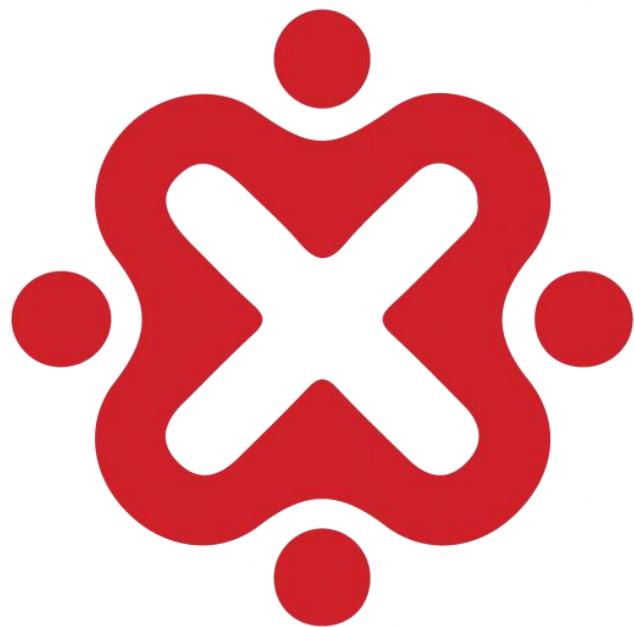




TENESYS

“We solve for fun, not for the damn write-up”



ID-Networkers
Indonesian IT Expert Factory



Introduction Team

Nama Team : TENESYS

Anggota : Erwin Wijaya, Akbar Oktaviadi, Ong Azis Saliem

The screenshot shows a dark-themed user interface for a platform. At the top, there are navigation links: 'Scoreboard', 'Challenges', 'Notifications' (with a bell icon), 'Team' (with a person icon), and 'Profile' (with a gear icon). Below this, a large dark box displays the team's name, location, and performance statistics. The team is named 'TENESYS' and is located in 'Indonesia'. It has participated in the 'ShellTrap' competition and achieved a '24th place' with a total of '680 points'. At the bottom of this box are five small icons: a gear, a person, a document, a trash can, and a refresh symbol.

Point : 10



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	7/8	70
Browser Forensic	7/10	70
Windows Forensic	15/15	150

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:

```
Vm0wd2VHUXhUWGhYV0d4VIYwZG9iMVJVU2pSVlZsbDNWMnQwYUZKc2NGW1  
ZWM1IzWVRBeFdHVkVSbHBoTVZwUVZrUkdXbVF5U2tWWGJHUnBWa1phTmxav  
VNqUIRNRFZ6VjI1V1ZXSlZXbFZWYWs1dlVsWmtjbFp0Um10TIYxSIIWbTAxVTJGR  
1NsbFJiRkpWVm0xb1ExUldXbXRXTVdSMFpFWmtUbUpGY0ZsWFZFSlhWVEZSZU  
ZOWWJGWmlSa3BoV1d0a2IyUnNiSEZTYlhSclZqQTFTbFl5TVVkvWJGcFZWbXhvV  
jJKSFVqWIViRnByVm1zeFzsZHJPVmRpU0VKWVYxZDRVMVp0VVhoaVJtUllZbX  
MxV1ZadGVFdE5SbkJXVmxBV2hvVFVoQ01sWnRNREZrTWsxM1RWWmtZVkpXV2xWW1  
pXWHBLUzFJeVJrZFdiV2hvVFVoQ01sWnRNREZrTWsxM1RWWmtZVkpXV2xWW1  
ZFNRWRREZhY1ZKcmRGUINiRVl6Vmkek5WZEdXbFZSYWxKV1RXcFdjbFl5TVV  
0VFJsWnpZVWRHVjJWcldtOVdiR1EwVVRGYVZrMVZWazVTUkVFNQ==
```

Author: Rafly Permana

Lampiran : None

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 dengan cyberchef sebanyak 7 kali”

Flag : IDN_CTF{base64_in_action_but_7_times}



Cryptography

Jadi gini lagi...

mau coba-coba aja terus, coba maen dino

Didapatkan sebuah gambar dengan judul jhlzhy.zip, untuk menyelesaikan challenge kami mengesektrak file gambar dari hasil ekstrakan file tadi menggunakan tools **steghide** dengan passphrase nama file gambar tersebut yaitu “jhlzhy”, lalu akan mendapatkan file flag.txt yang berisikan enkripsi caesar cipher.

```
└─(rommel@kowalski)-[~/IDN]
└─$ steghide extract -sf jhlzhy.jpg
Enter passphrase:
wrote extracted data to "flag.txt".

└─(rommel@kowalski)-[~/IDN]
└─$ cat flag.txt
PKU_JAM{ZalNhU0_Jv0sly}
```

Lalu kami decode menggunakan tools web cyberchef dan didapatkan flagnya

The screenshot shows the CyberChef interface with the following configuration:

- Recipe:** ROT13 Brute Force
- Input:** PKU_JAM{ZalNhU0_Jv0sly}
- Options:** Rotate lower case chars, Rotate upper case chars, Rotate numbers
- Sample length:** 100, **Sample offset:** 0, **Print amount:**
- Crib (known plaintext string):** (empty)
- Output:** (displayed text)

The Output section shows the decrypted text:

```
Amount = 14: DVI_XOA{NozBvI0_Xj0gzm}
Amount = 15: EZJ_YPB{OpaCwJ0_Yk0han}
Amount = 16: FAK_ZQC{PqbDxK0_Zl0ibo}
Amount = 17: GBL_ARD{QrcEyL0_Am0jcp}
Amount = 18: HCM_BSE{RsdFzMD_Bn0kdq}
Amount = 19: IDN_CTF{SteGaN0_Co0ler}
Amount = 20: JEO_DUG{Tufhfb00_Dp0mfs}
Amount = 21: KFP_EVH{UvgICP0_Eq0ngt}
Amount = 22: LG0_FW1{VvhJzD00_Fr0ohu}
```

Flag : IDN_CTF{SteGaN0_Co0ler}



Might Guy's Secret

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

Untuk mendapatkan flag, kami langsung mendecode ciphertextnya di tools web cyberchef dengan keynya **idnmantab** dan boom, didapatkan flagnya

The screenshot shows the CyberChef interface with the following details:

- Recipe:** Vigenère Decode
- Key:** idnmantab
- Input:** QGA_OTS{v067j1723qk40f5v33z656afwse60kdf67u9606}
- Output:** IDN_CTF{c067j1723pc40c5i33n656asd60cas67i9606}

Flag : IDN_CTF{c067j1723pc40c5i33n656asd60cas67i9606}



Rot1Aoka

Clue nya udah jelas kan?

VQA_SYNT{C3Z4A4F4A_QH1H_94F1u}

Author : Mohamad Fattyr

Sesuai judul, kami langsung mendecode disoal menggunakan cyberchef, dan didapatkan flagnya melalui ROT13 bruteforce

The screenshot shows the CyberChef interface with the following details:

- Recipe:** ROT13 Brute Force
- Input:** VQA_SYNT{C3Z4A4F4A_QH1H_94F1u}
- Options:** Rotate lower case chars (checked), Rotate upper case chars (checked), Rotate numbers (unchecked), Sample length: 100, Sample offset: 0, Print amount (checked).
- Crib (known plaintext string):** (empty)
- Output:** Shows the decoded string with various amounts (9 to 15) and their corresponding rotated outputs. The correct flag is highlighted in red: IDN_FLAG{P3M4N4S4N_DU1U_94S1h}

Flag : IDN_FLAG{P3M4N4S4N_DU1U_94S1h}



Pramuka

terjemahan kan pesan tersebut. Format Flag

IDN_CTF{****}

Author : Mohamad Fattyr

[morse.wav](#)

Didapatkan file morse.wav, kami langsung mendecode file morse.wav tersebut melalui website https://morsefm.com/#google_vignette

The screenshot shows the MorseFM web application. At the top, there's a purple header bar with the text "MorseFm" and a menu icon. Below the header, there's a form with "Upload File" and a "Choose File" button set to "morse.wav". Underneath, there's a "Language" dropdown set to "Latin". At the bottom of this section are three blue buttons: "Play", "Decode", and "Reset". Below this, under the heading "Text Result", is a text input field containing the Morse code "M0RS3C0D3R19HT". A "Copy" button is located at the bottom right of this field. At the very bottom, under the heading "Morse Result", there's some very small, illegible text.

Dan didapatkan isi dari flag M0RS3C0D3R19HT

Flag : IDN_CTF{M0RS3_C0D3_R19HT}



Classic Cryptography

Cn knud bqxosnfqzogx. zmc sgd ekzf:
HCM_BSE{xzxx_xnt_zqd_fqdzs}

Author: Rafly Permana

Didapatkan soal yang udah diencrypt, untuk solve chall ini saya menggunakan web dcode.fr dan didapatkan flagnya

The screenshot shows the dcode.fr ROT Cipher Decoder interface. On the left, under 'Results', there are three entries:

- [A-Z]+25: Do love cryptography. and the flag:
IDN_CTF{yayy_you_are_great}
- [A-Z]+12: Qb ybir pelcgbtencul. naq gur synt:
VQA_PGS{l111_1bh_ner_terng}
- [A-Z0-9]+35: Do love cryptogr0phy. 0nd the f10g:
IDN_CTF{y0yy_you_0re_gre0t}

On the right, under 'ROT CIPHER DECODER', the input text is:

★ ROTATED TEXT ?
Cn knud bqxosnfqzogx. zmc sgd ekzf:
HCM_BSE{xzxx_xnt_zqd_fqdzs}

Under 'AUTOMATIC DECRYPTION (BRUTE-FORCE)', the expected plaintext language is set to English, and the 'DECRYPT' button is visible.

Flag : IDN_CTF{yayy_you_are_great}



Simple Substitution Cipher

ORF_EZY{ziol.ol.g_yqsx_wxz_lg_tq_ln}

Author: Rafly Permana

Didapatkan enkripsi dengan judul Simple Substitution Cipher, kami membuka hint dengan isi
Alphabet mapping:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Substituted: QWERTYUIOPASDFGHJKLMZXCVBNM

The screenshot shows a web-based cipher tool interface. It has three main sections: Ciphertext, Alphabetical substitution settings, and Plaintext.

- Ciphertext:** Shows the input text: ORF_EZY{ziol.ol.g_yqsx_wxz_lg_tq_ln}.
- Alphabetical substitution settings:** Contains:
 - PLAINTEXT ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ
 - CIPHERTEXT ALPHABET: QWERTYUIOPASDFGHJKLMZXCVBNM
 - CASE STRATEGY: Maintain case
 - FOREIGN CHARS: Include
 - Note: Decoded 36 chars
- Plaintext:** Shows the output text: IDN_CTF{this_is_o_falu_but_so_ea_sy}.

Flag : IDN_CTF{this_is_o_falu_but_so_ea_sy}



Log Analysis

Log Analysis 1

Deskripsi :

pada file pcap dibawah, hacker mencoba untuk melakukan sesuatu yang berhubungan dengan recon pada service, silahkan cari...

Author : Aditya Firman Nugroho

Lampiran :

incident_response.pcapng

Solusi :

“Diberikan sebuah file pcapng dengan banyak history data, lalu saya langsung menggunakan tools string untuk melihat isi dari file nya dan melakukan filtering dengan command berikut “**strings incident_response.pcapng | grep -i idn_ctf{**” format flag dari idn maka didapatkan sebuah flag”

```
[hisoka@H3H3H3] - [/Downloads] - [Sun May 11, 20:29]
[$] >> strings incident_response.pcapng | grep -i idn_ctf{
<p>IDN_CTF{Re30N3C}</p>
<p>IDN_CTF{Re30N3C}</p>
```

Flag : IDN_CTF{Re30N3C}



Log analysis 2

Deskripsi :

awas, hati-hati, pelan-pelan, ada

Author : Aditya Firman Nugroho

Lampiran :

incident_response_2.pcapng

Solusi :

“Diberikan sebuah file pcapng dengan banyak history data, lalu saya langsung menggunakan tools string untuk melihat isi dari file nya dan melakukan filtering dengan command berikut “**strings incident_respone_2.pcapng | grep -i idn_ctf{**” format flag dari idn maka didapatkan sebuah flag”

```
[hisoka@H3H3H3] - [~/Downloads] - [Sun May 11, 20:19]
[$] >> strings incident_respone_2.pcapng | grep -i idn_ctf{
<div style="display: none;">IDN_CTF{M4l2Wre_S3ReM}</div>
<div style="display: none;">IDN_CTF{M4l2Wre_S3ReM}</div>
```

Flag : IDN_CTF{M4l2Wre_S3ReM}



Log Analysis 3

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

Format Flag : IDN_CTF{jawaban}

Didapatkan soal dan file auth.log, untuk solve soal ini kami menganalisis traffic dan didapatkan sebuah file python yang agak sus namanya dan kami coba submit ternyata benar

```
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /charts HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chat HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /chats HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /check HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checking HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:29 +0000] "GET /checkout_jclear HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
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; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /frand2 HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bash_history HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.bashrc HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cache HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.config HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cvs HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"  
192.168.18.6 - - [27/Apr/2025:12:55:33 +0000] "GET /.cyclicane HTTP/1.1" 404 436 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Flag : IDN_CTF{malware.py}



Log Analysis 4

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

Format Flag : IDN_CTF{user}

Author : Aditya Firman Nugroho

Didapatkan soal dan file auth.log, untuk solve soal ini saya hanya menggunakan command linux strings untuk membaca file dan grep untuk mencari log yang berhasil masuk. Dan didapat username yang berhasil masuk ke system yaitu :

```
[rommel@kowalski:~/IDN]
$ strings auth.log | grep -i "accepted"
Apr 27 13:05:10 test sshd[19014]: Accepted password for ghxyss from 192.168.18.6 port 5232
0 ssh2
```

Flag : IDN_CTF{ghxyss}



Log Analysis 5

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

Format Flag : IDN_CTF{service:file}

Author : Aditya Firman Nugroho

Didapatkan soal dan file pcap, karena format file sudah tertera, Kami cek satu per satu service di file log.pcapng menggunakan **tshark**. Saat filter FTP, terlihat ada perintah STOR malware, yang artinya ada file bernama *malware* di-upload via **FTP**.

```
[rommel@kowalski:~/] $ tshark -r log.pcapng -Y "ftp" -T fields -e ftp.request.command -e ftp.request.arg  
PASV  
STOR    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 eksploitasi tersebut?

Author: Rafly Permana

Lampiran :

log1.txt

Solusi :

“Diberikan sebuah file log1.txt dengan banyak data, lalu saya langsung menggunakan tools string untuk melihat isi dari file nya dan melakukan filtering dengan command berikut “**strings log1.txt | grep -i union**” lalu akan muncul beberapa history data yg dicoba exploitasi menggunakan sql注入, dan saya coba beberapa file tersebut dan ternyata berhasil yaitu file ring.php”

Flag : IDN_CTF{ring.php}

```
[hisoka@H3H3H3] - [~/Downloads] - [Sun May 11, 20:31]
[$] <> strings log1.txt | grep -i union
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)"
10.0.0.9 - - [21/Apr/2024:08:30:15 +0700] "GET /?id=105%20UNION%20SELECT%201,2,3
HTTP/1.1" 200 1342 "-" "curl/7.68.0"
198.51.100.45 - - [21/Apr/2024:08:40:12 +0700] "GET /index.php?id=105 UNION ALL
SELECT username, password FROM users-- HTTP/1.1" 500 1543 "-" "Mozilla/5.0 (Wind
ows NT 10.0; Win64; x64)"
```



Log Analysis 7

Challenge 201 Solves X

Log Analysis 7

10

Ada upaya eksplorasi menggunakan path traversal dalam permintaan ke endpoint API. Apa parameter lengkap yang digunakan penyerang?

IDN_CTF{jawaban}

Author: Rafly Permana

log2.txt

Flag Submit

Diberikan soal untuk mencari parameter lengkap yang digunakan penyerang, karena flagnya rada guessy dan beberapa parameter yang agak sus, disini sama menggunakan blackbox.ai dan mengupload file log2.txt dan didapatkan flagnya

- Log Permintaan:

```
[REDACTED]
] "GET /test.php?param=../../../../etc/shadow HTTP/1.1" 403 282 "-" "curl/7.54.0"
[REDACTED]
```

Kesimpulan:

- Penyerang menggunakan beberapa parameter dengan teknik path traversal untuk mencoba mengakses file sensitif di server.

parameternya masukan ke IDN_CTF{}

BLACKBOXAI | WEB | VIDEOS

Flag dengan Parameter Lengkap yang Digunakan Penyerang

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

Keterangan:

- Parameter yang digunakan penyerang untuk mencoba mengakses file sensitif

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



Log Analysis 8

Challenge 243 Solves ×

Log Analysis 8

10

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

[log3.txt](#)

Flag Submit

Diberikan sebuah chall untuk mencari salah satu user berhasil mendapatkan akses root melalui SSH. Berdasarkan log, berikan IP address asli dari user tersebut pada 22 april. Sama seperti chall sebelumnya disini saya menggunakan blackbox ai dan mengupload file log3.txt dan didapatkan flagnya

salah

BLACKBOXAI | WEB | VIDEOS

IP Address Asli dari User yang Mendapatkan Akses Root melalui SSH

- Tanggal: 22 April
- User yang Mendapatkan Akses: "user1"
- IP Address: "198.51.100.23"

Log yang Mendukung:

```
1 Apr 22 12:01:48 server1 sshd[2347]: Accepted password for user1 from
```

Flag:

- IDN_CTF: "IDN_CTF{198.51.100.23}"

Jika ada kesalahan lain atau jika Anda mencari user yang berbeda, silakan beri tahu saya!

Notifications

Flag : IDN_CTF{198.51.100.23}



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

Author: Rafly Permana

Lampiran :

log4.txt

Solusi :

“Diberikan sebuah file log1.txt dengan banyak data, lalu saya langsung menggunakan tools string untuk melihat isi dari file nya dan melakukan analisa bahwa kita mencari user yg berhasil masuk dengan user root, lalu saya lakukan pengecekan dan mendapatkan keywords failed dan accepted dan disini saya mendapatkan data alice dan mencoba sampai valid untuk di submit”

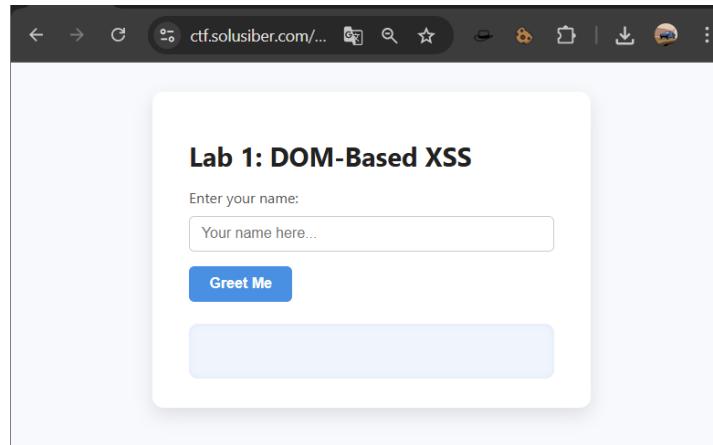
```
[hisoka@H3H3H3] - [~/Downloads] - [Sun May 11, 20:43]
[ $ ] <=> strings log4.txt | grep -i accepted
2024-04-23T14:05:12Z server1 sshd[1523]: Accepted publickey for alice from 192.1
68.0.5 port 58922 ssh2: RSA SHA256:AbCdEfGhIjKlMnOpQrStUvWxYz1234567890
2024-04-23T14:11:10Z server1 sshd[1801]: Accepted password for bob from 192.168.
0.7 port 55001 ssh2
2024-04-23T14:15:45Z server1 sshd[1921]: Accepted publickey for alice from 192.1
68.0.5 port 59123 ssh2: RSA SHA256:ZyXwVuTsRqPoNmLkJiHgFeDcBa9876543210
```

Flag : IDN_CTF{alice,192.168.0.5,SHA256:ZyXwVuTsRqPoNmLkJiHgFeDcBa9876543210}



WEB 303

DOM-Based XSS



Didapatkan sebuah website yang mana disini kita harus menginput nama, tapi saya punya cara lain untuk solve soal ini yaitu menggunakan command curl di terminal linux dan didapatkan FLAG yang terenkripsi base58

```
l3DtwXSI','2DJlgwu','1147484jJd0E','!\x20Welcome\x20to\x20Lab\x201.<br>');_0x3
n(){return _0x5e735d};};return _0x3aee();}function _0x3726(_0x112ff1,_0xf86640){
eec8=_0x3aee();return _0x3726=function(_0x3726b,_0x3dfe1){_0x3726b=_0x3726b
,_0x11bd34=_0x3aee[_0x3726bf];return _0x11bd34},_0x3726c=_0x112ff1,_0xf86640);
_0x1b4625,_0x51f589)for{const _0x4a9647=_0x3726,_0xdb1194,_0x1b4625();while(![])
{_0x16aca4=parseInt(_0x4a9647(0x1e7))/0x1+-parseInt(_0x4a9647(0x1ed))/0x2*(-parse
t(0x1ea))/0x3)+-parseInt(_0x4a9647(0x1f5))/0x4+-parseInt(_0x4a9647(0x1f2))/0x5
,_0x4a9647(0x1ee))/0x6+-parseInt(_0x4a9647(0x1ec))/0x7*(-parseInt(_0x4a9647(0x1e
a)/0x1b))/0x9;if(_0x16aca4==_0x51f589)break;else _0xdb1194[push
('if['shift'])());}catch{_0x2a9716)},{_0xdb1194['push'](_0xdb1194['shift'])});}}(_0
x1);const FLAG='27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn';function greet(){
_0xd3b=_0x3726,_0x568b5d=document._0x146d3b(0x1f4)('nameInput')_0x146d3b(0x1f3)
=document._0x146d3b(0x1f4)({_0x146d3b(0x1f0)},_0x3d5783[_0x146d3b(0x1f1)]=_0x14
,_0x5b8b5d+_0x146d3b(0x1ef);}
```

Lalu kami decrypt dan didapat flagnya

```
(rommel@kowalski)-[~]
$ echo "27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn" | base58 -d
IDN_CTF{dom_based_xss_executed}
```

Flag : IDN_CTF{dom_based_xss_executed}



Unsafe eval()

Didapatkan soal web, disini kami solve soal ini masih dengan cara yang sama yakni menggunakan command curl di terminal linux dan didapatkan FLAG yang terenkripsi base58

```
<script>
(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'])();}}}{_0xd37,0x8542f});const FLAG='8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnN9VguPSy71veTjEc';function runCode(){const _0x9c922c=_0x27e6,_0x3b2dce=document['getElementsById'](_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=func
t(_0x5d375b[_0x27e6(_0xb1b2e9,_0x5a07e4)])[_0x5d375b[_0x27e6(_0xb1b2e9,_0x5a07e4)]]}

```

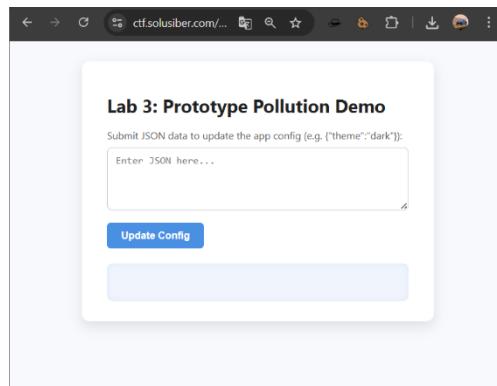
Lalu kami decrypt dan didapat flagnya

```
[rommel@kowalski:~/] $ echo "8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnN9VguPSy71veTjEc" | base58 -d
IDN_CTF{you_used_eval_successfully}
```

Flag : IDN_CTF{you_used_eval_successfully}



Prototype Pollution Demo



Didapatkan soal web, disini kami solve soal ini masih dengan cara yang sama seperti soal sebelumnya wkwkwk, yakni menggunakan command curl di terminal linux dan didapatkan FLAG yang terenkripsi base58

```
_0x525d85, for(let _0x411420 in _0x51be34){if(typeof _0x51be34[_0x411420]==_0x4d8080(0x84))  
&& _0x51be34[_0x4ff426]==null){if(!_0x8f18ef[_0x4ff426])_0x8f18ef[_0x4ff426]={};merge(_0x8  
f18ef[_0x4ff426],_0x51be34[_0x4ff426]);}else _0x8f18ef[_0x4ff426]=_0x51be34[_0x4ff426];}}f  
unction _0x47df(_0x206659,_0x26dc78){const _0xccee7d=_0xccee();return _0x47df=function(_0x  
47df86,_0xd69584){_0x47df86=_0x47df86-0x82;let _0x38ea1f=_0xccee7d[_0x47df86];return _0x38  
ea1f;}_0x47df(_0x206659,_0x26dc78);}function _0xccee(){const _0x5c4a91=[ 'ZGW9mAgck8zohQPm  
4DeKSakYAFRft9nPpb88Hj7nWrDtPcgyS', 'message', '3EBrghy', '6564dbeISw', 'output', '38q0Fssj', 'I  
nvalid\x20JSON\x20or\x20error:\x20', 'No\x20admin\x20rights\x20detected.', 'Config\x20update  
d:\x20', '20LMj0up', '2616849eVVcvL', '63QVALqW', 'value', '949448hBgiJA', 'light', 'admin', '1513  
956VvDeo', '480qNMqYS', 'getElementById', '27831936JkNoun', 'textContent', '904365sHjsom', '284  
11RqLoaZ', 'object', 'Admin\x20privilege\x20escalated!\x20Flag:\x20'];_0xccee=function(){ret
```

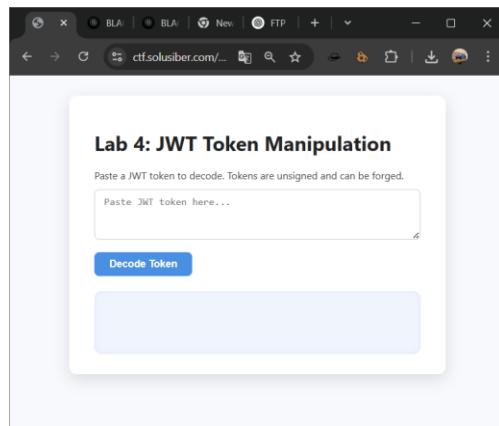
Lalu kamu decrypt dan didapatkan flagnya

```
[rommel@KowalskiJ-1~]  
$ echo "ZGW9mAgck8zohQPm4DeKSakYAFRft9nPpb88Hj7nWrDtPcgyS" | base58 -d  
IDN_CTF{prototype_pollution_success}
```

Flag : IDN_CTF{prototype_pollution_success}



JWT Token Manipulation



Didapatkan soal web, disini kami solve soal ini masih dengan cara yang sama seperti soal sebelumnya (lagi) wkwkwk, yakni menggunakan command curl di terminal linux dan didapatkan FLAG yang terenkripsi base58

```
x34bac7(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 _0x11808c=['8035280MmWsQD','Invalid\x20JWT','7ihwAza','output','2VRCfLA','5yrKYKV','getElementById','470644QwMWuc','169656ietXjY','\x5cn\x5cnUser\x20access\x20onl y.', 'length', 'parse', '371538eQiFXe', 'stringify', '7110078hUEqcQ', '7834552SFlzFK', '\x5cn\x5cnPayload:\x5cn\'18CE77cD\'!+textContent\'23245980Vnlfd\'\'\x5cn\x5cnAdmin\x20access\x20gra
```

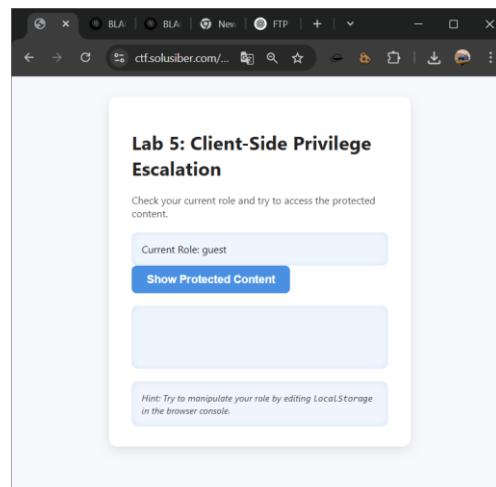
Lalu kami decrypt dan didapatkan flagnya

```
~/CTF>
└─[rommel@kowalski]─[~]
$ echo "FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY" | base58 -d
IDN_CTF{jwt_token_manipulated}
└─[rommel@kowalski]─[~]
$ |
```

IDN_CTF{jwt_token_manipulated}



Client-Side Privilege Escalation



Didapatkan soal web lagi, disini kami solve soal ini masih dengan cara yang sama seperti soal sebelumnya (lagi) wkwkwk, yakni menggunakan command curl di terminal linux dan didapatkan FLAG yang terenkripsi base58

```
_0x102201=['1557204u0zLfp','10UDjReA','content','status','1148160pJVUm','setItem','14788472LGGNdW','9FcRoOH','textContent','17180273etQYGo','4SaNdyB','admin','Access\x20denied.\x20You\x20must\x20be\x20an\x20admin\x20to\x20see\x20the\x20secret\x20content.','','Welcome,\x20mighty\x20admin!\x20Here\x20is\x20your\x20confidential\x20flag:\x0a\x0a','1058835WSHwsQ','2DvT8boTciwZu4ZctauqBoqJaMKWk8xbk5mAmgPqCTjQ9NX2xGEGgGHXFA','user_role','8792399VPCVDY','getItem','getElementById','31673880zsDsi','9nHyyMT','guest'];_0x3446=function(){return _0x102201};return _0x3446}();}(function(_0x3688fc,_0x4e2c93){const _0x316e03=_0x437e,_0x232658=_0x3688fc();while(![]){try{const _0x26c1d5=parseInt(_0x316e03(0x11c))/0x1+-parseInt(_0x316e03(0x120))/0x2*(-parseInt(_0x316e03(0x123))/0x3)+parseInt(_0x316e03(0x119))/0x6+-parseInt(_0x316e03(0x116))/0x7+-parseInt(_0x316e03(0x122))/0x8*(parseInt(_0x316e03(0x11a))/0x9)+parseInt(_0x316e03(0x11d)
```

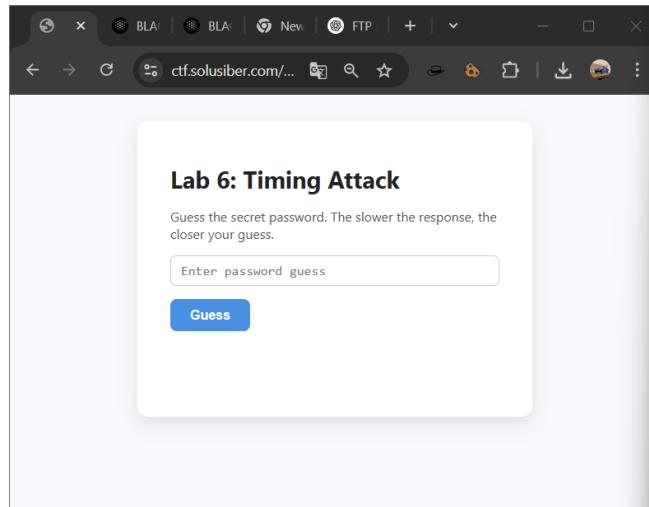
Lalu kami decrypt dan didapat flagnya

```
[rommel@kowalski:~]$ echo "2DvT8boTciwZu4ZctauqBoqJaMKWk8xbk5mAmgPqCTjQ9NX2xGEGgGHXFA" | base58 -d
IDN_FLAG{client_side_privilege_escalation}
```

Flag : IDN_FLAG{client_side_privilege_escalation}



Timing Attack



Didapatkan lagi soal web, disini kami solve soal ini masih dengan cara yang sama seperti soal sebelumnya (lagi) wkwkwk, yakni menggunakan command curl di terminal linux dan didapatkan FLAG yang terenkripsi base58

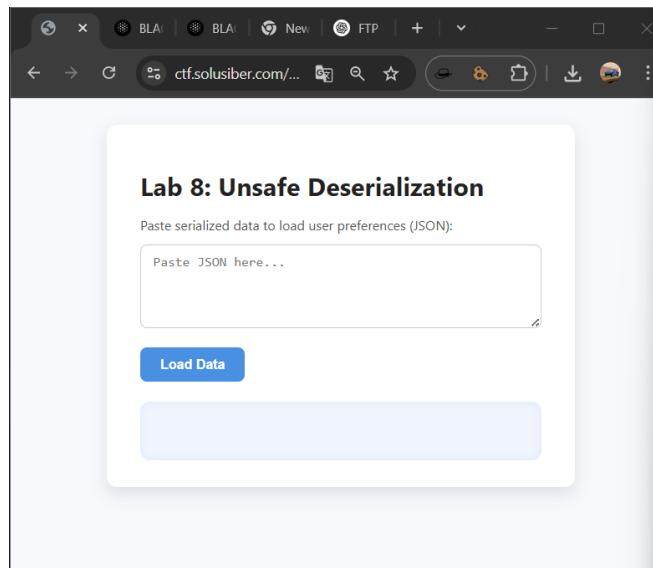
```
mance[_0xd03cba(0x1a8)]()_0x53d080;_0x5cb28e?_0x58ad0b[_0xd03cba(0x1ae)]=_0xd03cba(0x1a4)
+FLAG:_0x58ad0b[_0xd03cba(0x1ae)]=Incorrect\x20guess.\x20Response\x20time:\x20'+_0x312da0
['toFixed'](0x2)+_0xd03cba(0x19f);}function _0x22e6(_0xa0a7f9,_0x1ddd1a){const _0x2d3a27=_
0xd2d3a();return _0x22e6=function(_0x22e6e9,_0x2bacf1){_0x22e6e9=_0x22e6e9-0x19d;let _0x211
102=_0x2d3a27[_0x22e6e9];return _0x211102};_0x22e6(_0xa0a7f9,_0x1ddd1a);}function _0x2d3a
(){const _0x17a96b=[ 'NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLF6zqN2mVLuA' , '1121022UauDJn' , '70523
46GSZaGe' , 'charAt' , 'Correct!' , 'Flag:\x20' , 'guessInput' , '436DBIYUG' , '12882gLFSEx' , 'now' , 'l
ength' , 'getElementById' , '2500205abj5Xq' , '2165814pvNxDT' , '8076872fjBjIF' , 'textContent' , '1sK
nEmJ' , '1763018gdasee' , 'value' , '\x20ms' ];_0x2d3a=function(){return _0x17a96b};return _0x2d
```

Lalu kami decrypt dan didapatkan flagnya

```
[rommel@kowalski:~]
$ echo "NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLF6zqN2mVLuA" | base58 -d
IDN_CTF{timing_attack_successful}
```

Flag : IDN_CTF{timing_attack_successful}

Unsafe Deserialization



Didapatkan lagi lagi soal web, disini kami solve soal ini masih dengan cara yang sama seperti soal sebelumnya (lagi) wkwkwk, yakni menggunakan command curl di terminal linux dan didapatkan FLAG yang terenkripsi base58

Lalu kami decrypt dan didapat flagnya

Flag : IDN CTF{unsafe_deserialization_executed}



Web Exploitation

Hiden Buy Flag

Deskripsi :

Tim ID-Network baru saja membuat website, tetapi tim internal saja yang dapat masuk ke dalam website tersebut dengan pointing ke website (idn.id), kami menyuruh kalian para (Pentester) untuk mencoba menemukan celah disana dan masuk ke website tersebut. Didalam website tersebut kalian harus membeli sebuah Flag dengan harga 100000000.

Author : Faiz Ahmad Habibi

Lampiran :



Solusi :

“ diberikan sebuah website saldo sultan shop yg diinstruksikan jika ingin mendapatkan sebuah flag maka harus membeli flag dengan harga 10M tetapi hanya diberikan saldo 100 saja, lalu saya berpikir untuk menangkap request dengan burpsuite dan melakukan tampering data supaya cukup membeli flag lalu di dapatkan sebuah flag”

Request		Response	
Pretty	Raw	Pretty	Raw
1 POST /buy_the_flag/ HTTP/2		91	91
2 Host: idn.id		92	92
3 Cookie: session=723fe67_eba2_43cd_a040_0199ade00ble._JgXT5ovLBhTrUhw0DCXRAjY3Es; PHPSESSID=62bfef1718334350028a09e8c4675be		93	93
4 Content-Length: 19		94	94
5 Cache-Control: max-age=0		95	95
6 Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="B", "Chromium";v="129"		96	96
7 Sec-Ch-Ua-Mobile: ?0		97	97
8 Sec-Ch-Ua-Platform: "Linux"		98	98
9 Origin: https://ctf.solusiber.com		99	99
Dnt: 1		100	100
1 Upgrade-Insecure-Requests: 1		101	101
2 Content-Type: application/x-www-form-urlencoded		102	102
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)			
4 Accept: */*			
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			
6 Sec-Fetch-Site: same-origin			
7 Sec-Fetch-Mode: navigate			
8 Sec-Fetch-Dest: document			
9 Referer: https://ctf.solusiber.com/buy_the_flag/			
10 Accept-Encoding: gzip, deflate, br			
11 Accept-Language: en-US,en;q=0.9,id;q=0.8			
12 Priority: 0,1			
13			
14 saldo=1000000000000			

Flag : IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3r1ng_v3rry_3zzz}



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?

Author: Rafly Permana

Lampiran :

**Selamat Datang di Database
Pengelolaan Data Konoha**

Login

Login



Solusi :

“ diberikan sebuah website login page dengan deskripsi “celah klasik yang memungkinkan siapa pun melewati sistem login dan mengakses dashboard rahasia tanpa kredensial” lalu saya berpikir bahwa ada celah sql injection dan mencoba untuk login dengan user name ‘ **OR 1=1** --- dan password bebas, dan login pun dapat di bypass dan tampil sebuah daftar data

Daftar Data PII

Nama Lengkap	Email	No. Telepon	NIK	Alamat
Naruto Uzumaki	naruto@konoha.go	081234567890	1234567890123456	Konoha, Rumah Hokage
Sasuke Uchiha	sasuke@uchiha.org	082345678901	9876543210987654	Konoha, Distrik Uchiha
Sakura Haruno	sakura@medic.konoha	083456789012	1122334455667788	Konoha, Jalan Sakura
Kakashi Hatake	kakashi@konoha.go	081111111111	1001001001001001	Konoha, Jalan Ninja 7
Hinata Hyuga	hinata@hyuga.net	082222222222	2002002002002002	Konoha, Distrik Hyuga
Shikamaru Nara	shikamaru@nara.org	083333333333	3003003003003003	Konoha, Jalan Strategi
Ino Yamanaka	ino@yamanaka.co	084444444444	4004004004004004	Konoha, Toko Bunga Yamanaka
Choji Akimichi	choji@akimichi.food	085555555555	5005005005005005	Konoha, Jalan Kuliner
Rock Lee	lee@taijutsu.konoha	086666666666	6006006006006006	Konoha, Gym Gai Sensei
Tenten	tenten@weapon.konoha	087777777777	7007007007007007	Konoha, Toko Senjata
Neji Hyuga	neji@hyuga.org	088888888888	8008008008008008	Konoha, Markas Hyuga

namun saya tidak melihat ada flag di data tersebut, lalu saya coba liat page source nya dan didapatkan sebuah flag”

```
<tr>
<td data-label="Nama Lengkap">Rock Lee</td>
<td data-label="Email"><a href="/cdn-cgi/l/email-protection" class=__cf_email__>[REDACTED]</a></td>
<td data-label="No. Telepon">086666666666</td>
<td data-label="NIK">6006000006006006</td>
<td data-label="Alamat">Konoha, Gym Gai Sensei</td>
</tr>
<tr>
<td data-label="Nama Lengkap">Tenten</td>
<td data-label="Email"><a href="/cdn-cgi/l/email-protection" class=__cf_email__>[REDACTED]</a></td>
<td data-label="No. Telepon">087777777777</td>
<td data-label="NIK">7007007007007007</td>
<td data-label="Alamat">Konoha, Toko Senjata</td>
</tr>
<tr>
<td data-label="Nama Lengkap">Neji Hyuga</td>
<td data-label="Email"><a href="/cdn-cgi/l/email-protection" class=__cf_email__>[REDACTED]</a></td>
<td data-label="No. Telepon">088888888888</td>
<td data-label="NIK">8008008008008008</td>
<td data-label="Alamat">Konoha, Markas Hyuga</td>
</tr>
<tr>
<td data-label="Nama Lengkap">Might Guy</td>
<td data-label="Email"><a href="/cdn-cgi/l/email-protection" class=__cf_email__>[REDACTED]</a></td>
<td data-label="No. Telepon">089999999999</td>
<td data-label="NIK">9009009009009009</td>
<td data-label="Alamat">Konoha, Jalan Semangat</td>
</tr>
<!--IDN_CTF{c0NRats_you_goin_tohe_insideee}-->
```

Flag : IDN_CTF{c0NRats_you_goin_tohe_insideee}



ID-Networkers

Deskripsi :

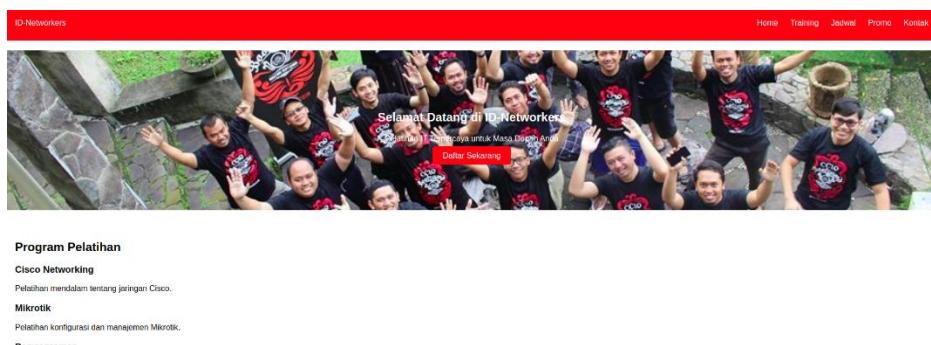
Sebuah situs publik baru saja diluncurkan ID-Networkers. Tampilannya sederhana dan tidak mencurigakan—hanya halaman beranda dengan ucapan “Selamat Datang di ID- Networkers” dan beberapa tambahan lainnya.

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.

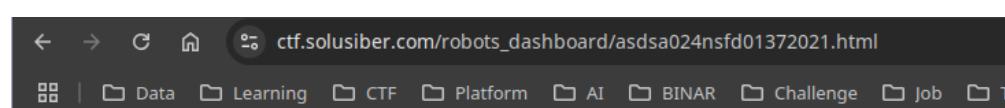
Author: Rafly Permana

Lampiran :



Solusi :

“ Diberikan sebuah tampilan website dan pada deskripsi ada sebuah clue yaitu tidak bisa dicari oleh crawler saya berpikir itu adalah file robots.txt. Lalu saat mengakses didapatkan sebuah url dan saya langsung mencari url tersebut dan di dapatkan sebuah flag”



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

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

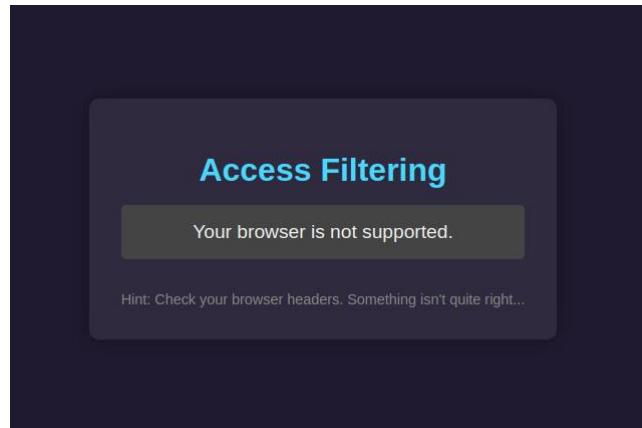
Support Force

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.

Author : Rafly Permana

Lampiran :



Solusi :

“Diberikan sebuah website dengan tulisan access filtering, ada hint untuk check browser header dan pada deskripsi mengacu pada clue “**Agent hackme**” lalu saya coba untuk intercept request dengan dan mengganti user agent menjadi hackme dan di dapatkan sebuah flag”

Request

Pretty Raw Hex

```
1 GET /support_force/ HTTP/2
2 Host: ctf.solusiber.com
3 Cookie: session=722ef6e67-eba2-42cd-a040-0199ade00b1e; JgXT5ovLBhTrUlw0DCXRAjY3Es;
4 PHPSESSID=92bf1eef17183435002a08c4679be
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Google Chrome";v="129", "Not=A?Brand";v="8", "Chromium";v="129"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Dnt: 1
10 Upgrade-Insecure-Requests: 1
11 User-Agent: hackme
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://ctf.solusiber.com/ctf/challenges
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9,id;q=0.8
20 Priority: u=0, i
21
```

Response

Pretty Raw Hex Render

```
45          font-size:1.2rem;
46          margin-top:1rem;
47          padding:1rem;
48          background-color:#444;
49          border-radius:5px;
50          word-break:break-all;
51      }
52
53      .hint{
54          margin-top:2rem;
55          font-size:0.9rem;
56          color:#888;
57      }
58  
```

Flag : IDN_CTF{r7x9_uaSwitch_delta44}



Kue Monster

Deskripsi :

Kamu cuma dikasih kue biasa? Bosen. Upgrade kue-mu jadi kue sultan dan lihat apa yang bisa kamu lakukan! (Jangan makan beneran ya)

Author : Rafly Permana

Lampiran :

```
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 🍪
```

Solusi :

“Diberikan sebuah website yang memberikan hint melihat cookies dan diharuskan mengubah user menjadi admin supaya bisa melihat isi dari flag, lalu saya coba ubah cookie dari guest menjadi admin dan reload browser nya dan di dapatkan sebuah flag”

```
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 🍪
```

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



I'm Not Me, You Are Me

Deskripsi :

Bukan cuma kamu yang punya profil! Coba-coba ganti ID di URL dan lihat apakah kamu bisa jadi orang lain. Mungkin kamu bisa mengakses sesuatu yang seharusnya nggak buatmu!

Author : Rafly Permana

Lampiran :

```
{ "id": 1,
  "username": "luffy",
  "role": "user",
  "bio": "Aku ingin menjadi raja bajak laut!"}
```

Solusi :

“Diberikan sebuah website untuk melihat informasi dari sebuah user dan kita bisa melihat informasi user lain dengan mengganti id nya, setelah saya ganti ganti id nya lalu di dapatkan data flag dengan menginputkan id 0 dan didapatkan sebuah flag”

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

Flag : IDN_CTF{Y0u_FF0D_the_heN_admin}



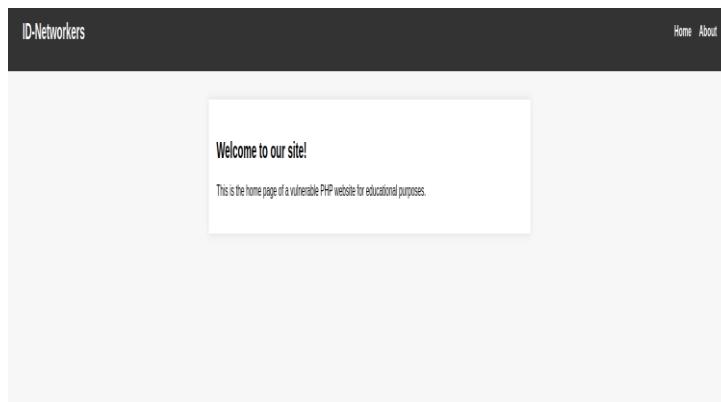
IDN Education

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!

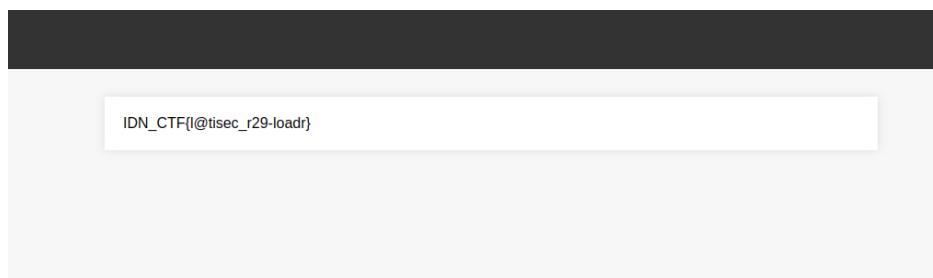
Author : Rafly Permana

Lampiran :



Solusi :

“Diberikan sebuah tampilan website biasa, lalu karna ada sebuah hint pada deskripsi yaitu file file tersembunyi maka saya berpikir ini ada kerentanan local file inclusion yg membuat kita bisa melihat file file yg ada di server, lalu saya coba untuk melakukan request ke server dengan payload berikut [“https://ctf.solusiber.com/idn_edu/?page=flag.txt”](https://ctf.solusiber.com/idn_edu/?page=flag.txt) lalu didapatkan sebuah flag”



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!



Author : Rafly Permana

Lampiran :

The screenshot shows the Red Mist Technologies website. The header features a shield icon with a keyhole and the text "Red Mist Technologies company security". Below the header, there are "About" and "Contact" links. The main content area is titled "About Us" and contains the following text:
Red Mist Technologies is a leading innovator in the field of software development, cybersecurity, and digital solutions. With a focus on delivering cutting-edge solutions to businesses worldwide, we ensure that our clients stay ahead of the curve in an ever-changing tech landscape.

Solusi :

“Diberikan sebuah tampilan website dengan clue “**Path**” maka saya berpikir lagi bahwa ini kerentanan lfi (local file inclusion) lalu saya mencoba coba beberapa payload untuk mendapatkan flag nya dan didapatkan sebuah flag dengan payload berikut ini
[“\[https://ctf.solusiber.com/search_free/?file=..//flag.txt\]\(https://ctf.solusiber.com/search_free/?file=../flag.txt\)”](https://ctf.solusiber.com/search_free/?file=../flag.txt) dan didapatkan sebuah flag nya ”

The screenshot shows the Red Mist Technologies website. The header features a shield icon with a keyhole and the text "Red Mist Technologies company security". Below the header, there are "About" and "Contact" links. The main content area shows a search result with the URL "IDN_CTF{tvec-resolver_41}" highlighted in red. At the bottom of the page, there is a footer bar with the text "Red Mist Technologies - Leading the Charge in Innovation & Security".

Flag : IDN_CTF{tvec-resolver_41}



Awesome Website

Deskripsi :

CARI!!

Author : Mohamad Fattyr

Lampiran :

The screenshot shows a website with a teal header bar containing the title 'Awesome Website' and navigation links for HOME, ABOUT, SERVICES, and SETTINGS. The main content area features a large heading 'Welcome to Our Amazing Website' and a sub-headline 'We create beautiful and functional websites that help you grow your business'. Below this is a 'Learn More' button. The footer section contains three service categories: 'Web Design' (Professional web design tailored to your needs.), 'Web Development' (Custom web applications to power your business.), and 'Digital Marketing' (Strategies to help your website reach more people.). At the bottom, there is a red footer bar with the copyright notice 'Copyright © 2025 | Your Awesome Website'.

Solusi :

“Diberikan sebuah website tanpa clue apapun hanya disuruh mencari, jadi saya coba untuk mengexplore website tersebut dengan mengakses fitur yg ada namun semua fitur access forbidden, jaid saya berpikir untuk melihat page source nya lalu ada satu hal yang menarik yaitu access token karna biasanya bersifat sensitif

```
// API configuration
api: {
  baseUrl: "https://api.example.com/v2",
  timeout: 5000,
  retryAttempts: 3,
  cacheTTL: 3600,
  accessToken: "SUROX0ZMQUd7VzNCXzN0Q29kM183UjFjazF9" // Access token for API authentication
},
```

lalu saya coba pastekan ke cyberchef dan di dapatkan sebuah flag”

The screenshot shows the CyberChef interface with a Base64 decoding recipe. The input field contains the string 'SUROX0ZMQUd7VzNCXzN0Q29kM183UjFjazF9'. The output field shows the decoded result: 'IDN_FLAG{w3B_3NCod3,_R1ck1}'.

Flag : Flag : IDN_FLAG{V3R7_e4S7_R!9HT} }



Casino 777

Challenge 220 Solves X

Casino 777

10

Ternyata aplikasi ini menerima input melalui query parameter. Cobalah eksplorasi URL dan manipulasi nilai slot-nya.

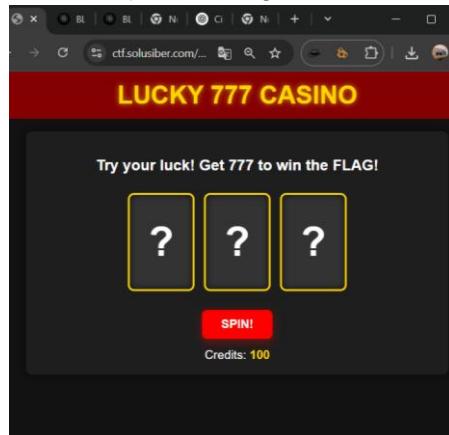
mungkin ada sesuatu yang jika sudah lengkap baru merespon

[Website](#)

Author : Mohamad Fattyr

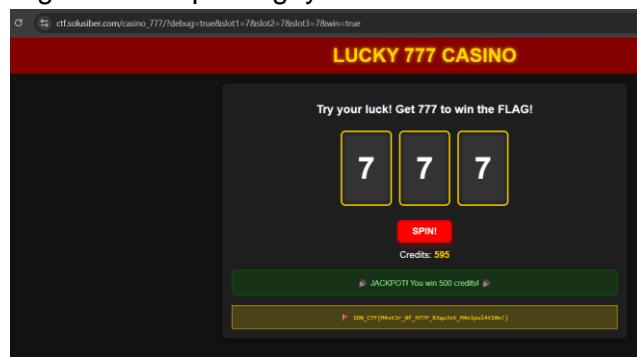
Flag Submit

Diberikan sebuah situs mesin slot dengan tombol spin, namun tidak ada input dari pengguna. Setelah menganalisis URL dan JavaScript yang ada, ditemukan beberapa parameter yang dapat dimodifikasi, seperti debug, slot1, slot2, slot3, dan win.



Mengubah parameter tersebut dengan nilai 7 pada setiap slot dan win=true, menghasilkan URL `?debug=true&slot1=7&slot2=7&slot3=7&win=true`

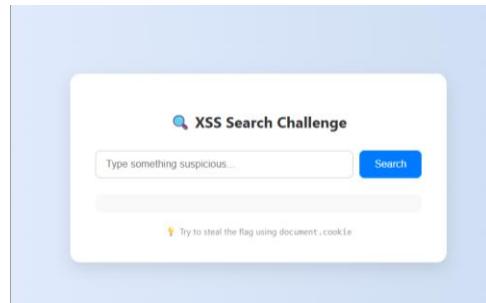
Setelah dimodifikasi, awalnya akan muncul XSS dengan kalimat “Sedikit Lagi” lalu kami tekan oke dan spin ulang. Voilaa dapat flagnya



Flag : IDN_CTF{M4st3r_0f_H77P_R3qu3st_M4n1pul4t10n!}



XSS

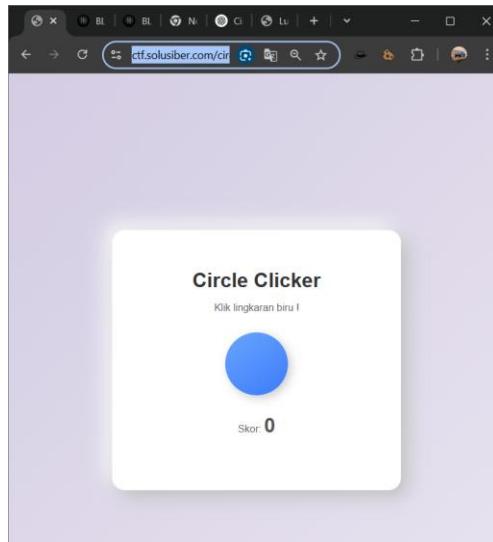


Didapatkan soal website, untuk mendapatkan flag kami hanya membuka burpsuite lalu mengintercept request dan voila didapatkan flagnya

```
1 GET /super_click HTTP/2
2 Host: ctf.solusiber.com
3 Cookie: flag=IDN FLAG{XSS_C00K13_ST34L3R}
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
5 Accept: */*, application/xhtml+xml,application/xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.9
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 If-Modified-Since: Sun, 04 May 2025 09:23:28 GMT
14 Priority: 0,0,1
15 To: trailers
16
17
```

Flag : IDN_FLAG{XSS_C00K13_ST34L3R}

Circle Clicker



Didapatkan soal yang dimana kita harus mengklik 1000 kali untuk mendapatkan flag, tapi disini saya hanya menggunakan command curl

Lalu saya decrypt sesuai soal yaitu Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana yang meruji pada base 58, dan didapatkan flagnya

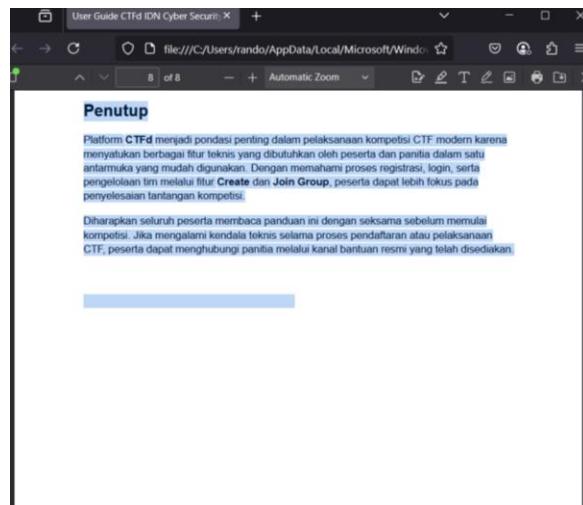
Flag : IDN_CTF{click_master}



Other

User Guide

Untuk mendapatkan flag, caranya hanya dengan membuka guide book yang ada di grup whatsapp. Dihalaman terakhir guide ada invisible word yang merupakan flag dari chall ini.



Flag : IDN_FLAG{makasih_sudah_baca_guide}



USB Forensic

USB Forensic 1

USB Forensic 1

10

ada hacker, physical acces ke laptop.. bantuin dong !

Merek usb apa yang dipakai oleh hacker untuk delivery file nya ?

format flag : IDN_FLAG{Nama_Device_Ukuran_USB_Device}

Auhor: Aditya Firman Nugroho



Flag

Submit

Didapatkan file **usb.zip** yang akan dipakai pada beberapa point dari usb forensic selanjutnya. Chall pertama disini untuk mencari Merek usb apa yang dipakai oleh hacker untuk delivery file nya?. Untuk solve soal ini cukup simple, disini saya memakai command linux yakni **cat** untuk melihat isi file **USBSTOR.hiv** dan didapatkan jawabannya.

```
*INDEVICEDESC*****@0ISKR.HTT, @ISKR_DEVDESC*, DISK DRIVE***** *Capabilities****vk
*Address****vk
    NpContainerID*****[117759d8-7a76-52b3-9bc7-19cb3d487774]****vk
    pHardwareID*****USBSTOR\DiskJetFlashTranscend_8GB____8_07USBSTOR\DiskJetFlash
    Transcend_8GB____USBSTOR\DiskJetFlash\USBSTOR\JetFlashTranscend_8GB____8jetFlas
    D\CompatibleIDs*****USBSTOR\DiskUSBSTOR\RAWGenDisk****vk NClassGUID*****{4d36e
    967-e325-11ce-bfc1-08002be10318}****vk
    xService*****disk****vkX\Drivers*****[4d36e967-e325-11ce-bfc1-08002be10318]\0
    001****vkf\Myg****disk.inf, %gemanufacturer%,(Standard disk drives)****vk
    D+
&FriendlyNameI!&***JetFlash Transcend 8GB USB Device****vk *ConfigFlags*****
(Hh*****nk ***z*
    *****.Device ParametersP***sk* p***t'?? * ****
    *****nk ***z.*****MediaChangeNotificationX***skx***t'?? *
    *****lf*****(*Partmgr****lf*****Media*
Part****vkD#
    DiskId*****{a4aa1f8-27d0-11f0-a0ac-000c2979b63d}****vk**
    Partition
    nTableCacheB*****wG*****vk
    *Attributes****vk*
        AttributesTableCache*****3D***h***&*****
```

Flag : IDN_FLAG{JetFlash_Transcend_8GB_USB_Device}



USB Forensic 2

Challenge 211 Solves ×

USB Forensic 2

10

ada hacker, physical acces ke laptop.. bantuin dong !

(Filanya ada di pertanyaan pertama)

ClassGUID Pada USB Hacker ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhor: Aditya Firman Nugroho

Flag Submit

Masih pada file yang sama, disini ditanyakan ClassGUID pada USB hacker. Untuk solve chall ini saya menggunakan tools **Autopsy** untuk membuka file **USBTOR.hiv**. dan didapatkan ClassGUID pada USB

File Details:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
USBTOR.hiv		2		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Allocated	Allocated	unknown	/LogicalFileSets/USBTOR

File Structure:

- USBTOR
 - Disk0Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07
 - XPVZQBR8.0

Properties:

- Device Parameters
 - DeviceDesc
 - Capabilities
 - Address
 - ContainerID
 - HardwareID
 - ConfigurableIDs
 - ClassGUID**
 - Service
 - Driver
 - Mfg
 - FriendlyName
 - ConfigFlags

Metadata:

- Name: **ClassGUID**
- Type: REG_SZ
- Value: {4d36e967-e325-11ce-bfc1-08002be10318}

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



USB Forensic 3

Challenge 203 Solves ×

USB Forensic 3
10

ada hacker, physical acces ke laptop.. bantuin dong !
(Filenya ada di pertanyaan pertama)

Apa Containder ID USB Yang dipakai Hacker ?
format flag : IDN_FLAG{jawaban yang disoal}

Auhor: Aditya Firman Nugroho

Masih pada file yang sama, disini ditanyakan ClassGUID pada USB hacker. Untuk solve chall ini saya menggunakan tools **Autopsy** untuk membuka file **USBTOR.hiv**. dan didapatkan **ContainderID** pada USB

The screenshot shows the Autopsy interface with the following details:

- File Path: USBSTOR\Disk0Ven_JetFlash&Prod_Transcend_8G\XPLZC8FR&0
- Selected Item: Device Parameters > Properties > ContainerID
- Panels:
 - Metadata: Shows 'ContainerID' with Type REG_SZ and Value '(11775948-7a76-52b3-9bc7-19cb3d487774)'.
 - Annotations: None.
 - Other Occurrences: None.

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



USB Forensic 4

Challenge 197 Solves

USB Forensic 4

10

ada hacker, physical acces ke laptop.. bantuin dong !
(Filenya ada di pertanyaan pertama)

Apa Disk ID yang dipakai hacker ?

format flag : IDN_FLAG{Jawaban yang disoal}

Autor: Aditya Firman Nugroho

Masih pada file yang sama, disini ditanyakan ClassGUID pada USB hacker. Untuk solve chall ini saya menggunakan tools **Autopsy** untuk membuka file **USBTOR.hiv**. dan didapatkan **DiskID** pada USB

The screenshot shows the Autopsy 4.22.1 interface. On the left, there's a sidebar with categories like Data Sources, File Views, and Data Artifacts. The main pane shows a table of results for a LogicalFileSet named 'LogicalFileSet5'. One row in the table is highlighted for 'USBTOR.hiv'. Below the table, a detailed view of the file's metadata is shown. Under the 'Metadata' tab, it lists 'Name: DiskId' and 'Type: REG_SZ'. The 'Value' field contains the string '(a4aaa1f8-27d0-11f0-a0ac-000c2979b63d)'. The status bar at the bottom indicates the date as 10/05/2025 and the time as 08:59.

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



USB Forensic 5

Challenge 165 Solves X

USB Forensic 5

10

ada hacker, physical acces ke laptop.. bantuin dong !
(Filenya ada di pertanyaan pertama)

Apa Serial ID USB Yang dipakai Hacker ?
format flag : IDN_FLAG{jawaban yang disoal}

Auhor: Aditya Firman Nugroho

Masih pada file yang sama, disini ditanyakan ClassGUID pada USB hacker. Untuk solve chall ini saya menggunakan tools **Registry Explorer** untuk membuka file **USBTOR.hiv**. dan didapatkan **SerialID** pada USB

The screenshot shows the Registry Explorer interface with the following details:

- File menu: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Content.
- USBSTOR key is expanded.
- Disk\Ven_JetFlash&Prod_Transcend_8G key is expanded.
- Device Parameters key is expanded.
- MediaChangeNotification key is selected.
- Metadata pane:
 - Name: XRVZQBFR&0
 - Number of subjects: 2
 - Number of values: 12
 - Modification Time: 2025-05-03 03:44:25 GMT+00
- Values pane:

Name	Type	Value
DeviceDesc	REG_SZ	@disk.inf%rd

Flag : IDN_FLAG{XRVZQBFR&0}



USB Forensic 6

Challenge 125 Solves X

USB Forensic 6
10

ada hacker, physical acces ke laptop.. bantuin dong !
(Filenya ada di pertanyaan pertama)

Nama File Yang ada di USB ?
format flag : IDN_FLAG{Jawaban yang disoal}

Auhor: Aditya Firman Nugroho

Masih pada file yang sama, disini ditanyakan ClassGUID pada USB hacker. Untuk solve chall ini saya menggunakan tools **Registry Explorer** untuk membuka file **USBTOR.hiv**. dan didapatkan nama file yang ada pada USB

Extension	Value Name	Target Name	Link Name	My Positon	Opened On	Extension Last Opened
+ .txt	0	4fu284428u5984-8308848.txt	4fu284428u5984-8308848.link	-	-	-
x					0 2025-05-03 03:48:32	

Flag : IDN_FLAG{4fu284428u5984-8308848.txt}



USB Forensic 8

Challenge 109 Solves x

USB Forensic 8
10

ada hacker, physical acces ke laptop.. bantuin dong !
(Filenya ada di pertanyaan pertama)

File dibuka pada jam ?

format flag : IDN_FLAG[Jawaban yang disoal] example : xxxx-xx-xx-xxxxxx

Auhor: Aditya Firman Nugroho

Flag Submit

Masih pada file yang sama, disini ditanyakan ClassGUID pada USB hacker. Untuk solve chall ini saya menggunakan tools **Registry Explorer** untuk membuka file **USBTOR.hiv**. dan didapatkan history waktu file dibuka yang ada pada USB

Extension	Value Name	Target Name	Link Name	File Position	Opened On	Extension Last Opened
#	0	4628402b5984-8308848.txt	4628402b5984-8308848.htm	-	-	-
txt	0	4628402b5984-8308848.txt	4628402b5984-8308848.htm	0	2025-05-03 03:48:32	2025-05-03 03:48:32

Flag : IDN_FLAG{2025-05-03 03:48:32}



Windows Forensic

Windows Forensic 1

Challenge 58 Solves

Windows Forensic 1
10

Ceritanya, udh ambil hivenya, mount, trus cari beberapa informasi tambahan lainnya !!

(Filenya ada di pertanyaan pertama)

Nama file yang menyimpan credential ?

format flag : IDN_FLAG{Jawaban yang disoal} example :
xxxxxxxxxx_0000xxx

Auhor: Aditya Firman Nugroho

[View Hint](#)

[windows.zip](#)

[Flag](#) [Submit](#)

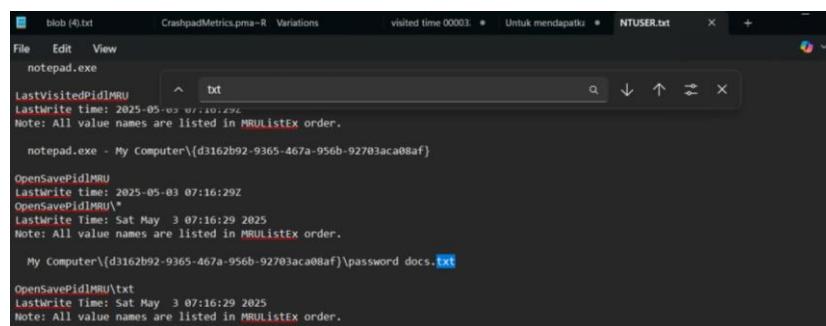
Didapatkan soal dan file zip yang akan digunakan sebanyak 15 challenge selanjutnya, Disini saya memakai beberapa tools sebagai berikut :

FTK Imager untuk mounting file ad1

Regripper untuk mengekstrak data file isi file dari hasil mounting

Registry Explorer untuk melihat isi dari hasil mounting file ad1

Chall pertama disini diberikan pertanyaan Nama file yang menyimpan credential, untuk solve chall ini saya ekstrak terlebih dulu file NTUSER.dat menggunakan regripper dan sesuai hint disini saya mencari file txt. Dan didapatkan file txt itu dari hasil ekstrakan yaitu



Flag : IDN_FLAG{password_docs.txt}



Windows Forensic 2

Challenge 58 Solves X

Windows Forensic 2

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!

(Filenya ada di pertanyaan pertama)

file yang menyimpan credential, dibuka pada tanggal berapa ?

format flag : IDN_FLAG[Jawaban yang disoal] example : xxxx-xx-xx XXXXXX

Auhtor: Aditya Firman Nugroho

Flag Submit

Chall kedua disini kita mencari informasi file yang menyimpan credential, dibuka pada tanggal berapa. Disini saya memakai registry explorer untuk membuka file NTUSER.dat dan didapatkan hasilnya

The screenshot shows the Registry Explorer interface. On the left, the registry tree is displayed under 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem'. A table on the right lists recent documents:

Extension	Value Name	Target Name	Link Name	Menu Position	Opened On	Extension Last Opened
.txt	2	password docs.txt	password docs.lnk	—	0 2025-05-03 07:16:29	—
.txt	1	flag.txt	flag (2).lnk	1		
.txt	0	4f28442b5984-8308848	4f28442b5984-8308848.lnk	2		

Flag : IDN_FLAG{2025-05-03 07:16:29}



Windows Forensic 3

Challenge 99 Solves X

Windows Forensic 3

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!

(Filenya ada di pertanyaan pertama)

User yang dibuat pada tanggal 2025-05-03 07:04:43,
Username nya ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

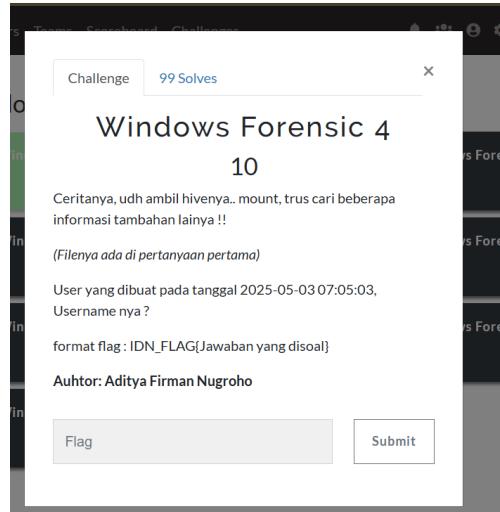
Pada challenge ke-3 disini ditanyakan User yang dibuat pada tanggal 2025-05-03 07:04:43, Username nya apa?. Untuk solve chall ini, hanya perlu mengekstrak file SAM menggunakan regripper dan mencocokkan waktu dan jam yang ada disoal. Didapatkan hasilnya

```
Answer 2 :  
Question 3 :  
Answer 3 :  
Name :  
Last Login Date : Sat May 3 03:42:49 2025 Z  
Pwd Reset Date : Never  
Pwd Fail Date : Never  
Login Count : 3  
--> Password does not expire  
--> Password not required  
--> Normal user account  
Username : Geraldin [1002]  
SID : S-1-5-21-2412307826-2007293762-2764304457-1002  
Full Name :  
User Comment :  
Account Type :  
Account Created : Sat May 3 07:04:43 2025 Z  
Name :  
Last Login Date : Never  
Pwd Reset Date : Sat May 3 07:04:43 2025 Z  
Pwd Fail Date : Never  
Login Count : 0  
--> Normal user account  
Username : Jon [1003]  
SID : S-1-5-21-2412307826-2007293762-2764304457-1003
```

Flag : IDN_FLAG{Geraldin}



Windows Forensic 4



Pada challenge ke-4 disini ditanyakan User yang dibuat pada tanggal 2025-05-03 07:05:03, Username nya apa?. Untuk solve chall ini, hanya perlu mengekstrak file SAM menggunakan regripper dan mencocokan waktu dan jam yang ada disoal. Didapatkan hasilnya

```
blob (4).txt CrashpadMetrics.j Variations visited time Untuk menc NTUSER.txt userclas.txt sam.txt
File Edit View
Account Type : 
Account Created : Sat M ^ 07:05:03
Name : 
Last Login Date : Never
Pwd Reset Date : Sat May 3 07:04:43 2025 Z
Pwd Fail Date : Never
Login Count : 0
--> Normal user account

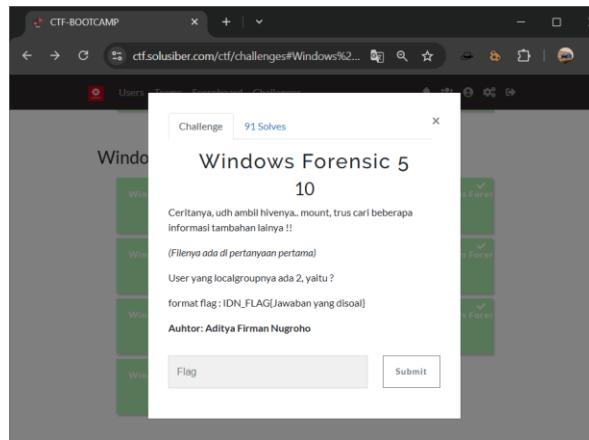
Username : Jon [1003]
SID : S-1-5-21-2412307826-2007293762-2764304457-1003
Full Name :
User Comment :
Account Type :
Account Created : Sat May 3 07:05:03 2025 Z
Name :
Last Login Date : Never
Pwd Reset Date : Sat May 3 07:05:03 2025 Z
Pwd Fail Date : Never
Login Count : 0
--> Normal user account

-----
Group Membership Information
Group Name : Event Log Readers [0]
LastWrite : Sat May 3 03:26:06 2025 Z
```

Flag : IDN_FLAG{Jon}



Windows Forensic 5



Pada challenge ke-5, disini ditanyakan User yang localgroupnya ada 2, yaitu ?. untuk solve soal ini, saya mengekstrak file SAM dari hasil mounting file ad1 dan didapatkan file txt. Lalu file txt tersebut saya copy dan paste file tersebut di chatgpt dan didapat hasilnya

Flag : IDN_FLAG{Geraldin}



Windows Forensic 6

Challenge 80 Solves X

Windows Forensic 6

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!
(Filenya ada di pertanyaan pertama)

Last Login Time dari User Cli.. ?

format flag : IDN_FLAG[Jawaban yang disoal] example : xxxx-xx-xx XXXX:XX

Auhtor: Aditya Firman Nugroho

Flag Submit

Chall ke-6 ditanyakan Last Login Time dari User Cli.. ?, untuk solve chall ini masih sama seperti chall sebelumnya, saya menggunakan chat gpt untuk mendapatkan flag

ChatGPT ~

Last Login Time dari User Cli.. ?

format flag : IDN_FLAG[jawaban yang diminta] example : xxxx-xx-xx XXXX:XX

Berdasarkan data dari file `sam.txt`, informasi untuk user CLIENT [1001] adalah sebagai berikut:

- Last Login Date : Sat May 3 03:42:49 2025 Z

Untuk memenuhi format flag yang diminta (`yyyy-mm-dd hh:mm:ss`), maka waktu tersebut diformat ulang menjadi:

2025-05-03 03:42:49

Jawaban dalam format flag:

css

IDN_FLAG{2025-05-03 03:42:49}

Perlu bantuan soal lainnya dari file ini?

Tanyakan apa saja

Flag : IDN_FLAG{2025-05-03 03:42:49}



Windows Forensic 7

Challenge 92 Solves [X](#)

Windows Forensic 7

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!

(Filenya ada di pertanyaan pertama)

User ID dari user dengan 3 huruf ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhor: Aditya Firman Nugroho

[Flag](#)

[Submit](#)

Chall ke 7 disini ditanyakan User ID dari user dengan 3 huruf?. Dikarenakan pada chalh windows ke 4 adalah user dengan 3 huruf, dapat disimpulkan user yang dimaksud adalah Jon dan user idnya adalah sebagai berikut

```
File Edit View
Account Type :
Account Created : Sat May 3 07:05:03 2025 Z
Name : Jon [1003]
Last Login Date : Never
Pwd Reset Date : Sat May 3 07:04:43 2025 Z
Pwd Fail Date : Never
Login Count : 0
--> Normal user account

Username : Jon [1003]
SID : S-1-5-21-2412307826-2007293762-2764304457-1003
Full Name :
User Comment :
Account Type :
Account Created : Sat May 3 07:05:03 2025 Z
Name :
Last Login Date : Never
Pwd Reset Date : Sat May 3 07:05:03 2025 Z
Pwd Fail Date : Never
Login Count : 0
--> Normal user account

-----
Group Membership Information
-----
Group Name : Event Log Readers [0]
LastWrite : Sat May 3 03:26:06 2025 Z
```

Flag : IDN_FLAG{1003}



Windows Forensic 8

Challenge 83 Solves X

Windows Forensic 8

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!

(Filenya ada di pertanyaan pertama)

SID Dari User Guest ?

format flag : IDN_FLAG[Jawaban yang disoal]

Auhtor: Aditya Firman Nugroho

Dichall ke 8 ini, ditanyakan SID Dari User Guest, untuk solve soal ini saya hanya membuka file sam.txt yang telah saya ekstrak sebelumnya dan mencari user guest, dan didapatkan hasilnya.

```
User Information ^ guest
Username : AUTHORITY\Guest [501]
SID : S-1-5-21-2412307826-2007293762-2764304457-501
Full Name :
User Comment : Built-in account for administering the computer/domain
Account Type :
Account Created : Sat May 3 03:27:38 2025 Z
Name :
Last Login Date : Never
Pwd Reset Date : Never
Pwd Fall Date : Never
Login Count : 0
--> Password does not expire
--> Account Disabled
--> Normal user account

Username : Guest [501]
SID : S-1-5-21-2412307826-2007293762-2764304457-501
Full Name :
User Comment : Built-in account for guest access to the computer/domain
Account Type :
Account Created : Sat May 3 03:27:38 2025 Z
Name :
Last Login Date : Never
Pwd Reset Date : Never
Pwd Fall Date : Never
Login Count : 0
--> Password does not expire
--> Account Disabled
--> Password not required
--> Normal user account
```

Flag : IDN_FLAG{S-1-5-21-2412307826-2007293762-2764304457-501}



Windows Forensic 9

Challenge 77 Solves X

Windows Forensic 9

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!
(Filenya ada di pertanyaan pertama)

CurrentBuild pada Windows ?

format flag : IDN_FLAG(Jawaban yang disoal)

Auhtor: Aditya Firman Nugroho

Di chall ke 8 ini ditanyakan CurrentBuild pada Windows, disini saya mengupload file software yang ada didalam evident.ad1 dan diekstrak menggunakan regripper ke chatgpt dan bertanya sesuai soal. Dan didapat versinya

software.txt
Document

menurut file ini, CurrentBuild pada Windows?

Berdasarkan isi file, nilai `currentBuild` untuk Windows adalah:
19045

Ini menunjukkan bahwa versi Windows yang digunakan adalah bagian dari Windows 10 versi 22H2 (build 19045). Anda ingin saya bantu menjelaskan versi Windows ini lebih lanjut?

Share

Flag : IDN_FLAG{19045}

Windows Forensic 10



Pada chall ke 10, ditanyakan DisplayVersion pada Windows, disini saya melanjutkan dari chall sebelumnya dan didapatkan display versionnya

Berdasarkan isi file, nilai `CurrentBuild` untuk Windows adalah: 19045
Ini menunjukkan bahwa versi Windows yang digunakan adalah bagian dari Windows 10 versi 22H2 (build 19045). Anda ingin saya bantu menjelaskan versi Windows ini lebih lanjut?

DisplayVersion pada Windows ?

Berdasarkan isi dari file `registry` yang Anda unggah, nilai `DisplayVersion` untuk sistem operasi Windows Anda adalah: 22H2
Ini berarti versi Windows Anda adalah Windows 10 22H2 atau Windows 11 22H2, tergantung dari edisi OS-nya (yang bisa ditentukan dari nilai `ProductName` atau `ReleaseId` lainnya). Ingin saya bantu konfirmasi apakah itu Windows 10 atau 11 berdasarkan entri lainnya?

Flag : IDN_FLAG{22H2}



Windows Forensic 11

Challenge 81 Solves X

Windows Forensic 11

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!

(Filenya ada di pertanyaan pertama)

Buildlab pada Windows ?

format flag : IDN_FLAG[Jawaban yang disoal]

Auhtor: Aditya Firman Nugroho

Dichall ke 11 ditanyakan Buildlab pada Windows, disini saya membuka file software yang sudah diekstrak sebelumnya menggunakan regripper, dan didapatkan buildlabnya

```
File Edit View
us\nlncim.mof %windir%\system32\whem\orientmanagementprovider.mof %windir%\system32\whem\netnrofm.mof %windir%\system32\wbem\nlncim.mof %indir%\system32\whem
windir\system32\wbem\s\dmnbridgeprov1.mof C ^ build
winver v.20200525
(Software) Get Windows version & build info

ProductName          Windows 10 Pro
ReleaseID           2009
BuildLab            19041.vb_release.191206-1406
BuildLabEx          19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID Enterprise
RegisteredOrganization
RegisteredOwner      CLIENT
UBR                 2965
InstallDate         2025-05-03 03:27:41Z
InstallTime          2025-05-03 03:27:41Z
UBR                 2965
```

Flag : IDN_FLAG{19041.vb_release.191206-1406}



Windows Forensic 12

Challenge 59 Solves X

Windows Forensic 12

10

Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!

(Filennya ada di pertanyaan pertama)

File exe yang ada di Desktop windows, yang berkaitan dengan attack hacker ?

format flag : IDN_FLAG[Jawaban yang disoal]

Auhor: Aditya Firman Nugroho

Dichall ke 12 ditanyakan File exe yang ada di Desktop windows, yang berkaitan dengan attack hacker, disini saya membuka file **NTUSER.dat** yang sudah diekstrak sebelumnya menggunakan regripper, dan setelah dicoba satu persatu format file .exe, didapatkan file exe yang correct setelah saya coba submit yaitu

```
File Edit View
StartButton SearchBox ^ .exe
-----
[-] SOFTWARE\HeidisOL not found.
[-] SOFTWARE\HeidisOL\Servers not found.

-----
[*] Desktop file Lists
:::{645FF040-5081-101B-9F08-00AA002F954E}>
Microsoft Edge.lnk> |
Rubeus.exe>
winPEASx64.exe>
debug.log>
ChromeSetup.exe>
Exterro FTK Imager.lnk> |
ID:\>

-----
identities v.20200525
(NTUSER.DAT) Extracts values from Identities key; NTUSER.DAT

identities not found.

-----
injectdll64 v.20200427
(NTUSER.DAT, Software) Retrieve values set to weaken chrome security

Ln 573, Col 11  4 of 42.808 characters
```

Flag : IDN_FLAG{Rubeus.exe}

Windows Forensic 13

Challenge	67 Solves	X
Windows Forensic 13		
10		
Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainnya !!		
(Filenya ada di pertanyaan pertama)		
Tools yang digunakan untuk privilege escalation di windows, yang disimpan di path desktop. Namanya apa ?		
format flag : IDN_FLAG[Jawaban yang disoal]		
Auhtor: Aditya Firman Nugroho		
Flag		Submit

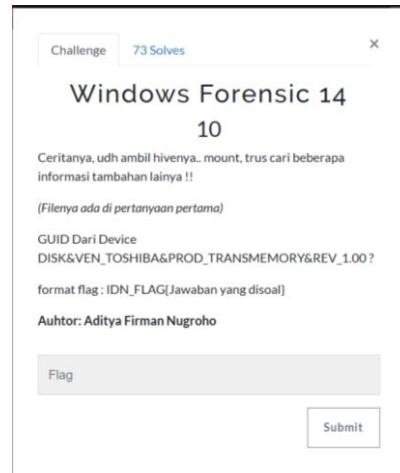
Dichall ke 13 ditanyakan Tools yang digunakan untuk privilege escalation di windows, yang disimpan di path desktop, Namanya apa?, masih di file yang sama seperti soal sebelumnya, disini saya membuka file **NTUSER.dat** yang sudah diekstrak sebelumnya menggunakan regripper, dan setelah dicoba satu persatu format file dan bertanya kepada lord chatgpt, didapatkan tools yang digunakan untuk privilege escalation di windows, yang disimpan di path desktop yang berformatkan .exe dibawah jawaban chall sebelumnya

```
blob(4).txt CrashpadMetrics Variations visited time Untuk mena SOFTWARE software.txt NTUSER.txt + File Edit View StartButton SearchBox Find [--] SOFTWARE\HeidisOL not found. [--] SOFTWARE\HeidisOL\Servers not found. ----- [*] Desktop file Lists ::{645FF040-5081-101B-9F08-00AA002F954E} Microsoft Edge.lnk> Google Chrome.lnk> | Rubeus.exe> WinPEASx64.exe> debug.log> ChromeSetup.exe> Exterro FTK Imager.lnk> | IDs\ ----- identities v.20200525 (NTUSER.DAT) Extracts values from Identities key; NTUSER.DAT Identities not found. ----- injectcdll64 v.20200427 (NTUSER.DAT, Software) Retrieve values set to weaken Chrome security Ln 574 Col 8 7 of 42,808 characters 100% Windows (CRLF) UTF-8
```

Flag : IDN FLAG{winPEASx64.exe}



Windows Forensic 14



Dichall ke 14 ditanyakan GUID Dari Device

DISK&VEN_TOSHIBA&PROD_TRANSMEMORY&REV_1.00. disini saya menggunakan tools registry explorer untuk mencari GUID dari device tersebut. Dan setelah mencoba beberapa GUID, akhirnya ada yang correct

Value Name	Type	Data	Value Slack	Is Deleted	Data Record Reallocated
Capabilities	RegWord	0x00000000			
ClassGUID	RegId	{eec5ad98-8080-425f-922a-dabf3de3f69a}	00-00-00-00-00-00		
CompuableIds	RegMultiSz	npdbusmuni\{s\} SVD\Generic	00-00-00-00-00-00		
ConfigFlags	RegWord	0			
ContainerID	RegId	{0d34acee-f10a-5741-b7bd-9d56e5f}	00-00-00-00-00-00		
DeviceDesc	RegId	TransMemory	64-00-65-00-76-02-69-00-63-00-65-0-		
Driver	RegId	{eec5ad98-8080-425f-922a-dabf3de3f69a}	00-00-00-00-00-00		
FriendlyName	RegId	TOSHIBA	66-00-3C-00-25-00-6D-00-69-00-63-		
Mfg	RegId				
Service	RegId	WUDFWipD's			

Flag : IDN_FLAG{eec5ad98-8080-425f-922a-dabf3de3f69a}



Windows Forensic 15



Dichall ke 15 ditanyakan Timestamp
DISK&VEN_TOSHIBA&PROD_TRANSMEMORY&REV_1.00. disini saya membuka file software pada mounting FTK Imager dan diekstrak menggunakan regripper. Disini saya hanya mencari DISK&VEN_TOSHIBA&PROD_TRANSMEMORY&REV_1.00 pada filter find dan didapatkan jawabannya

```
blob (4).txt CrashpadMetrics.prm Variations visited time 00 * Untuk mendap... SOFTWARE software.txt + - ×
File Edit View
cred v.20200427
(system) Checks for Use ^ DISK&VEN_TOSHIBA&PROD_TRANSMEMORY&REV_1.00 x q ↴ ↵ ↶ ↷ ×
UseLogonCredential value NOT found.
-----
dfrupnp v.20200525
(System) Parses data from networked media streaming devices
ControlSet001\Enum\SWD\DAFUPnPProvider not found.
devclass v.20200525
(System) Get USB device info from the DeviceClasses keys in the System hive
DeviceClasses - Disks
ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
2025-05-03 04:00:56
Disk&Ven_TOSHIBA&Prod_TransMemory&Rev_1.00,7427EA2C39F2CFB0E0080DC1&0
2025-05-03 03:44:25Z
Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07,KRVZQBF&0
DeviceClasses - Volumes
ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

-----
Ln 42203, Col 45 42 of 5,375,437 characters 100% Windows (CRLF) UTF-8
```

Flag : IDN_FLAG{ 2025-05-03 04:00:56}



Forensic

Jadi gini...

Deskripsi :

ngomongin crypto, selain encryption itu ada apa lagi ya ?

Author: Aditya Firman Nugroho

Lampiran :

Solusi :

“ Diberikan sebuah material.png yg berisi sebuah gambar idn, karna ini sebuah gambar lalu saya coba untuk melihat metadatanya menggunakan exiftool dan didapatkan sebuah flag pada comment nya”

```
[hisoka@H3H3H3] - [/Downloads] - [Sun May 11, 17:46]
[$] <> exiftool material.png | tail - 5
==> standard input <==
Chromaticity Colorant      : Unknown
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
```

Flag : IDN_CTF{W0W_wh4T_K03NC1D3CE}



QRIS

Deskripsi :

2 kali

Author : Mohamad Fattyr

Lampiran :

Solusi :

“ Diberikan sebuah barcode, lalu saya coba scan menggunakan web <https://www.imagetotext.info/barcode-scanner> lalu di dapatkan sebuah text base64 “U1VST1gwWk1RVWQ3VmpOU04xOWxORk0zWDFJaE9VaFVmUT09” lalu saya decode menggunakan cyberchef sebanyak 2x kali sesuai dengan deskripsinya lalu didapatkan sebuah flag”

The screenshot shows the CyberChef interface with two parallel decoders. Both decoders are set to 'From Base64' mode, with the alphabet set to 'A-Za-zA-Z0-9+='. The top decoder has 'Remove non-alphabet chars' checked. The input field contains the Base64 string 'U1VST1gwWk1RVWQ3VmpOU04xOWxORk0zWDFJaE9VaFVmUT09'. The output field shows the decoded result: 'IDN_FLAG{V3R7_e4S7_R!9HT}'. The bottom decoder also has 'Remove non-alphabet chars' checked and shows the same input and output.

Flag : IDN_FLAG{V3R7_e4S7_R!9HT}



Browser Forensic

Browser Forensic 1

Challenge 169 Solves X

Browser Forensic 1

10

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}

Auhor: Aditya Firman Nugroho

[browser.zip](#)

Flag Submit

Diberikan sebuah soal browser forensic 1, dikategori ini saya menggunakan sqllite viewer <https://inloop.github.io/sqlite-viewer/>

Untuk chall ini saya membuka file history pada folder default dan didapatkan user mencari tools pada database tersebut

SQLite Viewer
view sqlite file online

Drop file here to load content or click on this box to open file dialog.

keyword_search_terms (6 rows)

SELECT * FROM 'keyword_search_terms' LIMIT 0,30

Execute

keyword_id	url_id	term	normalized_term
2	1	vpn browswer	vpn browswer
2	6	netflix	netflix
2	9	bagaimana mencari pasangan	bagaimana mencari pasangan
2	22	extension vpn	extension vpn
2	27	lolbas	lolbas
2	29	mimikatz github	mimikatz github

Flag : IDN_FLAG{mimikatz}



Browser Forensic 2

Challenge 157 Solves X

Browser Forensic 2

10

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

Flag Submit

Diberikan sebuah pertanyaan Website apa yang dicari oleh user berkaitan dengan Teknik Persistence, Privilage Escalation, DLL Injection etc. Chall ini masih berkaitan sama chall sebelumnya, disini saya mencari dimana user mendapatkan atau mencari lolbas dan didapatkan hasilnya di file database history

12 https://www.muslima.co...	Muslim Matrimonials at ...	1	0	1339072
13 https://sso-terra.clickoce...	Muslim Matrimonials at ...	1	0	1339072
14 https://www.muslima.co...	Muslim Matrimonials at ...	1	0	1339072
15 https://www.muslima.co...	Muslim Matrimonials at ...	1	0	1339072
16 https://www.googleleader...	Muslim Matrimonials at ...	1	0	1339072
17 https://www.muslima.co...	Muslim Matrimonials at ...	1	0	1339072
18 https://sso-terra.clickoce...	Muslim Matrimonials at ...	1	0	1339072
19 https://www.muslima.co...	Muslim Matrimonials at ...	1	0	1339072
20 https://www.muslima.co...	Muslim Matrimonials at ...	1	0	1339072
21 https://www.cermati.com...	Cara Ampuh Temukan Pa...	1	0	1339072
22 https://www.google.com...	extension vpn - Google S...	1	0	1339072
23 https://chromewebstore....	Free VPN for Chrome - V...	1	0	1339072
24 https://www.cnnindonesia....	7 Cara Memilih Pasangan...	1	0	1339072
25 https://www.filma.com/r...	7 Cara Menemukan Pasa...	1	0	1339072
26 https://www.filma.com/r...	7 Cara Menemukan Pasa...	1	0	1339072
27 https://www.google.com...	lolbas - Google Search	1	0	1339072
28 https://lolbas-project.github.io/		1	0	1339072
29 https://lolbas-project.github.io/	lolbas - Googl...	1	0	1339072
30 https://github.com/Parro...	Github - ParrotSec/mimi...	1	0	1339072

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



Browser Forensic 3

Challenge 160 Solves X

Browser Forensic 3

10

Ada Violation 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

[Flag](#) [Submit](#)

Diberikan sebuah pertanyaan Streaming Website yang ditonton oleh user. Disini masih berkaitan dengan file history, karena user mencari netflix pada gambar yang ada pada challenge 1 maka bisa disimpulkan Streaming Website yang ditonton oleh user adalah netflix

2	https://chromewebstore....	Browsec VPN - Free VPN ...	1	0
3	https://accounts.google.c...	Browsec VPN - Free VPN ...	1	0
4	https://chromewebstore....	Browsec VPN - Free VPN ...	1	0
5	https://chromewebstore....	Browsec VPN - Free VPN ...	1	0
6	https://www.google.com...	netflix - Google Search	1	0
7	https://www.netflix.com/	Netflix Indonesia - Watch...	1	0
8	https://www.netflix.com/...	Netflix Indonesia - Watch...	1	0
9	https://www.google.com...	bagaimana mencari pasa...	1	0
10	https://www.fimela.com/r...	7 Cara Menemukan Pasa...	1	0
11	https://www.googleleader...	Muslim Matrimonials at ...	1	0
12	https://www.muslima.co...	Muslim Matrimonials at ...	1	0
13	https://sso-terra.clickoce...	Muslim Matrimonials at ...	1	0
14	https://www.muslima.co...	Muslim Matrimonials at ...	1	0
15	https://www.muslima.co...	Muslim Matrimonials at ...	1	0
16	https://www.googleleader...	Muslim Matrimonials at ...	1	0

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



Browser Forensic 5

Challenge 114 Solves X

Browser Forensic 5

10

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

(Filennya 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

Flag Submit

Diberikan sebuah pertanyaan Visit Duration di Website yang berkaitan dengan Persistence, Privilage Escalation, DLL Injection, disini saya menyimpulkan bahwa chall ini masih berkaitan dengan file history. Untuk melihat visited time karena disini saya tidak terlalu mengerti database saya memakai chatgpt untuk membuat kode atau script yang dijalankan di sqlite viewer

```
SELECT
    urls.url AS visited_website,
    datetime((visit_time/1000000)-11644473600, 'unixepoch')
    AS visit_time,
    visit_duration / 1000000.0 AS duration_seconds,
    strftime('%H:%M:%f', visit_duration / 1000000.0,
    'unixepoch') AS duration_flag_format
FROM
    visits
JOIN
    urls ON visits.url = urls.id
ORDER BY
    visit_time DESC
LIMIT 30;
```

Dan didapatkan hasilnya

The screenshot shows a SQLite database viewer interface. On the left, there is a SQL query window containing the provided SELECT statement. On the right, there is a results window displaying a table with four columns: visited_website, visit_time, duration_seconds, and duration_flag_format. The results show several rows of data, with the last two rows being identical (https://www.filela.com/relationship/read/5225982... and https://www.filela.com/relationship/read/5225982...). The duration_flag_format column for the first row is 00:00:18.911, and for the last two rows, it is 00:00:00.000.

visited_website	visit_time	duration_seconds	duration_flag_format
https://github.com/ParrotSec/mimikatz	2025-05-03 05:38:14	18.910599	00:00:18.911
https://www.google.com/search?q=mimikatz+gith...	2025-05-03 05:38:12	2.260442	00:00:02.260
https://lolbas-project.github.io/	2025-05-03 05:38:00	32.509459	00:00:32.509
https://www.google.com/search?q=lolbas&og=lol...	2025-05-03 05:37:58	2.345343	00:00:02.345
https://www.filela.com/relationship/read/5225982...	2025-05-03 05:37:49	0	00:00:00.000
https://www.filela.com/relationship/read/5225982...	2025-05-03 05:37:25	0	00:00:00.000

Flag : IDN_FLAG{00:00:32.509}

Browser Forensic 6



Diberikan pertanyaan Email yang digunakan pada browser, untuk mencari email disini saya membuka file local state dan mencari gmail, dan didapatkan hasilnya

Flag : IDN FLAG{ghxyssforunfun@gmail.com}



Browser Forensic 8

Challenge 135 Solves ×

Browser Forensic 8

10

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensik 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}

Auhor: Aditya Firman Nugroho

Diberikan sebuah pertanyaan url favicon, di website yang dicari oleh user ? (tidak berkaitan dengan hacker !!!), disini saya membuka file favicons yang ada pada folder default di sqllite viewer dan didapatkan urlnya

The screenshot shows the SQLite Database Browser interface. On the left, there's a tree view of tables: 'Tables' (favicon_bitmaps, favicons, icon_mapping, meta), 'Views' (None), 'Triggers' (None), and 'Indices' (None). The 'favicons' table is selected. The main area displays the data in the 'favicons' table:

	id	url	ico
1	1	https://ssl.gstatic.com/chrome/webstore/images/icon_4...	
2	2	https://assets.netflix.com/us/ffe/site/common/icons/i...	
3	3	https://www.muslima.com/lp/paid-search/terra-assets/l...	
4	4	https://github.githubassets.com/favicon/favicon.svg	
5	5	https://www.google.com/favicon.ico	
6	6	https://lolbas-project.github.io/assets/favicon.png	

On the right, the 'Selection' tab shows the current row selected: id=3, url='https://www.muslima.com/lp/paid-search/terra-assets/images/favicon-8b7d9ccfa1-3.ico', and icon_type=1.

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



Browser Forensic 9

Challenge 145 Solves X

Browser Forensic 9

10

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

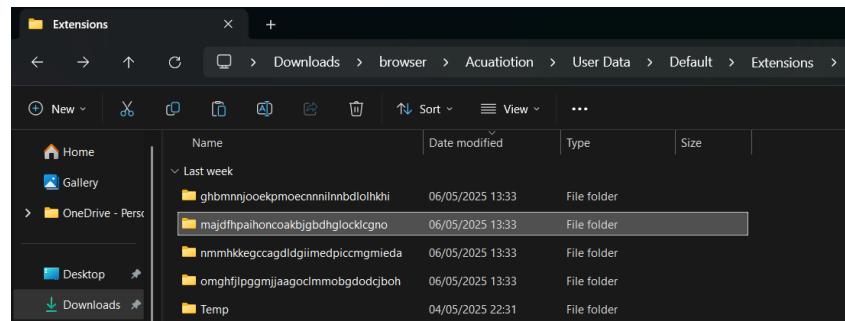
(Filennya ada di pertanyaan pertama)

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

format flag : IDN_FLAG{Jawaban yang disoal}

Auhor: Aditya Firman Nugroho

Diberikan sebuah pertanyaan extension id dengan icon salah satu vpn yang diinstall V.. ! disini saya membuka folder default dan masuk ke folder extension. Terlihat ada beberapa nama folder dengan huruf acak, yang ternyata itu merupakan extension id yang dimaksud dalam pertanyaan dan ditemukan jawabannya



Flag : IDN_CTF{majdfhpaihoncoakbjgbdhglocklcgno}