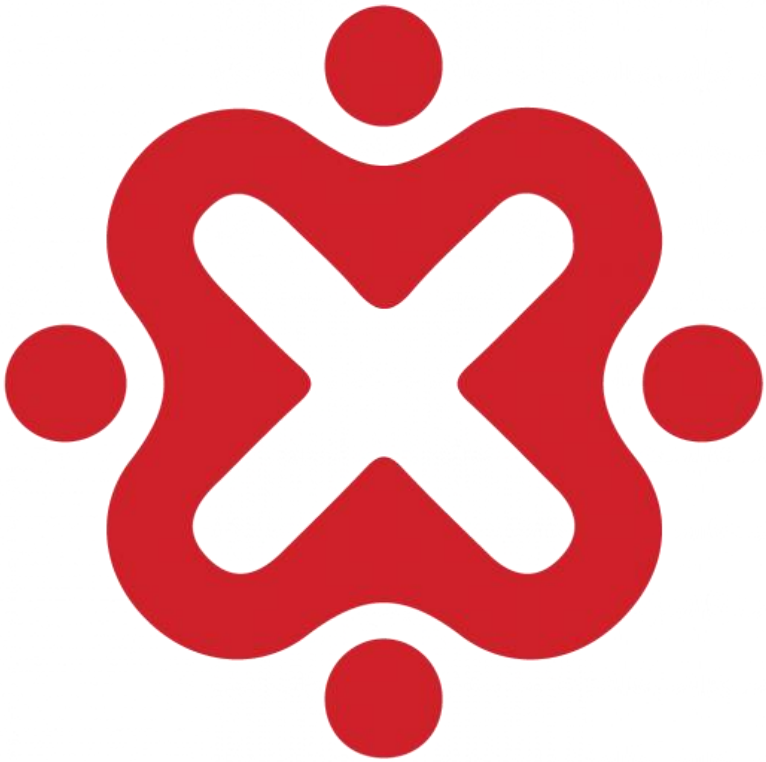
Depok Cybersec

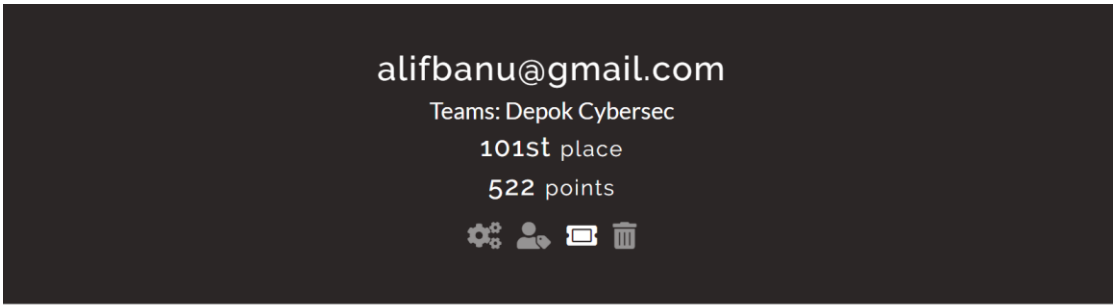
Any progress is better than none



ID-Networkers
Indonesian IT Expert Factory

Introduction Team

Nama Team : Depok Cybersec
Anggota : Alif Banu Nur Rachman, Raihan Putra Kurniawan, Ahmad Ferdiyansyah.



Members

User Name	Score
Alif Banu Nur Rachman Captain	32
Raihan Putra Kurniawan	280
Ahmad Ferdiyansyah	210

Point : 522

Summary Findings Each Category

Category	Soal Selesai / Dari Soal yang ada	Point
Web Exploit	12/13	120
Other	1/2	10
Welcome Flag	1/1	10
Web 303	7/7	70
Cryptography	5/7	50
Log Analysis	9/9	90
USB Forensic	8/8	80
Browser Forensic	0/10	0
Windows Forensic	8/15	80
Forensic	2/2	12

Pengurangan Nilai : 8 Point

Detail Challenge Solved

Others

User Guide

Deskripsi :

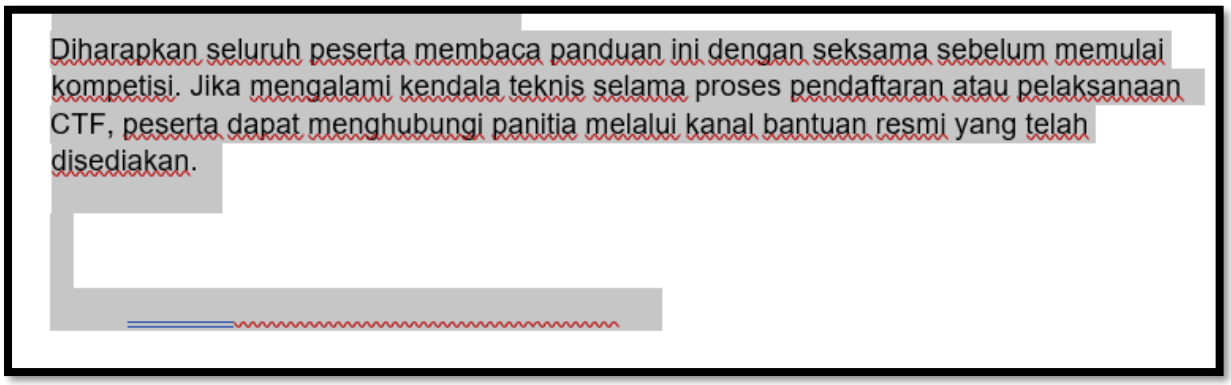
FLAG

Lampiran : none

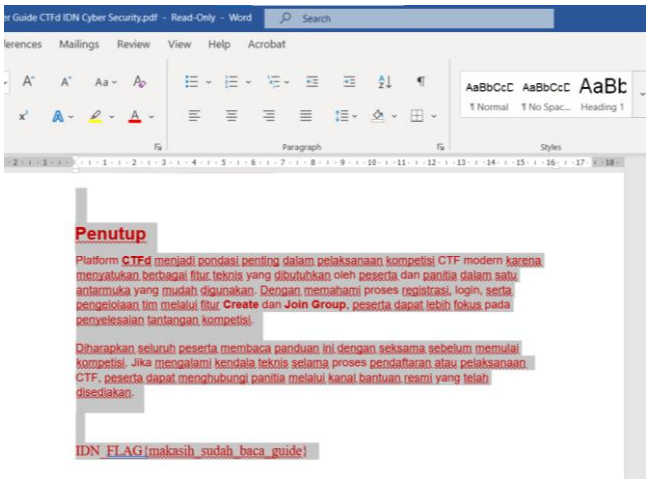
Solusi :

- Membaca seluruh **User Guide**.
- Menemukan format **flag**, lalu coba submit flag Namun **inccorect**.

- Mulai mencari text tersembunyi, dengan **CTRL + A** agar seluruh isi dalam document **ter-blok**. Menemukan baris yang ter-blok namun tidak ada textnya atau **tersembunyi**. Lalu coba **ubah warna** textnya.



- Setelah diubah warna textnya, menemukan **text yang tersembunyi**. Lalu coba submit sebagai **flag** dan **correct**.



Flag : IDN_FLAG{makasih_sudah_baca_guide}

Cryptography

Might Guy's Secret

Deskripsi :

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

Ini isi pesannya: QGA_OTS{v067j1723qk40f5v33z656afwse60kdf67u9606}

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

Tampaknya Might Guy menggunakan teknik enkripsi klasik namun ampuh

Authtor: Nur Cholis Majid

Lampiran :

Solusi :

- Petunjuk: "Giovan Battista Bellaso: 1553M: idnmantab" dengan jenis chipper Vigenère Cipher dan keynya adalah IDNMANTAB
- Gunakan decoder online

Flag: IDN_CTF{c067j1723pc40c5i33n656asdsd60cas67i9606}

Rot1Aoka

Deskripsi :

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

Lampiran :

Solusi :

- Petunjuk : Rot1Aoka : Jenis Cipher ROT = ROT1 / ROT13
- Gunakan decoder online
- Coba ROT-1 = Incorrect

- Coba ROT13 untuk seluruh string = correct

Flag : IDN_FLAG{P3M4N4S4N_DU1U_94S1H}

Pramuka

Deskripsi :

terjemahan kan pesan tersebut. Format Flag

IDN_CTF{****}

Author : Mohamad Fattyr

morse.wav

Lampiran : morse.wav

Solusi :

- Terlihat dari judul " Pramuka " dan Nama file audio bahwa ini adalah pesan sandi Morse.
- Lalu mencoba decode dengan decoder online sandi morse.
- Hasil decode " M0RS3C0D3R19HT ".
- Lalu ditambahkan spasi.

Flag : IDN_CTF{ M0RS3_C0D3_R19HT}

Classic Cryptography

Deskripsi :

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

Author: Rafly Permana

Lampiran :

Solusi :

- Terlihat dari judulu "Classic Cryptograpphy" maka kita akan mencoba Caecar Cipher
- Gunakan Decoder Online
- Geser huruf menjadi -1 a-z

Flag : IDN_CTF{yayy_you_are_great}

Simple Substitution Cipher

Deksripsi :

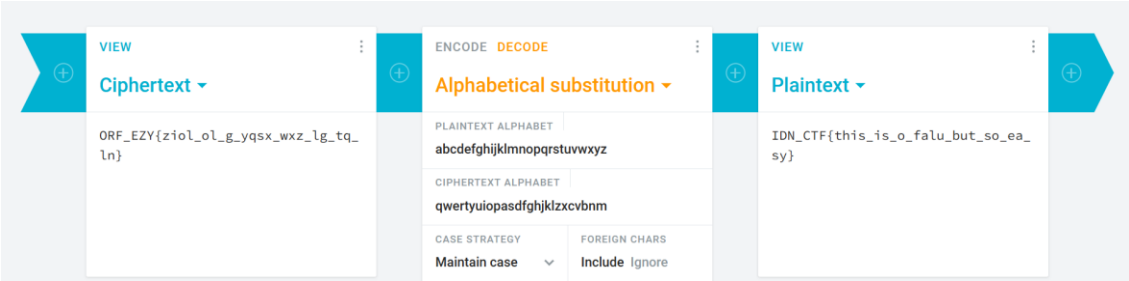
ORF_EZY{ziol_ol_g_yqsx_wxz_lg_tq_ln}

Author: Rafly Permana

Lampiran :

Solusi :

- Terlihat dari judul “Simple Subtitution Cipher”, jadi kita akan menggunakan Subtitution Chipher
- Dengan Plaintext “abcdefghijklmnopqrstuvwxyz” dan ciphertext “qwertyuiopasdfghjklzxcvbnm”



Flag : IDN_CTF{THIS_IS_O_FALU_BUT_SO_EA_SY}

USB Forensic

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}

Auhtor: Aditya Firman Nugroho

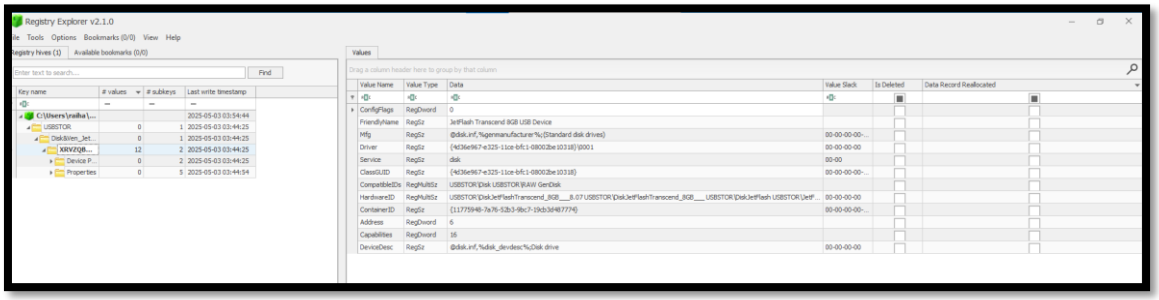
Lampiran : usb.zip

Solusi :

- Zip berisi file **Registry** :
  - MountPoints2.hiv = Volume & path USB yang dipasang
  - NTUSER.DAT = File dibuka, folder diakses, konfigurasi user
  - RecentDocs.hiv = Nama file terakhir yang dibuka

- USBTOR.hiv = Vendor USB, Serial Number, kapasitas
- USRCLASS.DAT = Folder terakhir yang diakses dari USB

➢ Gunakan tools forensic **Registry Explorer** (Eric Zimmerman's tools).
➢ Berdasarkan informasi di deskripsi, mulai lakukan forensik file **USBTOR.hiv** .
➢ Menemukan informasi Device USB di **" USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0 ".**
➢ Di value name **"friendlyName"** terdapat Value **"JetFlash Transcend 8GB USB Device".**



Flag : IDN_FLAG{JetFlash_Transcend_8GB_USB_Device}

USB Forensic 2

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

ClassGUID Pada USB Hacker ?

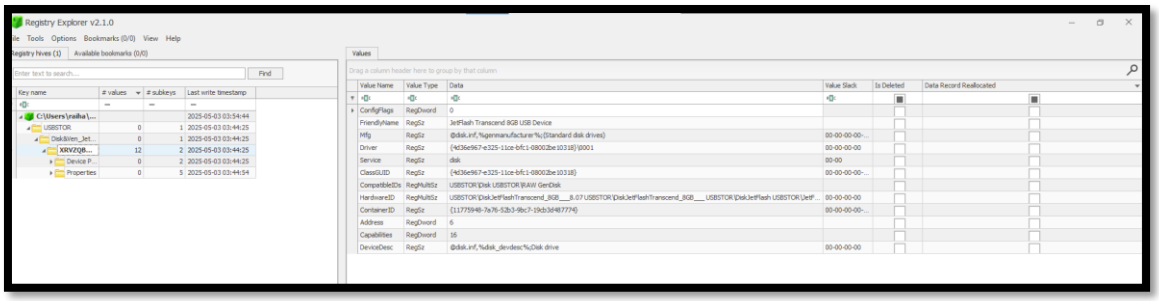
format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman NugrohoAuthor: Rafly Permana

Lampiran : None

Solusi :

➢ Menemukan informasi Device USB di **" USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0 ".**
➢ Di value name **"ClassGUID"** terdapat Value **"{4d36e967-e325-11ce-bfc1-08002be10318}".**



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

USB Forensic 3

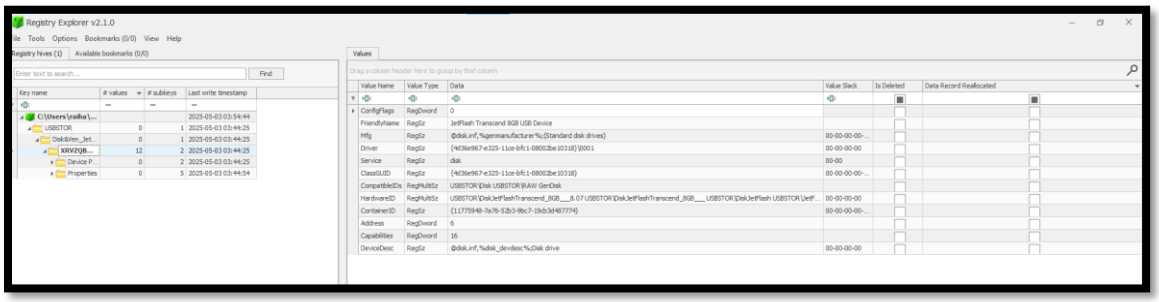
Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong ! (Filenya ada di pertanyaan pertama) Apa Containder ID USB Yang dipakai Hacker ? format flag : IDN_FLAG{Jawaban yang disoal}

Lampiran : None

Solusi :

- Menemukan informasi Device USB di **" USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0 ".**
- Di value name **"ContainerID"** terdapat Value **{11775948-7a76-52b3-9bc7-19cb3d487774}".**



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

USB Forensic 4

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

Apa Disk ID yang dipakai hacker ?

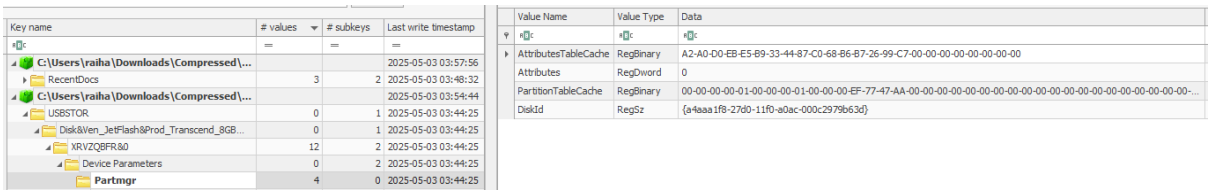
format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Menemukan informasi Device USB di **"USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0\Device Parameters\Partmgr ".**
- Di value name **"DiskId"** terdapat Value "**{a4aaa1f8-27d0-11f0-a0ac-000c2979b63d}}".**



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

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}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :
Serial ID USB biasanya terletak sebagai nama folder / subkey dari “ USBTOR.hiv “. Dan menemukan serial IDnya di path “USBTOR.hiv: Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07\XRVZQBFR&0” yaitu “XRVZQBFR&0”.

Flag : IDN_FLAG{XRVZQBFR&0}

USB Forensic 6

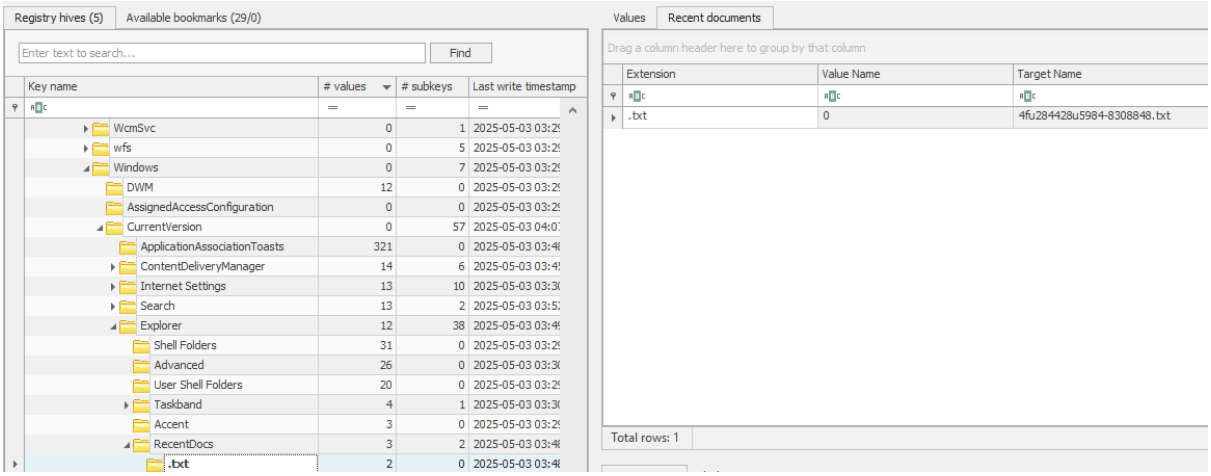
Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong ! (Filenya ada di pertanyaan pertama) Nama File Yang ada di USB ? format flag : IDN_FLAG{Jawaban yang disoal} Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- RecentDocs registry menyimpan file-file terakhir yang dibuka di komputer, termasuk file dari USB.
- Mencoba cari recentdocs registry Explorer di Ntuser.dat .
- Menemukan target name registry “4f624842b5984-8308848.txt “ di path “NTUSER.dat: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt “



Flag : IDN_FLAG{4f624842b5984-8308848.txt}

USB Forensic 7

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

Direktory Yang ada di usb ?

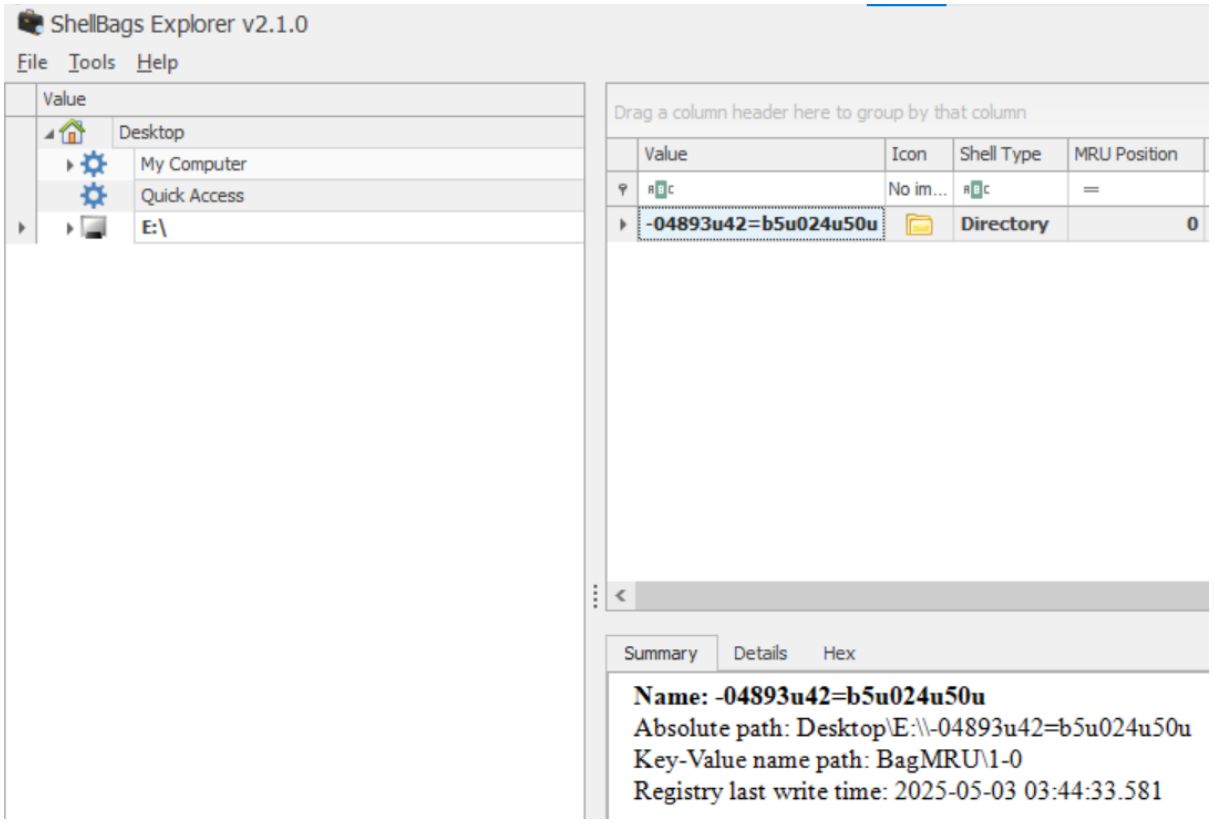
format flag : IDN_FLAG{Jawaban yang disoal} example : *:\directory

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Gunakan **ShellBags Explorer** untuk mengekstrak informasi dari ShellBags file " **USRCLASS.dat** "(karena Registry Explorer tidak menampilkan path direktori USB secara utuh).
- Mendapatkan informasi directory path USB yaitu " **Absolute path: Desktop\E:\\-04893u42=b5u024u50u** " .



Flag : IDN_FLAG{E:\-04893u42=b5u024u50u}

USB Forensic 8

Deskripsi :

> ada hacker, physical acces ke laptop.. bantuin dong !
>
> (Filenya ada di pertanyaan pertama)
>
> File dibuka pada jam ?
>
> format flag : IDN_FLAG{Jawaban yang disoal} example : xxxx-xx-xx xx:xx:xx
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- RecentDocs registry menyimpan file-file terakhir yang dibuka di komputer, termasuk file dari USB.
- Mencoba cari recentdocs registry Explorer di Ntuser.dat .
- Menemukan target name registry “4f624842b5984-8308848.txt “ di path “NTUSER.dat: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt “
- Di registry tersebut terdapat informasi “ opened On “ yang berisi kapan file tersebut dibuka.

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
.txt	0	4fu284428u5984-8308848.txt	4fu284428u5984-8308848.lnk	0	2025-05-03 03:48:32

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

Windows Forensic

Windows Forensic 1

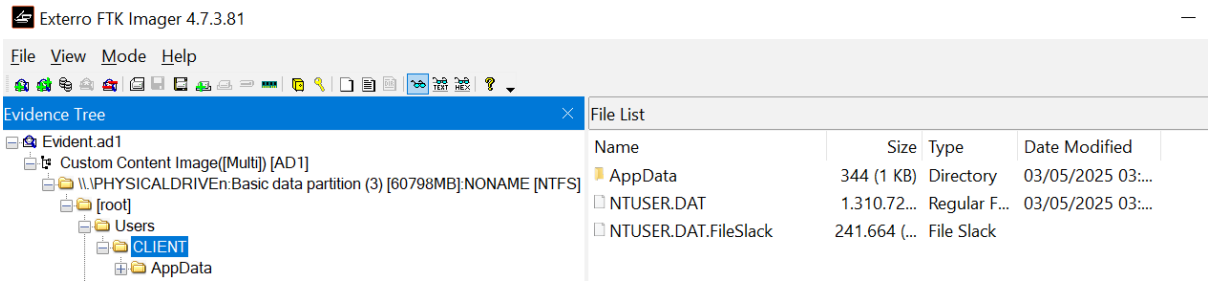
Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> Nama file yang menyimpan credential ?
>
> format flag : IDN_FLAG{Jawaban yang disoal} example : xxxxxxxx_xxx.xxx
>
> Auhtor: Aditya Firman Nugroho

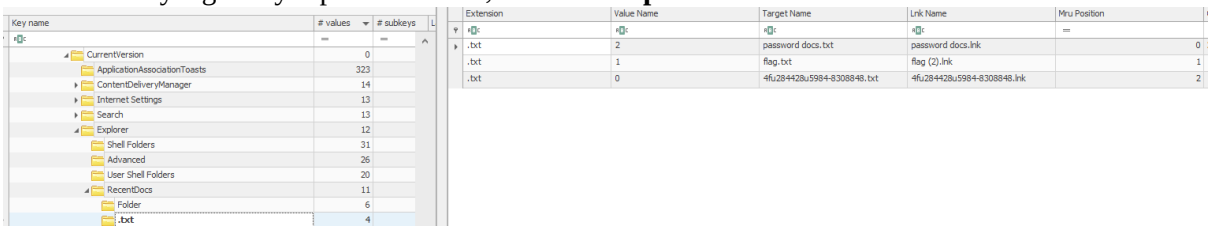
Lampiran : Windows.zip

Solusi :

- Mount Evident.ad1 menggunakan **FTK Imager**.
- Masuk ke folder: \Users\CLIENT. Lalu export file **NTUSER.DAT**



- Buka file NTUSER.DAT menggunakan **Registry Explorer**.
- Lalu cari registry RecentDocs. Ketemu di path "NTUSER.DAT: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs ".
- Didalam folder RecentDocs terdapat folder .txt yang berisi beberapa nama file. Deskripsi meminta file yang menyimpan credential, berarti file "**password docs.txt**".



Flag : IDN_FLAG{ password_docs.txt }

Windows Forensic 2

Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> file yang menyimpan credential, dibuka pada tanggal berapa ?
>
> format flag : IDN_FLAG{Jawaban yang disoal} example : xxxx-xx-xx xx:xx:xx
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :
Di Registry RecentDocs dengan path “NTUSER.DAT: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt” terdapat keterangan file “password_docs.txt” dibuka pada “ 2025-05-03 07:16:29 “.

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
.txt	2	password docs.txt	password docs.lnk	0	2025-05-03 07:16:29
.txt	1	flag.txt	flag (2).lnk	1	
.txt	0	4fu284428u5984-8308848.txt	4fu284428u5984-8308848.lnk	2	

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

Windows Forensic 3

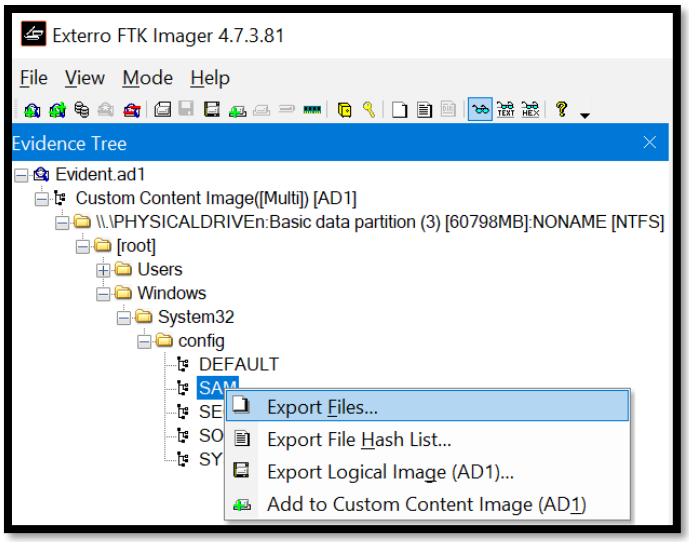
Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> User yang dibuat pada tanggal 2025-05-03 07:04:43, Username nya ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

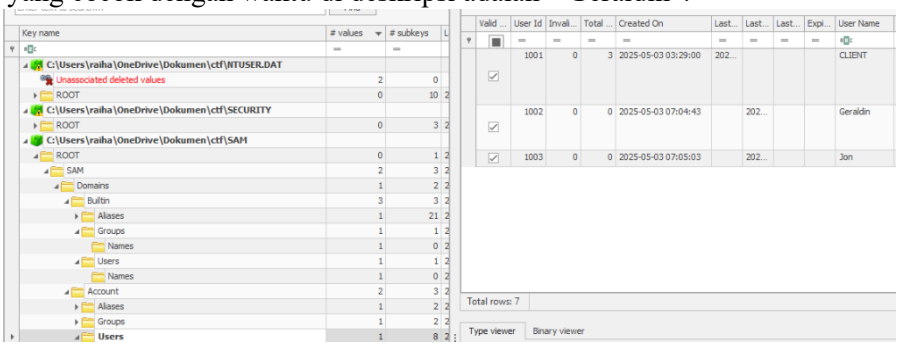
Lampiran : None

Solusi :

- Mount Evident.ad1 menggunakan **FTK Imager**.
- Masuk ke folder: \Windows\System32\Config. Lalu export file **SAM.**



- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- User yang cocok dengan waktu di deskripsi adalah “ Geraldin”.



Flag : IDN_FLAG{Geraldin}

Windows Forensic 4

Deskripsi :

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

(Filenya ada di pertanyaan pertama)

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

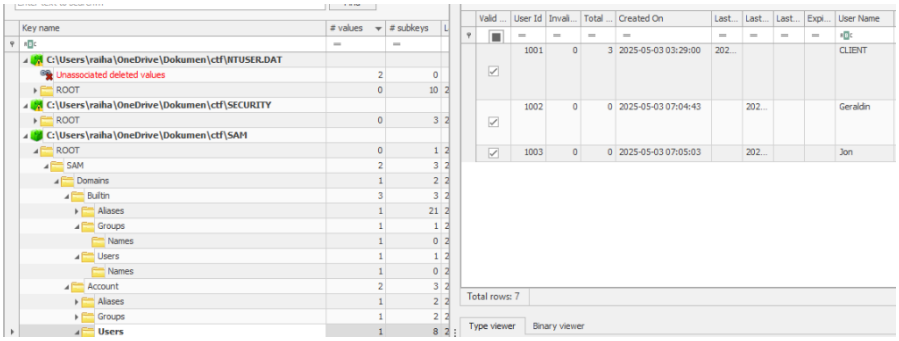
format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- User yang cocok dengan waktu di deskripsi adalah “Jon”.



Flag : IDN_FLAG{ Jon}

Windows Forensic 5

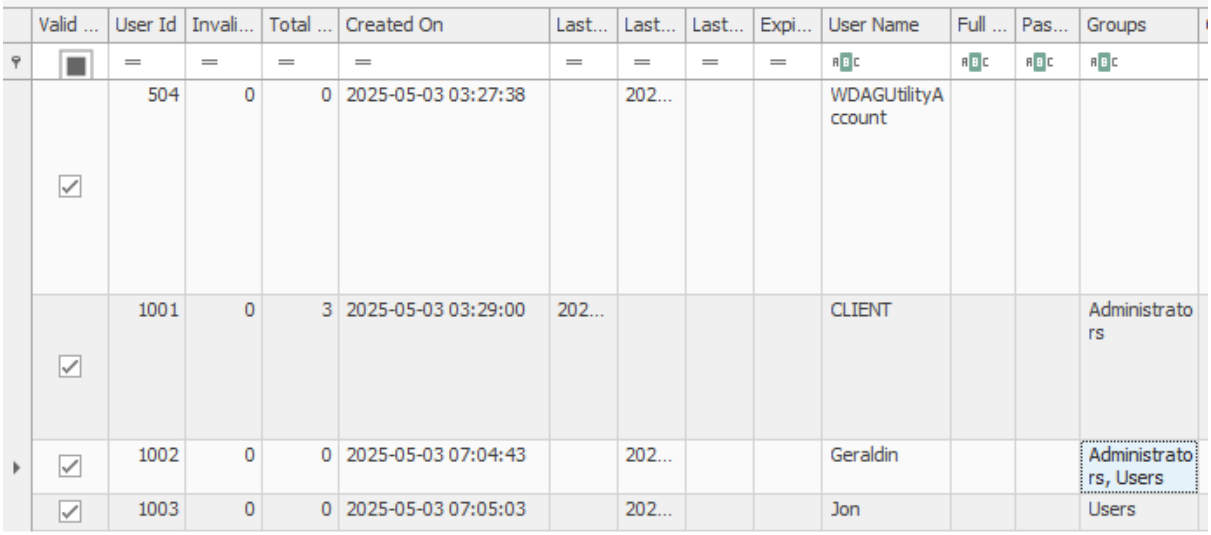
Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> User yang localgroupnya ada 2, yaitu ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- User yang local groupnya ada 2 yaitu “ Geraldin”. Ia termasuk dalam group “ administrators “ dan “ Users” .



Valid ...	User Id	Invali...	Total ...	Created On	Last...	Last...	Last...	Expi...	User Name	Full ...	Pas...	Groups
☑	504	0	0	2025-05-03 03:27:38		202...			WDAGUtilityAccount			
☑	1001	0	3	2025-05-03 03:29:00	202...				CLIENT			Administrators
☑	1002	0	0	2025-05-03 07:04:43		202...			Geraldin			Administrators, Users
☑	1003	0	0	2025-05-03 07:05:03		202...			Jon			Users

Flag : IDN_FLAG{Geraldin}

Windows Forensic 6

Deskripsi :

> Ceritanya,udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> Last Login Time dari User Cli.. ?
>
> format flag : IDN_FLAG{Jawaban yang disoal} example : xxxx-xx-xx xx:xx:xx
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- Deskripsi memberikan clue user “ CLI.. “. Yang mendekati clue deskripsi adalah User “ CLIENT “. Last Login Time dari user CLIENT adalah “ 2025-05-03 03:42:49 “ .

Valid ...	User Id	Invali...	Total ...	Creat...	Last Login Time	Last ...	Last ...	Expi...	User N...
☐	=	=	=	=	=	=	=	=	ABC
☑	1001	0	3	2025...	2025-05-03 03:42:49				CLIENT
☑	1002	0	0	2025...		202...			Geraldin
☑	1003	0	0	2025...		202...			Jon

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

Windows Forensic 7

Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> User ID dari user dengan 3 huruf ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User. Ketemu di path “SAM: SAM\Domains\Account\Users “
- Dari informasi yang ada, user dengan 3 huruf hanya “ Jon “. Dan user ID “ Jon “ adalah “ 1003 “.

User Id	Invali...	Total ...	Creat...	Last Login Time	Last ...	Last ...	Expi...	User N...
1001	0	3	2025...	2025-05-03 03:42:49				CLIENT
1002	0	0	2025...		202...			Geraldin
1003	0	0	2025...		202...			Jon

Flag : IDN_FLAG{1003}

Windows Forensic 8

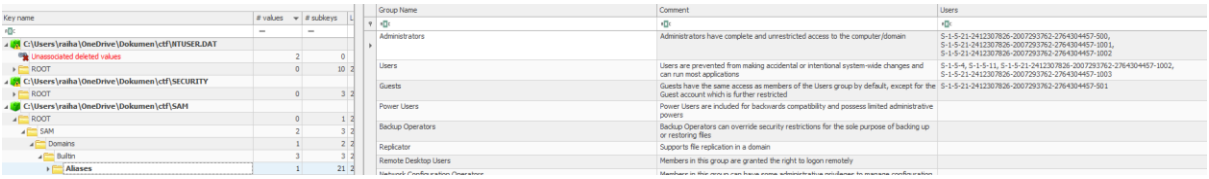
Deskripsi :

> Ceritanya, udh ambil hivenya.. mount, trus cari beberapa informasi tambahan lainya !!
>
> (Filenya ada di pertanyaan pertama)
>
> SID Dari User Guest ?
>
> format flag : IDN_FLAG{Jawaban yang disoal}
>
> Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

- SID (Security Identifier) adalah kode unik yang digunakan oleh Windows untuk mengidentifikasi user, group, dan akun lainnya dalam sistem. Mirip seperti NIK di KTP untuk user account di Windows.
- Buka file SAM menggunakan **Registry Explorer**.
- Cari registry yang berisikan informasi User dan ada SID. Ketemu di path “SAM: SAM\Domains\Builtin\Aliases “.



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

Web Exploit

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.

Author : Faiz Ahmad Habibi

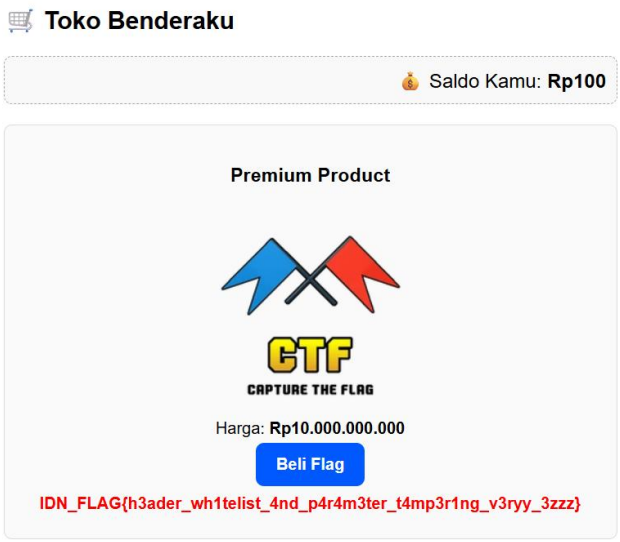
Lampiran : https://ctf.solusiber.com/buy_the_flag/

Solusi :

- Disini kita memiliki saldo Rp. 100 dan harga untuk flag Rp. 10.000.000.000
- Kita inspect element untuk mengubah value dari yang Rp. 100 menjadi Rp. 10.000.000.00

```
<input type="hidden" name="saldo" value="10000000000">
<button type="submit">Beli Flag</button>
```

- Karna valuenya sudah di ubah kita coba klik beli flag



Flag: IDN_FLAG{h3ader_wh1telist_4nd_p4r4m3ter_t4mp3r1ng_v3ryy_3zzz}

Konoha Breach

Deskripsi :

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

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

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

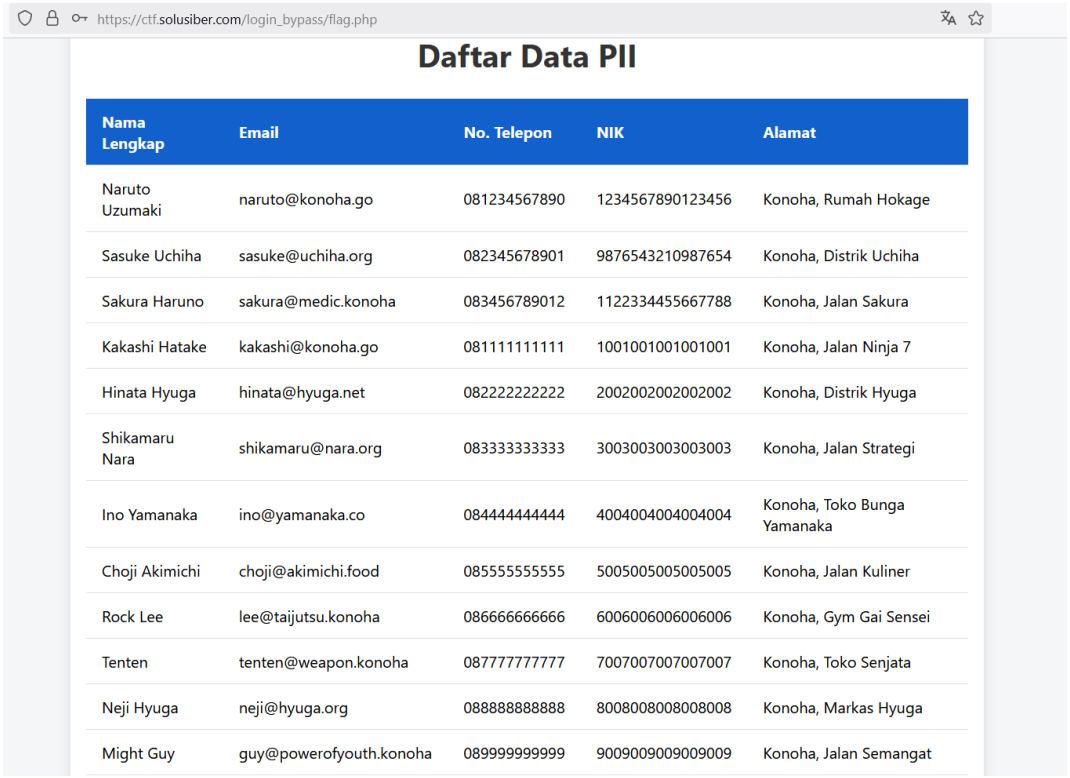
Bisakah kamu menyusup ke sistem tanpa login dan menemukan yang tersembunyi?

Author: Rafly Permana

Lampiran : Isi dari web menggunakan SQL Injection

Solusi :

- Menggunakan Exploitasi SQL Injection, Payload untuk Bypass Login
- Isi Username dengan : ' OR 1=1-- -
- Dan isi Password dengan : password
- Setelah berhasil login, lalu Buka ”View Page Source”



Nama Lengkap	Email	No. Telepon	NIK	Alamat
Naruto Uzumaki	naruto@konoha.go	081234567890	1234567890123456	Konoha, Rumah Hokage
Sasuke Uchiha	sasuke@uchiha.org	082345678901	9876543210987654	Konoha, Distrik Uchiha
Sakura Haruno	sakura@medic.konoha	083456789012	1122334455667788	Konoha, Jalan Sakura
Kakashi Hatake	kakashi@konoha.go	081111111111	1001001001001001	Konoha, Jalan Ninja 7
Hinata Hyuga	hinata@hyuga.net	082222222222	2002002002002002	Konoha, Distrik Hyuga
Shikamaru Nara	shikamaru@nara.org	083333333333	3003003003003003	Konoha, Jalan Strategi
Ino Yamanaka	ino@yamanaka.co	084444444444	4004004004004004	Konoha, Toko Bunga Yamanaka
Choji Akimichi	choji@akimichi.food	085555555555	5005005005005005	Konoha, Jalan Kuliner
Rock Lee	lee@taijutsu.konoha	086666666666	6006006006006006	Konoha, Gym Gai Sensei
Tenten	tenten@weapon.konoha	087777777777	7007007007007007	Konoha, Toko Senjata
Neji Hyuga	neji@hyuga.org	088888888888	8008008008008008	Konoha, Markas Hyuga
Might Guy	guy@powerofyouth.konoha	089999999999	9009009009009009	Konoha, Jalan Semangat

Flag : IDN_CTF{c0NRats_you_goin_tohe_insideee}

ID-Networkers

Deskripsi :

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

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

Tapi kamu bukan crawler, kamu seorang penyusup yang teliti.

Author: Rafly Permana

Solusi :

- Buka Website https://ctf.solusiber.com/robots_dashboard/
- Gunakan text robots.txt setelah slash dashboard
- Akan tampil Dissalow message : asdsa024nsfd01372021.html
- Copy Dissalow message : asdsa024nsfd01372021.html , ke slash terakhir

https://ctf.solusiber.com/robots_dashboard/robots.txt

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

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

Support Force

Deskripsi :

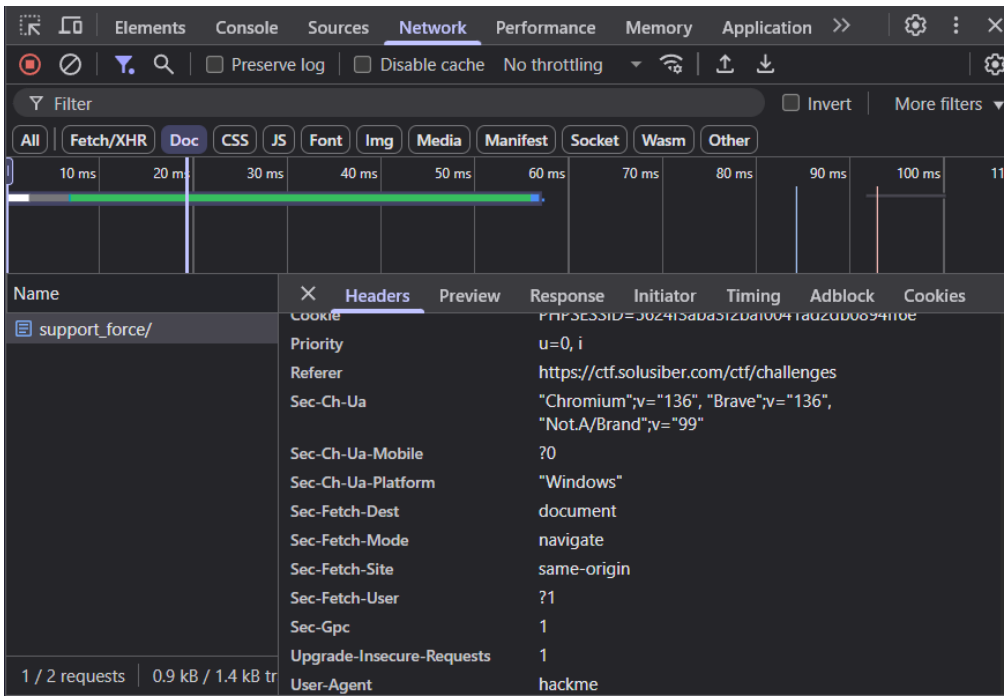
Ini klub eksklusif buat agen rahasia. Browser biasa? Maaf, Anda tidak terdaftar. Tapi kalau kamu bisa pura-pura jadi "Agent hackme", pintu rahasia mungkin bakal terbuka buatmu.

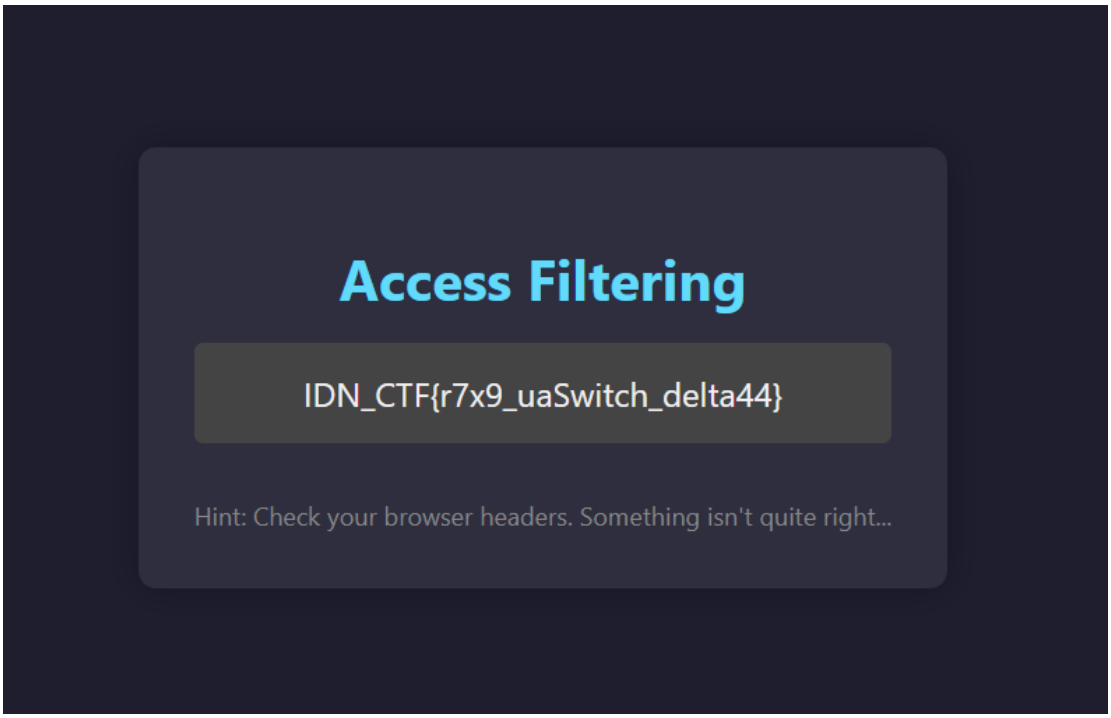
Author : Rafly Permana

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

Solusi :

- Diwebsitenya kita diberi hint untuk lihat browser header, dan dari deskripsi kita disuruh untuk menjadi Agent hackme.
- kita akan memanipulasi headernya tersebut menggunakan chrome ekstantion yaitu requestly
- masuk ke requestly > pilih modify headers > masukan URL https://ctf.solusiber.com/support_force/ > add request header : user-agent dan Value : hackme > safe rule.





Flag : IDN_CTF{r7x9_uaSwitch_delta44}

Kue Monster

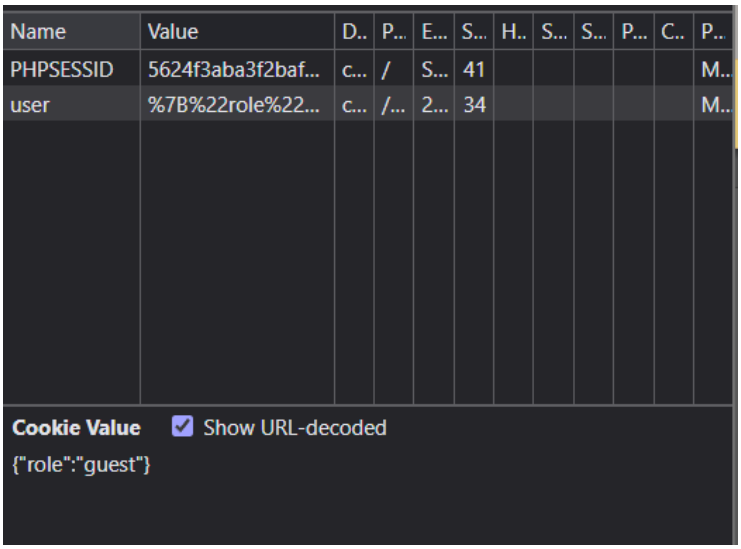
Deskripsi :

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

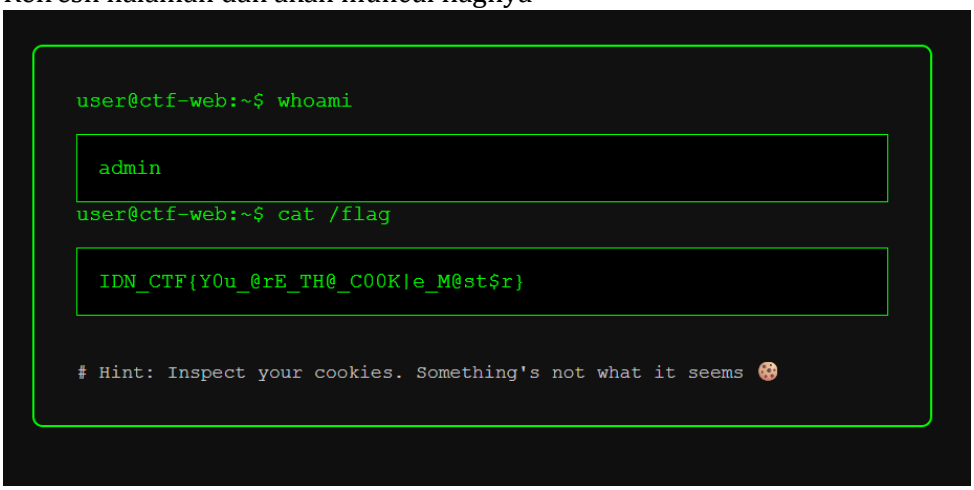
Lampiran : https://ctf.solusiber.com/kue_monster/

Solusi:

- disini kita diberi hint untuk inspect cookies kita.
- Terlihat juga disini kita menggunakan user guest dan disuruh untuk merubah menjadi admin untuk mendapatkan flagnya
- Masuk ke devtool (F12) > application > cookies > karna kita disuruh merubah user kita pilih user > ubah valuenya dari yang %7B%22role%22%3A%22guest%22%7D Menjadi %7B%22role%22%3A%22admin%22%7D



- Refresh halaman dan akan muncul flagnya



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

IDN Education

Deskripsi :

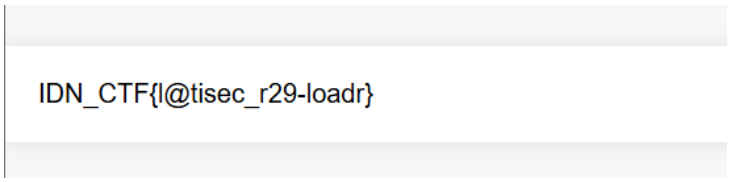
Siapa sangka file-file tersembunyi di balik input sederhana? Coba kamu buka celahnya, biar file yang terpendam itu bisa keluar. Siapa tahu ada kejutan!

Author : Rafly Permana

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

Solusi :

- Dsini kita diberi hint yaitu LFI
- Kita akan mecoba – coba path yang megekploitasi https://ctf.solusiber.com/idn_edu/?page=../../../../etc/passwd
- Setelah itu kita mencoba path yang memungkin kan mendapat flag https://ctf.solusiber.com/idn_edu/?page=../../../../var/www/html/flag.txt



Flag : IDN_CTF{l@tisec_r29-loadr}

Beyond Way

Deskripsi :

Mungkin kamu nggak pernah diajari buat berjalan keluar dari jalan yang benar... tapi kalau kamu bisa, kamu bakal dapetin sesuatu yang terlarang. Ayo jalanin manipulasi path-nya!

Author : Rafly Permana

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

Solusi :

- kita disini disuruh untuk manipulasi pathnya
- untuk path awal kita coba masuk https://ctf.solusiber.com/search_free/?file=../../../../etc/passwd
- coba untuk mencari flagnya dengan mengubah path menjadi https://ctf.solusiber.com/search_free/?file=../flag.txt

Flag: IDN_CTF{tvec-resolver_41}

I'm Not Me, You Are Me

Deskripsi :

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

Author : Rafly Permana

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

Solusi :

- Kita disini disuruh untuk coba ganti ID yang diberikan
- Kita akan mencoba memasukan id 1

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

- Kita coba lagi untuk memasukan id 0

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


- Flag ditemukan

Flag: IDN_CTF{Y0u_FF0D_the_heN_admin}

Circle Clicker

Deskripsi :

Click Sampai 1000 kali!

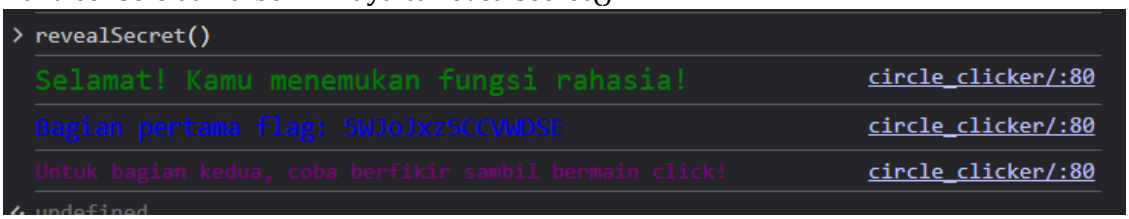
Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Author : Mohamad Fattyr

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

Solusi :

- Hint Click sampai 1000 kali, jadi kita coba click dan ternyata berubah disaat click ke 20
- Buka console dan diberi hint yaitu revealsecret()



- Setelah mengetahui bagian pertama flagnya yaitu 5WJoJxz5CCVWDSE, kita menuju ke sources dan mencari kode yang ngacu 5WJoJxz5CCVWDSE, dan ditemukan WJoJxz5CCVWDSEpH4E1n77BT5Fec
- Buka decoder online pilih base 58 karna dari hint kita menggunakan encoder bitcoin dan solana

Flag : IDN_CTF{click_master}

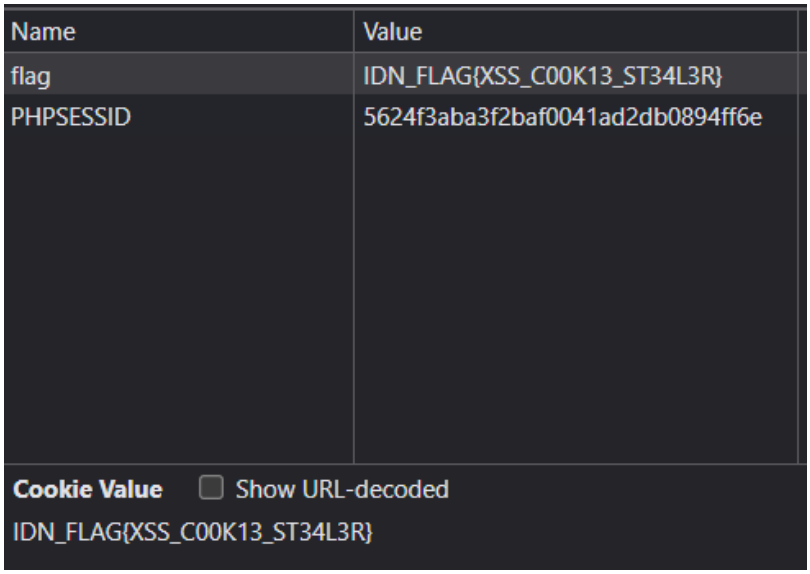
Xss

Deskripsi :

CURI! **Author : Mohamad Fattyr**

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

Solusi :

- Kita diberi hint untuk melihat cookie
- Masuk ke cookie melalui devtools dan menemukan
- 

Flag : IDN_FLAG{XSS_C00K13_ST34L3R}

Awesome Website

Deskripsi :

CARI!! **Author : Mohamad Fattyr**

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

Solusi :

- Saya membuka sources code
- Lalu menemukan API token yaitu SUROX0ZMQUd7VzNCXzNOQ29kM183UjFjazF9
- Encode melalui base64
- Dan menghasilkan flag

Flag: IDN_FLAG{W3B_3NCod3_7R1ck1}

Casino 777

Deksripsi :

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

Author : Mohamad Fattyr

Lampiran : https://ctf.solusiber.com/casino_777/

Solusi :

- Buka source code lalu find flag disana terlihat flag terletak di script yaitu

Flag : IDN_CTF{M4st3r_0f_H77P_R3qu3st_M4n1pul4t10n!}

Welcome Flag

Forgot Encode

Deskripsi :

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

bantu orang tersebut untuk menemukan rahasianya:

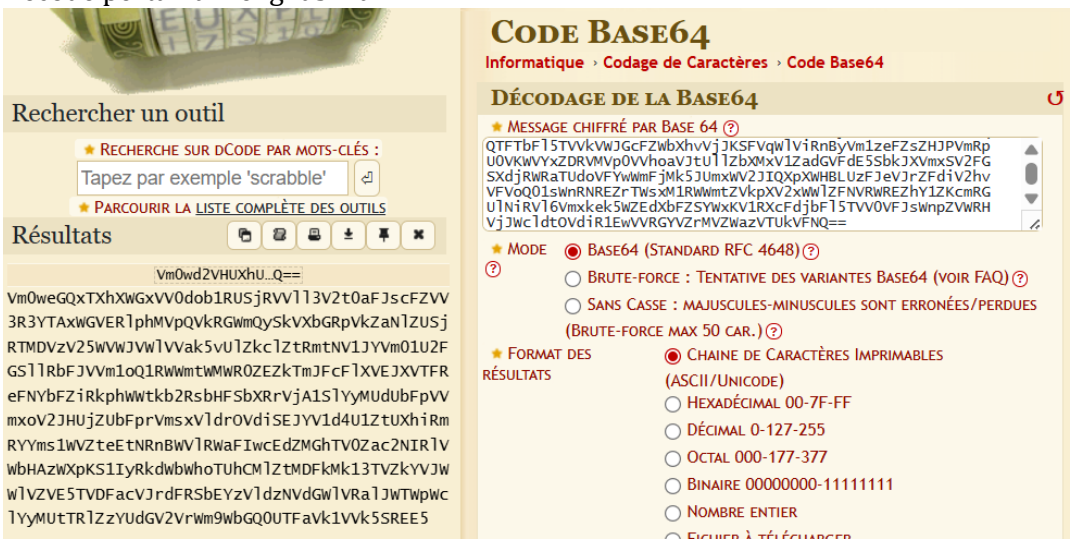
Vm0wd2VHUXhUWGhYV0d4VlYwZG9iMVJVU2pSVlZsbDNWMnQwYUZKc2NG
WlZWM1IzWVRBeFdHVkVSbHBoTVZwUVZrUkdXbVF5U2tWWGJHUnBWa1ph
TmxaVVNqUlRNRFZ6VjI1V1ZXSlZXbFZWYWs1dlVsWmtjbFp0Um10TlYxSlIWbT
AxVTJGR1NsbFJiRkpWVm0xb1ExUldXbXRXTVdSMFpFWmtUbUpGY0ZsWFZFSl
hWVEZSZUZOWWJGWmlSa3BoV1d0a2IyUnNiSEZTYlhSclZqQTFTbFl5TVVkVWJ
GcFZWbXhvVjJKSFVqWlViRnByVm1zeFZsZHJPVmRpU0VKWVYxZDRVMVp0VV
hoaVJtUllZbXMxV1ZadGVFdE5SbkJXVmxSV2FGSXdjRWRaTUdoVFYwWmFjMk5
JUmxWV2JIQXpXWHBLUzFJeVJrZFdiV2hvVFVoQ01sWnRNREZrTWsxM1RWW
mtZVkpXV2xWWlZFNVRWREZhY1ZKcmRGUlNiRVl6Vmxkek5WZEdXbFZSYWx
KV1RXcFdjbFl5TVV0VFJsWnpZVWRHVjJWcldtOVdiR1EwVVRGYVZrMVZWazV
TUkVFNQ==

Author: Rafly Permana

Lampiran :

Solusi :

- Gunakan decode base64
- Decode pertama menghasilkan



- Karna masih belum menemukan kita coba decode lagi
- Decode kedua juga masih gagal

- Kita coba decode untuk ketiga kalinya
- Ternyata masih gagal

- Decode lagi

- Decode lagi

- Kita coba decode sampai berhasil disini terlihat decoder semakin sedikit

- Setelah 7 kali decode akhirnya menemukan flagnya

Flag : IDN_CTF{base64_in_action_but_7_times}

Web 303

DOM-Based XSS

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana **Author: Rafly Permana **

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

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code 27oFx9NE945YFuBYFshct2G4Mi3hmKpS7UTWS87yKMn
- Lakukan decoder menggunakan base 58

Flag : IDN_CTF{dom_based_xss_executed}

Unsafe eval()

Deskripsi ;

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana **Author: Rafly Permana **

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

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code 8K1iQbpVVMPdiYxaREW9wJvvCmBnKZnNn9VguPSy71veTjEc
- Lakukan decoder menggunakan base 58

Flag : IDN_CTF{you_used_eval_successfully}

Prototype Pollution Demo

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana **Author: Rafly Permana **

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

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code ZGW9mAgck8zohQPm4DeKSaKYAFRft9nPpb88Hj7nWrDtPcgyS
- Lakukan decoder menggunakan base 58
- 

Flag : IDN_CTF{prototype_pollution_success}

JWT Token Manipulation

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana **Author: Rafly Permana **

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

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code FgUreh9sJv91wCs9a98YnG7VDuumwf96zBUnieQzY
- Lakukan decoder menggunakan base 58

Flag : IDN_CTF{jwt_token_manipulated}

Client-Side Privilege Escalation

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana **Author: Rafly Permana **

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

Solusi :

- Ubah role pada console menggunakan localStorage.setItem('user_role', 'admin');
- Ditemukan code 2DvT8boTciwZu4ZctauqBoqJaMKWk8xbK5mAmgPqCTjQ9NX2xGEGgGHXFA
- Lakukan decoder menggunakan base 58

Flag : IDN_FLAG{client_side_privilege_escalation}

Timing Attack

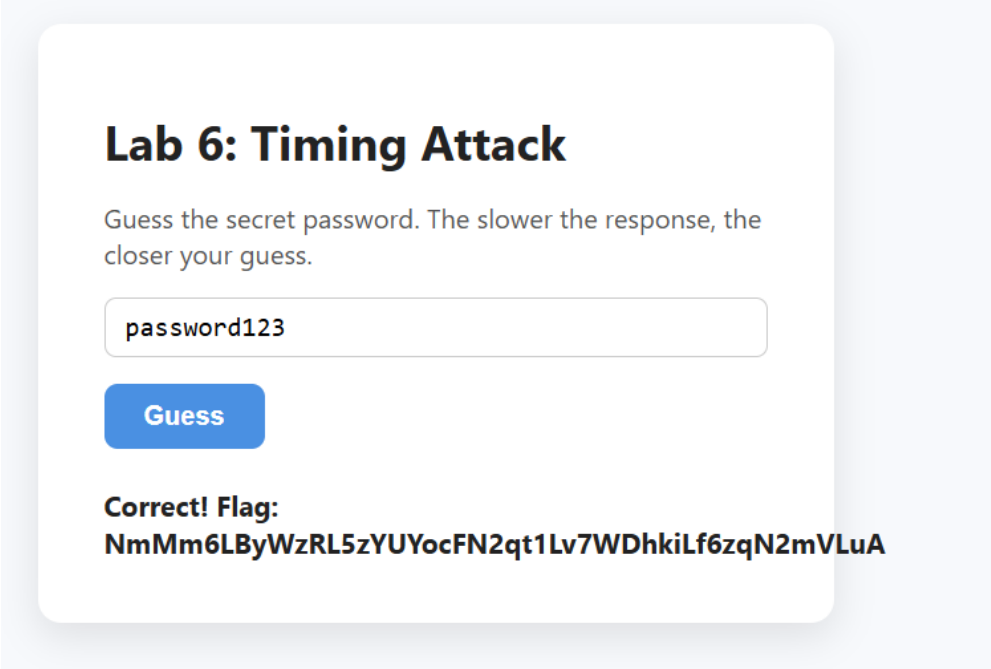
Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana **Author: Rafly Permana **

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

Solusi :

- Disini kita langsung masuk ke sources dan menemukan passwordnya yaitu password123



-
- Lakukan decoder menggunakan base 58

-

Unsafe Deserialization

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana **Author: Rafly Permana **

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

Solusi :

- Disini kita langsung masuk ke sources dan mencari flagnya dikarenakan flag terletak pada script
- Ditemukan code 4e9THmJfgagHkvXRC2T99EoKiSvisvU8PqSyvB3Fz3hnbKxJCNNeEYk
- Lakukan decoder menggunakan base 58
- 

Log Analysis

Log Analysis 1

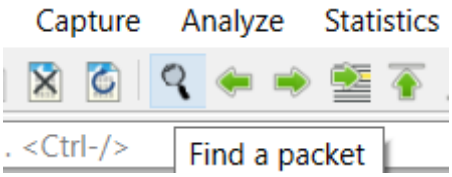
Deskripsi :

pada file pcap dibawah, hacker mencoba untuk melakukan sesuatu yang berhubungan dengan recon pada service, silahkan cari... Format Flag : IDN_CTF{jawaban} **Author : Aditya Firman Nugroho**

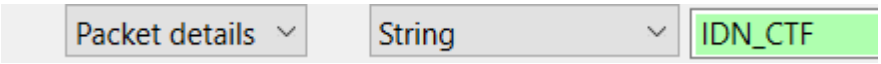
Lampiran : incident_respone_.pcapng

Solusi :

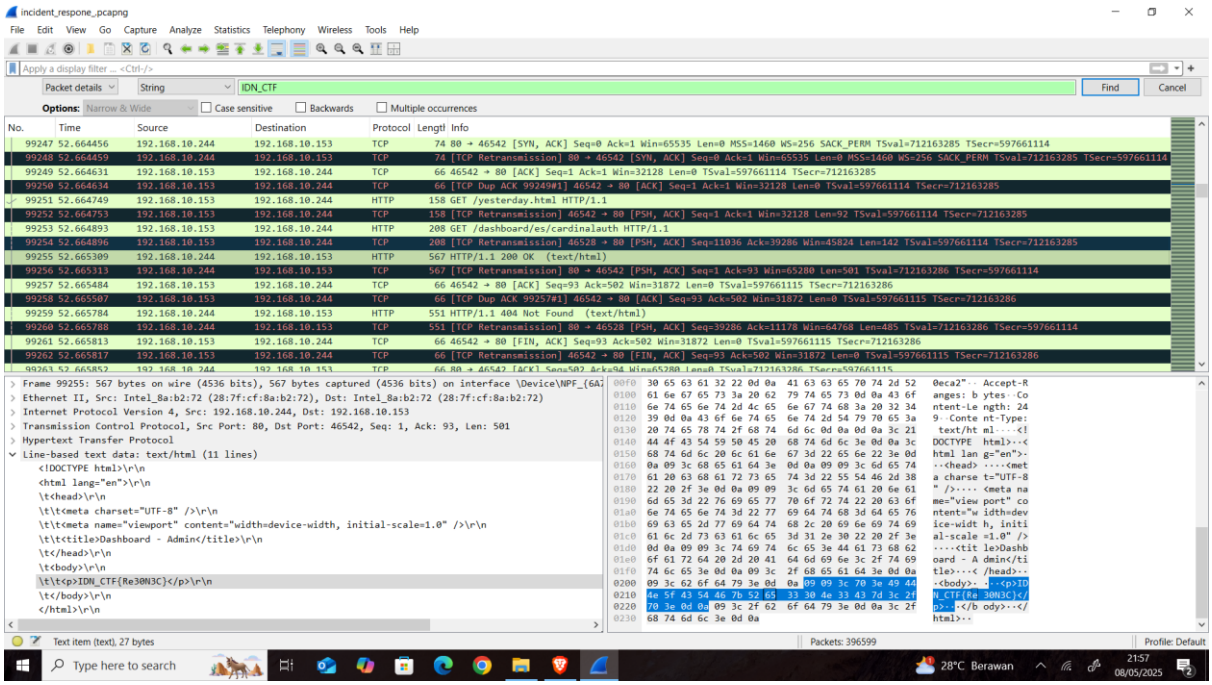
- Buka file pcap menggunakan wireshark.
- Lalu coba gunakan fitur **" find a packet".**



- Gunakan opsi **“ packet Details “** dan **“ string “** lalu cari text **“ IDN_CTF”**



- Menemukan packet yang berisi text html yang berisikan **“IDN_CTF”** .



Flag : IDN_CTF{Re30N3C}

Log Analysis 2

Deskripsi :

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

Format Flag : IDN_CTF{jawaban}

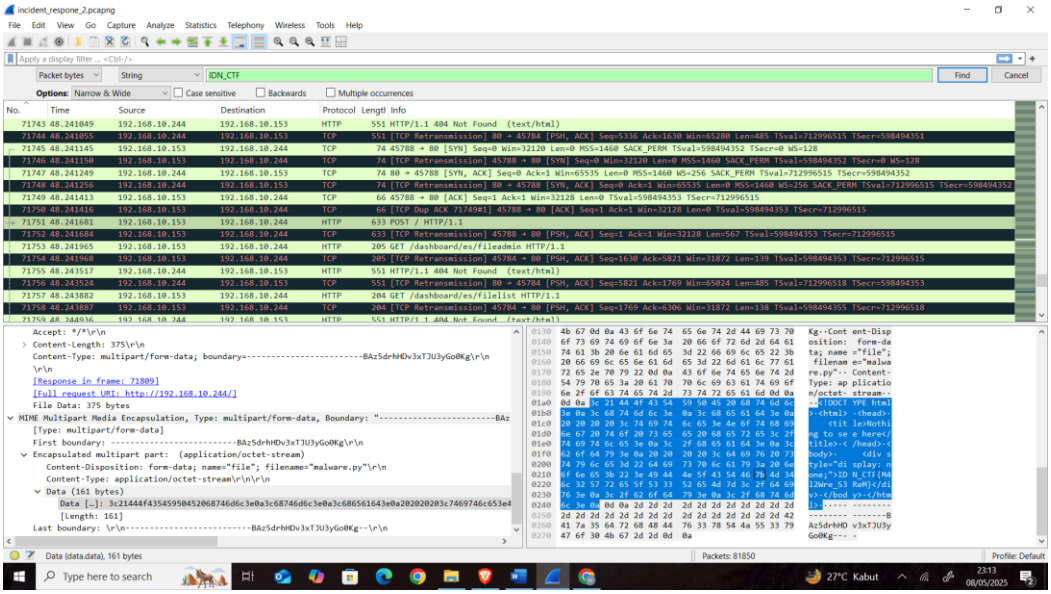
Author : Aditya Firman Nugroho

Lampiran : incident_respone_2.pcapng

Solusi :

- gunakan fitur **“ find a packet”.** Gunakan opsi **“ packet Details “** dan **“ string “** lalu cari text **“ IDN_CTF”** .

- Tidak ketemu, lalu coba keywords lain.
- Masih tidak ketemu juga. mulai mengamati lalu lintas jaringan, mungkin flag adalah nama serangannya.
- Lalu coba lagi gunakan fitur **" find a packet".** namun gunakan opsi **" packet bytes "** dan **" string "** lalu cari text **" IDN_CTF".** Ketemu.



Flag : IDN_CTF{M4l2Wre_S3ReM}

Log Analysis 3

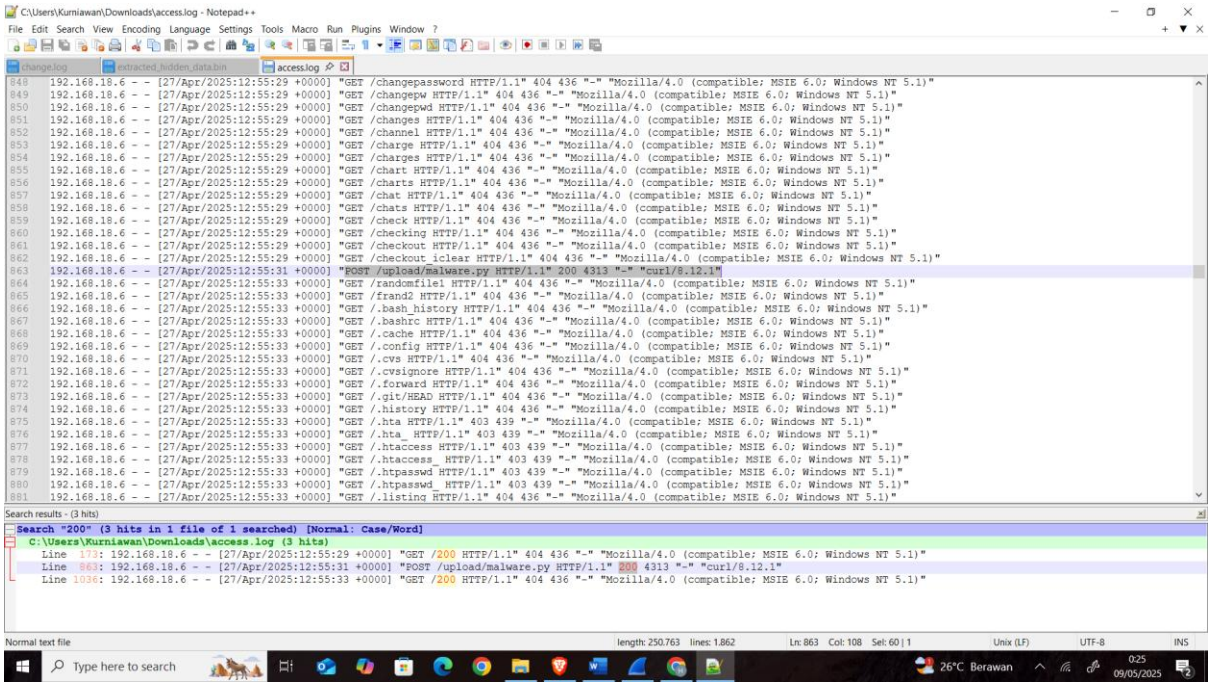
Deskripsi :

analisis log acces.log ini, file ip yang dimasukan pada system ? Format Flag : IDN_CTF{jawaban} Author : Aditya Firman Nugroho

Lampiran : access.log

Solusi :

- Menggunakan aplikasi Notepad++ untuk membuka file lognya.
- Gunakan fitur Find untuk mencari kata kunci **"200",** karena kode **HTTP 200** menandakan akses berhasil.
- Dari hasil pencarian, ditemukan bahwa file **malware.py** berhasil dikirim ke endpoint /upload menggunakan metode POST.



Flag : IDN_CTF{malware.py}

Log Analysis 4

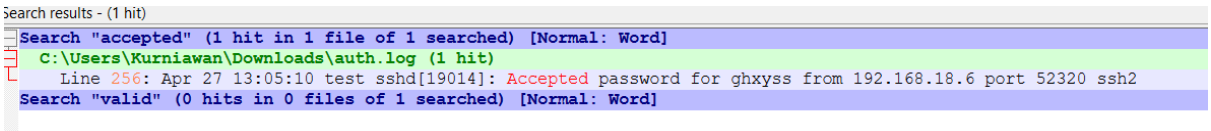
Deskripsi :

analis log auth.log, user apa yang sukses masuk ke dalam system ? Format Flag : IDN_CTF{user} Author : Aditya Firman Nugroho

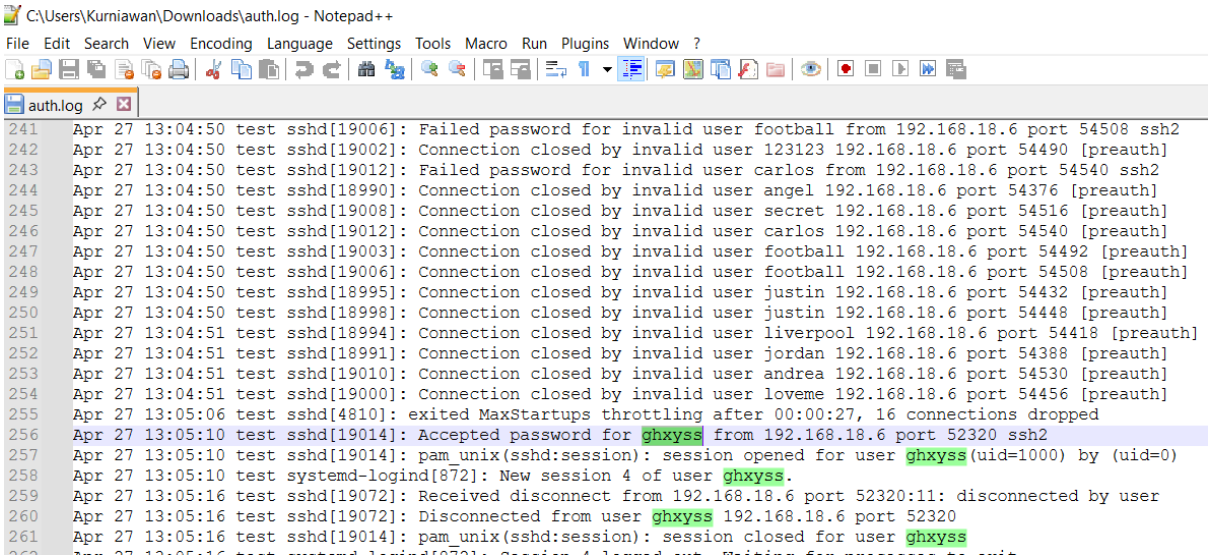
Lampiran : auth.log

Solusi :

- Gunakan aplikasi notepad, lalu gunakan fitur findnya untuk mencari keyword **“ valid “** (match whole word only) tidak ditemukan.
- Lalu cari keyword **“ accepted “,** ditemukan.



- Dari keyword itu ditemukan **“ghxyss”**. Selanjutnya di line berikutnya dapat mengetahui bahwa itu merupakan nama user dan berhasil masuk ke system.



Flag : IDN_CTF{ghxyss}

Log Analysis 5

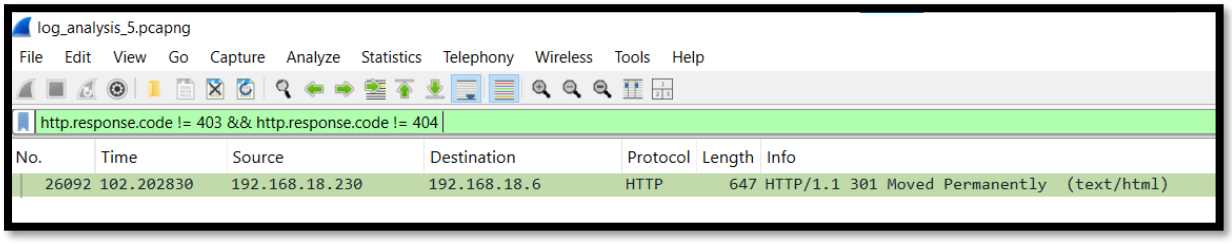
Deskripsi :

> "dengan service ... file ... di dalam server " - administrator
>
> Format Flag : IDN_CTF{service:file}
>
> Author : Aditya Firman Nugroho

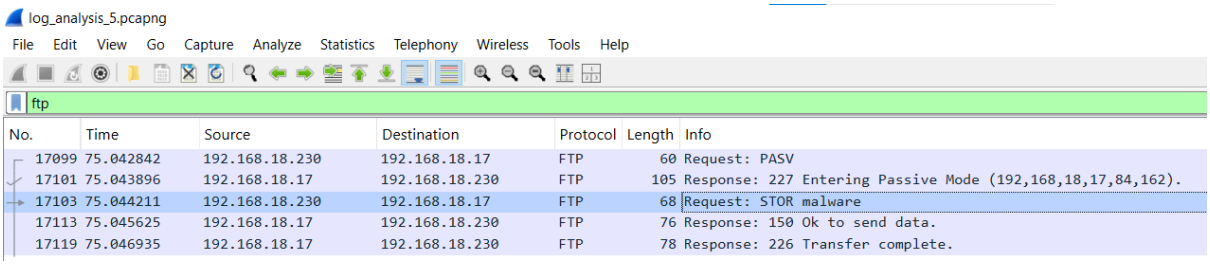
Lampiran : log_analysis_5.pcapng

Solusi :

- Dari deskripsi bisa diartikan men-upload file ke server, untuk upload file biasanya menggunakan service **HTTP dan FTP**.
- Gunakan fitur **"display filter"** , input keyword **HTTP.** Data yang ditampilkan masih banyak dan **HTTP response** nya banyak yang sama yaitu **not found**, lalu gunakan keyword filter tambahan **" http.response.code != 403 && http.response.code != 404".** Hasilnya tidak ada yang berhasil masuk.



- mencoba gunakan filter dengan keyword **FTP**. Lalu menemukan perintah **STOR**. Dan di line selanjutnya menunjukkan **transfer complete**.



Flag : IDN_CTF{ftp:malware}

Log Analysis 6

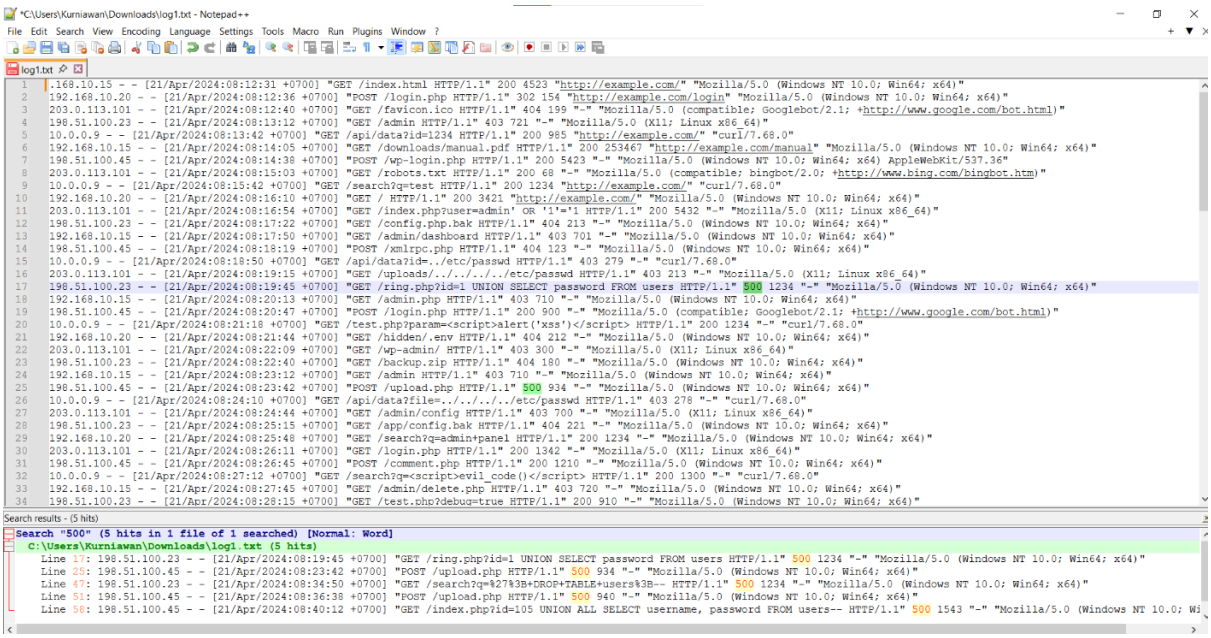
Deskripsi :

> Seseorang mencoba mengeksploitasi endpoint dengan teknik SQL Injection, menghasilkan internal server error. Apa nama file yang ditargetkan dalam eksploitasi tersebut?
>
> IDN_CTF{jawaban}
>
> Author: Rafly Permana

Lampiran : log1.txt

Solusi :

- kode **internal server error = 500**
- gunakan fitur **find** untuk mencari keyword **"500".**



- Terdapat query **UNION SELECT**, teknik umum dalam **SQL Injection** Dan **Target kolom sensitive** yaitu **password FROM users.**
- **“ GET /ring.php? “** menunjukkan bahwa file **ring.php** adalah **endpoint** yang diminta.

Flag : IDN_CTF{ring.php}

Log Analysis 7

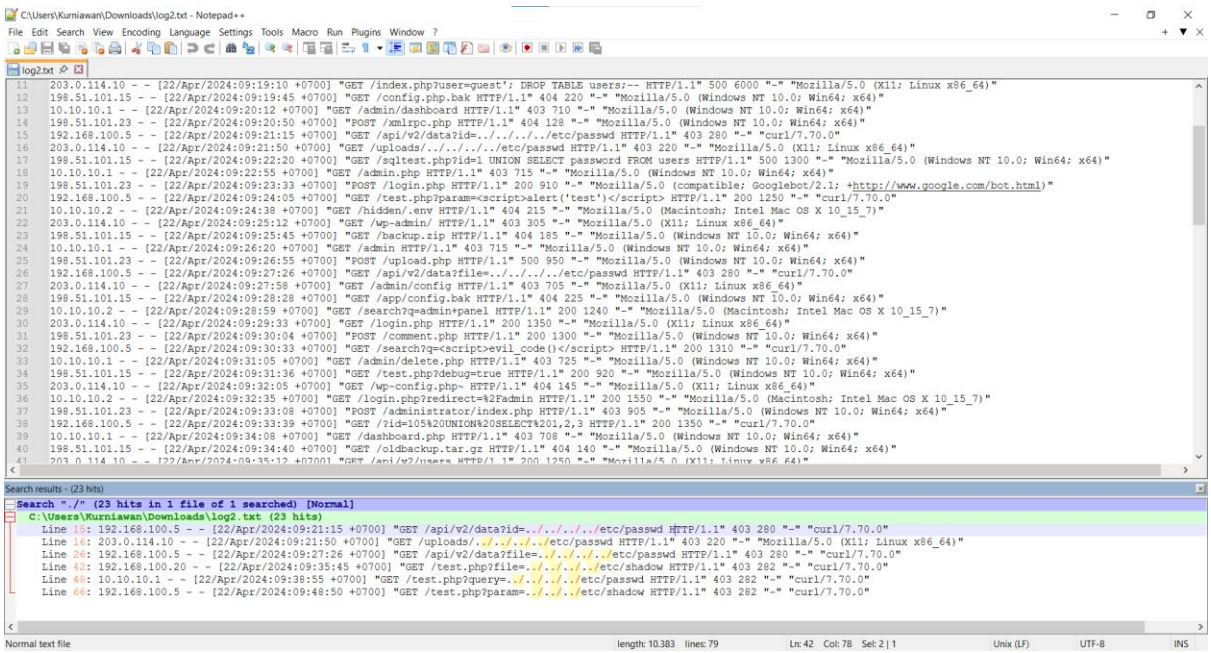
Deskripsi :

> Ada upaya eksploitasi menggunakan path traversal dalam permintaan ke endpoint API. Apa parameter lengkap yang digunakan penyerang?
>
> IDN_CTF{jawaban}
>
> Author: Rafly Permana

Lampiran : log2.txt

Solusi :

- **Path traversal** biasanya path yang mengandung path **..** , // , **../../../** .
- Menggunakan fitur **find** untuk mencari **pattern path traversal**.
- Ditemukan beberapa line yang mengandung **pattern** path traversal dan yang paling **sensitive** adalah **../../../../etc/passwd**.



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

Log Analysis 8

Deskripsi :

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

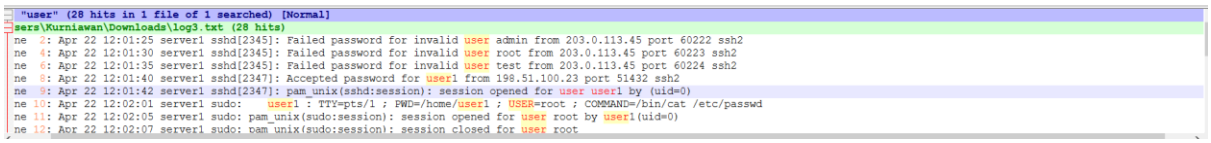
IDN_CTF{jawaban}

Author: Rafly Permana

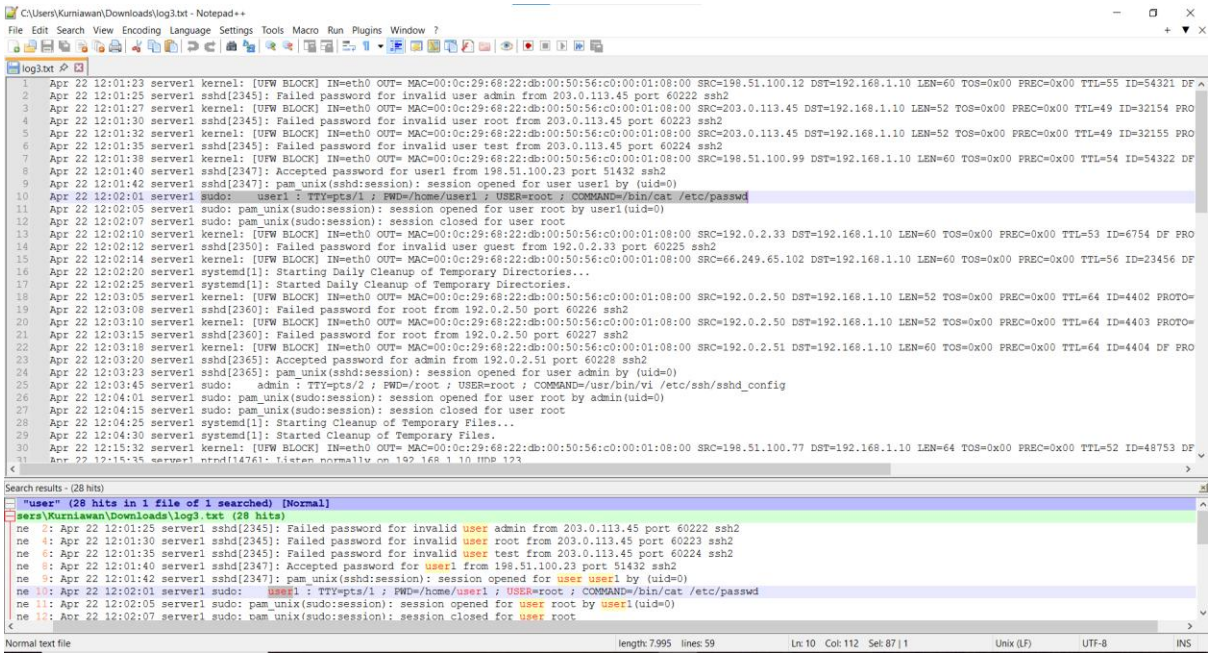
Lampiran : log3.txt

Solusi :

- Gunakan fitur find untuk mencari keyword " **USER** ".



- Di line yang berisi **user1** , terdapat informasi bahwa **user1** mendapatkan akses **root**.
- IP Adress **user1** adalah : **198.51.100.23**



Flag : IDN_CTF{198.51.100.23}

Log Analysis 9

Deskripsi :

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

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

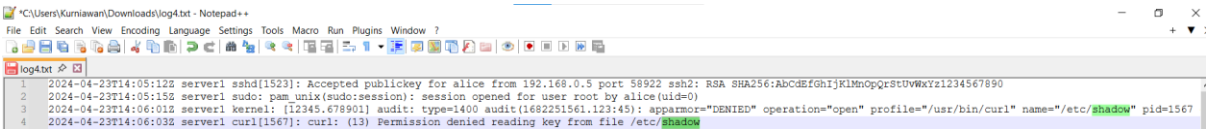
IDN_CTF{jawaban}

Author: Rafly Permana

Lampiran : log4.txt

Solusi :

- Cari baris yang mengandung " **shadow** ".



- Dari baris yang ditemukan. mendapatkan informasi bahwa ada yang mencoba membaca file **shadow** menggunakan **curl** namun ditolak oleh **AppArmor**.
- sebelum baris itu hanya user **Alice** saja yang tercatat **login**. Dan pada baris 2, user **alice** mendapatkan akses **root**.

Flag : IDN_CTF{alice,192.168.0.5,SHA256:AbCdEfGhIjKlMnOpQrStUvWxYz1234567890}

Forensic

Forensic 1

Deskripsi :

ngomongin crypto, selain encryption itu ada apa lagi ya ?

material.png

Author: Aditya Firman Nugroho

Lampiran : Material.png

Solusi :

- Download file Material tersebut
- untuk melihat, memodifikasi, dan menghapus metadata (data informasi tentang file) dalam berbagai jenis file seperti gambar
- Cari di kolom Comment pada data foto nya

Flag : IDN_CTF{W0W_wh4T_K03NC1D3CE}

Forensic 2

Deskripsi :

Qris

2 kali

Author : Mohamad Fattyr

Solusi :

- Scan Kode QRIS menggunakan aplikasi Scanner
- Akan tampil kode U1VST1gwWk1RVWQ3VmpOU04xOWxORk0zWDFJaE9VaFVmUT09

- Segera decode menggunakan base decode 64
- Akan tampil kode lagi SUROX0ZMQUd7VjNSN19lNFM3X1IhOUhUfQ==
- Kemudian ulangi decode lagi dan akan tampil Flag nya

Flag : IDN_FLAG{V3R7_e4S7_R!9HT}