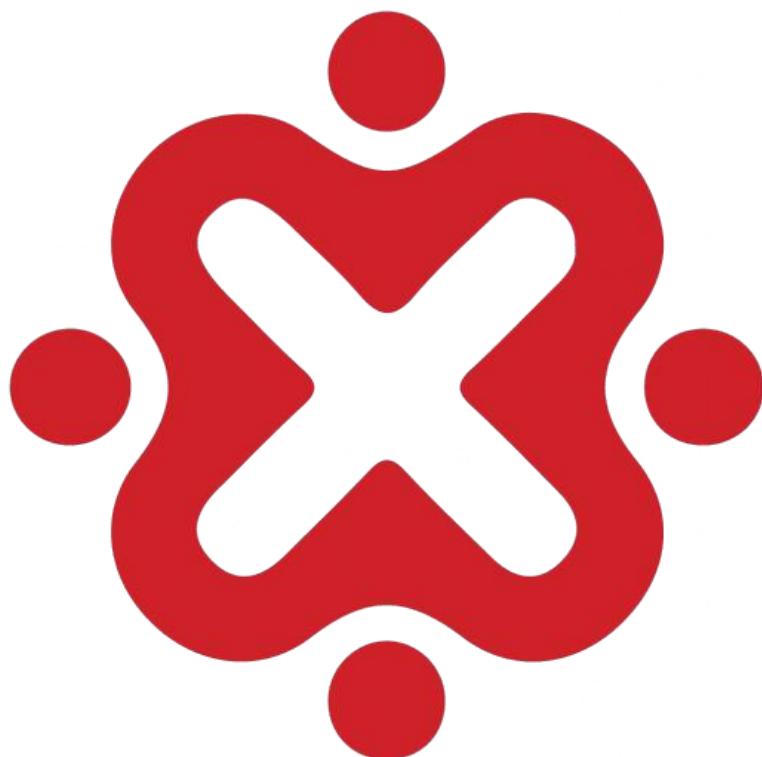




Team Hore  
Terobos aja walau sendiri



**ID-Networkers**  
Indonesian IT Expert Factory



## Daftar Isi

Daftar Isi.....	2
Introduction Team .....	4
Detail Challenge Solved.....	5
A. Welcome Flag.....	5
1) Forgot Encode .....	5
B. Forensic .....	7
1) jadi gini.....	7
2) QRIS.....	8
C. Web 303 .....	9
1) DOM-Based XSS .....	9
2) Unsafe eval() .....	10
5) Client-Side Privilege Escalation.....	14
D. Cryptography.....	17
1) jadi gini lgi.....	17
2) Might Guy's Secret.....	19
3) Rot1Aoka .....	20
4) Pramuka.....	21
5) Classic Cryptography .....	22
E. USB Forensic .....	24
1) USB Forensic 1 .....	24
F. Web Exploit.....	32
1) Hidden Buy Flag .....	32
2) Konoha Breach.....	33
3) ID-Networkers.....	34
4) Kue Monster.....	35
7) I'm Not Me, You Are Me.....	38
8) Circle Clicker .....	39
9) Xss.....	40



10) Awesome Website.....	41
11) Casino 777.....	43
G. Other.....	44
1) User Guide .....	44
H. Browser Forensic.....	45
1) Browser Forensic 1.....	45
2) Browser Forensic 2.....	46
3) Browser Forensic 3.....	47



## Introduction Team

Nama Team : Team Hore

Anggota : Muhammad Mukhlis Robani



## Detail Challenge Solved

### A. Welcome Flag

#### 1) 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:

```
Vm0wd2VHUXhUWGhYV0d4VIYwZG9iMVJVU2pSVlZsbDNWMnQwYUZKc2NGWI  
ZWM1IzWVRBeFdHVkVSbHBoTVZwUVZrUkdXbVF5U2tWWGJHUnBWa1phTmxav  
VNqUlRNRFZ6Vj1V1ZXS1ZXbFZWYWs1dlVsWmtjbFp0Um10TIYxS1lWbTAxVTJGR  
1NsbFJiRkpWVm0xb1ExUldXbXRXTVdSMFpFWmtUbUpGY0ZsWFZFSlhWVEZSZU  
ZOWWJGWmlSa3BoV1d0a2IyUnNiSEZTYlhSc1ZqQTFTbFl5TVVkvWJGcFZWbXhv  
jJKSFVqWIViRnByVm1zeFzsZHJPVmRpU0VKWVYxZDRVMVp0VVhoavJtUllZbX  
MxV1ZadGVFdE5SbkJXVmxB2FGSXdjRWRaTUdoVFYwWmFjMk5JUmxWV2JIQX  
pxWHBLUzFJeVJrZFdiV2hvVFVoQ01sWnRNREZrTWsxM1RWWmtZVkpXV2xWWI  
ZFNVRWREZhY1ZKcmRGU1NiRVl6Vmxkek5WZEdXbFZSYWxKV1RXcFdjbFl5TVV  
0VFJsWnpZVWRHVjJWcldtOVdiR1EwVVRGYVZrMVZWazVTUkVFNQ==
```

Author: Rafly Permana

Lampiran :

The screenshot shows a terminal window with two tabs: 'Input' and 'Output'.  
In the 'Input' tab, there is a large amount of encoded base64 text.  
In the 'Output' tab, the decoded text is shown: "Welcome to your new meta friend. Flag: IDN\_CTF{base64\_in\_action\_but\_7\_times}"



Solusi :

Dari pernyataan yang ada di deskripsi bahwa pesan tersebut merupakan pesan yang di encoding yang dimana seseorang tersebut lupa sudah berapa kali dia melakukannya. Berarti dari pernyataan diatas bahwasannya pesan encoding tersebut adalah encoding berlapis. Jadi untuk menyelesaikan permasalahan di atas saya melakukan decoding menggunakan tools CyberChef dengan base64 karena ciri pesannya ada simbol “==”. Lalu saya melakukan decode berulang kali dan ternyata setelah melakukan berulang kali FLAGnya muncul. Saya melakukan decodenya sebanyak 7 kali.

Flag : IDN\_CTF{base64\_in\_action\_but\_7\_times}



## B. Forensic

1) jadi gini...

Deskripsi :

ngomongin crypto, selain encryption itu ada apa lagi ya?

material.png

Lampiran :

```
File Actions Edit View Help
root@kali: /home/kali/Downloads
Primary Platform : Microsoft Corporation
CMM Flags : Not Embedded, Independent
Device Manufacturer :
Device Model :
Device Attributes : Reflective, Glossy, Positive, Color
Rendering Intent : Perceptual
Connection Space Illuminant : 0.9642 1 0.82491
Profile Creator : Little CMS
Profile ID : 0
Profile Description : sRGB IEC61966-2.1
Profile Copyright : No copyright, use freely
Media White Point : 0.9642 1 0.82491
Chromatic Adaptation : 1.04788 0.02292 -0.05022 0.02959 0.99048 -0.01707 -0.00925 0.01508 0.75168
Red Matrix Column : 0.43604 0.22249 0.01392
Blue Matrix Column : 0.14305 0.06061 0.71391
Green Matrix Column : 0.38512 0.7169 0.09706
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Chromaticity Channels : 3
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
```

Solusi :

Dari pernyataan di atas menyatakan bahwa cluenya adalah berbicara tentang aspek crypyography selain enkripsi ada apa saja?. Jadi dari pernyataan di atas saya bahwa selain enkripsi masih ada hashing atau steganografi. Oleh karena itu saya menggunakan terminal di kali linux dan menggunakan tools exiftool untuk mengecek metadata pada file foto .png tersebut. Setelah saya cek terdapat sebuah comment dengan deskripsi FLAG.

Flag : IDN\_CTF{W0W\_wh4T\_K03NC1D3CE}



## 2) QRIS

Deskripsi :

2 kali

forensic.jpeg

Lampiran :

The screenshot shows the CyberChef interface with two sections: 'Input' and 'Output'. In the 'Input' section, the base64 encoded string 'U1VST1gwWk1RVWQ3VmpOU04xOWxORk0zWDFJaE9VaFVmUT09' is pasted. Below the input field, there are decoding parameters: 'ABC 48', '1', and '0 → 46 (46 selected)'. In the 'Output' section, the decoded result is shown as 'IDN\_FLAG{V3R7\_e4S7\_R!9HT}'.

Solusi :

Dari pernyataan di atas memberikan sebuah clue 2 kali dan terdapat file forensic.jpeg. Selanjutnya saya membuka file tersebut yang ternyata sebuah foto barcode. Setelah saya scan ternyata muncul sebuah kode pesan seperti ini “U1VST1gwWk1RVWQ3VmpOU04xOWxORk0zWDFJaE9VaFVmUT09”. Setelah itu saya mendapatkan kodennya lalu saya melakukan decode dengan tools CyberChef dengan base64. Saya melakukannya sebanyak 2 kali sesuai dari cluenya dan setelahnya muncul sebuah FLAG yang telah di decode.

Flag : IDN\_FLAG{V3R7\_e4S7\_R!9HT}



## C. Web 303

### 1) DOM-Based XSS

Deskripsi :

[https://ctf.solusiber.com/web\\_101/lab1/](https://ctf.solusiber.com/web_101/lab1/)

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran :

The image shows two side-by-side screenshots. On the left is a web browser displaying a challenge titled 'Lab 1: DOM-Based XSS'. It has a text input field containing the XSS payload: <img src=x onerror="document.getElementById('resu...'. The user has entered their name and clicked the 'Greet Me' button. The resulting message in the box below is: 27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn. On the right is a screenshot of CyberChef, a tool for decoding and encoding messages. The 'Input' section shows the encoded flag: 27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn. The 'Output' section shows the decoded flag: IDN\_CTF{dom\_based\_xss\_executed}.

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa tantangannya berupa DOM\_Based XSS dan Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana. Pertama saya membuka websitenya dan melakukan payload XSS dengan event handler di tag HTML ke bagian textfield dan mengklik tombol Greet Me untuk memunculkan FLAG dan setelah saya klik ternyata sebuah pesan yang di encode yang muncul. Setelahnya saya memahami cluenya bahwa encodenya sama dengan bitcoin dan solana. Ternyata encodingnya menggunakan base58. Berarti setelah saya dapat pesan dari XSSnya, selanjutnya saya decode menggunakan base58 dengan tools CyberChef.

Flag : IDN\_CTF{dom\_based\_xss\_executed}



## 2) Unsafe eval()

Deskripsi :

[https://ctf.solusiber.com/web\\_101/lab2/](https://ctf.solusiber.com/web_101/lab2/)

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran :

The image shows two side-by-side screenshots. On the left, a modal window titled 'ctf.solusiber.com says' displays a base64-encoded string: '8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc'. Below this is a text input field containing 'alert(FLAG)' and a 'Run' button. On the right, a terminal window titled 'Input' shows the same base64-encoded string. The terminal window has tabs labeled 'Input' and 'Output'. The 'Output' tab shows the decoded result: 'IDN\_CTF{you\_used\_eval\_successfully}'.

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa tantangannya berupa Unsafe eval yang artinya di JavaScript, aplikasi memakai fungsi eval() untuk mengeksekusi input dari user. Lalu Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana. Pertama saya membuka websitenya dan melakukan payload ke bagian textfield untuk memunculkan popup FLAG. Setelah saya payload ternyata ada sebuah pesan yang di encode yang muncul. Setelahnya saya memahami cluenya bahwa encodenya sama dengan bitcoin dan solana. Ternyata encodingnya menggunakan base58. Berarti setelah saya dapat pesannya, selanjutnya saya decode menggunakan base58 dengan tools CyberChef.

Flag : IDN\_CTF{you\_used\_eval\_successfully}



### 3) Prototype Pollution Demo

Deskripsi :

[https://ctf.solusiber.com/web\\_101/lab3/](https://ctf.solusiber.com/web_101/lab3/)

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran :

The screenshot shows two panels. The left panel is a web application titled "Lab 3: Prototype Pollution Demo". It has a text input field containing JSON code that adds an "\_\_proto\_\_" property to an object. Below it is a blue "Update Config" button. A message box below the button says "Config updated" followed by the JSON payload and a success message. The right panel is a terminal window titled "Input" showing the encoded flag, and "Output" showing the decoded flag.

```
Input
ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgys

Output
IDN_CTF{prototype_pollution_success}
```

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa tantangannya berupa Prototype Pollution Demo. Lalu Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana. Pertama saya membuka websitenya dan melakukan payload ke bagian textfield untuk memunculkan popup FLAG. Setelah saya payload dengan JSON ternyata ada sebuah pesan yang di encode yang muncul. Setelahnya saya memahami cluenya bahwa encodenya sama dengan bitcoin dan solana. Ternyata encodingnya menggunakan base58. Berarti setelah saya dapat pesannya, selanjutnya saya decode menggunakan base58 dengan tools CyberChef.

Flag : **IDN\_CTF{prototype\_pollution\_success}**



## 4) JWT Token Manipulation

Deskripsi :

[https://ctf.solusiber.com/web\\_101/lab4/](https://ctf.solusiber.com/web_101/lab4/)

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran :

The screenshot shows the jwt.io interface. On the left, under 'HEADER: ALGORITHM & TOKEN TYPE', there is a JSON object: { "alg": "none", "typ": "JWT" }. Under 'PAYLOAD: DATA', there is another JSON object: { "role": "admin" }. On the right, the 'JSON WEB TOKEN' section displays the token: eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJyb2xlIjoiYWRtaW4ifQ. Below the token, a note says 'This is an Unsecured JWT as defined by [Section 6 of RFC 7519](#)'. A 'Generate example' button is at the top right.

The screenshot shows a challenge titled 'Lab 4: JWT Token Manipulation'. It has a text input field containing the forged JWT token: eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJyb2xlIjoiYWRtaW4ifQ.. Below it is a 'Decode Token' button. To the right, there's a terminal window showing the decoded token: Header: { "alg": "none", "typ": "JWT" } \n\n Payload: { "role": "admin" } \n\n Admin access granted! Flag: FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY. The terminal also shows 'Input' and 'Output' fields.

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa tantangannya berupa JWT Token Manipulation. Lalu Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana. Pertama saya membuka websitenya dan melakukan pengecekan di source code dan ternyata dari script tersebut, bahwa server tidak memverifikasi signature JWT, jadi bisa dilakukan forge token sendiri. Selanjutnya saya membuat token JWOT dengan tools jwt debugger. Setelah saya mendapatkan token encodenya saya melakukan payload ke bagian textfield untuk memunculkan popup FLAG. Setelah saya payload dengan krim JWOT token ternyata ada sebuah pesan yang di encode yang muncul. Setelahnya saya memahami cluenya bahwa encodenya sama dengan bitcoin dan solana. Ternyata encodingnya menggunakan base58.



Berarti setelah saya dapat pesannya, selanjutnya saya decode menggunakan base58 dengan tools CyberChef.

Flag : IDN\_CTF{jwt\_token\_manipulated}



## 5) Client-Side Privilege Escalation

Deskripsi :

[https://ctf.solusiber.com/web\\_101/lab5/](https://ctf.solusiber.com/web_101/lab5/)

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran :

The screenshot shows a browser window with two main sections: 'Input' and 'Output'. The 'Input' section contains a long string of characters: 'r recipe 2DvT8boTciwZu4ZctauqBoqJaMKWk8xbK5mAmgPqCTjQ9NX2xGEGgGHxFAl'. The 'Output' section shows the decoded flag: 'IDN\_FLAG{client\_side\_privilege\_escalation}'. To the right, there's a panel titled 'Lab 5: Client-Side Privilege Escalation'. It says 'Check your current role and try to access the protected content.' A message box shows 'Current Role: admin' and a blue button labeled 'Show Protected Content'. Another message box displays the flag: 'Welcome, mighty admin! Here is your confidential flag: 2DvT8boTciwZu4ZctauqBoqJaMKWk8xbK5mAmgPqCTjQ9NX2xGEGgGHxFAl'. A hint at the bottom says 'Hint: Try to manipulate your role by editing LocalStorage in the browser console.'

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa tantangannya berupa Client-Side Privilege Escalation. Lalu Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana. Pertama saya membuka websitenya dan langsung mengklik tombol show protected content. Setelah saya klik ternyata ada sebuah pesan yang di encode yang langsung muncul. Setelahnya saya memahami cluenya bahwa encodenya sama dengan bitcoin dan solana. Ternyata encodingnya menggunakan base58. Berarti setelah saya dapat pesannya, selanjutnya saya decode menggunakan base58 dengan tools CyberChef.

Flag : **IDN\_FLAG{client\_side\_privilege\_escalation}**



## 6) Timing Attack

Deskripsi :

[https://ctf.solusiber.com/web\\_101/lab6/](https://ctf.solusiber.com/web_101/lab6/)

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran :

The screenshot shows two side-by-side interfaces. On the left is a web-based challenge titled "Lab 6: Timing Attack". It contains a text input field with "password123", a blue "Guess" button, and a message below stating "Correct! Flag: NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA". On the right is a screenshot of the CyberChef tool. The "Input" pane shows the encoded flag "NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA". The "Output" pane shows the decrypted flag "IDN\_CTF{timing\_attack\_successful}".

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa tantangannya berupa Timing Attack. Lalu Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana. Pertama saya membuka websitenya dan mengidentifikasi source codenya. Setelah saya cek terdapat sebuah script "secretPassword = 'password123';" dan saya mencoba memasukkan script tadi ke textfield dan mengklik tombol guess. Setelah saya klik ternyata ada sebuah pesan yang di encode yang langsung muncul. Setelahnya saya memahami cluenya bahwa encodenya sama dengan bitcoin dan solana. Ternyata encodingnya menggunakan base58. Berarti setelah saya dapat pesannya, selanjutnya saya decode menggunakan base58 dengan tools CyberChef.

Flag : IDN\_CTF{timing\_attack\_successful}



## 7) Unsafe Deserialization

Deskripsi :

[https://ctf.solusiber.com/web\\_101/lab8/](https://ctf.solusiber.com/web_101/lab8/)

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Lampiran :

ctf.solusiber.com says

4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNeEYk

OK

{"run": "alert(FLAG)"}

Load Data

Input

4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNeEYk

Output

IDN\_CTF{unsafe\_deserialization\_executed}

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa tantangannya berupa Unsafe Deserialization. Lalu Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana. Pertama saya membuka websitenya dan mengidentifikasi source codenya. Setelah di cek saya melakukan eksekusi payload sederhana dengan kode javascript di dalam JSON untuk memnunculkan FLAGnya. Setelah saya eksekusi ternyata ada sebuah pesan yang di encode yang langsung muncul. Setelahnya saya memahami cluenya bahwa encodenya sama dengan bitcoin dan solana. Ternyata encodingnya menggunakan base58. Berarti setelah saya dapat pesannya, selanjutnya saya decode menggunakan base58 dengan tools CyberChef.

Flag : IDN\_CTF{unsafe\_deserialization\_executed}



## D. Cryptography

1) jadi gini lgi...

Deskripsi :

mau coba-coba aja terus, coba maen dino

jhlzhy.zip

Lampiran :

```
(kali㉿kali)-[~/Downloads]
$ exiftool jhlzhy.jpg
ExifTool Version Number : 13.10
File Name : jhlzhy.jpg
Directory : .
File Size : 254 kB
File Modification Date/Time : 2025:04:22 10:59:56-04:00
File Access Date/Time : 2025:05:08 07:45:59-04:00
File Inode Change Date/Time : 2025:05:08 07:45:59-04:00
File Permissions : -rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.02
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Comment : YnVrYW4gZGlzaW5pIGtv
Image Width : 2048
Image Height : 1361
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 2048x1361
Megapixels : 2.8
```

```
(kali㉿kali)-[~/Downloads]
$ echo "YnVrYW4gZGlzaW5pIGtv" | base64 -d
bukan disini ko
```

```
(root㉿kali)-[~/home/kali/Downloads]
# steghide extract -sf jhlzhy.jpg
Enter passphrase:
wrote extracted data to "flag.txt".

(kali㉿kali)-[~/home/kali/Downloads]
#
```

```
(root㉿kali)-[~/home/kali/Downloads]
# cat flag.txt
PKU_JAM{ZalNhU0_Jv0sly}
```



The screenshot shows the dCode Caesar Cipher tool interface. On the left, there's a search bar and a results section displaying three decoded messages based on different shift values. On the right, there's a Caesar Cipher Decoder section where a ciphertext is input and a button to perform a brute-force decryption.

**Search for a tool**

★ SEARCH A TOOL ON DCODE BY KEYWORDS:  
e.g. type 'caesar'

★ BROWSE THE FULL DCODE TOOLS' LIST

**Results**

Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.

↑↑	↑↑
→7 (←19) IDN_CTF{SteGaN0_Co0ler}	
→9 (←17) GBL_ARD{QrcEyL0_Am0jcp}	
→22 (←4) TOY_NEQ{DepR1Y0_Nz0wpc}	

**CAESAR CIPHER**  
Cryptography > Substitution Cipher > Caesar Cipher

**CAESAR CIPHER DECODER**

★ CAESAR SHIFTED CIPHERTEXT ?  
PKU\_JAM{Za1NhU0\_3v0s1y}

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

Solusi :

Dari pernyataan di atas memberikan sebuah clue bahwa mau coba-coba aja terus, coba maen dino dan adu file jhlzhy.zip. Pertama saya cek dulu file itu apa dan ternyata ada sebuah file foto dengan format .jpeg. Karena di tantangan forensic bagian “jadi gini...” sama sama file foto, jadi saya coba mengecek metadatanya dan terdapat sebuah comment “YnVrYW4gZGlzaW5pIGtv”. Setelahnya saya coba decode dengan base64 dan ternyata hasilnya bukan disitu. Jadi mungkin FLAGnya ada di dalam gambar dengan steganografi. Selanjutnya saya coba ekstrak menggunakan tools steghide dan setelahnya disuruh memasukkan password. Karena tadi ada clue dino saya coba masukkan kata sandi dino akan tetapi salah. Saya coba identifikasi lagi dengan mencari sebuah kata unik dan saya melihat bahwa file .zip tadi bernama “jhlzhy” yang kemungkinan passwordnya. Lalu saya memasukkan password tersebut dan ternyata benar dan setelahnya muncul file ekstrak “flag.txt”. Ketika saya buka flagnya ketemu akan tetapi masih berupa encode. Lalu saya decode flagnya menggunakan Caesar Chipher dan ketemu pesannya.

Flag : **IDN\_CTF{SteGaN0\_Co0ler}**



## 2) 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

Lampiran :

The screenshot shows the Cryptii web application interface. On the left, under 'Ciphertext' view, the encoded message 'QGA\_OTS{v067j1723qk40f5v33z656afwse60kdf67u9606}' is displayed. In the center, the 'DECODE' section is selected, showing 'Vigenère cipher' as the variant. The key input field contains 'idnmantab'. The output on the right, under 'Plaintext' view, shows the decoded message: 'IDN\_CTF{c067j1723pc40c5i33n656asd60cas67i9606}'.

Solusi :

Dari pernyataan di atas bahwa Might Guy mengirimkan sebuah pesan dan pesannya masih berupa pesan yang terencode. Akan tetapi ada clue bahwa "Giovan Battista Bellaso: 1553M: idnmantab" yang setelah diidentifikasi ternyata Giovan Battista Bellaso adalah seorang penemu cipher klasik yang terkenal yaitu yang berarti pesan tersebut terencode menggunakan Vigenère cipher. Lalu ada kata idnmantab yang kemungkinan sebuah key untuk mengencode pesan tersebut. Jadi saya lakukan decode menggunakan tools cryptii dengan Vigenere chiper dan memasukkan keynya idnmantab. Setelahnya didapatkan sebuah FLAG.

Flag : IDN\_CTF{c067j1723pc40c5i33n656asd60cas67i9606}



### 3) Rot1Aoka

Deskripsi :

Clue nya udah jelas kan?

VQA\_SYNT{C3Z4A4F4A\_QH1H\_94F1u}

Lampiran :

The screenshot shows the CyberChef interface with the following steps:

- Input:** VQA\_SYNT{C3Z4A4F4A\_QH1H\_94F1u}
- Operations:** rot 30
- Output:** IDN\_FLAG{P3M4N4S4N\_DU1U\_94S1h}

Solusi :

Dari pernyataan di atas bahwa cluenya Rot1Aoka dengan sebuah pesan terencode. Jadi saya langsung melakukan decode menggunakan tools CyberChef dengan Rot13. Setelah saya lakukan decode langsung muncul sebuah pesan yang terdecode dan FLAG pun ketemu.

Flag : IDN\_FLAG{P3M4N4S4N\_DU1U\_94S1h}



#### 4) Pramuka

Deskripsi :

terjemahan kan pesan tersebut. Format Flag  
IDN\_CTF{\*\*\*\*}

Morse.wav

Lampiran :

The screenshot shows a web-based Morse code decoder. At the top, it says "Morse Decoder". Below that, a message states: "This is an experimental tool for listening to, analysing and decoding [redacted] transmitted to the server, but the connection to the server is encrypted no". It then says: "If you cannot produce your own Morse code sounds then try using my [redacted]". A dropdown menu labeled "Alphabet to decode into" is set to "Latin". To its right, a note says: "All these alphabets can be sent in Morse code". Below this, there's a section for microphone input with buttons for "Listen" (with a microphone icon) and "Stop" (with a square icon). To the right, there's a section for audio file upload with buttons for "Upload" (with a cloud icon) and "Play" (with a play button icon). A note below says: "Or analyse an audio file containing Morse code". Underneath these controls, it says: "Filename: \"morse.wav\"". At the bottom, there's a text area containing the decoded text: "M0RS3C0D3R19HT".

Solusi :

Dari pernyataan di atas bahwa diberikan sebuah file morse.wav. Berarti pada tantangan ini ada sebuah pesan dari kode morse. Jadi saya coba melakukan decode menggunakan morse decoder dan hasilnya “M0RS3C0D3R19HT”. Setelahnya saya submit dengan format flag yang sudah tertera. Akan tetapi setelah saya submit masih salah dan say coba berulang kali masih salah. Saya pun mencoba menganalisis apa yang salah dan ternyata ketemu permasalahannya yaitu pada penulisan formatnya harus ada simbol “\_” untuk penulisan pesannya. Jadi setiap kata saya tambahkan simbol tersebut dan setelah submit jawabanpun benar.

Flag : IDN\_CTF{M0RS3\_C0D3\_R19HT}



## 5) Classic Cryptography

Deskripsi :

Cn knud bqxsnfqzogx. zmc sgd ekzf: HCM\_BSE{xzxx\_xnt\_zqd\_fqdzs}

Lampiran :

The screenshot shows the 'CAESAR CIPHER DECODER' section of the dCode website. The input ciphertext is 'Cn knud bqxsnfqzogx. zmc sgd ekzf'. The decrypted message is 'Do love cryptography. and the flag'. There is also another result listed: 'qb ybir pelcgbtencul. naq gur synt'.

The screenshot shows the 'CAESAR CIPHER DECODER' section of the dCode website. The input ciphertext is 'HCM\_BSE{xzxx\_xnt\_zqd\_fqdzs}'. The decrypted message is 'IDN\_CTF{yayy\_you\_are\_great}'. There are other results listed: 'CXH\_WNZ{suss\_sio\_uly\_alyun}' and 'WRB\_OHT{momm\_mci\_ofs\_ufsoh}'.

Solusi :

Dari pernyataan di atas bahwa pesannya di encode semua dengan metode klasik kriptografi dan pesan tersebut kelihatan menggunakan Caesar Cipher. Saya pun mencoba melakukan decode dengan Bruteforce agar mempercepat mendapatkan pesan tersebut. Setelah melakukan bruteforce saya mendapatkan FLAGnya.

Flag : IDN\_CTF{yayy\_you\_are\_great}



## 6) Simple Substitution Chiper

Deskripsi :

ORF\_EZY{ziol\_ol\_g\_yqsx\_wxz\_lg\_tq\_ln}

Lampiran :

The screenshot shows a search interface for dCode tools, specifically the Mono-Alphabetic Substitution Decoder. The cipher text input field contains "ORF\_EZY{ziol\_ol\_g\_yqsx\_wxz\_lg\_tq\_ln}" with a note that spaces are relevant. The plaintext language is set to English. Under "OTHER DECRYPTION METHODS", the radio button for "KNOWING THE SUBSTITUTION ALPHABET" is selected, with the QWERTYUIOPASDFGHJKLZXCVBNM alphabet listed. The "DECRYPT AUTOMATICALLY" button is visible.

Solusi :

Dari pernyataan di atas bahwa tantangannya berupa simple substitution chiper, yang berarti setiap huruf plaintextnya diganti dengan huruf lain menggunakan substitusi tetap. Jadi saya mencoba dengan mendecodenya dengan Monoalphabetic Substitution Decoder. Setelah saya decode saya menemukan pesannya.

Flag : IDN\_CTF{this\_is\_o\_falu\_but\_so\_ea\_sy}



## E. USB Forensic

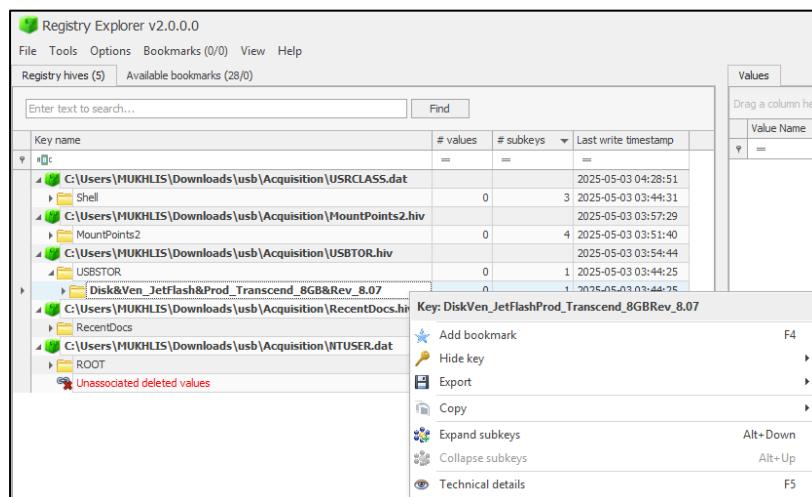
### 1) USB Forensic 1

Deskripsi :

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}

usb.zip

Lampiran :



Solusi :

Dari pernyataan di atas bahwa tantangannya adalah mengidentifikasi merk usb yang digunakan dari hacker untuk delivery filenya. Jadi pertama saya download file zipnya dan mengekstraknya. Setelahnya saya menggunakan tools Registry Explorer untuk mengidentifikasinya. Setelah saya masukkan filenya ke Registry Explorer saya mulai identifikasi merk usbnya melalui file USBTOR.hiv dan setelah diidentifikasi didapatkan merk usbnya yaitu, Jet Flash dari produk Transcend dengan kapasitas 8gb. Lalu saya submit sesuai dengan format yang tertera akan tetapi salah. Ternyata harus menambahkan kata USB\_Device di kata terakhirnya dan tantangan terselesaikan.

Flag : IDN\_FLAG{JetFlash\_Transcend\_8GB\_USB\_Device}



## 2) USB Forensic 2

Deskripsi :

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

(Filennya ada di pertanyaan pertama)

ClassGUID Pada USB Hacker ?

format flag : IDN\_FLAG {Jawaban yang disoal}

Lampiran :

Value Name	Value Type	Data	Value Stack
ClassGUID	RegSz	@disk.inf.%disk_devdesc%;Disk drive	00-00-00-00
Capabilities	RegDword	16	
Address	RegDword	6	
ContainerID	RegSz	{11775948-7a76-52b3-9b7-19db3d...}	00-00-00-00-00-00
HardwareID	RegMultiSz	USBSTOR\Disk\USBDisk\RawDiskTranscend_8...	00-00-00-00
CompatibleIDs	RegMultiSz	USBSTOR\Disk\USBDisk\RawDisk	00-00-00-00-00-00
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002b...	00-00-00-00-00-00
Service	RegSz	disk	00-00
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002b...	00-00-00-00-00
Mfg	RegSz	@disk.inf.%manufacturer%{St...	00-00-00-00-00-00
FriendlyName	RegSz	JetFlash Transcend 8GB USB Device	
ConfigFlags	RegDword	0	

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari ClassGUID dari USB hacker tersebut. Jadi saya gunakan lagi registry explorer untuk mengidentifikasinya lagi. Saya cari di file USBTOR.hiv dan didapat dalam folder USBSTOR / Disk&Ven\_JetFlash&Prod\_Transcend\_8GB&Rev\_8.07 / XRVZQBFR&0 dengan value name ClassGUID dan valuenya didapat.

Flag : IDN\_FLAG {4d36e967-e325-11ce-bfc1-08002be10318}



### 3) USB Forensic 3

Deskripsi :

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

(Filennya ada di pertanyaan pertama)

Apa Contaider ID USB Yang dipakai Hacker ?

format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :

Value Name	Value Type	Data	Value Slack
ContainerID	RegSz	{11775948-7a76-52b3-9bc7-19d3487774}	00-00-00-00-00-00
DeviceDesc	RegDword	16	00-00-00-00
Capabilities	RegDword	6	
Address	RegDword		
HardwareID	RegMultiSz	USBSTOR\Disk\USBSTOR\RAVEN\Gen1\...	00-00-00-00
CompatibleIDs	RegMultiSz	USBSTOR\Disk\USBSTOR\RAVEN\Gen1\...	00-00-00-00
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}	00-00-00-00-00-00
Service	RegSz	disk	00-00
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be1031...	00-00-00-00
Mfg	RegSz	@ddk.inf,%genericmanufacturer%\standard	00-00-00-00-00
FriendlyName	RegSz	JetFlesh Transcend 8GB USB Device	
ConfigFlags	RegDword	0	

Type viewer	Slack viewer	Binary viewer
Value name	ContainerID	
Value type	RegSz	
Value	{11775948-7a76-52b3-9bc7-19d3487774}	

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari Contaider ID. Sama seperti di tantangan USB Forensic 2 saya menemukan value name dengan nama Container ID beserta valuenya. Jadi FLAnya ketemu.

Flag : IDN\_FLAG{4d36e967-e325-11ce-bfc1-08002be10318}



## 4) USB Forensic 4

Deskripsi :

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

(Filennya ada di pertanyaan pertama)

Apa Disk ID yang dipakai hacker ?

format flag : IDN\_FLAG {Jawaban yang disoal}

Lampiran :

The screenshot shows the Registry Explorer interface with two panes. The left pane displays a tree view of registry keys under 'Registry hives (5)'. Key paths include 'C:\Users\MUHILIS\Downloads\usb\Acquisition\MountPoints2.hiv', 'C:\Users\MUHILIS\Downloads\usb\Acquisition\NTUSER.dat', 'C:\Users\MUHILIS\Downloads\usb\Acquisition\RecentDocs.hiv', and 'C:\Users\MUHILIS\Downloads\usb\Acquisition\USBTOR.hiv'. The right pane is titled 'Values' and shows a table with columns 'Value Name', 'Value Type', 'Data', and 'Value Slack'. One entry is highlighted: 'DiskId' of type 'RegSz' with data 'a4aaa1f8-27d0-11f0-a0ac-000c2979b63d'. Below the table is a viewer section with tabs for 'Type viewer', 'Slack viewer', and 'Binary viewer', showing the same value name and data.

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari DiskID dari USBnya. Jadi saya mencarinya ke file USBTOR.hiv dan sampai ke folder \Partmgr dan disana terdapat value name dan valuenya. FLAG pun ketemu.

Flag : **IDN\_FLAG{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}**



## 5) USB Forensic 5

Deskripsi :

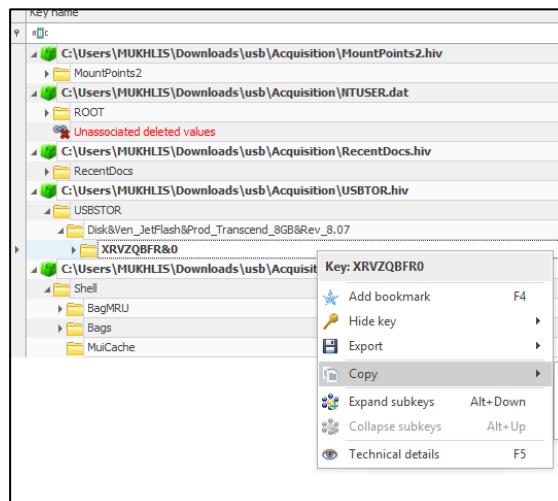
ada hacker, physical acces ke laptop.. bantuin dong !

(Filenya ada di pertanyaan pertama)

Apa Serial ID USB Yang dipakai Hacker ?

format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :



Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari Serial Idnya. Jadi saya masih tetap menggunakan Registry Explorer untuk mencarinya dan ketemu di file USBTOR.hiv seperti pada gambar.

Flag : IDN\_CTF{XRVZQBFR&0}



## 6) USB Forensic 6

Deskripsi :

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

(Filennya ada di pertanyaan pertama)

Nama File Yang ada di USB ?

format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :

The screenshot shows the Registry Explorer interface. In the left pane, there is a search bar with '.txt' typed in and a 'Find' button. Below it, a table lists registry keys. One key, 'FileExts', is expanded, showing several sub-keys including '.txt'. In the right pane, there is a table titled 'Values' with one entry:

Extension	Value Name	Target Name	Link Name
.txt	4fu284428u5984-8308848	4fu284428u5984-8308848	4fu284428u5984-8308848.lnk

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari nama file yang ada di usb. Jadi saya mencarinya di pencarian untuk menemukan kata “.txt” agar mempercepat pencarian. Setelahnya saya mendapatkan nama filenya sesuai yang ada pada gambar yaitu “4fu284428u5984-8308848.txt”.

Flag : IDN\_FLAG{4fu284428u5984-8308848.txt }



## 7) USB Forensic 7

Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong !  
*(Filennya ada di pertanyaan pertama)*  
Direkotry Yang ada di usb ?  
format flag : IDN\_FLAG{Jawaban yang disoal} example : \*:\directory

Lampiran :

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Reallocated
(default)	RegDword	"D:\setup64.exe"			

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari direktori yang ada di USB. Saya menggunakan mencarinya dengan fitur MountPoints2 karena biasanya informasi direktori pada folder tersebut. Setelah saya cek ketemu di AutoRun/command dengan value D:/setup64.exe, setelah saya submit ternyata jawabannya masih salah.

Flag : IDN\_CTF{D:/setup64.exe }



## 8) USB Forensic 8

Deskripsi :

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

(Filennya ada di pertanyaan pertama)

File dibuka pada jam ?

format flag : IDN\_FLAG{Jawaban yang disoal} example : xxxx-xx-xx xx:xx:xx

Lampiran :

The screenshot shows the Registry Explorer interface with a search bar set to '.txt'. The main pane displays a tree view of registry keys under 'C:\Users\MIKHLIS\Downloads\usb\Acquisition'. A tooltip at the bottom right of the window indicates the last write timestamp for a file is 2025-05-03 03:48:32.

Key name	# values	# subkey	Last write timestamp
C:\Users\MIKHLIS\Downloads\usb\Acquisition\RecentDocs.hiv	=	=	2025-05-03 03:57:56
RecentDocs	3	2	2025-05-03 03:48:32
.txt	2	0	2025-05-03 03:48:32
C:\Users\MIKHLIS\Downloads\usb\Acquisition\NTUSER.dat	=	=	2025-05-03 03:48:32
ROOT	0	10	2025-05-03 03:44:06
SOFTWARE	0	6	2025-05-03 03:42:49
Microsoft	0	61	2025-05-03 03:48:33
Windows	0	7	2025-05-03 03:29:37
CurrentVersion	0	57	2025-05-03 04:07:48
Explorer	12	38	2025-05-03 03:49:12
FileExts	0	190	2025-05-03 03:48:20
.txt	0	3	2025-05-03 03:29:08
RecentDocs	3	2	2025-05-03 03:48:32
.txt	2	0	2025-05-03 03:48...

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari jam berapa filenya dibuka. Jadi sama seperti pada USB Forensic 6, saya melakukan pencarian ke kata “.txt” dan melihat pada kolom “Last Write timestamp” bahwa tertera tanggal dan jam berapa filenya diakses.

Flag : IDN\_FLAG{2025-05-03 03:48:32}



## F. Web Exploit

### 1) Hidden 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.

[https://ctf.solusiber.com/buy\\_the\\_flag/](https://ctf.solusiber.com/buy_the_flag/)

Lampiran :

The screenshot shows two side-by-side views. On the left is a screenshot of the browser's developer tools, specifically the Elements tab. It displays the HTML source code of a webpage. A specific line of code is highlighted: <input type="hidden" name="saldo" value="1000000000000000" == \$0. This indicates a hidden input field used for manipulating the balance. On the right is a screenshot of a web application interface titled "Toko Benderaku". It features a header with "Saldo Kamu: Rp100". Below it is a section labeled "Premium Product" with a logo for "CTF CAPTURE THE FLAG". A price of "Harga: Rp10.000.000.000" is shown, along with a blue button labeled "Beli Flag". At the bottom of the page, there is a red warning message: "IDN\_FLAG{h3ader\_wh1telist\_4nd\_p4r4m3ter\_t4mp3rlng\_v3ryy\_3zzz}".

Solusi :

Dari pernyataan di atas bahwa tantangannya cara menemukan celah agar dapat membeli sebuah Flag di dalam website yang tertera. Jadi pertama saya melakukan identifikasi terlebih dahulu ke source kode HTML nya melalui inspect. Ketika setelah di identifikasi ternyata saldo yang tertera dikirim dari sisi klien (browser) melalui hidden input. Yang berarti bisa mengubah value saldo menjadi cukup untuk membeli flagnya. Jadi setelah saya ganti dan saya beli flagnya, FLAG pun didapatkan.

Flag : **IDN\_FLAG{h3ader\_wh1telist\_4nd\_p4r4m3ter\_t4mp3rlng\_v3ryy\_3zzz}**



## 2) 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?

[https://ctf.solusiber.com/login\\_bypass/](https://ctf.solusiber.com/login_bypass/)

Lampiran :

The screenshot shows a login interface with two entries in the database table. The first entry is 'OR 1=1 --' and the second is '.....'. The database table structure is as follows:

NIK	Alamat
9009009009009009	Konoha, Markas Hyuga
Might Guy	089999999999
9009009009009009	Konoha, Jalan Semangat
Tsunade Senju	080808080808
10101010101010	Konoha, Kantor Hokage

Source code snippet from the database table:

```
<td data-label="NIK">9009009009009009</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-...</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}-->
<tr>
<td data-label="Nama Lengkap">Tsunade Senju</td>
<td data-label="Email"><a href="/cdn-cgi/l/email-...</a></td>
<td data-label="No. Telepon">080808080808</td>
<td data-label="NIK">10101010101010</td>
<td data-label="Alamat">Konoha, Kantor Hokage</td>
```

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk menyusup ke sistemnya tanpa login dan menemukan yang tersembunyi yang kemungkinan FLAGnya. Tantangan ini merupakan tipe login bypass dengan memanfaatkan celah klasik pada backendya. Jadi saya mengecek source kodennya dengan inspect. Setelah di cek saya mencoba untuk login dengan username “ OR 1=1 --” dan password “apasaja”. Ternyata setelah saya masukkan username dan passwordnya saya bisa akses flag.php dan saya melakukan pencarian flagnya. Setelah saya lihat tidak ada yang mencurigakan. Jadi saya mencoba melakukan inspect ke bagian source kodennya dan setelah saya amati ketemu sebuah comment FLAGnya.

Flag : IDN\_CTF{c0NRats\_you\_goin\_tohe\_insideee}



### 3) 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.

[https://ctf.solusiber.com/robots\\_dashboard/](https://ctf.solusiber.com/robots_dashboard/)

Lampiran :

The screenshot shows a browser window with the URL `ctf.solusiber.com/robots_dashboard/robots.txt`. The page content is as follows:

```
User-agent: *
Disallow: /asdsa024nsfd01372021.html
```

The screenshot shows a browser window with the URL `ctf.solusiber.com/robots_dashboard/asdsa024nsfd01372021.html`. The page content is as follows:

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

Solusi :

Dari pernyataan di atas bahwa developer terlalu percaya pada "aturan" untuk mesin pencari dan menyembunyikan direktori rahasia dengan harapan crawler tidak melihatnya. Yang berarti ada kemungkinan besar adanya file robots.txt untuk menyembunyikan direktori penting. Jadi pada url saya tambahkan /robots.txt dan setelah di enter muncul sebuah disallow pada halaman webnya. Disallow yang sudah diketahui saya copy dan saya paste ke url dengan mengganti kata robots.txt menjadi kata yang disallow tadi. Setelah saya enter FLAG pun ketemu.

Flag : **IDN\_CTF{@W\*\_FOuN&\_th@\_#|\*\*\$N\_F|@&}**



#### 4) 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 )

[https://ctf.solusiber.com/kue\\_monster/](https://ctf.solusiber.com/kue_monster/)

Lampiran :

```
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 right.

Cookie Value: %7B%22role%22%3A%22admin%22%7D
```

Solusi :

Dari pernyataan di atas bahwa ada clue kue yang berarti ada keterkaitan dengan cookies yang dimana jika di terjemahkan berarti kue. Berarti tantangannya untuk memahami cara kerja cookies pada browser. Jadi saya coba inspect halamannya websitenya dan menuju menu Application dan cookies. Pada bagian cookies terdapat sebuah nama user dan valuenya "%7B%22role%22%3A%22guest%22%7D" yang berarti masih guest atau tamu. Jadi saya ganti valuenya agar menjadi admin. Setelah saya ganti dan refresh halaman websitenya FLAGpun ketemu.

Flag : IDN\_CTF{Y0u\_@rE\_TH@\_C00K|e\_M@st\$r}



## 5) 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!

[https://ctf.solusiber.com/idn\\_edu/](https://ctf.solusiber.com/idn_edu/)

Lampiran :

The screenshot shows a browser window with the URL `ctf.solusiber.com/idn_edu/?page=secret`. The page content includes a dark header with the word 'workers' and a main area containing two warning messages:

```
Warning: include(secret): Failed to open stream: No such file or directory in /var/www/html/index.php on line 29
Warning: include(): Failed opening 'secret' for inclusion (include_path='.:usr/local/lib/php') in /var/www/html/index.php on line 29
```

The screenshot shows a browser window with the URL `ctf.solusiber.com/idn_edu/?page=flag.txt`. The page content includes a dark header with the word 'workers' and a main area containing the text:

```
IDN_CTF{l@tisec_r29-loadr}
```

Solusi :

Dari pernyataan di atas bahwa tantangannya eksloitasi input pengguna yang tidak aman, yang kemungkinan ada file tersembunyi yang dapat diekstrak melalui celah keamanan. Saya melakukan search dengan menambahkan urlnya seperti “?page=secret” untuk melihat apakah ada file yang tersembunyi. Setelah saya masukkan ada sebuah peringatan. Karena ini sebuah CTF dan kemungkinan ada file bernama flag. Jadi saya coba beberapa kali dan setelahnya ketemu dengan flag.txt, jadi FLAGnya ketemu.

Flag : **DN\_CTF{l@tisec\_r29-loadr}**



## 6) 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!



[https://ctf.solusiber.com/search\\_free/](https://ctf.solusiber.com/search_free/)

Lampiran :



Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencoba melakukan manipulasi pathnya. Jadi saya mencoba untuk menambahkan di urlnya beberapa kata sampai berapa kali dan saya terakhir saya mencoba menambahkan “?file=../flag.txt” untuk melihat apakah akan memunculkan sebuah flag, karena ini CTF yang harus mencari sebuah flag dan kemungkinan ada format file bernama flag.txt. Ternyata setelah saya tambahkan FLAGnya ketemu.

Flag : IDN\_CTF{tvec-resolver\_41}



## 7) 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!

[https://ctf.solusiber.com/user\\_information/](https://ctf.solusiber.com/user_information/)

Lampiran :

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

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencoba beberapa ID pada website yang diberikan agar bisa mengakses sesuatu yang seharusnya bukan untuk saya. Jadi pertama-tama saya mengecek source kode nya melalui inspect untuk menganalisisnya. Ternyata sistem memungkinkan saya dapat mengakses data pengguna lain dengan mengganti parameter id di URL. Yang berarti website ini memiliki kelemahan umum yang terjadi jika tidak ada validasi otorisasi. Jadi saya mengganti ID di Url dari 1-10 untuk melihat apakah ada FLAG dan ternyata hanya IDnya hanya sampai 1-5 yang menampilkan informasi dan belum ketemu untuk FLAGnya. Jadi saya coba melakukan brute-force ID sampai 1-100 dan ternyata tidak ada juga. Jadi saya coba analisis ID yang belum saya coba dan karena angka 0 belum saya coba jadi saya coba masukkan dan ternyata FLAGnya ada di ID 0 dan FLAGpun ketemu.

Flag : **IDN\_CTF{Y0u\_FF0D\_the\_heN\_admin}**



## 8) Circle Clicker

Deskripsi :

Click Sampai 1000 kali!  
Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

[https://ctf.solusiber.com/circle\\_clicker/](https://ctf.solusiber.com/circle_clicker/)

Lampiran :

The screenshot shows a browser's developer tools with the 'Console' tab selected. On the left, the source code is visible:

```
Selamat datang di Circle Clicker! Game sederhana atau...?
> revealSecret()
score = 1000;
Selamat! Kamu menemukan fungsi rahasia!
Bagian pertama flag: 5WJoJxz5CCVWDSE
Untuk bagian kedua, coba berfikir sambil bermain click!
< 1000
Luar biasa! Kamu mendapatkan bagian kedua flag: master}
Flag lengkap: 5WJoJxz5CCVWDSEpH4E1n77BT5Fec
Hmm, ini hanya permainan klik biasa?
>
```

On the right, the 'Input' panel contains the string: 5WJoJxz5CCVWDSEpH4E1n77BT5Fec. The 'Output' panel shows the result: IDN\_CTF{click\_master}.

Solusi :

Dari pernyataan di atas bahwa tantangannya disuruh melakukan 1000 klik pada sebuah bulatan untuk memunculkan FLAGnya, akan tetapi jika di klik satu-satu akan lama. Jadi setelah saya analisis source kodennya melalui inspect, bahwa setiap klik skor akan bertambah dan setelah score mencapai 1000 maka FLAG akan muncul, jadi saya menggunakan fungsi javascript rahasia di console browser dengan menambahkan sebuah script seperti di gambar untuk memanipulasi bahwa telah mencapai 1000 klik. Setelah saya masukkan ada muncul sebuah flag yang masih terencode. Dari clue pernyataan diatas bahwa flagnya di encode dengan encoder yang sama dengan bitcoin dan solana yang berarti menggunakan encode base58. Jadi saya menggunakan tools CyberChef untuk melakukan decodenya dan FLAG pun ketemu.

Flag : IDN\_CTF{click\_master}



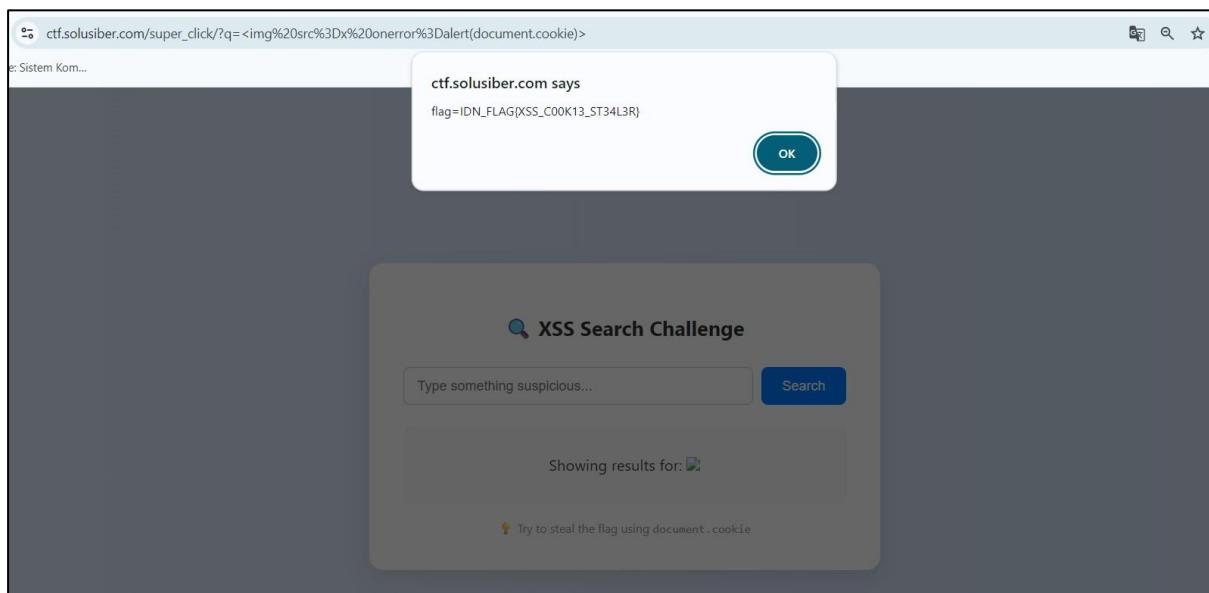
## 9) XSS

Deskripsi :

CURI!

[https://ctf.solusiber.com/super\\_click/](https://ctf.solusiber.com/super_click/)

Lampiran :



Solusi :

Dari pernyataan di atas bahwa tantangannya untuk melakukan pencurian pada website yang diberikan. Jadi pertama saya melihat bagaimana input dari user ditampilkan kembali di halaman, apakah ada tempat upload atau input HTML didalamnya. Setelah saya cek dan saya coba untuk menambahkan pada URL seperti “?q=<script>alert(1)</script>” itu apakah ada popup yang akan keluar dan ternyata tidak. Jadi saya coba lagi dengan menambahkan URL lain seperti “?q=<script>alert(flag)</script>” itu dan ternyata tidak ada hasil. Lalu saya coba lihat pada tampilan websitenya ada tulisan “Try to steal the flag using document.cookie” yang berarti perlu mencari cara agar JavaScript tetap bisa dieksekusi, bukan hanya alert biasa, yang kemungkinan dengan XSS yang disisipkan melalui event handler atau tag selain <script>. Jadi saya coba tambahkan URL lain untuk memunculkan flagnya seperti “?q=<img%20src%3Dx%20onerror%3Dalert(document.cookie)>” dan setelah di enter FLAG pun ketemu.

Flag : IDN\_CTF{this\_is\_o\_falu\_but\_so\_ea\_sy}



## 10) Awesome Website

Deskripsi :

CARI!!

[https://ctf.solusiber.com/awesome\\_website/](https://ctf.solusiber.com/awesome_website/)

Lampiran :

```
295     userAccounts: true,
296     notifications: true
297   },
298
299   // API configuration
300   api: {
301     baseUrl: "https://api.example.com/v2",
302     timeout: 5000,
303     retryAttempts: 3,
304     cacheTTL: 3600,
305     accessToken: "SUROX0ZMQd7VzNCxzN0Q29kM183UjFjazF9" // Access token for API authentication
306   },
307
308   // Analytics configuration
309   analytics: {
310     provider: "GoogleAnalytics",
311     trackingId: "UA-XXXXX-Y",
312     anonymizeIp: true,
313     sessionTimeout: 30
314 }
```

The screenshot shows a browser window with the URL [https://ctf.solusiber.com/awesome\\_website/](https://ctf.solusiber.com/awesome_website/). The page title is "Awesome Website". The navigation bar includes links for HOME, ABOUT, SERVICES, and SETTINGS. The main content area features a large heading "Welcome to Our Amazing Website" and a subtext "We create beautiful and functional websites that help you grow your business". Below the main content is a "Learn More" button. At the bottom of the page, there is a developer console output from the Chrome DevTools. The console shows the following message:  
Failed to load resource: the server responded with a status of 404 ()  
> atob("SUROX0ZMQd7VzNCxzN0Q29kM183UjFjazF9")  
< IDN\_FLAG{W3B\_3NCod3\_7R1ck1}'

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk mencari dan karena ini sebuah CTF berarti untuk mencari sebuah FLAG. Jadi saya buka websitenya dan melakukan inspect pada source codenya untuk melakukan identifikasi. Setelah saya cek ketemu sebuah access Token dengan pesan yang masih terencode. Jadi saya perlu melakukan decode dulu untuk mengetahui isi pesannya. Saya menggunakan console pada browser dengan menggunakan perintah atob untuk melakukan decode. Setelah di decode pesannya pun muncul dan FLAG ketemu.

Flag : **IDN\_FLAG{W3B\_3NCod3\_7R1ck1}**



**ID-Networkers**  
Indonesian IT Expert Factory



## 11) Casino 777

Deskripsi :

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

[https://ctf.solusiber.com/casino\\_777/?debug=true&slot1=7&slot2=7&slot3=7](https://ctf.solusiber.com/casino_777/?debug=true&slot1=7&slot2=7&slot3=7)

Lampiran :

Solusi :

Dari pernyataan di atas bahwa tantangannya untuk melakukan eksplorasi di URL dan memanipulasi nilai slotnya. Jadi saya cek source codenya dan setelah di cek ada parameter query yang dicek di scriptnya. Jadi saya coba tambahkan di URL dengan seperti berikut “?debug=true&slot1=7&slot2=7&slot3=7” yang berfungsi agar mengatur slot1, slot2, slot3 sesuai yang saya berikan di query param. Setelah saya tambahkan ternyata muncul popup dengan kalimat sedikit lagi dan setelah saya oke tidak ada perubahan. Jadi saya coba lakukan spin apakah dengan melakukan spin akan memunculkan flagnya dan ternyata setelah dispin FLAGnya muncul.

Flag : IDN\_CTF{M4st3r\_0f\_H77P\_R3qu3st\_M4n1pul4t10n!}



## G. Other

### 1) User Guide

Deskripsi :

FLAG

Lampiran :

The top screenshot shows a PDF document titled 'User\_Guide\_CTFd\_IDN\_Cyber\_Security[1].pdf'. It contains text about the competition organization and participation. The bottom screenshot shows a Bing search results page for the query 'idn\_flag{makasih\_sudah\_baca\_guide}'. It displays the search bar, search results, and various filters.

Solusi :

Dari pernyataan di atas bahwa keterangannya FLAG dengan kategori other, yang dimana membuat membingungkan. Saya coba cari di source codenya apakah ada FLAG yang kemungkinan diletakkan di comment, ketika saya cek tidak ada dan saya cari lagi di cookies pada bagian inspect siapa tau ada disana. Setelah berpikir cukup lama saya coba buka grup Whatsapp dan disana ada file pdf dengan nama User\_Guide yang saya rasa ada FLAG didalamnya. Jadi saya coba baca satu persatu akan tetapi tidak ada kejanggalan sampai saya gunakan fitur Find untuk menemukan kata yang familiar dengan FLAG dan yahh setelah saya cek sampai ke halaman terakhir ada sesuatu yang janggal dengan warna kuning tanpa kata yang terlihat. Setelah saya coba copy paste ternyata itu FLAG. FLAGnya disembuyikan dengan warna yang diganti menjadi putih agar tidak terlihat. Sangat plottwist.

Flag : IDN\_FLAG{makasih\_sudah\_baca\_guide}



## H. Browser Forensic

### 1) 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}

Lampiran :

```
root@kali: /home/.../browser_dump/Acuatiotion/User Data/Default
# sqlite3 History "SELECT url, title FROM urls ORDER BY last_visit_time DESC;"
```

The terminal window shows the results of a SQLite query on a database named 'History'. The query selects 'url' and 'title' from the 'urls' table, ordered by 'last\_visit\_time' in descending order. The results list several URLs, mostly from Google searches related to 'mimikatz' and 'lolbas-project.github.io'. The output is truncated at the bottom.

Solusi :

Dari pernyataan di atas bahwa keterangannya disuruh melakukan browser forensic sesuai dengan kategorinya. Akan tetapi disuruh melakukan pencarian tools apa yang dicari oleh user. Jadi pada kategori ini saya menggunakan kali linux dengan tools sqlite3. Pertama-tama saya melakukan ekstrak file yang sudah didownload dan masuk ke folder \Default pada folder browser yang sudah di ekstrak. Pada folder \Default saya mencari apakah ada file bernama history secara manual dan ternyata ada, setelah mengetahui ada, jadi saya langsung melakukan pengecekan untuk melihat isi tabel url yang pernah dikunjungi, setelah saya cek ada tools bernama "mimikatz" dan setelah saya submit sesuai dengan format ternyata benar. Jadi flag ketemu.

Flag : **IDN\_FLAG{mimikatz}**



## 2) Browser Forensic 2

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

Website apa yang dicari oleh user berkaitan dengan Teknik Persistence, Privilage Escalation, DLL Injection etc ?

format flag : IDN\_FLAG {Jawaban yang disoal}

Lampiran :

```
[root@kali]~[/home/.../browser_dump/Acuatiotion/User Data/Default]
# sqlite3 History "SELECT url, title FROM urls ORDER BY last_visit_time DESC;"
```

https://github.com/ParrotSec/mimikatz|GitHub - ParrotSec/mimikatz  
https://www.google.com/search?q=mimikatz+github&oq=mimikatz+github&gs\_lcrp=EgZjaHJv  
gCEAAgAQyBwgDEAAgAQyBwgEEAAgAQyBwgFEAAgAQyDQgGEAAYhgMYgAQYigUyDQgHEAAYhgMYgAQY  
rceid=chrome&ie=UTF-8|mimikatz github - Google Search  
https://lolbas-project.github.io/||LOLBAS  
https://www.google.com/search?q=lolbas&oq=lolbas&gs\_lcrp=EgZjaHJvbWUqBwgAEAAgAQyBw  
ABiABDIHCAUQABiABDIJCAYQLhgKGIAEMg8IBxAuGAoYxwEY0QMYgAQyCQgIEAAChiABDIHCAkQABiABN  
|lolbas - Google Search

Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari website yang dicari tetapi berkaitan dengan Teknik Persistence, Privilage Escalation, DLL Injection etc. Jadi sama seperti browser forensic 1, bahwa pada baris dibawahnya ada website LOLBAS yang dimana sangat berkaitan dengan teknik Persistence, Privilage Escalation, DLL Injection etc. FLAG ketemu.

Flag : IDN\_FLAG {https://lolbas-project.github.io/}



### 3) Browser Forensic 3

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

Streaming Website yang ditonton oleh user ?

format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :

```
root@kali: /home/kali/Downloads/browser_dump/Acuatiotion/User Data/Default
File Actions Edit View Help
https://www.fimela.com/relationship/read/5225982/7-cara-menemukan-pasangan-hidup-yang-te|nikah|7 Cara Menemukan Pasangan Hidup yang Tepat agar Tidak Menyesal Setelah Menikah - Re|https://www.google.com/search?q=bagaimana+mencari+pasangan&oq=bagaimana+mencari+pasangan-GDkyCAgBEAAYFhgeMggIAhAAGBYYHjIICAMQABgWGB4yCAgEEAAYFhgeMggIBRAAGBYYHjIHCAYQABjvBTIHAcQ/EyOTQyajBqN6gCALACAA&sourceid=chrome&ie=UTF-8|bagaimana mencari pasangan - Google Search|https://www.netflix.com/|Netflix Indonesia - Watch TV Shows Online, Watch Movies Online|https://www.netflix.com/id-en/|Netflix Indonesia - Watch TV Shows Online, Watch Movies O|https://www.google.com/search?gs_ssp=eJzj4tTP1TcwNC9Ki1dgNGB0YPBiz0stScvJrAAASpUGiw&q=ne|WlInGΔσΔFΔYΔxΔRΔiHΔRiΔxΔRΔxΔRΔiKRTTYCΔΔ0I hhDGTMRGMcRGI EDGNEDGTΔEGTnEMσ0TΔRΔΔG1ECCGTΔEG|
```

Solusi :

Dari pernyataan di atas bahwa keterangannya mencari streaming website yang ditonton dari user. Jadi sama seperti pada browser forensic 1, saya menggunakan fitur FIND untuk mencari website yang familiar dengan streaming seperti Youtube, netflix, disney, vidio, dan lain-lain. Setelah saya cek ternyata ketemu website streaming yang dicari adalah Netflix.

Flag : IDN\_FLAG{https://www.netflix.com/}



## 4) Browser Forensic 4

Deskripsi :

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

(*Filenya ada di pertanyaan pertama*)

Vpn apa saja yang diinstal oleh user ?

format flag : IDN\_FLAG{VPN\_1-VPN\_2} example : IDN\_FLAG{IPSEC\_SECURITY-L2TP\_SECURITY}

Lampiran :

```
ela-mgid-underarticle|7 Cara Menemukan Pasangan Hidup yang Tepat agar Tidak Menyesal Setelah Menikah - Relationship Fimela.com
https://www.cnnindonesia.com/gaya-hidup/20221220155211-289-889807/7-cara-memilih-pasangan-hidup-yang-tepat-agar-tak-menyesal|7 Cara Memilih Pasangan Hidup yang Tepat agar Tak Menyesal
https://chromewebstore.google.com/detail/free-vpn-for-chrome-vpn-p/majdfhpaihoncoakbjgbdhglocklcno?hl=en|Free VPN for Chrome - VPN Proxy VeePN
[Chrome Web Store]
https://www.google.com/search?q=extension+vpn&oq=extension+vpn&gs_lcrp=EgZjaHJvbWUqDAgAEAYFBiHAhiABDIMCAAQABgUGIcCGIAEMgcIARAAGIAEMgcIAhAAGIAEMgcIAEAErgcIBhAAGIAEMgcIBxAAIGIAEMgcICBAAGIAEMgcICRAAGIAE0gEINDY3N2oawajeoAgewAgIxBQGcE6yQTBNK6sourceid=chrome&ie=UTF-8extension vpn - Google Search
https://www.cermati.com/artikel/cara-ampuh-temukan-pasangan-bagi-kamu-yang-masih-single|Cara Ampuh Temukan Pasangan bagi Kamu yang Masih Single
RixAxjRAXiABBiKBTIYCAAQLhhDGIMBGmCBGLEDGNEGDIAEGIoFMg@IARAAGJECGIAEGIoFMHzAIhAAGJECGLEDGIAEGIoFMgwIAxXAGEEMYgAQYigUyEggEEAYQxiDARixAxjABBiKBTI
PCAUOABhDGLEDGIAEGIoFMg8IBhAAGEMYsQMYgAQYigUyDAgHEAYQxiABBiKBTIMCAGQABhDGIAEGIoF0gEIMTA4NmowajeoAgCwAgA&sourceid=chrome&ie=UTF-8|netflix - Google Search
https://chromewebstore.google.com/detail/browsec-vpn-free-vpn-for/omghfjlpggmjjaagoclmmobgdodcjboh?hl=en|Browsec VPN - Free VPN for Chrome - Chrome Web Store
https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://chromewebstore.google.com/detail/browsec-vpn-free-vpn-for/omghfjlpggmjjaagoclmmobgdodcjboh?hl=en&authuser=0|Browsec VPN - Free VPN for Chrome - Chrome Web Store
https://chromewebstore.google.com/accounts/SetOSID?authuser=0&continue=https://chromewebstore.google.com/detail/browsec-vpn-free-vpn-for/omghfjlpggmjjaagoclmmobgdodcjboh?hl=en&authuser=0|Browsec VPN - Free VPN for Chrome - Chrome Web Store
```

Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari VPN yang diinstal dari user. Sama seperti pada langkah-langkah browser forensic 1. Jadi saya hanya menggunakan fitur FIND dengan kata kunci vpn dan membuka satu persatu link yang mengandung kata vpn dan ternyata vpn yang diinstal adalah VeePN dan Browsec akan tetapi setelah saya submit jawaban masih salah.

Flag : IDN\_FLAG{ VEEPN\_SECURITY-BROWSEC\_SECURITY }



## 5) Browser Forensic 5

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

Visit Duration di Website yang berkaitan dengan Persistence, Privilage Escalation, DLL Injection ?

format flag : IDN\_FLAG{Jawaban yang disoal} example : XX:XX:XX.XXX

Lampiran :

The screenshot shows a terminal window with a dark background and white text. At the top, there's a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu, the command line shows the path: root@kali:/home/kali/Downloads/browser\_d. The user runs three SQLite commands against a database named 'Acuationtion/User Data/Default':  
1. A query to select 'id', 'url', and 'title' from the 'urls' table where the URL contains '%lolbas'. The results show a single row for a Google search result.  
2. A query to select 'visit\_duration' from the 'visits' table where the URL is '28'. The result is the value '32509459'.  
3. A final command prompt at the bottom.

Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari visit duration di websote yang berkaitan dengan Persistence, Privilage Escalation, DLL Injection. Jadi pada browser forensic 2 dan browser forensic 6 ini saling berkaitan jadi saya menyimpulkan bahwa websitenya adalah LOLBAS. Jadi saya mencari durasi kunjungan nya seperti pada gambar dan setelah ketemu bahwa waktunya adalah 32509459. Dimana waktu tersebut adalah mikrodetik yang harus dikonversi dulu ke detik, setelah di konversi hasilnya 32,509459 detik. Lalu saya inputkan waktu tersebut sesuai dengan format “00:00:32.459”.

Flag : IDN\_FLAG{00:00:32.509 }



## 6) Browser Forensic 6

Deskripsi :

Ada Violation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !! (*Filenya ada di pertanyaan pertama*)  
Email yang digunakan pada browser ?  
format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :

```
laptop-service
virtual_card_usage_data
web_app_manifest_section

[root@kali]~[/home/.../browser_dump/Acuatiotion/User Data/Default]
# sqlite3 Web\ Data "SELECT value FROM autofill WHERE value LIKE '%@%';"
ghxyssforunfun@gmail.com

[root@kali]~[/home/.../browser_dump/Acuatiotion/User Data/Default]
#
```

Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari email yang digunakan pada browser. Jadi biasanya untuk mencari informasi tersebut biasanya terdapat pada file Web Data. Jadi saya langsung melakukan pengecekan seperti pada gambar agar mempercepat pencarian. Setelah di eksekusi perintah email langsung ketemu.

Flag : IDN\_FLAG{ghxyssforunfun@gmail.com}



## 7) Browser Forensic 7

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

date\_created pada email menggunakan tools DB Browser SQLite ?

format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :

```
[root@kali)-[~/home/.../browser_dump/Acuatiotion/User Data/Default]
# sqlite3 Web\ Data "SELECT * FROM autofill"
identifier|ghxyssforunfun@gmail.com|ghxyssforunfun@gmail.com|1746250363|1746250363|1
[root@kali)-[~/home/.../browser_dump/Acuatiotion/User Data/Default]
# ]
```

Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari date\_created pada emailnya. Jadi saya melakukan pengecekan dengan sqlite3 dengan mengecek seluruh isi pada tabel autofill. Setelah mengeksekusi perintahnya, date\_created pun muncul dan teridentifikasi.

Flag : IDN\_FLAG{1746250363}



## 8) Browser Forensic 8

Deskripsi :

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

Lampiran :

```
[root@kali)-[~/home/.../browser_dump/Acuatiotion/User Data/Default]
  # sqlite3 Top\ Sites "SELECT * FROM top_sites;" 
https://chrome.google.com/webstore?hl=en-GB|0|Web Store

[root@kali)-[~/home/.../browser_dump/Acuatiotion/User Data/Default]
  # sqlite3 Favicons ".tables"
favicon_bitmaps  favicons      icon_mapping     meta

[root@kali)-[~/home/.../browser_dump/Acuatiotion/User Data/Default]
  # sqlite3 Favicons "SELECT * FROM favicons;" 
1|https://ssl.gstatic.com/chrome/webstore/images/icon_48px.png|1
2|https://assets.nflxext.com/us/ffe/siteui/common/icons/nficon2023.ico|1
3|https://www.muslima.com/lp/paid-search/terra-assets/images/favicon-8b7d9ccfa1-3.ico|1
4|https://github.githubassets.com/favicons/favicon.svg|1
5|https://www.google.com/favicon.ico|1
6|https://lolbas-project.github.io/assets/favicon.png|1

[root@kali)-[~/home/.../browser_dump/Acuatiotion/User Data/Default]
  # ]
```

Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari url favicon yang tidak berkaitan dengan hacker. Jadi saya melakukan pengecekan secara manual untuk melihat apakah ada file bernama favicon, setelah dicari ternyata ada. Jadi selanjutnya saya langsung melakukan pengecekan pada file favicon dengan tabel favicons. Setelah eksekusi perintahnya muncul beberapa URL. Setelah itu saya lakukan identifikasi untuk melihat url mana yang tidak berkaitan dengan hacker. Ternyata ada website tentang muslima yang tidak berkaitan dengan hacker. Jadi saya submit url tersebut dan benar.

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

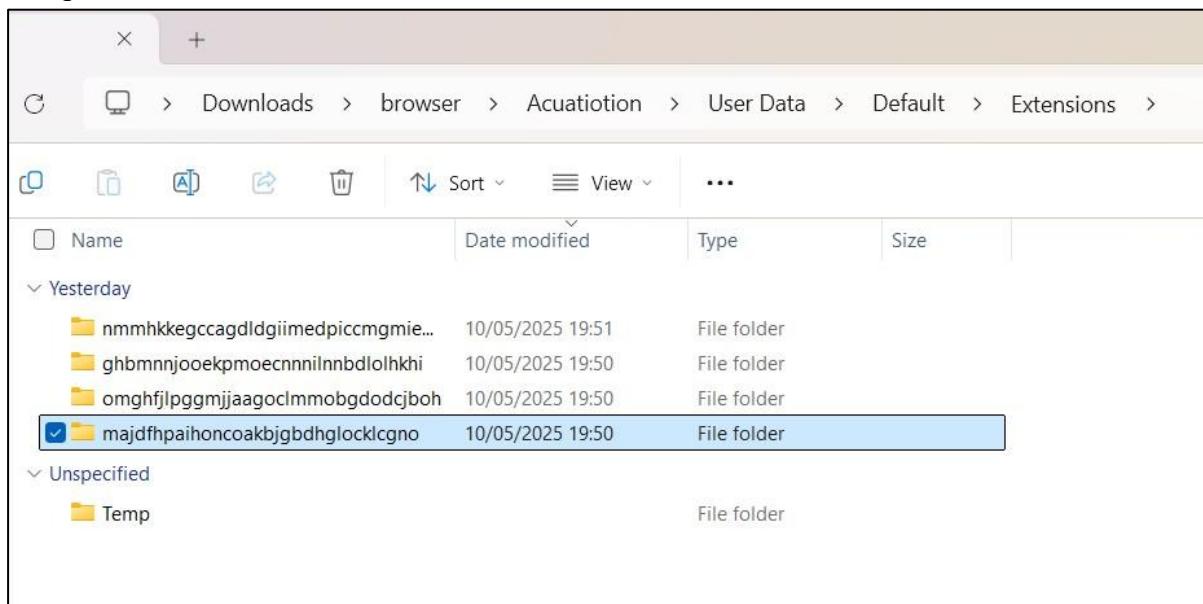


## 9) Browser Forensic 9

Deskripsi :

Ada Volation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !!  
*(Filenya ada di pertanyaan pertama)*  
extension id dengan icon salah satu vpn yang diinstal V.. !  
format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :



Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari extension id dengan icon salah satu vpn yang diinstal V... Yang berarti jika ada kata "V.." kemungkinan VPN VeePN. Jadi saya melakukan pengecekan manual pada folder extension dan setelah saya buka terdapat 5 folder akan tetapi pada folder \temp kemungkinan besar bukan. Jadi saya cek 4 folder tersebut dan melakukan pengecakan pada file manifest.json untuk mencari apakah ada unsur kata VeePN didalam file tersebut. Setelah saya cek ternyata hanya folder ke 4 yang ada dan berarti extension idnya adalah nama folder tersebut. Ketika saya submit jawabannya benar.

Flag : IDN\_FLAG{majdfhpaihoncoakbjgbdhglocklcgno}

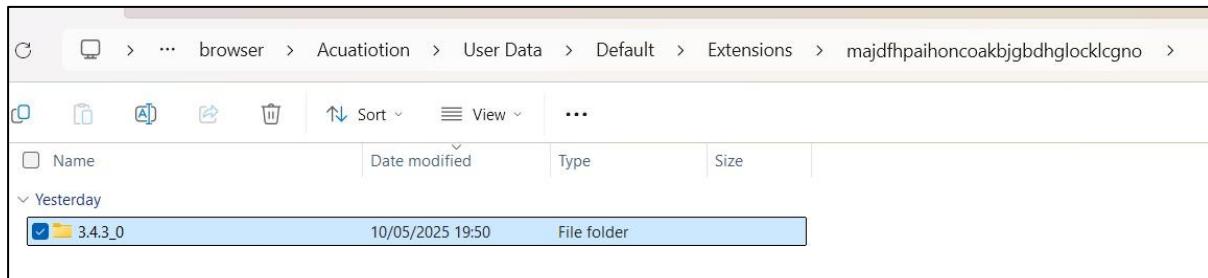


## 10) Browser Forensic 10

Deskripsi :

Ada Violation yang dilakukan oleh user di satu laptop, coba bantu forensic browsernya dong !! (*Filenya ada di pertanyaan pertama*)  
Version vpn V.. yang diinstal oleh user ?  
format flag : IDN\_FLAG{Jawaban yang disoal}

Lampiran :



Solusi :

Dari pernyataan di atas bahwa keterangannya untuk mencari Version vpn. Jadi setelah tau extensions IDnya saya buka folder extensions ID dan keluar sebuah folder lagi yang merupakan versi vpnnya. Setelah saya submit jawaban benar.

Flag : IDN\_FLAG{3.4.3\_0 }