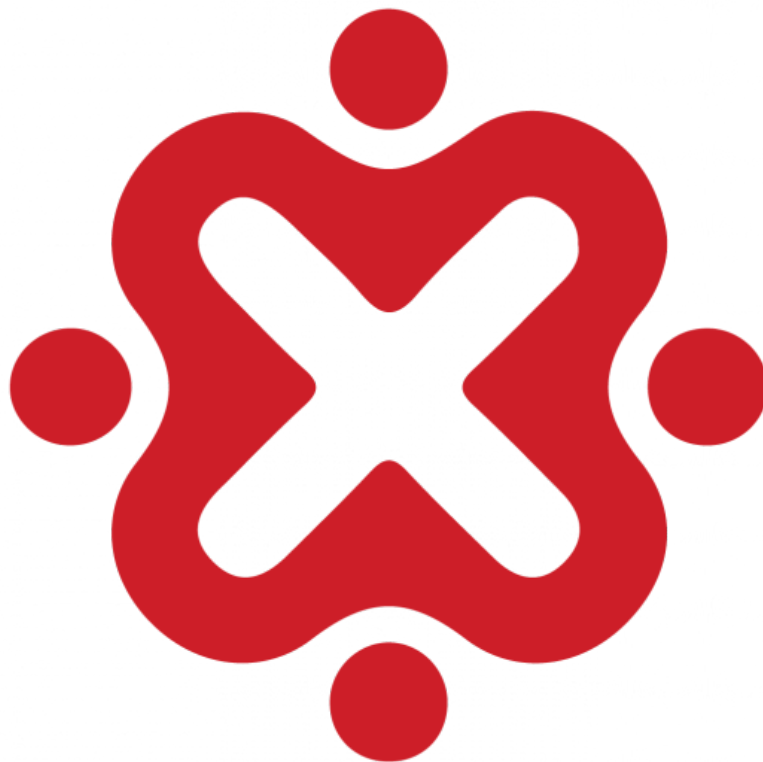




Team Huraaa

Team yang sangat ingin masuk Bootcamp



ID-Networkers
Indonesian IT Expert Factory



Introduction Team	3
Summary Findings Each Category	4
Detail Challenge Solved	5
Welcome Flag	5
Forgot Encode	5
Other	6
User Guide	6
Cryptography	7
Might Guy's Secret	7
Rot1Aoka	7
Pramuka	8
Classic Cryptography	8
Simple Substitution Cipher	9
USB Forensic	10
USB Forensic 1	10
USB Forensic 2	10
USB Forensic 3	11
USB Forensic 4	12
USB Forensic 5	12
USB Forensic 6	13
USB Forensic 7	14
USB Forensic 8	14
Browser Forensic	16
Browser Forensic 1	16
Browser Forensic 2	16
Browser Forensic 3	17
Browser Forensic 4	18
Browser Forensic 5	18
Browser Forensic 6	19
Browser Forensic 7	20
Browser Forensic 8	20
Browser Forensic 9	21
Browser Forensic 10	22
Web Exploit	23
Hidden Buy Flag	23
Konoha Breach	23
ID-Networkers	24
Kue Monster	25
Code Analysis	25
IDN Education	26



Beyond Way	26
I'm Not Me, You Are Me	27
Circle Clicker	27
XSS	28
Awesome Website	28
Casino 777	29
Web 303	30
DOM-Based XSS	30
Unsafe eval()	30
Prototype Pollution Demo	31
JWT Token Manipulation	31
Client-Side Privilege Escalation	32
Timing Attack	32
Unsafe Deserialization	33
Log Analysis	34
Log Analysis 1	34
Log Analysis 2	34
Log Analysis 3	35
Log Analysis 4	35
Log Analysis 6	36
Log Analysis 7	36
Log Analysis 8	37
Log Analysis 9	38
Forensic	39
jadi gini...	39
QRIS	39



Introduction Team

Nama Team : Team Huraaa





Anggota : Zotac, ReyhanAlFarel, abdullahfakih

Team Huraaa

Teams: Team yang sangat ingin masuk Bootcamp

94th place

540 points



Members

User Name	Score
zotac	20
ReyhanAlFarel Captain	410
abdullahfakih	110

Point : 540



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	8/9	80
USB Forensic	8/8	80
Browser Forensic	10/10	100
Windows Forensic	0/15	0
Forensic	2/2	20

Pengurangan Nilai : 0 Point



Detail Challenge Solved

Welcome Flag

Forgot Encode

Deskripsi :

seseorang menggunakan encoding untuk menyimpan rahasianya tapi dia melakukannya sambil berbincang dengan orang lain sehingga dia lupa.

bantu orang tersebut untuk menemukan rahasianya:

```
Vm0wd2VHUXhUWGhYV0d4VIYwZG9iMVJVU2pSVlZsbDNWMnQwYUZKc2NGWI  
ZWM1IzWVRBeFdHVkVSbHB0TVZwUVZrUkdXbVF5U2tWWGJHUnBWalphTmxaV  
VNqUIRNRfZ6VjI1V1ZXSlZXbFZWYWs1dIVsWmtjbFp0Um10TIYxSllWbTAxVTJGR  
1NsbFJiRkpWVm0xb1ExUldXbXRXTVdSMFpFWmtUbUpGY0ZsWFZFSlhWVEZSZU  
ZOWWJGWmlSa3BoV1d0a2IyUnNiSEZTYlhScjZqQTFTbFl5TVVkvVWJGcFZWbXhvV  
jJKSFVqWlViRnByVm1zeFZsZHJPVmRpU0VKWVYxZDRVMVp0VVhoaVJtUllZbXM  
xV1ZadGVFdE5SbkJXVmxSV2FGSXdjRWRaTUdoVFYwWmFjMk5JUmxWV2JlQXp  
XWHBLUzFJeVJrZFdiV2hvVFVoQ01sWnRNREZrTWsxM1RWWmtZVkpXV2xWWlZ  
FNVRWREZhY1ZKcmRGUlniRVl6Vmxkek5WZEdXbFZSYWxKV1RXcFdjbfFl5TVV0  
VFJsWnpZVWRHVjJWcldtOVdiR1EwVVRGYVZrMVZWazVTUkVFNQ==
```

Author: Rafly Permana

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“ Terlihat dari Deskripsi bahwa ini adalah pesan encoding, dan dia lupa sampai berapa dia encoding.. terlihat bahwa yang dia gunakan juga base64 dengan ciri “==”, maka dari itu saya mencoba untuk melakukan decoding dengan cyberchef beberapa kali...”

Flag : IDN_CTF{base64_in_action_but_7_times}



Other

User Guide

Deskripsi :

FLAG

Lampiran : None

Solved by : Reyhan Al Farel

Solusi :

“Terdapat flag di akhir PDF yang tidak terlihat kasat mata. Namun, ketika kita block semua pada page terakhir, akan muncul flagnya”

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

Author : Nur Cholis Majid

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

"Pertama-tama kita mengenali referensi "Giovan Battista Bellaso: 1553" yang menandakan penggunaan cipher Bellaso (Vigenère) dan kunci idnmantab; dengan menerapkan dekripsi Vigenère pada teks dalam kurung kurawal menggunakan kunci tersebut"

Flag : IDN_CTF{c067j1723pc40c5i33n656asdsd60cas67i9606}

Rot1Aoka

Deskripsi :

Clue nya udah jelas kan?

VQA_SYNT{C3Z4A4F4A_QH1H_94F1u}

Author : Mohamad Fatty



Lampiran : None

Solved by : Reyhan Al Farel

Solusi :

“Terdapat flag di code tersebut. Code tersebut menggunakan Caesar Cipher (Rot13), lalu saya decode di online decode dan menghasilkan flag dibawah ini.”

Flag : **IDN_FLAG{P3M4N4S4N_DU1U_94S1h}**

Pramuka

Deskripsi :

terjemahan kan pesan tersebut. Format Flag

IDN_CTF{****}

Author : Mohamad Fattyr

morse.wav

Lampiran : None

Solved by : Reyhan Al Farel

Solusi :

“Terdapat flag di dalam audio morse tersebut. Caranya adalah kita decode dulu di website decode morse, lalu saya mendapatkan m0rs3c0d3r19ht. Saya pikir hanya itu saja flagnya, namun saya tambahkan underscore di setiap katanya.”

Flag : **IDN_CTF{m0rs3_c0d3_r19ht}**

Classic Cryptography

Deskripsi :



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

Author: Rafly Permana

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Terdapat flag di dalam code tersebut. Code tersebut di encode menggunakan Caesar Cipher (Shift) dengan pergeseran +1. Saya decode dan menghasilkan code berikut.”

Flag : IDN_CTF{yayy_you_are_great}

Simple Substitution Cipher

Deskripsi :

ORF_EZY{ziol_ol_g_yqsx_wxz_lg_tq_ln}

Author: Rafly Permana

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Code tersebut di encode menggunakan Simple Substitution Cipher dengan Substitusinya sesuai dengan layout keyboard, yaitu : QWERTYUIOPASDFGHJKLZXCVBNM. Setelah itu saya mendapatkan flagnya.”

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}
Author: Aditya Firman Nugroho
usb.zip

Lampiran : None

Solved by: ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . Nama merek ada di dalam file USBTOR.hiv, saya menggunakan reglookup untuk melihat isinya dan mendapatkan flagnya.”

Flag : IDN_FLAG{JetFlash_Transcend_8GB_USB_Device}

USB Forensic 2

Deskripsi :

ada hacker, physical acces ke laptop.. bantuin dong !
(Filanya ada di pertanyaan pertama)
ClassGUID Pada USB Hacker ?
format flag : IDN_FLAG{Jawaban yang disoal}



usb.zip

Lampiran : None

Solved by: Reyhan Al Farel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . ClassGUID juga ada pada USBTOR.hiv, saya menggunakan reglookup dengan combine pipe grep untuk mendapatkan GUID tersebut.”

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

Masih salah, wait.

USB Forensic 3

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Apa Containder ID USB Yang dipakai Hacker ?

format flag : **IDN_FLAG{Jawaban yang disoal}**

usb.zip

Lampiran : None

Solved by: Reyhan Al Farel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . ContainerID USB ada di USBTOR.hiv, saya menggunakan reglookup dan combine dengan pipe grep.”

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



USB Forensic 4

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Apa Disk ID yang dipakai hacker ?

format flag : IDN_FLAG{Jawaban yang disoal}

usb.zip

Lampiran : None

Solved by : Reyhan Al Farel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . DiskID yang dipakai hacker ada didalam USBTOR.hiv, saya juga menggunakan reglookup untuk mencarinya.”

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

USB Forensic 5

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Apa Serial ID USB Yang dipakai Hacker ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho



usb.zip

Lampiran : None

Solved by : Reyhan Al Farel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . SerialID USB ada didalam file USBTOR.hiv, saya menggunakan reglookup untuk mendapatkannya.”

Flag : IDN_FLAG{XRVZQBFR&0}

USB Forensic 6

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Nama File Yang ada di USB ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

usb.zip

Lampiran : None

Solved by : Reyhan Al Farel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . Nama File ada didalam NTUSER.dat. Saya menggunakan tools Registry Explorer GUI.
—>NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs. Disitu saya menemukan nama filanya.”

Flag : IDN_FLAG{4fu284428u5984-8308848.txt}



USB Forensic 7

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Direktory Yang ada di usb ?

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

usb.zip

Lampiran : None

Solved by : Reyhan Al Farel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . Nama Direktori ada didalam NTUSER.dat. Saya menggunakan tools Registry Explorer GUI. ->NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer. Disitu nama foldernya masih di encode, jadi saya decode terlebih dahulu dan mendapatkan hasilnya.”

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

USB Forensic 8

Deskripsi :

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

(Filanya 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

Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada 5 file, yaitu adalah MountPoints2.hiv, NTUSER.dat, RecentDocs.hiv, USBTOR.hiv, USRCLASS.dat . File dibuka ada pada file {lupa}, namun saya memakai reglookup untuk melihat isinya dan terdapat waktu xxxx-xx-xx xx:xx:xx”

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



Browser Forensic

Browser Forensic 1

Deskripsi :

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

Tools apa yang di cari oleh user ?

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

browser.zip

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Namun saya mengeceknya di folder Default dan bahkan saya masuk ke dalam browser tersebut dengan perintah **chromium --user-data-dir="\$HOME/Downloads/browser/Acuatiation/User Data"** . Disitu user men search 7 website, salah satunya tools github yaitu mimikatz. “

Flag : IDN_FLAG{mimikatz}

Browser Forensic 2

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Website apa yang dicari oleh user berkaitan dengan Teknik Persistence, Privilage



Escalation, DLL Injection etc ?

format flag : IDN_FLAG{Jawaban yang disoal}

browser.zip

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Namun saya mengeceknya di folder Default dan bahkan saya masuk ke dalam browser tersebut dengan perintah **chromium** **--user-data-dir="\$HOME/Downloads/browser/Acuatation/User Data"** . Disitu user men search 7 website, salah satunya Website yang berkaitan dengan Persistence, Privilege Escalation, dll. “

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

Browser Forensic 3

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

Streaming Website yang ditonton oleh user ?

format flag : IDN_FLAG{Jawaban yang disoal}

Author: Aditya Firman Nugroho

Lampiran : None

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Namun saya mengeceknya di folder Default dan bahkan saya masuk ke dalam browser tersebut dengan perintah **chromium** **--user-data-dir="\$HOME/Downloads/browser/Acuatation/User Data"** . Disitu user men search 7 website, salah satunya Website Streaming yang ditonton oleh user, yaitu : Netflix “

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



Browser Forensic 4

Deskripsi :

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

(Filanya 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}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Namun saya mengeceknya di folder Default dan bahkan saya masuk ke dalam browser tersebut dengan perintah **chromium** **--user-data-dir="\$HOME/Downloads/browser/Acuatition/User Data"** . Disitu user men search 7 website, user memakai 2 vpn yaitu adalah Browsec VPN dan VPN Proxy VeePN. “

Flag : IDN_FLAG{Browsec_VPN-VPN_Proxy_VeePN}

Browser Forensic 5

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

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

format flag : IDN_FLAG{Jawaban yang disoal} example : XX:XX:XX.XXX



Auhtor: Aditya Firman Nugroho

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Saya mengecek visit duration dengan menggunakan tools DB Browser, dan saya cari di file History sql. Pada tabel visits terdapat column visit duration, namun saya menggunakan query untuk mendapatkan visit duration yang sesuai dengan XX:XX:XX.XXX“

Flag : **IDN_FLAG{00:00:32.509}**

Browser Forensic 6

Deskripsi :

Ada Volation 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}**

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Saya menggunakan DB Browser SQLite untuk mendapatkan email tersebut, ke /Default/ dan cari emailnya tersebut di dalam DB Browser.“

Flag : **IDN_FLAG{ghxyssforunfun@gmail.com}**



Browser Forensic 7

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

date_created pada email menggunakan tools DB Browser SQLite ?

format flag : IDN_FLAG{Jawaban yang disoal}

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Date_created saya menggunakan tools DB Browser SQLite yang berada di file Web Data. Dan saya menemukannya di table {lupa} di column date_created“

Flag : IDN_FLAG{1746250363}

Browser Forensic 8

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

url favicon, di website yang dicari oleh user ? (tidak berkaitan dengan hacker !!!)

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : None



Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Url falcon juga menggunakan DB Browser terdapat di file Favicon, disitu terdapat jawaban url favicon.”

Flag :

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

Browser Forensic 9

Deskripsi :

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

(Filanya ada di pertanyaan pertama)

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

format flag : IDN_FLAG{Jawaban yang disoal}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Extension Id dari vpn VeePN ada folder Default/Extensions, disitu ada 3 / 4 macam extension id, lalu tinggal dicocokkan saja satu per satu.”

Flag : **IDN_FLAG{majdfhpaihoncoakbjgbdhglocklegno}**



Browser Forensic 10

Deskripsi :

Ada Volation 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}

Auhtor: Aditya Firman Nugroho

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Dalam zip tersebut ada banyak sekali folder dan file. Extension version dari VPN VeePN berada di file Default/Extensions/{majdfhpaihoncoakbjgbdhglocklegno}. Disitu terdapat versionnya.

Flag : IDN_FLAG{3.4.3_0}



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.

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

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada website tersebut saya menggunakan tools Burp Suite dan menaruhnya di intruder dengan merubah saldo kamu : 100000000000. Setelah itu membeli barang tersebut dan mendapatkan flagnya.”

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?

Website : https://ctf.solusiber.com/login_bypass/

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada website tersebut saya menggunakan tools nmap untuk mendapatkan credentials dari admin. Setelah masuk ke admin, disitu terdapat banyak data, dan saya mendapatkan flagnya di source code yang dikomentari.”

Flag : `IDN_CTF{c0NRats_you_goin_tohe_insideee}`

ID-Networkers

Deskripsi :

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

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

Tapi kamu bukan crawler, kamu seorang penyusup yang teliti.

Website : https://ctf.solusiber.com/robots_dashboard/

Lampiran : None

Solusi :

“Pada website tersebut saya langsung kasih query /robots.txt, dan disitu terdapat html yang tersembunyi. Setelah itu saya buka dan mendapatkan flagnya..”

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



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)

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

Lampiran : None

Solved by : zotac

Solusi :

“Pada website tersebut saya inspect element dan mendapatkan encode dari cookie tersebut. Setelah itu saya decode hingga menghasilkan flagnya.”

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

Code Analysis

Deskripsi :

Tanjiro terus berlatih tanpa henti untuk menguasai Hinokami Kagura demi mengalahkan iblis Bulan Atas. Bantu dia membuka kekuatan sejatinya dengan menganalisis kode yang diberikan. Kunci untuk tingkat kekuatan berikutnya terletak pada pemahaman alur kerjanya kode.

Website : https://ctf.solusiber.com/tanjiro_code/

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada website tersebut saya langsung menambahkan query parameter ?secret=tanjirotanjiro. Dan langsung mendapatkan flagnya.”

Flag : `IDN_CTF{d0ub!e_t4njiro_m4ke_u_H4ppy?}`



IDN Education

Deskripsi :

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

Website : https://ctf.solusiber.com/tanjiro_code/

Author : Rafly Permana

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada website tersebut menggunakan banyak sekali decode, yang pertama saya kasih parameter https://ctf.solusiber.com/idn_edu/?page=php://filter/read=convert.base64-encode/resource=index.php

lalu mendapatkan encode yang berisikan main elemennya, lalu saya tambahkan /resource=flag.txt pada parameter dan mendapatkan value : SUROX0NURntsQHRpc2VjX3IyOS1sb2Fken0K“

Flag : **IDN_CTF{l@tisecc_r29-loadr}**

Beyond Way

Deskripsi :

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



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

Author : Rafly Permana

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :



“Pada website tersebut saya menggunakan tools ffuf untuk mendapatkan enumerate dan coba coba setelah itu dapat flagnya.”

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!

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

Author : Rafly Permana

Lampiran : None

Solved by : zotac

Solusi :

“Pada id nya tinggal ganti menjadi 0, dan langsung keluar data admin beserta flagnya”

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

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

Author : Mohamad Fatty



Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada website tersebut saya menggunakan DOM pada event clicker hingga 1000x, setelah itu mendapatkan code bahwa harus memanggil function resolve(lupa), namun akhirnya terdapat code encode, lalu saya decode dan akhirnya mendapatkan flagnya.”

Flag : **IDN_CTF{click_master}**

XSS

Deskripsi :

CURI!!

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

Author : Mohamad Fatty

Lampiran : None

Solusi :

“Pada website tersebut saya langsung console.log(document.cookie) ataupun melihat cookienya, dan langsung mendapatkan cookienya.”

Flag : **IDN_FLAG{XSS_C00K13_ST34L3R}**

Awesome Website

Deskripsi :

CARI!!



Author : Mohamad Fatty

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Pada website tersebut saya hanya memakai console untuk mendapatkan token idnya. Token ID tersebut di encode dengan base 64 dan saya decode untuk mendapatkan flagnya.”

Flag : **DN_FLAG{W3B_3NCod3_7R1ck1}**

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

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

Author : Mohamad Fatty

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Pada website tersebut saya eksplorasi URLnya dan saya manipulasi DOMnya untuk mendapatkan flag tersebut.”

Flag : **IDN_CTF{M4st3r_of_H77P_R3qu3st_M4n1pul4t10n!}**



Web 303

DOM-Based XSS

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

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

Author : Rafly Permana

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Pada website tersebut saya melihat source code dulu, setelah itu menjalankan functionnya dan mendapatkan code base58 dan saya decode untuk menghasilkan flagnya tersebut.”

Flag : **IDN_CTF{dom_based_xss_executed}**

Unsafe eval()

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

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

Author : Rafly Permana

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Pada website tersebut saya melihat source code dulu, setelah itu menjalankan functionnya dan mendapatkan code base58 dan saya decode untuk menghasilkan flagnya tersebut.”

Flag : **IDN_CTF{you_used_eval_successfully}**



Prototype Pollution Demo

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

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

Author : Rafly Permana

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Pada website tersebut saya melihat source code dulu, setelah itu menjalankan functionnya dan mendapatkan code base58 dan saya decode untuk menghasilkan flagnya tersebut.”

Flag : **IDN_CTF{prototype_pollution_success}**

JWT Token Manipulation

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

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

Author : Rafly Permana

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Pada website tersebut saya melihat source code dulu, setelah itu menjalankan functionnya dan mendapatkan code base58 dan saya decode untuk menghasilkan flagnya tersebut.”

Flag : **IDN_CTF{jwt_token_manipulated}**



Client-Side Privilege Escalation

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

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

Author : Rafly Permana

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada website tersebut saya langsung ganti local storage menjadi role : admin. Setelah itu mendapatkan code base54 yang nantinya saya decode dan dapat flagnya.”

Flag : **IDN_FLAG{client_side_privilege_escalation}**

Timing Attack

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Website : https://ctf.solusiber.com/web_101/lab6/

Author : Rafly Permana

Lampiran : None

Solved by : abdullahfakih

Solusi :

“Pada website tersebut saya melihat source code dulu, setelah itu menjalankan functionnya dan mendapatkan code base58 dan saya decode untuk menghasilkan flagnya tersebut.”

Flag : **IDN_CTF{timing_attack_successful}**



Unsafe Deserialization

Deskripsi :

Flagnya Di Encode Dengan Encoder yang sama dengan bitcoin dan solana

Website : https://ctf.solusiber.com/web_101/lab8/

Author : Rafly Permana

Lampiran : None

solved by : abdullahfakih

Solusi :

“Pada website tersebut saya melihat source code dulu, setelah itu menjalankan functionnya dan mendapatkan code base58 dan saya decode untuk menghasilkan flagnya tersebut.”

Flag : **IDN_CTF{unsafe_deserialization_executed}**



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 : None

Solved by : abdullahfakih

Solusi :

“Saya mencarinya menggunakan Wireshark dan saya arahkan ke file pcap tersebut dengan find tcp dan analisa 1 per 1.”

Flag : IDN_CTF{Re30N3C}

Log Analysis 2

Deskripsi :

awas, hati-hati, pelan-pelan, ada

Format Flag : IDN_CTF{jawaban}

Author : Aditya Firman Nugroho

Lampiran : None

Solved by : abdullahfakih



Solusi :

“Saya analisis 1 per 1 dari file tersebut menggunakan Wireshark dan mendapatkan flagnya tersebut.”

Flag : **IDN_CTF{M4I2Wre_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 : None

Solved by : ReyhanAlFarel

Solusi :

“untuk menganalisis access.log tersebut saya memakai tools {lupa} dia GUI based on terminal yang saya temukan dari github. Disitu saya bisa melihat log dan bahkan ada file yang mencurigakan di dalam log tersebut.”

Flag : **IDN_CTF{malware.py}**

Log Analysis 4

Deskripsi :

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

Format Flag : **IDN_CTF{jawaban}**

Author : Aditya Firman Nugroho

Lampiran : None

Solved by : ReyhanAlFarel



Solusi :

“untuk menganalisis auth.log tersebut saya menggunakan cat untuk menampilkan value dari log, lalu di combine dengan pipe grep “acc” dan disitu muncul 2 user, saya mencoba 2 2 nya dan akhirnya ketemu jawabannya.”

Flag : **IDN_CTF{ghxyss}**

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 : None

Solved by : ReyhanAlFarel

Solusi :

“untuk menganalisis log1.txt tersebut saya menggunakan cat untuk menampilkan value dari log tersebut, dan menggunakan grep pipe untuk mendapatkan ekstensi file, contohnya .txt, .php, .html, .js, dll.”

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 : None

Solved by : ReyhanAlFarel

Solusi :

“untuk menganalisis log2.txt tersebut saya menggunakan cat untuk menampilkan value dari log tersebut, dan mencarinya satu per satu, mana endpoint API tersebut dan saya coba 1 per 1.”

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 : None

Solved by : ReyhanAlFarel

Solusi :

“untuk menganalisis log3.txt tersebut saya menggunakan cat untuk menampilkan value dari log tersebut, dan dicombine dengan pipe grep “acc” lalu saya cocokan 1 per 1.”

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 : None

Solved by : ReyhanAlFarel

Solusi :

“untuk menganalisis log4.txt tersebut saya menggunakan cat untuk menampilkan value dari log tersebut, dan dicombine dengan pipe grep “acc” lalu saya cocokan 1 per 1.”

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



Forensic

jadi gini...

Deskripsi :

ngomongin crypto, selain encryption itu ada apa lagi ya ?

Author : Aditya Firman Nugroho

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada image tersebut, saya langsung cari dengan menggunakan strings <namafilename> dan mendapatkan flag tersebut di dalam gambarnya.”

Flag : **IDN_CTF{W0W_wh4T_K03NC1D3CE}**

QRIS

Deskripsi :

2 kali

Author : Mohamad Fatty

Lampiran : None

Solved by : ReyhanAlFarel

Solusi :

“Pada image tersebut, saya scan image tersebut dan mendapatkan code base64, lalu saya decode sebanyak 2x dan dapat flagnya.”

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