB Forensic	55
USB Forensic 1	55
USB Forensic 2	56
USB Forensic 3	57
USB Forensic 4	58
USB Forensic 5	59
USB Forensic 6	60
Cryptography	78
jadi gini lgi...	78
Might Guy's Secret	79
Rot1Aoka	80
Pramuka	81
Simple Substitution Cipher	82
Classic Substitution	83



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:

```
Vm0wd2VHUXhUWGhYV0d4VIYwZG9iMVJRU2pSVIZsbDNWMnQwYUZKc2NGW1  
ZWM1IzWVRBeFdHVkVSbHBoTVZwUVZrUkdXbVF5U2tWWGJHUnBWa1phTmxav  
VNqUlRNRFZ6VjI1V1ZXSlZXbFZWYWs1dlVsWmtjbFp0Um10TIYxSllWbTAxVTJGR  
1NsbfJiRkpWVm0xb1ExUldXbXRXTvdsMFpFWmtUbUpGY0ZsWFZFSlhWVEZSZU  
ZOWWJGWmlSa3BoV1d0a2IyUnNiSEZTYlhSc1ZqQTFTbFl5TVVkvWJGcFZWbXhvV  
jJKSFVqWIViRnByVm1zeFzsZHJPVmRpU0VKWVYxZDRVMVp0VVhoaVJtUllZbX  
MxV1ZadGVFdE5SbkJXVmxFV2FGSXdjRWRaTUDoVFYwWmFjMk5JUmxWV2JIQX  
pxWHBLUzFJeVJrZFdiV2hvVFVoQ01sWnRNREZrTWsxM1RWWmtZVkpXV2xWW1  
ZFNVRWREZhY1ZKcmRGUINiRVl6Vmxkek5WZEEdXbFZSYWxKV1RXcFdjbFl5TVV  
0VFJsWnpZVWRHVjJWcldtOVdiR1EwVVRGYVZrMVZWazVTUkVFNQ==
```

Author: Rafly Permana

Lampiran :



BASE64

[Decode](#)

[Decode and Encode](#) [Encode](#)

Language: English Español

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format

Simply enter your data then push the decode button.

```
V2VsY29tZSB0byB5b3VylG5ldyBtZXRhIGZyaWVuZC4gRmxhZzogSUROX0NURntiYXNINjRfaW5fYWNoaW9uX2J1dF83X3RpWVzfQ==
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set: UTF-8

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

Welcome to your new meta friend. Flag: IDN_CTF{base64_in_action_but_7_times}

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

Copyright © 2025, All rights reserved



Kami decode menggunakan base64

```
[kali㉿kali)-[~/Downloads]
$ echo U1VST1gwWk1RVWQ3VmmpOU04xOWx0Rk0zWDFJaE9VaFVmUT09 | 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

Lab 8: Unsafe Deserialization

Paste serialized data to load user preferences (JSON):

Paste JSON here...

Load Data

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

```
function _0x50ef(){const _0x3adffbe[ 'output' , '4398tkUrEg' , 'textContent' , '2440668hwBdtZ' , '158824hAaAk0' , 'aData\20loaded:\x20' , 'userData' , 'message' , 'light' , 'stringify' , '615YI51QW' , '12zD0BPL1' , '301161QjDGea' , '3069225FmJmV' , '3522250vUXIW' , '4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk' , 'run' , 'getElementById' , '2388065o08hBh' , '217RHjACM' ];_0x50ef=function(){return _0x3adffbe[ 'run' ]};const _0x50ef=_0x3adffbe[ 'run' ];function _0x3fb6(_0x197a89 , _0x249e49){const _0x50ef3a=_0x50ef();return _0x3fb6=function(_0x3fb623 , _0x3cca71){_0x3fb623=_0x3fb623-\0xfb;let _0x25a3b3=_0x50ef3a[_0x3fb623];return _0x25a3b3},_0x3fb6(_0x197a89 , _0x249e49)};function _0x40e67a(_0x3c571e){const _0x7797db8=_0x3fb6 , _0x1c995d=_0x40e67a();while(![]){try{const _0x19e65b=_0x19e65b+parseInt(_0x7797db8(0x101))/0x2*(parseInt(_0x7797db8(0x10a))/0x3)+parseInt(_0x7797db8(0x103))/0x4+parseInt(_0x7797db8(0x10e))/0x5+(-parseInt(_0x7797db8(0x10f))/0x7*(-parseInt(_0x7797db8(0x104))/0x8)+-parseInt(_0x7797db8(0x10d))/0x9+parseInt(_0x7797db8(0x10e))/0xa;if(_0x19e65b==_0x3c571e)break;else _0x1c995d['push'](_0x1c995d['shift']);}catch(_0x5899eb){_0x1c995d['push'](_0x1c995d[_0x3cc9f9]);const FLAG=_0x58a49e(0xfb);function unsafeDeserialize(_0x3cc9f9){const _0x4086b2=_0x58a49e;let _0x20cf4a=JSON['parse'](_0x3cc9f9);return _0x20cf4a&&typeof _0x20cf4a[_0x4086b2(0xfc)]==='string'&&eval(_0x20cf4a[_0x4086b2(0xfc)]),_0x20cf4a;let userPrefs={'theme':_0x58a49e(0x108),'language': 'en'};function loadData(){const _0x5cee44=_0x58a49e,_0x5c19a0=document[_0x5cee44(0xfd)](_0x5cee44(0x100)),_0x50da0d=document[_0x5cee44(0xfd)](_0x5cee44(0x106))['value'];try{let _0xe9de80=unsafeDeserialize(_0x50da0d);_0x5c19a0[_0x5cee44(0x102)]=_0x5cee44(0x105)+JSON[_0x5cee44(0x109)];_0xe9de80;catch(_0x216ea5){_0x5c19a0[_0x5cee44(0x102)]= Error:\x20+_0x216ea5[_0x5cee44(0x107)];}}}}}};
```

Pada bagian javascript saya menemukan code acak mencurigakan yaitu:

```
3522250vUXIW' , '4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk' , 'run' ,  
4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk
```

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

```
[kali㉿ kali) ~]# python3 -c "import base58; print(base58.b58decode('4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk').decode())"
```

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



Lab 4: JWT Token Manipulation

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

Paste JWT token here...

Decode Token

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’

```
function _0x5314(_0x1d66ca,_0x46b201){const _0x380dab=_0x380d();return _0x5314=function(..._0x5314a=_0x5314a-0x11b;let _0x428c63=_0x380dab[_0x5314a];return _0x428c63);,_0x5314(_0x1d66ca,_0x46b201);}(function(_0x398988,_0x2b8f80){const _0x34bac7=_0x5314,_0x541a8f=_0x398988() ;while(![]){try{const _0xd27f1f=parseInt(_0x34bac7(0x122))/0x1+parseInt(_0x34bac7(0x121))/0x2*(parseInt(_0x34bac7(0x129))/0x3)+parseInt(_0x34bac7(0x11d))/0x4+parseInt(_0x34bac7(0x127))/0x5*(parseInt(_0x34bac7(0x124))/0x6)+parseInt(_0x34bac7(0x12f))/0x7*(parseInt(_0x34bac7(0x11e))/0x8)+parseInt(_0x34bac7(0x127))/0x9*(parseInt(_0x34bac7(0x12d))/0xa)+parseInt(_0x34bac7(0x125))/0xb;if(_0xd27f1f===_0x2b8f80)break;else _0x541a8f['push'](_0x541a8f['shift']);}catch(_0x36655c){_0x541a8f['push'](_0x541a8f['shift']);}})}(_0x380d,_0xca009);const FLAG='FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY';function _0x380d(){const _0x1808c=['8035280MmQsQD','Invalid\x203WT','jihwaza','output','2VRCFLA','5yNKKV','getElementById','470644QWNUc','1696561etXjY','\x2cn\x5cnUser\x20access\x20only','parse','371538eQfXe','stringify','7110078NUeqCQ','78345525FlzFK','\x2cn\x5cnPayload\x2cn','18CFZZc0','textContent','2324598QVplFd','\x5cn\x5cnAdmin\x20access\x20granted!\x20flag:\x20','Invalid\x20token\x20Format','jwtToken'],_0x380d=function(){return _0x1808c};return _0x380d();}function parseJwt(_0x327c3a){const _0xd1485=_0x5314;try{const _0x546c4a=_0x327c3a['split'][0];if(_0x546c4a[_0x1d1485(0x120)]!=0x3)throw new Error(_0xd1485(0x120));const _0x181a51=JSON[_0xd1485(0x121)](atob(_0x546c4a[0x0])),_0xe4e403a=JSON['parse'](atob(_0x546c4a[0x1]));return{'header':_0x181a51,'payload':_0x4e403a};}catch(_0x58159a){throw new Error('0xd1485(0x12e)');}}function decodeToken(){const _0x54431c=_0x5314,_0xec70a=document[_0x54431c(0x11c)](_0x54431c(0x130)),_0x10ecc5=document[_0x54431c(0x11c)](_0x54431c(0x12c))['value']['trim'];try{const _header:_0x5a154f,_payload:_0x8ad96e=parseJwt(_0x10ecc5);let _0x1c0d7f=_header['header'].split'+3SON[_0x54431c(0x123)](_0x54431c(0x123))(_0x54431c(0x126)+3SON[_0x54431c(0x123)])_0x8ad96e,null,0x2);_0x8ad96e['role']=='admin'?_0x1c0d7f=_0x54431c(0x12a)+FLAG:_0x1c0d7f=_0x54431c(0x11f),_0x5ec70a[_0x54431c(0x128)]=_0x1c0d7f;}catch(_0xb0322){_0x5ec70a[_0x54431c(0x128)]=Error:_x20+'_0x2b0322['message']);}}
```

Ditemukan kode obfuscated, namun setelah diperhatikan, terdapat variabel:

```
const FLAG='FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY';
```

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(!_1[]){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(_0x5edbd2){_0x4e904d['push'](_0x4e904d['shift']);}})(_0xccce,0xb1890);const FLAG=_0x323d89(0x86);let appConfig={theme:_0x323d89(0x94),secure:_1[],admin:_1[]};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]);}else _0x8f18ef[_0x4ff426]=_0x51be34[_0x4ff426];}}function _0x47df(_0x206659,_0x26dc78){const _0xccce7d=_0xccce;return _0x47df=function(_0x47df86,_0xd69584){_0x47df86=_0x47df86-0x82;let _0x38ea1f=_0xccce7d[_0x47df86];return _0x38ea1f;},_0x47df(_0x206659,_0x26dc78);function _0xccce(){const _0x5ca91=[{"ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS","message","3EBrghy","6564dbe1Sw","output","38qFssj","Invalid:x2050NVx20or:x20error:\x20","No\x20admin\x20rights\x20detected.",'Config\x20updated:\x20','201Mj0Up','2616849eVvCvL','63QVALqm','value','949448h8giJA','light','admin','1513956VvDeo','480qNMqYS','getElementById','27831936JkNoun','textContent','904365shijsm','28411RqLoaZ','object','Admin\x20privilege\x20escalated!\x20flag\x20'];_0xccce=Function()(return _0x5ca91);return _0xccce();}function updateConfig(){const _0xa00427=_0x323d89,_0x3aac91=document['getElementById'](_0xa00427(_0x8a));try{const _0xfa0a0a1=JSON['parse'](_document._0xa00427(_0x98))['jsonInput'][_0xa00427(_0x92)];merge(appConfig,_0xfa0a0a1);let _0x3c731d=_0xa00427(_0x8d),_0x3aac91[_0xa00427(_0x9a)]=_0x3c731d;}catch(_0x5cdb2){_0x3aac91['textContent']=_0xa00427(_0x8c)+_0x5cdb2[_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

The screenshot shows a web-based challenge interface. At the top, it says 'Lab 2: Unsafe eval()'. Below that, there's a text input field with the placeholder 'Enter some JavaScript code to evaluate:' and 'Enter JS code' inside. Below the input field is a blue 'Run' button. Below the button is a large, empty rectangular area where the results of the code execution would be displayed.

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

```
(function(_0x384b11,_0x47f0a0){const _0x3e68ed=_0x27e6,_0x4f8372=_0x384b11();while(!!![]){try{const _0x5460fa=-parseInt(_0x3e68ed(0x17f))/0x1*(parseInt(_0x3e68ed(0x17d))/0x2)+-parseInt(_0x3e68ed(0x172))/0x3+parseInt(_0x3e68ed(0x181))/0x4+-parseInt(_0x3e68ed(0x178))/0x5+parseInt(_0x3e68ed(0x17c))/0x6*(parseInt(_0x3e68ed(0x182))/0x7)+parseInt(_0x3e68ed(0x17a))/0x8+-parseInt(_0x3e68ed(0x177))/0x9*(-parseInt(_0x3e68ed(0x17e))/0xa);if(_0x5460fa===-_0x47f0a0){break;}else{_0x4f8372['push'](_0x4f8372['shift']());}catch(_0x34f187){_0x4f8372['push'](_0x4f8372['shift']());}}}_0x5d37,_0x8542f));const FLAG='8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc';function runCode(){const _0x9c922c=_0x27e6,_0x3b2dce=document['getElementById'](_0x9c922c(0x173))[_0x9c922c(0x180)],_0x3fd49c=document[_0x9c922c(0x176)]._0x9c922c(0x17b));try{let _0x3bc687=eval(_0x3b2dce);_0x3fd49c[_0x9c922c(0x179)]=_0x9c922c(0x175)+_0x3bc687;}catch(_0x1c7c4e){_0x3fd49c[_0x9c922c(0x179)]=`Error: \x20'+_0x1c7c4e[_0x9c922c(0x174)];}}function _0x27e6(_0xb1b2e9,_0x5a07e4){const _0x5d375b=_0x5d37();return _0x27e6=function(_0x27e64e,_0x304cc6){_0x27e64e=_0x27e64e-0x172;let _0x36499e=_0x5d375b[_0x27e64e];return _0x36499e;},_0x27e6(_0xb1b2e9,_0x5a07e4);}}function _0x5d37(){const _0x54d05f=['244639dPbyev','value','4199984KeIDRc','78191dczIc','320151668rQP1','codeInput','message','Result':\x20+', getElementById,'998CUkHq','2102405ftaDVA','textContent','6096936Nswga','output','1686RdUkwj','2zQBSXH','138310CH5nND'];_0x5d37=function(){return _0x54d05f;};return _0x5d37();}}
```

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 menggunakan python3 lagi

```
[kali㉿kali] -[~/Downloads]
$ python3 -c "import base58; print(base58.b58decode('8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc').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/

Lab 5: Client-Side Privilege Escalation

Check your current role and try to access the protected content.

Current Role: admin

Show Protected Content

Welcome, mighty admin! Here is your confidential flag:

2DvT8boTciwZu4ZctauqBoqJaMKWk8xbK5mAmgPqCTjQ9NX2xGEggGHXFA

Hint: Try to manipulate your role by editing LocalStorage in the browser console.

Encoder Decoder

Base64 Base32 **Base58** URL HTML

IDN_FLAG{client_side_privilege_escalation}

Encode Decode

The tool uses UTF-8 charset.

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/

```
$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:

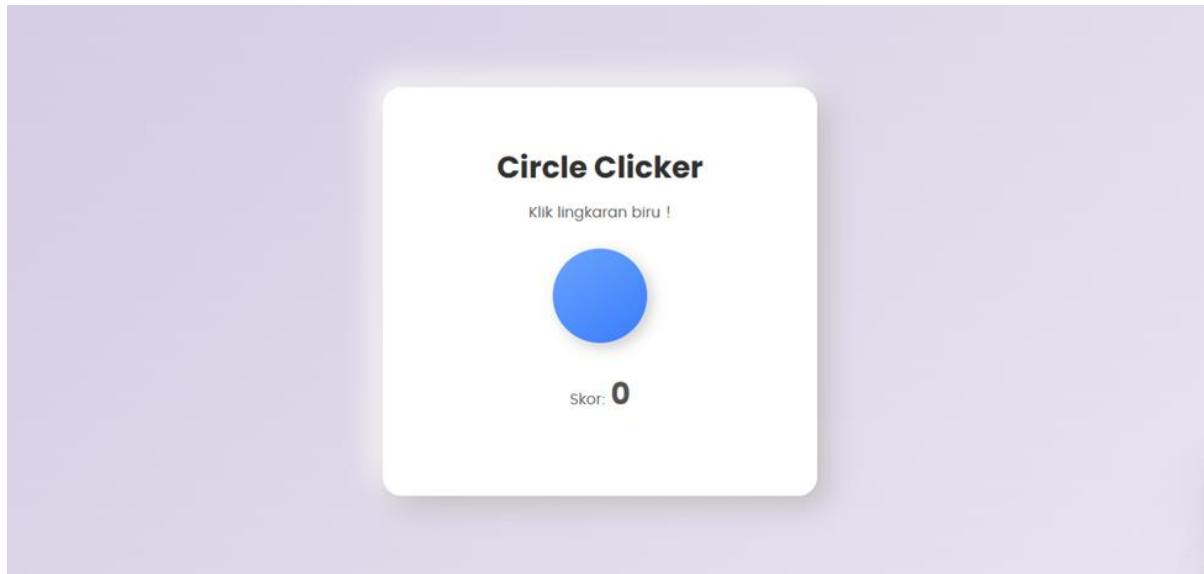
IDN_CTF(d0ub!e_t4njiro_m4ke_u_H4ppy?)

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

Dalam code ini , ada beberapa hal yang menarik ya.



```
const _0x29d5cb=_0x4910;(function(_0x506ef4,_0xac128){const _0x26b33e=_0x4910,_0x35c114=_0x506ef4();while(![]){try{const _0x36e50e=parseInt(_0x26b33e(0x16c))/0x1+parseInt(_0x26b33e(0x171))/0x2+-parseInt(_0x26b33e(0x16b))/0x3)+parseInt(_0x26b33e(0x170))/0x4*(-parseInt(_0x26b33e(0x182))/0x5)+-parseInt(_0x26b33e(0x189))/0x6+-parseInt(_0x26b33e(0x179))/0x7+-parseInt(_0x26b33e(0x18a))/0x8+-parseInt(_0x26b33e(0x17f))/0x9*(-parseInt(_0x26b33e(0x16d))/0xa);if(_0x36e50e==_0xac128)break;else{_0x35c114['push'](_0x35c114['shift']());}}}_0x2650,0xlabbf);function _0x4910(_0x5bf19c,_0xb1b4f1){const _0x26509d=_0x2650;return _0x4910=function(_0x491010,_0x4fec78){_0x491010=_0x491010-0x164;let _0x4cad16=_0x26509d[_0x491010];return _0x4cad16};_0x4910=_0x5bf19c,_0xb1b4f1});function _0x2650(){const _0x4425db=['1258754FpkIMF', 'Petunjuk: \x20coba\x20ketik\x20revealSecret()\x20di\x20console', 'addEventlistener', 'floor', '%Untuk\x20bagian\x20kedua', '\x20coba\x20berfirik\x20sambil\x20bermain\x20click!', 'color:\x20purple;', '35658ZKovph', '%Bagian\x20pertama\x20flag:\x205WJoJxz5CCVWDSE', 'clientWidth', '585yFtq', 'log', 'textContent', 'click', 'Warna\x20berubah!', 'green', 'background', '99648UXPhAp', 'color:\x20green;\x20font-size:\x2014px;', 'translate()', 'color:\x20green;\x20font-size:\x2016px;', 'querySelector', 'color:\x20red;\x20font-size:\x2016px;\x20font-weight:\x20bold;', '%Flag\x20lengkap', '224240MFCRQU', 'color:\x20blue;\x20font-size:\x2014px;', 'fontWeight', '19218AxtNky', '148212VIBNNA', '1380kAmwU', 'game-container', 'style', '598428OnQWfe', '66whiAa', 'Selamat! \x20datang\x20di\x20circle\x20Clicker!\x20game\x20sederhana\x20atau...?', 'clientHeight', 'bold', 'linear-gradient(145deg,\x20gold,\x20orange)', 'target', 'random', 'linear-gradient(145deg,\x20ff7eb9,\x20#ff65a3)';_0x2650=function(){getScore=_0x425d8();let score=0x0,clickCount=0x0,secretUnlocked=![];const target=document[_0x29d5cb(0x167)](_0x29d5cb(0x176)),scoreDisplay=document[_0x29d5cb(0x167)]('score'),messageEl=document[_0x29d5cb(0x167)]('message');target[_0x29d5cb(0x170)](_0x29d5cb(0x185),function(){const _0x123bed=_0x29d5cb;score++,clickCount++,scoreDisplay[_0x123bed(0x184)]=score;const _0x89a8a2=document[_0x123bed(0x186)](_0x1a605e-_0x89a8a2[_0x123bed(0x181)]-0x78,_0x3575a3-_0x89a8a2[_0x123bed(0x173)])-0x96,_0xa7d77c=Math['floor'](Math[_0x123bed(0x177)])-_0x1a685e,_0x298643=Math[_0x123bed(0x17c)](Math[_0x123bed(0x177)])_*_0x3575a3;target[_0x123bed(0x16f)][_0x123bed(0x183)]['transform']=_0x123bed(0x18c)+_0xa7d77c+'px',_0x20'+_0x298643+'px',clickCount==0x5&&!secretUnlocked&&console[_0x123bed(0x183)]('Atau\x20hanya\x20permainan\x20lik\x20biasa?'),clickCount==0x8&&!secretUnlocked&&console[_0x123bed(0x183)](_0x123bed(0x17a)),score==0x1488(target[_0x123bed(0x16f)]-_0x123bed(0x188))=_0x123bed(0x178),messageEl[_0x123bed(0x184)]=_0x123bed(0x186),setTimeout(()=>messageEl[_0x123bed(0x184)]=''),_0xd0));});function revealSecret(){const _0x1a2725=_0x29d5cb;secretUnlocked=![],console[_0x1a2725(0x18d)],console[_0x1a2725(0x181)](_0x1a2725(0x180),_0x1a2725(0x168)),console['log'](_0x1a2725(0x17d),_0x1a2725(0x17e));setInterval(function(){const _0x1faaeef=_0x29d5cb;score=0x3e8&&!secretUnlocked&&console['log']('Luar\x20biasa!\x20Kamu\x20mendapatkan\x20bagian\x20kedua\x20flag:\x20master'),_0x1faaeef(0x18b),console['log'](_0x1faaeef(0x165),_0x1faaeef(0x164)),secretUnlocked!=[],target[_0x1faaeef(0x16f)][_0x1faaeef(0x188)]=_0x1faaeef(0x175),messageEl[_0x1faaeef(0x184)]=_0x1faaeef(0x166),messageEl['style'][_0x1faaeef(0x169)]=_0x1faaeef(0x187),messageEl['style'][_0x1faaeef(0x16a)]=_0x1faaeef(0x174),_0x3e8),console[_0x123bed(0x172)];});}
```

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:

```
revealSecret()
Selamat! Kamu menemukan fungsi rahasia!
Bagan pertama flag: 5WJoJxz5CCVWDSE
untuk bagian kedua, coba berfirik simbol bermain click!
```

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}',_0x1faaeef(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.

```
(kali㉿kali)-[~/Downloads]
$ python3 -c "import base58; print(base58.b58decode('5WJoJxz5CCVWDSEpH4E1n77BT5Fec')).decode()"
```



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 lainnya.

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/

The image shows two screenshots of a web browser. Both screenshots display the URL https://ctf.solusiber.com/robots_dashboard/robots.txt.
Screenshot 1 (Top): The page content is:
`User-agent: *
Disallow: /asdsa024nsfd01372021.html`
Screenshot 2 (Bottom): The page content is:
`User-agent: *
Disallow: /asdsa024nsfd01372021.html`

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

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/

The screenshot shows a two-column interface. On the left, there's a 'Login' form with fields for 'Email' (containing '123'OR'1=1') and 'Password' (containing '*****'), and a blue 'Login' button. On the right, there's a table titled 'Daftar Data PII' (PII Data Register) with columns: Nama Lengkap, Email, No. Telepon, NIK, and Alamat. The table lists 15 entries of shinobi data, such as Naruto Uzumaki, Sasuke Uchiba, Sakura Haruno, Kakashi Hatake, Hinata Hyuga, Shikamaru Nara, Ino Yamanaka, Choji Akimichi, Rock Lee, Tenten, Neji Hyuga, Might Guy, and Tsunade Senju. Below the table, a black bar displays the flag: <!-- IDN_CTF{c0NRats_you_goin_tohe_insideee} -->

Solusi :

SQL Injection

Flag : IDN_CTF{c0NRats_you_goin_tohe_insideee}

Support Force

Deskripsi :

Ini klub eksklusif buat agen rahasia. Brower 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/

The screenshot shows the NetworkMiner interface with 'Network conditions' selected. Under 'User agent', 'Custom...' is chosen, and the value 'hackme' is entered. To the right, a browser window displays a challenge titled 'Access Filtering' with the flag 'IDN_CTF{r7x9_uaSwitch_delta44}' and a hint: 'Hint: Check your browser headers. Something isn't quite right...'. The browser's address bar shows the URL '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/



The screenshot shows a browser window with the URL https://ctf.solusiber.com/idn_edu/?page=../../var/www/html/flag.txt. The page content is mostly obscured by a large black redaction box, but a small white box in the bottom right corner contains the flag: IDN_CTF{l@tisec_r29-loadr}

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

The Wireshark interface shows a packet capture named "incident_response_.pcapng". A green filter bar at the top displays "frame contains \"IDN_CTF\" or frame contains \"IDN_FLAG\"". The main pane lists two captured frames:

No.	Time	Source	Destination	Protocol	Length Info
99255	52.665309	192.168.10.244	192.168.10.153	HTTP	567 HTTP/1.1 200 OK (text/html)
99256	52.665313	192.168.10.244	192.168.10.153	TCP	567 [TCP Retransmission] 80 → 46542

A detailed view of the selected HTTP response (Frame 99255) is shown in the bottom pane. The packet details show the raw HTTP response body:

```
> Frame 99255: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface
> Ethernet II, Src: Intel_8a:b2:72 (28:7f:cf:8a:b2:72), Dst: Intel_8a:b2:72 (28:7f:cf:8a:b2:72)
> Internet Protocol Version 4, Src: 192.168.10.244, Dst: 192.168.10.153
> Transmission Control Protocol, Src Port: 80, Dst Port: 46542, Seq: 1, Ack: 93, Len: 567
> Hypertext Transfer Protocol
-> Line-based text data: text/html (11 lines)
    <!DOCTYPE html>\r\n    <html lang="en">\r\n        <t><head>\r\n            <t><meta charset="UTF-8" />\r\n            <t><meta name="viewport" content="width=device-width, initial-scale=1.0" />\r\n        </t></head>\r\n        <t><body>\r\n            <t><p>IDN_CTF{Re30N3C}</p>\r\n        </t></body>\r\n    </html>\r\n
```

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

No.	Time	Source	Destination	Protocol	Length	Info
71751	48.241681	192.168.10.153	192.168.10.244	HTTP	633	POST / HTTP/1.1
71752	48.241684	192.168.10.153	192.168.10.244	TCP	633	[TCP Retransmiss]

Packet details (selected frame 0100):

Hex	Dec	Text
0100	0d 0a 2d
0110	2d 42 41 7a 35	-----BAz5
0120	64 72 68 48 44 76 33 78 54 4a 55 33 79 47 6f 30	drhHDv3x TJU3yGo0
0130	4b 67 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70	Kg..Cont ent-Disp
0140	6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61	osition: form-da
0150	74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b	ta; name = "file";
0160	20 66 69 6c 65 6e 61 6d 65 3d 22 6d 61 6c 77 61	filename="malwa
0170	72 65 2e 70 79 22 0d 0a 43 6f 6e 74 65 6e 74 2d	re.py" Content-
0180	54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f	Type: ap plicatio
0190	6e 2f 6f 63 74 65 74 2d 73 74 72 65 61 6d 0d 0a	n/octet- stream..
01a0	0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c	..<!DOCT YPE html
01b0	3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a	><html> <head>..
01c0	20 20 20 20 3c 74 69 74 6c 65 3e 4e 6f 74 68 69	<tit le>Nothi
01d0	6e 67 20 74 6f 20 73 65 65 20 68 65 72 65 3c 2f	ng to se e here</
01e0	74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c	title>< /head><
01f0	62 6f 64 79 3e 0a 20 20 20 20 3c 64 69 76 20 73	body>.. <div s
0200	74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 20 6e	tyle="di splay:n
0210	6f 6e 65 3b 22 3e 49 44 4e 5f 43 54 46 7b 4d 34	one;">ID N_CTF{M4
0220	6c 32 57 72 65 5f 53 33 52 65 4d 7d 3c 2f 64 69	l2Wre_S3 ReM}</di
0230	76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d	v></bod y></htm
0240	6c 3e 0a 0d 0a 2d	l>.....
0250	2d 42	-----B
0260	41 7a 35 64 72 68 48 44 76 33 78 54 4a 55 33 79	Az5drhHD v3xTJU3y
0270	47 6f 30 4b 67 2d 2d 0d 0a	Go0Kg--- .

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; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charges HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chart HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charts HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chat HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chats HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /check HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checking HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout_iclear HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
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 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /frand2 HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bash_history HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bashrc HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cache HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.config HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cvs HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cvignore HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.forward HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.git/HEAD HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

```
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.history HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSI; Windows NT 5.1; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36"
```

Solusi :

POST merupakan suatu perintah untuk mengirim file, oleh karena itu mencari keyword POST

Flag : IDN_CTF{malware.py}

Log Analysis 4

Deskripsi :

analisis 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

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
17099	75.042842	192.168.18.230	192.168.18.17	FTP	60	Request: PASV
17101	75.043896	192.168.18.17	192.168.18.230	FTP	105	Response: 227 Entering
17103	75.044211	192.168.18.230	192.168.18.17	FTP	68	Request: STOR malware
17113	75.045625	192.168.18.17	192.168.18.230	FTP	76	Response: 150 Ok to se
17119	75.046935	192.168.18.17	192.168.18.230	FTP	78	Response: 226 Transfer

Solusi :

Melakukan filtering pada protocol dan menemukan request pada file malware

Flag : IDN_CTF{ftp:malware}

Log Analysis 6

Deskripsi :

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

IDN_CTF{jawaban}

Author: Rafly Permana

Lampiran : log1.txt

```
198.51.100.23 - - [21/Apr/2024:08:19:45 +0700] "GET /ring.php?id=1 UNION SELECT password FROM users HTTP/1.1" 500 1234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
```

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

```
2024-04-23T14:05:12Z server1 sshd[1523]: Accepted publickey for alice from 192.168.0.5 port 58922 ssh2: RSA SHA256:AbCdEfGhIjKlMnOpQrStUVwXyZ1234567890
2024-04-23T14:05:15Z server1 sudo: pam_unix(sudo:session): session opened for user root by alice(uid=0)
2024-04-23T14:06:01Z server1 kernel: [12345.67890] audit: type=1400 audit(1682251561.123:45): apparmor="DENIED" operation="open" profile="/usr/bin/curl" name="/etc/shadow" pid=1567 comm="curl" requested_mask="r" denied_mask="r" fsuid=1001 ouid=0
2024-04-23T14:06:03Z server1 curl[1567]: curl: (13) Permission denied reading key from file /etc/shadow
2024-04-23T14:07:12Z server1 sshd[1579]: Failed password for invalid user guest from 203.0.113.77 port 43122 ssh2
2024-04-23T14:07:14Z server1 sshd[1579]: Received disconnect from 203.0.113.77 port 43122:11: Bye Bye [preauth]
2024-04-23T14:07:15Z server1 sshd[1581]: Failed password for root from 203.0.113.77 port 43123 ssh2
2024-04-23T14:07:18Z server1 sshd[1581]: Failed password for root from 203.0.113.77 port 43124 ssh2
2024-04-23T14:07:20Z server1 sshd[1581]: Connection closed by 203.0.113.77 port 43125 [preauth]
```



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 !!

(Filanya 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

	normalized_url	url_for_display
3	https://www.netflix.com/id-en/	netflix.com/id-en/
4	https://www.google.com/search?...	google.com/search?...
5	https://www.fimela.com/relationship...	fimela.com/relationship/re...
6	https://www.muslima.com/en/lp/paid...	muslima.com/en/lp/paid-sea...
7	https://www.muslima.com/en/lp/paid...	muslima.com/en/lp/paid-sea...
8	https://www.muslima.com/en/lp/paid...	muslima.com/en/lp/paid-sea...
9	https://www.muslima.com/en/lp/paid...	muslima.com/en/lp/paid-sea...
10	https://www.muslima.com/en/lp/paid...	muslima.com/en/lp/paid-sea...
11	https://www.muslima.com/en/lp/paid...	muslima.com/en/lp/paid-sea...
12	https://www.cermati.com/artikel/...	cermati.com/artikel/cara-ar...
13	https://www.cnnindonesia.com/gaya-...	cnnindonesia.com/gaya-hidup...
14	https://www.google.com/search?...	google.com/search?...
15	https://chromewebstore.google.com/...	chromewebstore.google.com/...
16	https://www.google.com/search?...	google.com/search?...
17	https://lolbas-project.github.io/	lolbas-project.github.io
18	https://www.google.com/search?...	google.com/search?...

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 !!

(Filennya ada di pertanyaan pertama)

Streaming Website yang ditonton oleh user ?

format flag : IDN_FLAG{Jawaban yang disoal}



Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip

parent_score	url_for_deduping	normalized_u
3	https://netflix.com/	https://www.netflix.com/
4	https://www.google.com/search?...	https://www.google.com
5	https://fimela.com/	https://www.fimela.com
6	https://muslima.com/	https://www.muslima.cc
7	https://muslima.com/	https://www.muslima.cc
8	https://muslima.com/	https://www.muslima.cc
9	https://muslima.com/	https://www.muslima.cc
10	https://muslima.com/	https://www.muslima.cc
11	https://muslima.com/	https://www.muslima.cc
12	https://cermati.com/	https://www.cermati.cc
13	https://cnnindonesia.com/	https://www.cnnindonesia.com/
14	https://www.google.com/search?...	https://www.google.com
15	chromewebstore.google.com/	https://chromewebstore.google.com/
16	https://www.google.com/search?...	https://www.google.com
17	https://lolbas-project.github.io/	https://lolbas-project.github.io/
18	https://www.google.com/search?...	https://www.google.com

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 !!

(Filennya ada di pertanyaan pertama)

Vpn apa saja yang diinstall oleh user ?

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

Auhtor: Aditya Firman Nugroho



Lampiran : browser.zip

	<u>id</u>	url	title
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 !!

(Filanya 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

```
visit time : 13390724280712417
visit duration : 32509459
last visit time : 13390724280712417
duration since last visit : -1000000
```

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

(Filanya 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

□ ↻ < 4 / 4 >

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 Violation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!
(Filanya ada di pertanyaan pertama)

Email yang digunakan pada browser ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : browser.zip

name	value	value_lower	date_created	date_last_used	count
1 identifier	ghxyssforunfun@gmail.com	ghxyssforunfun@gmail.com	1746250363	1746250363	1

Solusi :

Menemukan email pada file Web Data menggunakan SQLite

Flag : IDN_FLAG{ghxyssforunfun@gmail.com}

Browser Forensic 7

Deskripsi :

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

(Filanya 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



	<u>name</u>	<u>value</u>	<u>value_lower</u>	<u>date_created</u>	<u>date_last_used</u>	count
Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	identifier	ghxyssforunfun@gmail.com	ghxyssforunfun@gmail.com	1746250363	1746250363	1

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 !!

(Filennya 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



DB Browser for SQLite - C:\Users\Farrel Aditya\OneDrive\Documents\SMKN 1

	<u>id</u>	<u>url</u>	<u>icon_type</u>
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 !!

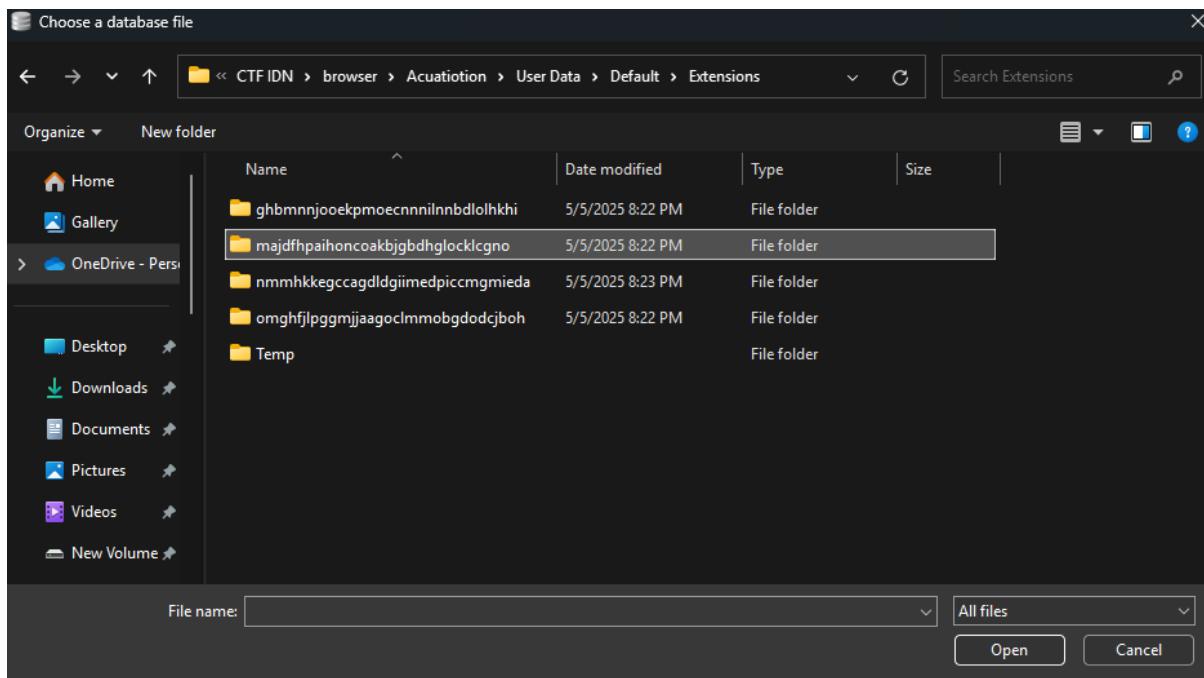
(Filennya ada di pertanyaan pertama)

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 :

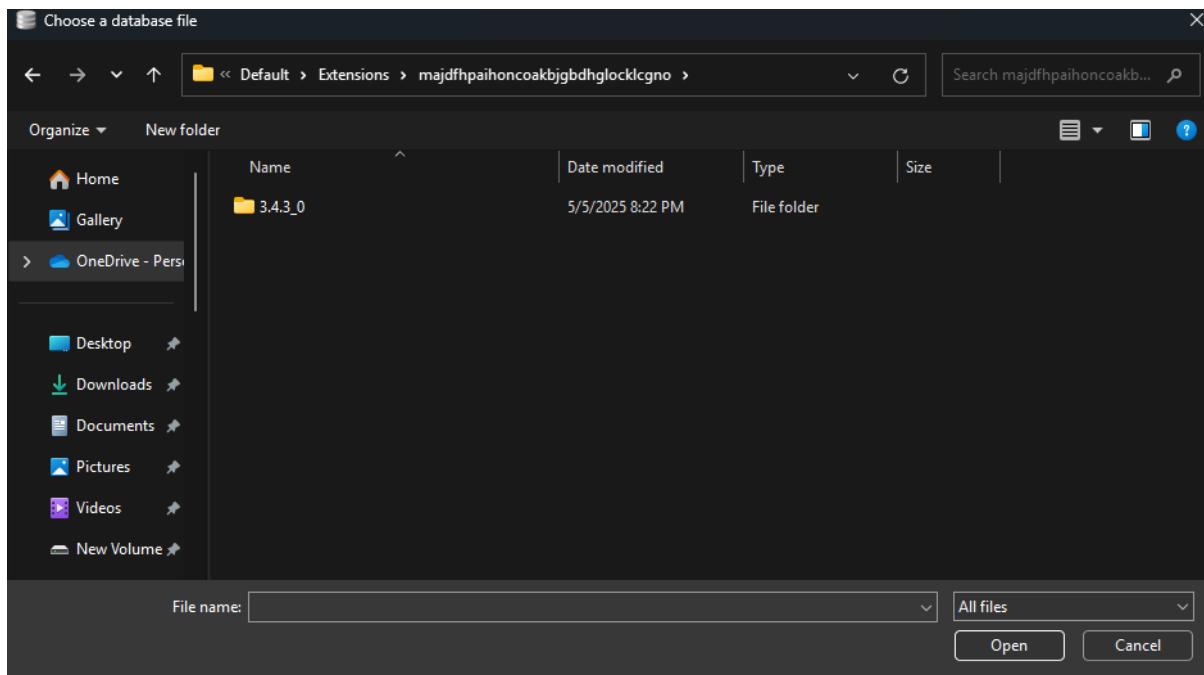
Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!
(Filennya ada di pertanyaan pertama)

Version vpn V.. yang diinstall oleh user ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhor: Aditya Firman Nugroho

Lampiran : browser.zip



Solusi :

Memasukan versi ekstensi yang sebelumnya

Flag : IDN_FLAG{3.4.3_0}

Usb Forensic

Cryptography

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 :

cryptii

The screenshot shows the cryptii web interface with three main sections: Ciphertext, Variant, and Plaintext.

- Ciphertext:** Contains the string `VQA_SYNT{C3Z4A4F4A_QH1H_94F1u}`.
- Variant:** A dropdown menu titled "ROT13" is selected, with other options including ROT5, ROT18, and ROT47.
- Plaintext:** Displays the decoded string `IDN_FLAG{P3M4N4S4N_DU1U_94S1h}`.

Below the Variant section, a message indicates "Decoded 30 chars".

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 :

The screenshot shows the dCode website interface for the Vigenere cipher. On the left, there's a search bar and a results section displaying the decrypted message: IDN_CTF{c067j1723pc40c5i33n656asd60cas67i9606}. On the right, the 'VIGENERE CIPHER' section is active, showing the ciphertext QGA_OTS{v067j1723qk40f5v33z656afwse60kdf67u9606}, the plaintext language set to English, and the alphabet set to ABCDEFGHIJKLMNOPQRSTUVWXYZ. A large button labeled 'AUTOMATIC DECRYPTION' is visible.

Solusi :

Vigenere Cipher dari GPT

Flag : IDN_CTF{c067j1723pc40c5i33n656asd60cas67i9606}

XSS



The screenshot shows a browser window with a search bar containing "Type something suspicious...". Below it is a search button labeled "Search". A results section displays the message "Showing results for: test". At the bottom, a note says "Try to steal the flag using document.cookie". Below the browser window is a screenshot of the developer tools' Network tab, showing two cookies: "flag" and "session".

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	Partition Key
flag	IDN_FLAG{XSS_C00K13_ST34L3R}	ctf.solusiber.com	/super_click	Session	32	false	false	None	Sun, 11 May 2025 10:38:42 GMT	
session	78d34209-9a20-4b62-b07d-4e823de5285f.WraNUsMPY7gGdXk6bzmrpx5aM	ctf.solusiber.com	/	Mon, 12 May 2025 09:44:51 GMT	71	true	false	Lax	Sun, 11 May 2025 10:38:01 GMT	

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

The screenshot shows a browser window for "Toko Benderaku". It features a "Premium Product" section with a logo for "CTF CAPTURE THE FLAG" and a price of "Rp10.000.000.000". A "Beli Flag" button is present. Below the product details, a note says "IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3rlng_v3ryy_3zzz}". The developer tools' Network tab is open, showing the source code of the page. A specific line of code is highlighted:

```
<input type="hidden" name="saldo" value="100">
```

Solusi:

Inspect di bagian type="hidden", lalu menggantikannya dengan "show". Maka, flag akan muncul.

Flag: IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3rlng_v3ryy_3zzz}



I'm Not Me, You Are Me

Search User Information

0

Search

```
{  
    "id": 0,  
    "username": "rafly",  
    "role": "admin",  
    "bio": "Aku ingin menjadi hacker!",  
    "flag": "IDN_CTF{Y0u_FF0D_the_heN_admin}"  
}
```

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

```
user@ctf-web:~$ whoami  
guest  
user@ctf-web:~$ cat /flag  
permission denied: you're not admin  
# Hint: Inspect your cookies. Something's not what it seems ☺
```

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	Partition
flag	IDN_CTF{XSS_COOKIES}	ctfsousiber.com	/super_click	Session	32	false	false	None	Sun, 11 May 2025 10:36:42 GMT	1
PHPSESSID	4b22921845c7e996cad82e0bb0151	ctfsousiber.com	/	Session	41	false	false	None	Sun, 11 May 2025 10:58:53 GMT	
session	78e34209-9e20-4e62-9b7d-4e823de5285tWhaNUsMPYP7gGdXLkEbzmfpx5eM	ctfsousiber.com	/	Mon, 12 May 2025 09:44:51 GMT	71	true	false	Lax	Sun, 11 May 2025 10:58:53 GMT	
user	%7B%23%7D%22%3A%23%7D%22%7D	ctfsousiber.com	/kue_monster	Sun, 11 May 2025 11:57:57 GMT	34	false	false	None	Sun, 11 May 2025 10:59:08 GMT	



```
user@ctf-web:~$ whoami
admin
user@ctf-web:~$ cat /flag
IDN_CTF{Y0u_@rE_TH@_C00K|e_M@st$r}

# Hint: Inspect your cookies. Something's not what it seems 😊
```

Name	Value	Domain	Path	Expires/Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
flag	IDN_CTF{Y0u_@rE_TH@_C00K e_M@st\$r}	ctfsolusiber.com	/super_click	Session	32	false	false	None	Sun, 11 May 2025 10:38:42 GMT
PHPSESSID	4b229210457ef695a2ed82ab0c9151	ctfsolusiber.com	/	Session	41	false	false	None	Sun, 11 May 2025 11:00:09 GMT
session	7bd34209-9e20-4b6b-bb7d-4eb23d45285fWraNUmPyP7gGxLk8bzmfpxSaM	ctfsolusiber.com	/	Mon, 12 May 2025 09:44:51 GMT	71	true	false	Lax	Sun, 11 May 2025 11:00:09 GMT
user	%7B%22role%22%3A%22admin%22%7D	ctfsolusiber.com	/kue_monster	Sun, 11 May 2025 11:57:37 GMT	34	false	false	None	Sun, 11 May 2025 11:00:09 GMT

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...

Chromaticity Channel 1	0.64 0.33
Chromaticity Channel 2	0.3 0.60001
Chromaticity Channel 3	0.14999 0.06
Pixels Per Unit X	11811
Pixels Per Unit Y	11811
Pixel Units	meters
Comment	IDN_CTF{W0W_wh4T_K03NC1D3CE}
Image Size	720x720
Megapixels	0.518

Output from file command:

```
file.png: PNG image data, 720 x 720, 8-bit/color RGBA, non-interlaced
```

ImageMagick identify output:

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
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

The screenshot shows a web application for a slot machine. The main content area has a red header with the text "LUCKY 777 CASINO". Below it, there's a message "Try your luck! Get 777 to win the FLAG!". Three dark rectangular boxes contain the numbers 8, 4, and 7 respectively. Below these boxes is a red button labeled "SPIN!". At the bottom left, there's some text: "Credits: 60". The bottom portion of the image shows the browser's developer tools, specifically the "Elements" tab, with the source code of the page visible. The code includes various JavaScript functions and variables, including one named "spin.php" which handles the spin logic.

Solusi:

Setelah memanipulasi nilai menjadikan 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



Lab 6: Timing Attack

Guess the secret password. The slower the response, the closer your guess.

password123

Guess

Correct! Flag:

NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA

Solusi:

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

Flag: IDN_FLAG{NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA}

Pramuka

DATA BORDER

Morse Code Sound & Vibration Listener

This is javascript only morse code listener. Use it with something that emits Morse code as sound or vibrations

Audio Input

Microphone:

Pre-Recorded Audio File: File: "morse.wav"

Decoder Settings & Info...

Minimum volume	-60	WPM	20	<input type="checkbox"/> Manual
Maximum volume	-30	Farnsworth WPM	20	<input type="checkbox"/>
Volume threshold	200	Frequency (Hz)	689	<input type="checkbox"/> Manual

Received Data

M0RS3C0D3R19HT

Range: 172.265625 to 22050 Hz



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

The screenshot shows a Windows Registry Explorer window titled "Values". The table lists various registry keys with their names, types, and data values. The data column contains some redacted values represented by green hex boxes. The columns are: Value Name, Value Type, Data, Value Slack, Is Deleted, and Data Record Reallocated. The table includes entries for DeviceDesc, Capabilities, Address, ContainerID, HardwareID, CompatibleID, ClassGUID, Service, Driver, Mfg, FriendlyName, and ConfigFlags.

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Capabilities	RegDword	16		<input type="checkbox"/>	<input type="checkbox"/>
Address	RegDword	6		<input type="checkbox"/>	<input type="checkbox"/>
ContainerID	RegSz	{11775948-7a76-52b3-9bc7-19cb3d487774}	00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
HardwareID	RegMultiSz	USBSTOR\Disk\JetFlashTranscend_8GB_____8.07 USBSTOR\...	00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
CompatibleID	RegMultiSz	USBSTOR\Disk\USBSTOR\RAW GenDisk		<input type="checkbox"/>	<input type="checkbox"/>
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}	00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Service	RegSz	disk	00-00	<input type="checkbox"/>	<input type="checkbox"/>
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Mfg	RegSz	@disk.inf,%genmanufacturer%;(Standard disk drives)	00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
FriendlyName	RegSz	JetFlash Transcend 8GB USB Device		<input type="checkbox"/>	<input type="checkbox"/>
ConfigFlags	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>

Solusi:

Menggunakan tool Registry Explorer untuk ekstrak 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



Values					
Drag a column header here to group by that column					
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%:Disk drive	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Capabilities	RegDword	16		<input type="checkbox"/>	<input type="checkbox"/>
Address	RegDword	6		<input type="checkbox"/>	<input type="checkbox"/>
ContainerID	RegSz	{11775948-7a76-52b3-9bc7-19cb3d487774}	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
HardwareID	RegMultiSz	USBSTOR\Disk\JetFlashTranscend_8GB_8.07 USBSTOR...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
CompatibleID	RegMultiSz	USBSTOR\Disk\USBSTOR\RAW\GenDisk		<input type="checkbox"/>	<input type="checkbox"/>
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Service	RegSz	disk	00-00	<input type="checkbox"/>	<input type="checkbox"/>
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Mfg	RegSz	@disk.inf,%genmanufacturer%,(Standard disk drives)	00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
FriendlyName	RegSz	JetFlash Transcend 8GB USB Device		<input type="checkbox"/>	<input type="checkbox"/>
ConfigFlags	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>

Solusi:

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

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

USB Forensic 1

Values					
Drag a column header here to group by that column					
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%:Disk drive	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Capabilities	RegDword	16		<input type="checkbox"/>	<input type="checkbox"/>
Address	RegDword	6		<input type="checkbox"/>	<input type="checkbox"/>
ContainerID	RegSz	{11775948-7a76-52b3-9bc7-19cb3d487774}	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
HardwareID	RegMultiSz	USBSTOR\Disk\JetFlashTranscend_8GB_8.07 USBSTOR...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
CompatibleID	RegMultiSz	USBSTOR\Disk\USBSTOR\RAW\GenDisk		<input type="checkbox"/>	<input type="checkbox"/>
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Service	RegSz	disk	00-00	<input type="checkbox"/>	<input type="checkbox"/>
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Mfg	RegSz	@disk.inf,%genmanufacturer%,(Standard disk drives)	00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
FriendlyName	RegSz	JetFlash Transcend 8GB USB Device		<input type="checkbox"/>	<input type="checkbox"/>
ConfigFlags	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>

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 USBT0R.hiv dan prompt di ChatGPT.

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

USB Forensic 5



The screenshot shows a Windows Registry viewer window titled "Values". It displays a table of registry entries for a disk device. The columns are: Value Name, Value Type, Data, Value Slack, Is Deleted, and Data Record Reallocated. The data table includes the following rows:

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%:Disk drive	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Capabilities	RegDword	16		<input type="checkbox"/>	<input type="checkbox"/>
Address	RegDword	6		<input type="checkbox"/>	<input type="checkbox"/>
ContainerID	RegSz	{11775948-7a76-52b3-9bc7-19cb3d487774}	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
HardwareID	RegMultiSz	USBSTOR\DiskJetFlashTranscend_8GB_8.07 USBSTOR...	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
CompatibleID	RegMultiSz	USBSTOR\Disk USBSTOR\RAW GenDisk		<input type="checkbox"/>	<input type="checkbox"/>
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Service	RegSz	disk	00-00	<input type="checkbox"/>	<input type="checkbox"/>
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001	00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
Mfg	RegSz	@disk.inf,%genericmanufacturer%,(Standard disk drives)	00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
FriendlyName	RegSz	JetFlash Transcend 8GB USB Device		<input type="checkbox"/>	<input type="checkbox"/>
ConfigFlags	RegDword	0		<input type="checkbox"/>	<input type="checkbox"/>

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

