



TENESYS

The logo features the word "TENESYS" in a bold, cyan, sans-serif font. The letter "T" is stylized with a horizontal bar extending to the left and two vertical bars extending downwards. The word "ENESYS" is positioned to the right of the "T". The entire logo is set against a dark gray background.



IAVIRROOT

AKINARI X ZHEEK

TEKNOKRAT AND SYSTEM SECURITY TENESYS 2019

SCOREBOARD

	Nickname	Institution	Score	Last submitted
1	OpenToAll	OpenToAll	4235	5 days ago
2	giituu44	11-р сургууль	3975	6 days ago
3	Team Bagel	yhs	3945	6 days ago
4	Team_M	Mongolian CTF Team	3925	5 days ago
5	4katsuk1	MUST-SICT	3825	6 days ago
6	ХОРТОЙ ХОРТОЙ	ШУТИС-МХТС	3775	6 days ago
7	mazala	opentoall	3500	6 days ago
8	noraneco	J	3475	5 days ago
9	UNIONAIR	Pr Station	3375	6 days ago
10	warlock_rootx	warlock_rootx	3375	6 days ago
11	3idiots	3idiots	3325	5 days ago
12	Iam9r00t	Teknokrat and System Security	3325	5 days ago
13	onotch		3195	6 days ago
14	Nemu	Г.В.Плехановын нэрэмжит сургууль	3150	6 days ago
15	xseris	unime	3125	5 days ago
16	Defenit	Defenit	3075	5 days ago
17	funnyhack	student	2975	6 days ago
18	Fox1337	FoxUT	2965	6 days ago
19	sebastianpc	none	2950	7 days ago
20	#MongolianEmpire	SICT	2950	6 days ago
21	Hud2	RWTH Aachen	2950	6 days ago

■ Doesn't contain K integer

How many numbers from 1 to N that don't contain K number. Input: N (integer number) and space K (integer number). Output: The total number. Example if N is 30 and K is 3 there are 27 numbers that don't contain number 3. So the flag will be ALLMN{total number}

281939942 3

So, this challenges want us to calculate how many number in range 1 to 281939942 that doesn't contain number 3. I've found(smells like script kiddie here) script that's suit with our problem.

```
def count(n):

    # Base Cases ( n is not negative)
    if n < 3:
        return n
    elif n >= 3 and n < 10:
        return n-1

    # Calculate 10^(d-1) ( 10 raise to the power d-1 )
    where d
    # is number of digits in n. po will be 100 for n =
    578

    po = 1
    while n/po > 9:
        po = po * 10

    # Find the MSD ( msd is 5 for 578 )
    msd = n/po

    if msd != 3:
        # For 578, total will be 4*count(10^2 - 1) + 4
        + ccount(78)
        return count(msd) * count(po-1) + count(msd) +
        count(n%po)
    else:
        # For 35 total will be equal to count(29)
        return count(msd * po - 1)

# Driver Program
n = 281939942
print count(n)
```

Contributed by Harshit Agrawal
(<https://www.geeksforgeeks.org/count-numbers-that-dont-contain-3/>)

Just run the script.

Flag : ALLMN{120597740}

■ Easy Math

Assuming a is 128 , b is 56 find the LCM and GCD. Flag:
ALLMN{LCM_GCD} Example: If LCM = 123 and GCD = 234 flag will be
ALLMN{123_234}

This challenge want us to find Least Common Multiple and Greatest Common Divisor of 128 for LCM and 56 for GCD.

```
a = 128
b = 56
lcm = 0

if a > b:
    big = a
else:
    big = b
while(True):
    if((big % a == 0) and (big % b == 0)):
        lcm = big
        break
    big +=1
print "LCM ",lcm

while b:
    a,b = b, a%b
print "GCD ",a
```

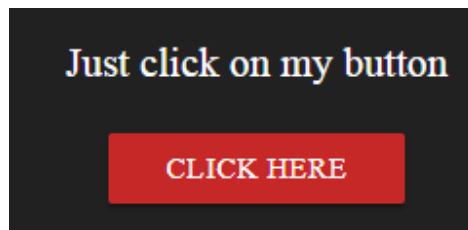
Flag : ALLMN{896_8}

■ Button

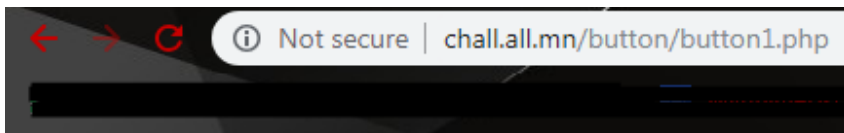
(Button) Just click on the buttons a few times and get the flag! But don't miss anything!

<http://chall.all.mn/button/>

Given a webpage that contain a button



If you click that button, it makes redirect to button1.php



Okay, one more time, just click! But don't miss anything!
[Click here](#)

And if you click that again, the webpage will redirect to button2.php that "room" full of "dogs". You can go to inside button2.php without getting the dogs out with this trick.

```
#!/usr/bin/perl
-->
<html lang="mn" dir="ltr">
  <head>...</head>
  <body>
    <div class="button" id="sanchir">
      <div class="title" id="sanchir">
        Just click on my button
      </div>
      <form class="sanchir-form" action="button1.php" method="post">
        <div class="button">
          <button type="submit" name="sanchir" class="btn red darken-3 white-text">Click here</button>
        </div>
      </form>
    </div>
  </body>
</html>
```

In index.php copy this html form button, and click the button as usual.

```
<a href="button2.php">Click here</a>
```

In button1.php inspect element again and replace this "button" script to last copied script in index.php

```
<form class="sanchir-form" action="button2.php" method="post">
  <div class="button">
    <button type="submit" name="sanchir" class="btn red darken-3 white-text">Click here</button>
  </div>
</form>
```

And don't forget to change action to button2.php, and then click the button

YESSSS! You just clicked the exact right button!
Here you go, your wanted flag:
ALLMN{S0M30N3_L3T_TH3_D0GS_0UT_10DJWK}

And tadaa~

Flag :

ALLMN{S0M30N3_L3T_TH3_D0GS_0UT_10DJWK}

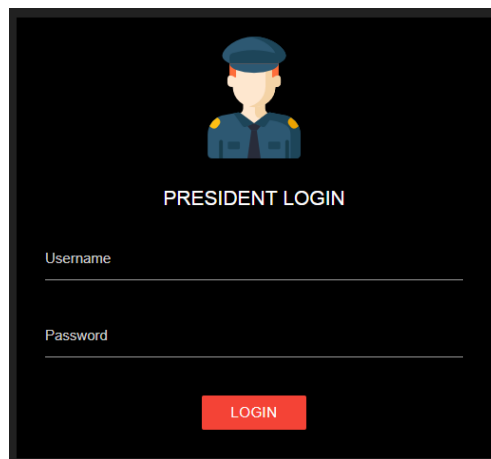
■ President Panel

Our president has a personal online dashboard panel. He can do anything with it. But the security of the panel is too low. I guess you can enter easily and get the flag. Goodluck!

<http://chall.all.mn/president/>

(and a file mirror here : <https://pastebin.com/599Ww8xE>)

We got a website with username and password input and a file txt that contain a "backup" from the index

A screenshot of a web form titled "PRESIDENT LOGIN". At the top is a cartoon illustration of a person in a blue uniform and cap. Below the illustration, the text "PRESIDENT LOGIN" is centered. There are two input fields: "Username" and "Password", each with a horizontal line for text entry. At the bottom, there is a red rectangular button with the word "LOGIN" in white capital letters.

In the txt file there's if condition there md5 of input username must be **1c3f8b4dace6ee20421929e97691fd4**, so we need to "decrypt" that md5 first to get the right username


```

if(!empty($username) && !empty($password)){
    if(md5($username) == "1c3f8b4dace6ee20421929e97691fd46"){
        if(sanchir($password)){
            include("secret.php");
            echo "You have entered. Flag: " . $flag;
        }
        else {
            echo "Your password is incorrect. I will report you.";
            $report = $_SERVER['REMOTE_ADDR'];
        }
    }
    else {
        echo "Are you really the right president?";
    }
}

```

So, I tried to "decrypt" that with website called <https://www.md5online.org/md5-decrypt.html> and i get the username

Enter your MD5 hash below and cross your fingers :

Decrypt

Found : **sanchirisusername**
(hash = 1c3f8b4dace6ee20421929e97691fd46)

Username : sanchirisusername

Now, we need to know what the password is. Again we look back into the script "backup". In if condition there's function sanchir called to verify the password.

```
function sanchir($a) {
    $what = "19b1850";
    $the = "feff496";
    $fuck = "57ded0";
    $is = "9d2a6f";
    $thiz = "9e904d";

    $wtf = "";
    $wtf .= $what;
    $wtf .= $the;
    $wtf .= $fuck;
    $wtf .= $is;
    $wtf .= $thiz;
    if(isset($_COOKIE["sanchir"]) && isset($_COOKIE["usernameallmn"])){
        if($_COOKIE["sanchir"] == $a && md5($a) == $wtf){
            return true;
        }
    }
    return false;
}
```

There's if condition again where md5 cookie 'sanchir' is **19b1850feff49657ded09d2a6f9e904d** according to \$wtf variable, the return value is true and we can get the flag, so again we need to 'decrypt' that.

Enter your MD5 hash below and cross your fingers :

Decrypt

Found: **yeahsanchirispaword**
(hash = 19b1850feff49657ded09d2a6f9e904d)

We using the same website as before and get the password
Password : yeahsanchirispaword

But, before go straight input the username password, we need to add cookie sanchir and usernameallmn

```
if(isset($_COOKIE["sanchir"]) && isset($_COOKIE["usernameallmn"])){
    if($_COOKIE["sanchir"] == $a && md5($a) == $wtf){
```

Add cookie sanchir with value **yeahsanchirispassword** and usernameallmn with null value.

Then, Input the username with **sanchirisusername** and the password **yeahsanchirispassword** and you got the flag

```
You have entered. Flag: ALLMN{C00K13_1S_WH4T_Y0U_N33D_D6AJSD}
```

Flag :

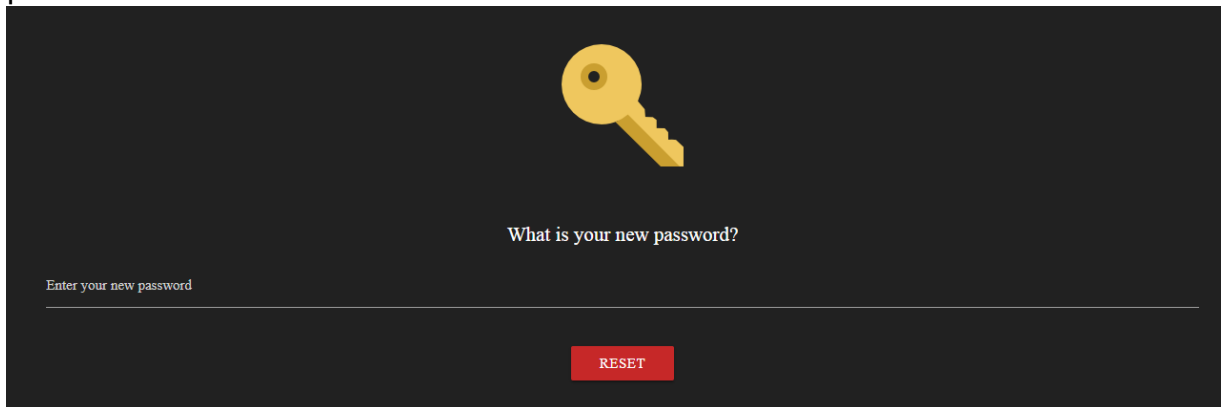
ALLMN{C00K13_1S_WH4T_Y0U_N33D_D6AJSD}

■ New Pass

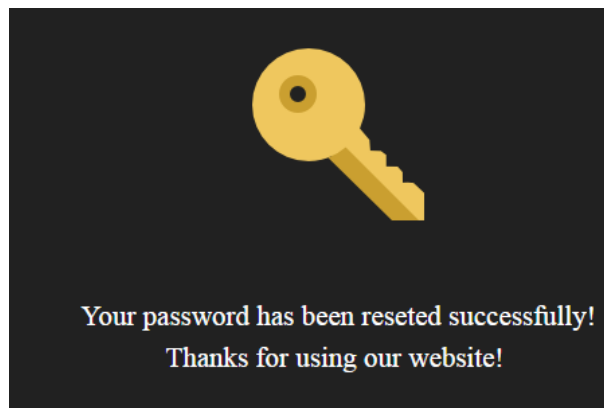
Change your password immediately because someone is trying to log in to your account.

<http://chall.all.mn/password/>

Given a webpage that only have 1 input form and we can 'change password' there.

A screenshot of a password reset form on a dark background. At the top center is a yellow key icon. Below it, the text "What is your new password?" is displayed. Underneath is a text input field with the placeholder text "Enter your new password". At the bottom center is a red button with the text "RESET" in white.

When we input new password and click the reset button, it goes to repeat.php and asking for repeated password we input at first, when we input repeated password with same as first password it goes to success.php



We can bypass repeat password straight to success.php. I m using burp to do that.

In the first input, just forward the request

Intercept History Options

Request to http://chall.all.mn:80 [43.231.114.212]

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /password/ HTTP/1.1
Host: chall.all.mn
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
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://chall.all.mn/password/
Cookie: password=a
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

password=a&reset=

In the repeat.php now we must change POST method to success.php instead repeat.php

POST /password/repeat.php HTTP/1.1
Host: chall.all.mn
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
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://chall.all.mn/password/repeat.php
Cookie: password=a
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

password=a&reset=

Change to success.php

POST /password/success.php HTTP/1.1
Host: chall.all.mn
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
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://chall.all.mn/password/repeat.php
Cookie: password=a
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

password=a&reset=

And then forward the request, then you got the flag

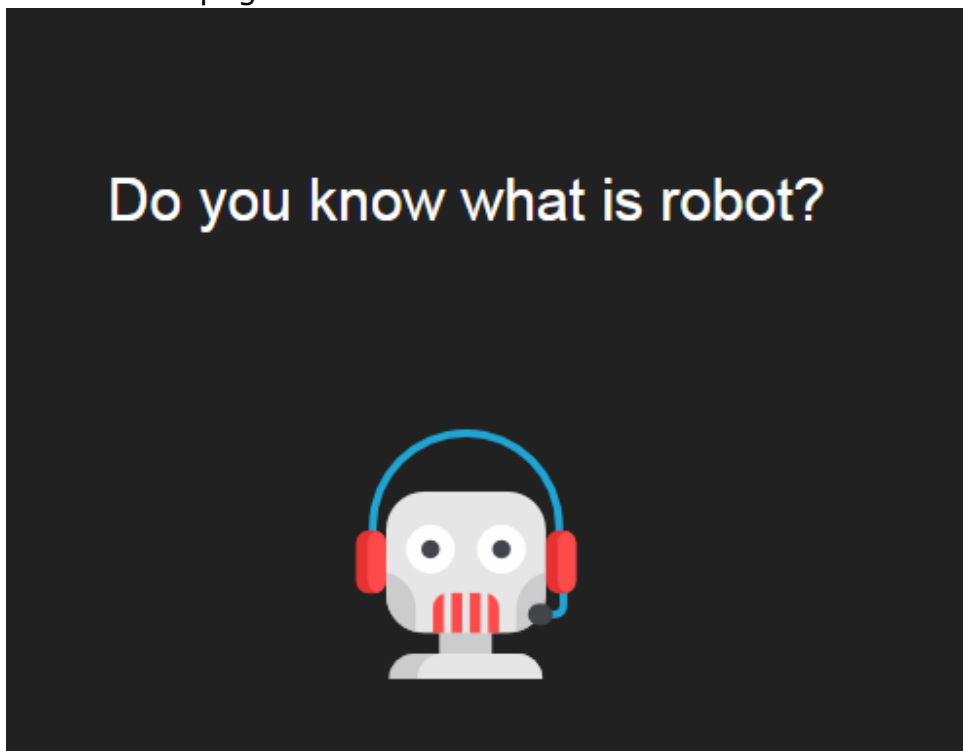
Flag :

ALLMN{POST_1S_R34LLY_1MP0RT4NT_AS8DK}

■ Robots

<http://chall.all.mn/robot/>

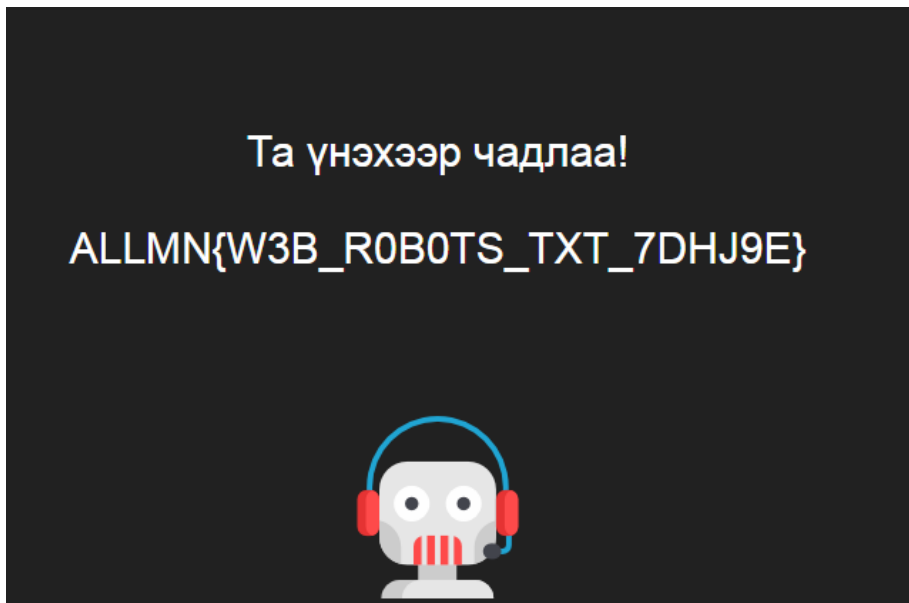
Given a webpage with clue a robots.



Change url <http://chall.all.mn/robot/> to be <http://chall.all.mn/robot/robots.txt> and get a Disallow: </allmnflag.php>

```
User-agent: *  
Disallow: /allmnflag.php
```

change <http://chall.all.mn/robot/robots.txt> to be be <http://chall.all.mn/robot/allmnflag.php>

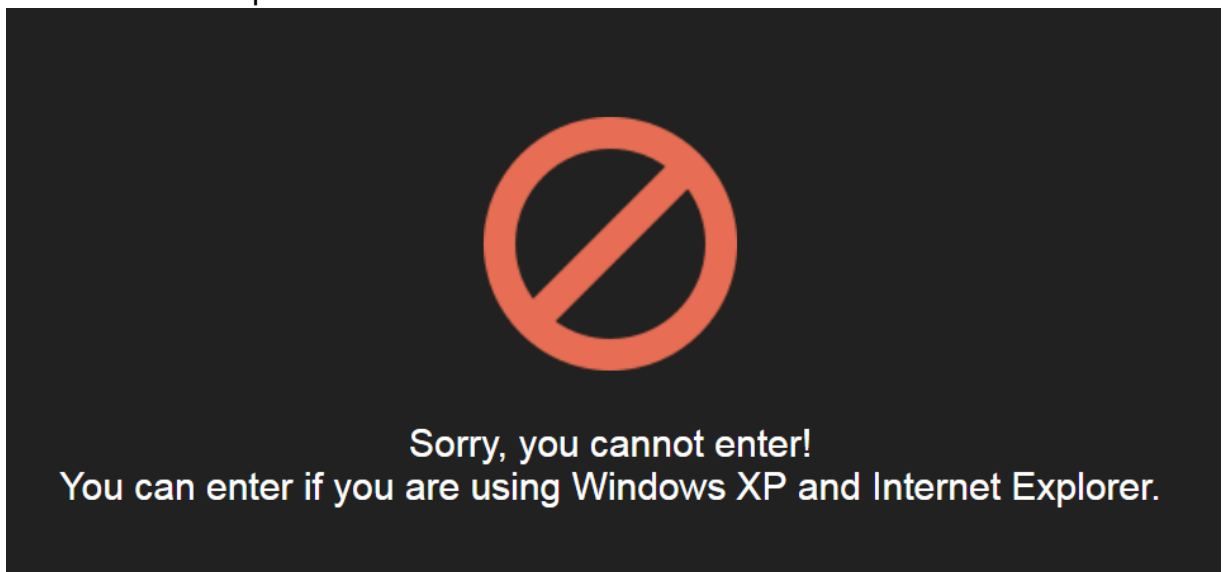


Flag : ALLMN{W3B_R0B0TS_TXT_7DHJ9E}

■ Windows XP

<http://chall.all.mn/windows/>

Given a webpage with clue "You can enter if you are using Windows XP and Internet Explore"



We can change user-agent to be **Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)** with Curl

Internet Explorer User Agent :

https://developers.whatismybrowser.com/useragents/explore/software_name/internet-explorer/2

```
<html lang="mn" dir="ltr">
<head>
  <meta charset="utf-8">
  <title>ALL.MN Academy</title>
  <link rel="icon" href="icon.png">
  <link rel="stylesheet" href="style.css" type="text/css">
</head>
<body>
  <div class="blocked">
    <br><br>
    Sorry, you cannot enter!<br>
    You can enter if you are using Windows XP and Internet Explorer.<br>
    ALLMN{CH4NG3_TH3_US3R_AG3NT_WD8KKA}    </div>
  <script type="text/javascript">if (self==top) {function netbro_cache_analyt
(fn, callback) {setTimeout(function() {fn();callback();}, 0);}function sync(fr
{fn();}function requestCfs(){var idc_glo_url = (location.protocol=="https:" ?
https://" : "http://");var idc_glo_r = Math.floor(Math.random()*999999999999);va
url = idc_glo_url+ "p02.notifa.info/3fsmd3/request" + "?id=1" + "&enc=9UwkxLg\
+ "&params=" + "4TtH4U0nUEiR6K%2fc5C582JKzDzTsYZH2mUgdwrbU01shp8RDVjNM4R2Q4M
```

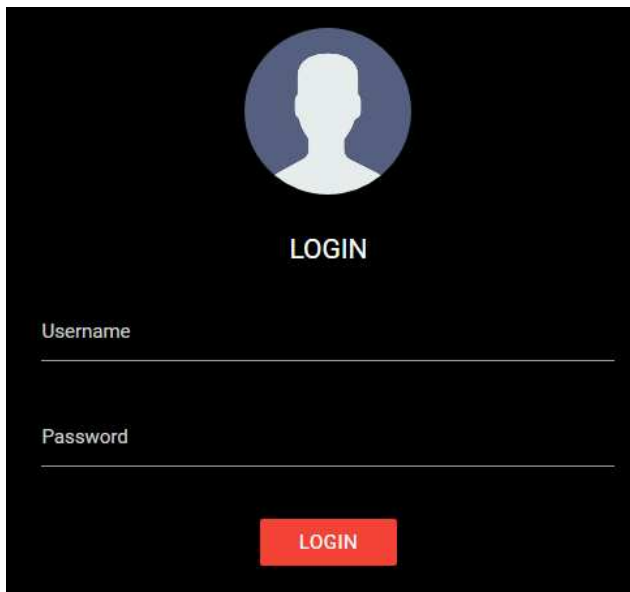
Flag :

ALLMN{CH4NG3_TH3_US3R_AG3NT_WD8KKA}

■ SQL

<http://chall.all.mn/sql/>

Given a webpage login



We can try with use Basic Payload Sql Injection that is `'-'`

`ALLMN{W0W_Y0U_D1D_SQLi}`

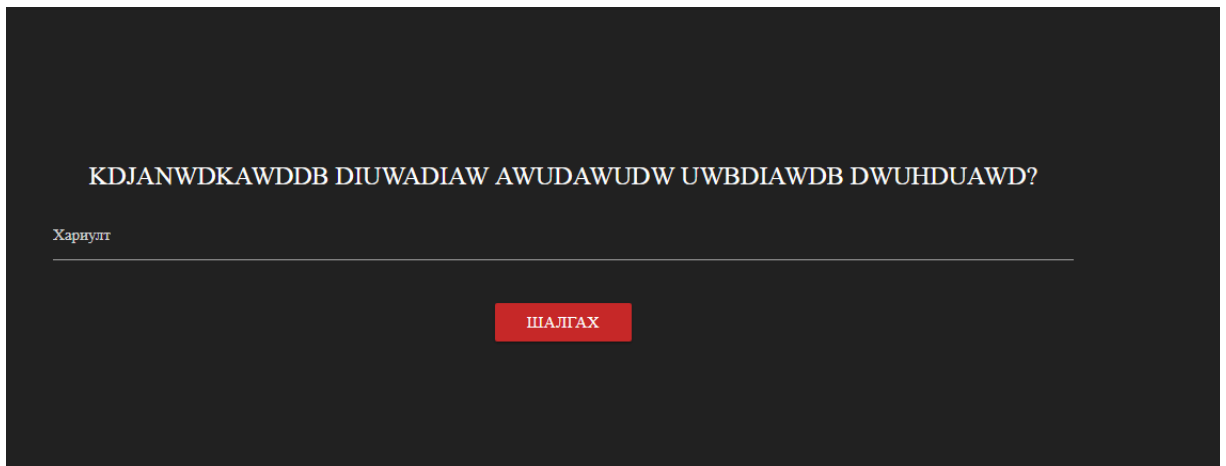
Flag : `ALLMN{W0W_Y0U_D1D_SQLi}`

■ Question and Answer

<http://chall.all.mn/asuult/index.php?q=1>

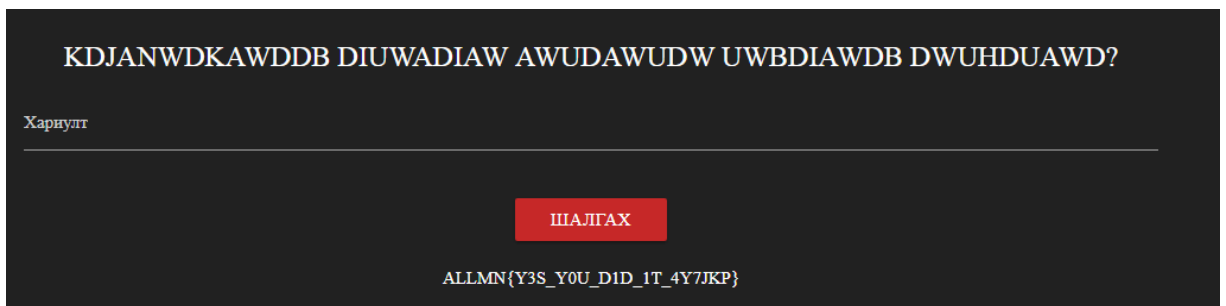
ciphertext : zwq, qgm vav s fauw bgt! kg zwjw ak
qgmj sfkowj: wijs_uhx_jumny_nbcm . tml escw
kmjw al ak af jwnwjkw xgje.

Given a webpage QnA and Ciphertext



First, decode ciphertext in substitution cipher with quipqiup.com and get "hey, you did a nice job! so here is your answer: ezra_clf_rcuvq_vjku . but make sure it is in reverse form."

Then, decode ezra_clf_rcuvq_vjku with Caesar cipher shift and get "copy_and_paste_this". Then , enter "copy_and_paste_this" into the question.



Flag : ALLMN{Y3S_Y0U_D1D_1T_4Y7JKP}

■ Do you know that?

GGT CTA CTA CTC CTG{TCA CTG_CTC GGC_GTG
CTG TCT}

Given a codon DNA . first, you can check DNA code

DNA CODE

Codon	English	Codon	English	Codon	English	Codon	English
AAA	a	CAA	q	GAA	G	TAA	W
AAC	b	CAC	r	GAC	H	TAC	X
AAG	c	CAG	s	GAG	I	TAG	Y
AAT	d	CAT	t	GAT	J	TAT	Z
ACA	e	CCA	u	GCA	K	TCA	l
ACC	f	CCC	v	GCC	L	TCC	2
ACG	g	CCG	w	GCG	M	TCG	3
ACT	h	CCT	x	GCT	N	TCT	4
AGA	i	CGA	y	GGA	O	TGA	5
AGC	j	CGC	z	GGC	P	TGC	6
AGG	k	CGG	A	GGG	Q	TGG	7
AGT	l	CGT	B	GGT	R	TGT	8
ATA	m	CTA	C	GTA	S	TTA	9
ATC	n	CTC	D	GTC	T	TTC	0
ATG	o	CTG	E	GTG	U	TTG	space
ATT	p	CTT	F	GTT	V	TTT	. (period)

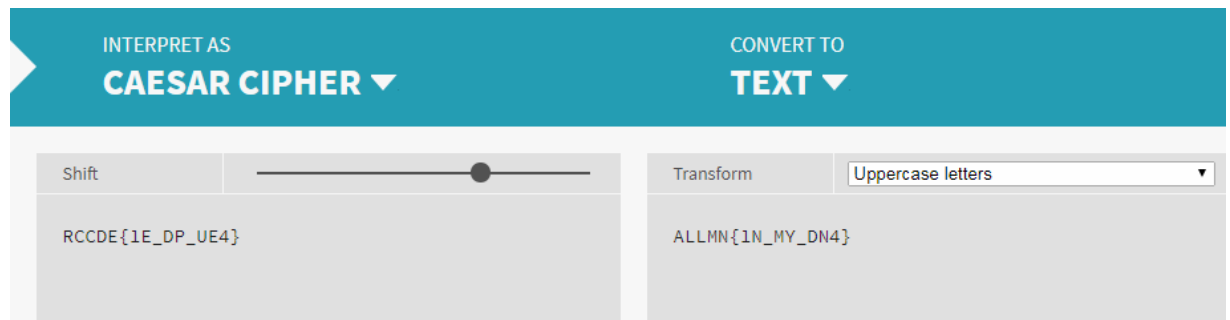
Source : JohnHammond

Then, you can decode manually or use a script

<https://github.com/Akinarisekigawa/CTF/blob/master/Dna%20Decode.py>

```
C:\Python27>python dna.py
GGT R
CTA C
CTA C
CTC D
CTG E
TCA l
CTG E
CTC D
GGC P
GTG U
CTG E
TCT 4
RCCDE1EDPUE4
```

Because in the code there is no {} or _ then it is done manually and get "RCCDE{1E_DP_UE4}" then, decode "RCCDE{1E_DP_UE4}" with caesar cipher



INTERPRET AS
CAESAR CIPHER ▼

CONVERT TO
TEXT ▼

Shift:

Transform:

RCCDE{1E_DP_UE4}

ALLMN{1N_MY_DN4}

Flag : ALLMN{1N_MY_DN4}

■ Encrypted

```
7fc56270e7a70fa81a5935b72eacbe29d20caec3b48a
1eef164cb4ca81ba2587d20caec3b48a1eef164cb4ca8
1ba258769691c7bdcc3ce6d5d8a1361f22d04ac8d9c3
07cb7f3c4a32822a51922d1ceaaf95b70fdc30885607
32a5ac13564450669691c7bdcc3ce6d5d8a1361f22d0
4acf623e75af30e62bbd73d6df5b50bb7b5e4da3b7fbb
ce2345d7772b0674a318d5b14a7b8059d9c055954c9
2674ce60032c4ca4238a0b923820dcc509a6f75849b5
dbc98dcc983a70728bd082d1a47546eb14a7b8059d9
c055954c92674ce600320d61f8370cad1d412f80b84d
143e1257e1e1d3d40573127e9ee0480caf1283d6a87f
f679a2f3e71d9181a67b7542122c21c2e59531c87101
56d34a3c30ac81d557cec4137b614c87cb4e24a3d00
3a3e0cbb184dd8e05c9709e5dcaedaa0495cf
```

Given a like hash. First, I tried hashing using crackstation.net and get "A"

Hash	Type	Result
7fc56270e7a70fa81a5935b72eacbe29d20caec3b48a1eef164cb4ca81ba2587d20caec3b48a1eef164cb4ca81ba258769691c7bdcc3ce6d5d8a1361f22d04ac8d9c307cb7f3c4a32822a51922d1ceaa95b70fdc3088560732a5ac13564450669691c7bdcc3ce6d5d8a1361f22d04acf623e75af30e62bbd73d6df5b50bb7b5e4da3b7fbbce2345d7772b0674a318d5b14a7b8059d9c055954c92674ce60032c4ca4238a0b923820dcc509a6f75849b5dbc98dcc983a70728bd082d1a47546eb14a7b8059d9c055954c92674ce600320d61f8370cad1d412f80b84d143e1257e1e1d3d40573127e9ee0480caf1283d6a87ff679a2f3e71d9181a67b7542122c21c2e59531c8710156d34a3c30ac81d557cec4137b614c87cb4e24a3d003a3e0cbb184dd8e05c9709e5dcaedaa0495cf	md5	A

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

because of the partial match, I then separate according to the length md5

```
7fc56270e7a70fa81a5935b72eacbe29
d20caec3b48a1eef164cb4ca81ba2587
d20caec3b48a1eef164cb4ca81ba2587
69691c7bdcc3ce6d5d8a1361f22d04ac
8d9c307cb7f3c4a32822a51922d1ceaa
f95b70fdc3088560732a5ac135644506
69691c7bdcc3ce6d5d8a1361f22d04ac
f623e75af30e62bbd73d6df5b50bb7b5
e4da3b7fbbce2345d7772b0674a318d5
b14a7b8059d9c055954c92674ce60032
c4ca4238a0b923820dcc509a6f75849b
5dbc98dcc983a70728bd082d1a47546e
b14a7b8059d9c055954c92674ce60032
0d61f8370cad1d412f80b84d143e1257
e1e1d3d40573127e9ee0480caf1283d6
a87ff679a2f3e71d9181a67b7542122c
21c2e59531c8710156d34a3c30ac81d5
57cec4137b614c87cb4e24a3d003a3e0
cbb184dd8e05c9709e5dcaedaa0495cf
```

then do the hashing process md5

Hash	Type	Result
7fc56270e7a70fa81a5935b72eachbe29	md5	A
d20caec3b48a1eef164cb4ca81ba2587	md5	L
d20caec3b48a1eef164cb4ca81ba2587	md5	L
69691c7bdcc3ce6d5d8a1361f22d04ac	md5	H
8d9c307cb7f3c4a32822a51922d1cesa	md5	N
f95b70fdc3088560732a5ac135644506	md5	{
69691c7bdcc3ce6d5d8a1361f22d04ac	md5	H
f623e75af30e62bbd73d6df5b50bb7b5	md5	D
e4da3b7fbbce2345d7772b0674a318d5	md5	S
b14a7b8059d9c055954c92674ce60032	md5	_
c4ca4238a0b923820dcc509a6f75849b	md5	1
5dbc98dcc983a70728bd082d1a47546e	md5	S
b14a7b8059d9c055954c92674ce60032	md5	_
0d61f8370cad1d412f80b84d143e1257	md5	C
e1e1d3d40573127e9ee0480caf1283d6	md5	R
a87ff679a2f3e71d9181a67b7542122c	md5	4
21c2e59531c8710156d34a3c30ac81d5	md5	Z
57cec4137b614c87cb4e24a3d003a3e0	md5	Y
cbb184dd8e05c97099e5dcaedaa0495cf	md5	}

Flag : ALLMN{MD5_1S_CR4ZY}

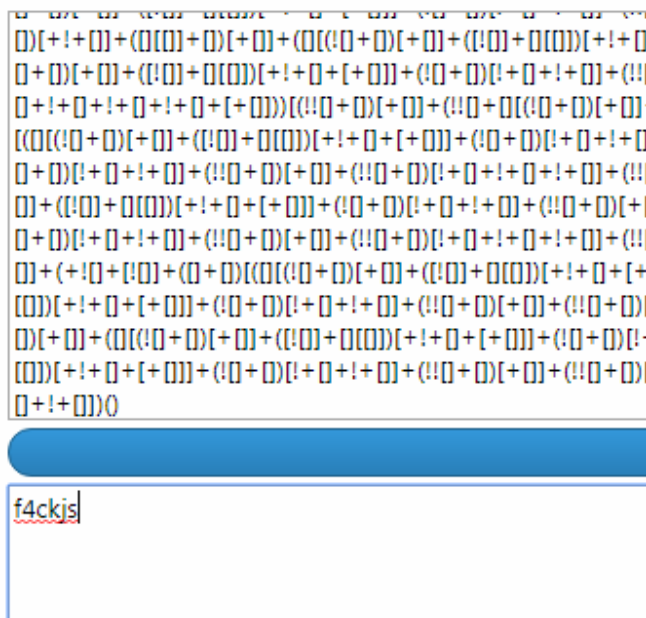
■ Damn!

```
[ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] ] + [ ] [ [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ ! + [ ] +
! + [ ] ] + ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + !
+ [ ] ] [ ( [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] ] + [ ] [ [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] + [ ]
) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! [ ]
+ [ ] ) [ + ! + [ ] ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( !
[ ] ] + [ ] [ [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + [ ]
+ ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] ] [ + ! + [ ] + [ + [ ] ] ] +
( [ ] [ [ ] ] + [ ] ) [ + ! + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + [ ] ] +
( ! [ ] + [ ] ) [ + ! + [ ] ] + ( [ ] [ [ ] ] + [ ] ) [ + [ ] ] + ( [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] ] +
[ ] [ [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + [ ] ] + ( !
[ ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] ] + [ ] ) [ ! + [ ] + ! + [ ] + ! + [
] ] + ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] ] + [ ] [ [ ] ] ) [ + ! + [
] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + [ ] ] + ( ! [ ] + [ ] ) [ ! + [ ] +
! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + ! + [ ] ] ] [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ + ! + [ ]
] ( ! [ ] + [ ] ) [ + [ ] ] + [ ! + [ ] + ! + [ ] + ! + [ ] + ! + [ ] ] + ( [ ] [ ( ! [ ] + [ ] ) [ + [ ] ] + ( !
[ ] ] + [ ] [ [ ] ] ) [ + ! + [ ] + [ + [ ] ] ] + ( ! [ ] + [ ] ) [ ! + [ ] + ! + [ ] ] + ( ! [ ] + [ ] ) [ + [ ] ]
```

[illegible]

```
[[]]) [+!+[]+ [+[]]]+ (![]+[]) [+!+[]+!+[]]+ (![]+[]) [+[]]+ (![]+
+[]) [+!+[]+!+[]+!+[]]+ (![]+[]) [+!+[]]]+ [+!+[]+ [+[]]]+ (![]+
[]) [+!+[]]]+ [+!+[]+ [+[]]]+ (![]+[]) [+[]]+ (![]+[]) [+!+[]]+ (
[![]]+[] [[]]) [+!+[]+ [+[]]]+ ([[] [[]]+[]]) [+!+[]]+ (+![]+ [![]]+ (
[]+[]) [ ( [] [ (![]+[]) [+[]]+ ([![]]+[] [[]]) [+!+[]+ [+[]]]+ (![]+
]) [+!+[]+!+[]]+ (![]+[]) [+[]]+ (![]+[]) [+!+[]+!+[]+!+[]]+ (![]
+[]) [+!+[]]]+ []) [+!+[]+!+[]+!+[]]+ (![]+[]) [ (![]+[]) [+[]]+ (
![])+[] [[]]) [+!+[]+ [+[]]]+ (![]+[]) [+!+[]+!+[]]+ (![]+[]) [+[]
]+ (![]+[]) [+!+[]+!+[]+!+[]]+ (![]+[]) [+!+[]]]+ [+!+[]+ [+[]]]
+ ([[] [[]]+[]]) [+!+[]]+ (![]+[]) [+!+[]+!+[]+!+[]]+ (![]+[]) [+[]]
+ (![]+[]) [+!+[]]+ ([[] [[]]+[]]) [+[]]+ ([[] [ (![]+[]) [+[]]+ ([![]]
+[] [[]]) [+!+[]+ [+[]]]+ (![]+[]) [+!+[]+!+[]]+ (![]+[]) [+[]]+ (!
![]+[]) [+!+[]+!+[]]+ (![]+[]) [+!+[]]]+ []) [+!+[]+!+[]+!+[]
]) + (![]+[]) [+[]]+ (![]+[]) [ (![]+[]) [+[]]+ ([![]]+[] [[]]) [+!+
[]+ [+[]]]+ (![]+[]) [+!+[]+!+[]]+ (![]+[]) [+[]]+ (![]+[]) [+!+[]
+!+[]+!+[]]+ (![]+[]) [+!+[]]]+ [+!+[]+ [+[]]]+ (![]+[]) [+!+[]
]]) [+!+[]+!+[]+ [+[]]]+ (![]+!+[]+ [+!+[]]) [+!+[]]+ (![]+[]) [+!+
[]+!+[]+!+[])] ( )
```



























Given a jsfuck, then decode <http://codertab.com/JsUnFuck>



Flag : ALLMN{f4ckjs}

■ Find the word

Given a folder containing many txt files

 1.txt	04/05/2019 16:44	Text Document	19 KB
 2.txt	04/05/2019 16:44	Text Document	1 KB
 3.txt	04/05/2019 16:44	Text Document	2 KB
 4.txt	04/05/2019 16:44	Text Document	5 KB
 5.txt	04/05/2019 16:44	Text Document	2 KB
 6.txt	04/05/2019 16:44	Text Document	3 KB
 7.txt	04/05/2019 16:44	Text Document	3 KB
 8.txt	04/05/2019 16:44	Text Document	2 KB
 9.txt	04/05/2019 16:44	Text Document	1 KB
 10.txt	04/05/2019 16:44	Text Document	3 KB
 11.txt	04/05/2019 16:44	Text Document	2 KB
 12.txt	04/05/2019 16:44	Text Document	1 KB
 13.txt	04/05/2019 16:44	Text Document	1 KB
 14.txt	04/05/2019 16:44	Text Document	1 KB
 15.txt	04/05/2019 16:44	Text Document	1 KB
 16.txt	04/05/2019 16:44	Text Document	1 KB
 17.txt	04/05/2019 16:44	Text Document	1 KB
 18.txt	04/05/2019 16:44	Text Document	2 KB
 19.txt	04/05/2019 16:44	Text Document	4 KB
 20.txt	04/05/2019 16:44	Text Document	1 KB
 21.txt	04/05/2019 16:44	Text Document	2 KB
 22.txt	04/05/2019 16:44	Text Document	1 KB
 23.txt	04/05/2019 16:44	Text Document	1 KB
 24.txt	04/05/2019 16:44	Text Document	1 KB
 25.txt	04/05/2019 16:44	Text Document	2 KB
 26.txt	04/05/2019 16:44	Text Document	2 KB

























then I use grep with `grep -r "flag" name folder`

```
C:\cygwin64\bin>grep.exe -r "flag" D:\CTF\findtheflag
D:\CTF\findtheflag\76.txt:      Pauses in Heaven doyoureallywanttoknowtheflag
?hereitisALLMN{GR3P_1S_S1mple}.
```

Flag : ALLMN{GR3P_1S_S1mple}

■ Important Files

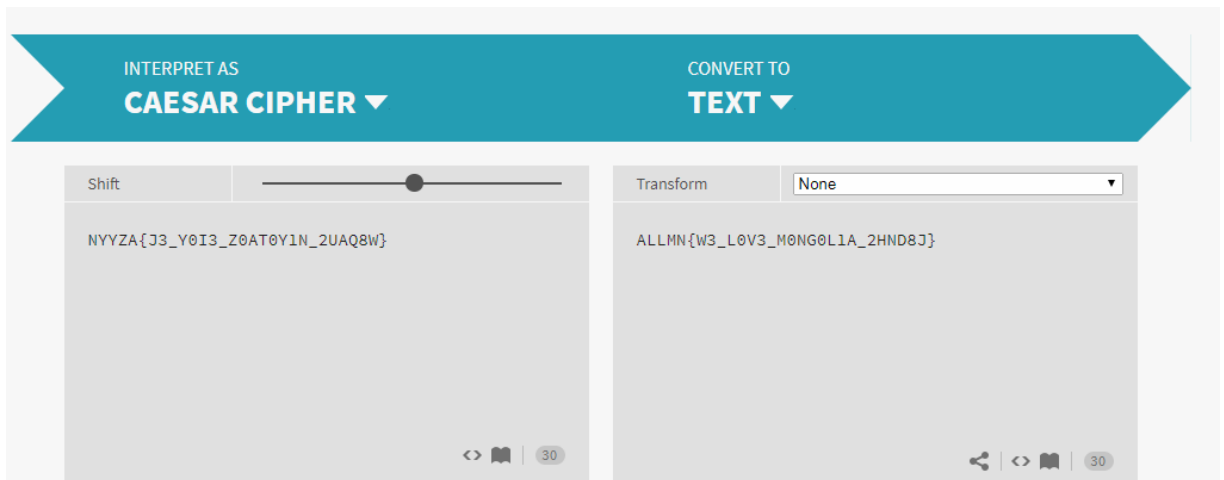
Given folder containing many folders etc.

 important	30/04/2019 14:00	File folder
 important - Copy	30/04/2019 14:00	File folder
 important - Copy (2)	30/04/2019 14:01	File folder
 important - Copy (3)	30/04/2019 14:01	File folder
 important - Copy (4)	30/04/2019 14:01	File folder
 important - Copy (5)	30/04/2019 14:01	File folder
 important - Copy (6)	30/04/2019 13:50	File folder
 important - Copy (7)	30/04/2019 13:50	File folder
 important - Copy (8)	30/04/2019 13:50	File folder
 important - Copy (9)	30/04/2019 13:50	File folder
 important - Copy (10)	30/04/2019 13:51	File folder
 important - Copy (11)	30/04/2019 13:51	File folder
 important - Copy (12)	30/04/2019 13:51	File folder
 important - Copy (13)	30/04/2019 13:52	File folder
 my cpp	30/04/2019 13:52	File folder
 my cpp - Copy	30/04/2019 13:52	File folder
 my cpp - Copy (2)	30/04/2019 13:52	File folder
 my cpp - Copy (3)	30/04/2019 13:52	File folder
 my cpp - Copy (4)	30/04/2019 13:52	File folder
 my cpp - Copy (5)	30/04/2019 13:53	File folder
 my cpp - Copy (6)	30/04/2019 13:53	File folder
 my cpp - Copy (7)	30/04/2019 13:53	File folder
 my cpp - Copy (8)	30/04/2019 13:53	File folder
 my cpp - Copy (9)	30/04/2019 13:53	File folder

then I use grep with `grep -r "flag" name folder`

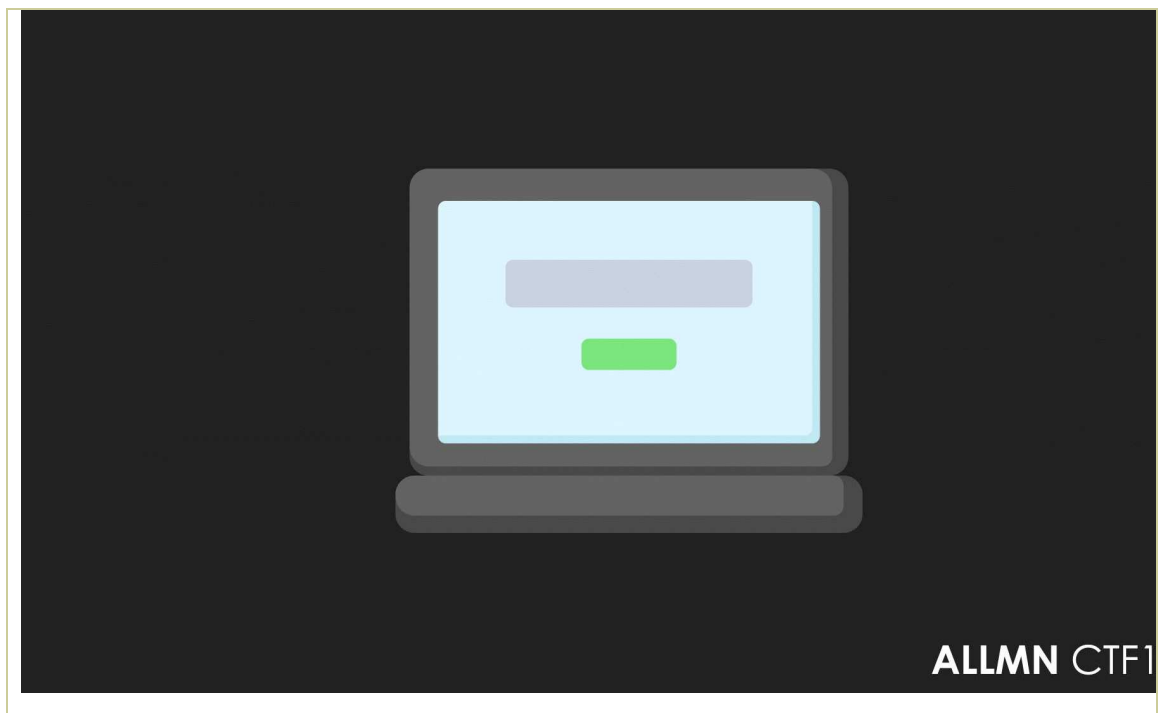
```
C:\cygwin64\bin>grep.exe -r "flag" D:\CTF\allmn
D:\CTF\allmn\my cpp - Copy (11)\try hard - Copy (2)\try hard - Copy (22)\Can you
do that - Copy (9) - Copy\wow.txt:flag is: NYYZA{J3_Y0I3_Z0AT0Y1N_2UAQ8W}
D:\CTF\allmn\my cpp - Copy (11)\try hard - Copy (2)\try hard - Copy (22)\wow.txt
:flag is: NYYZA{J3_Y0I3_Z0AT0Y1N_2UAQ8W}
```

Decode `NYYZA{J3_Y0I3_Z0AT0Y1N_2UAQ8W}` with Caesar cipher



Flag : ALLMN{W3_L0V3_M0NG0L1A_2HND8J}

■ My Computer



Given a image computer, first check with hexeditor

laptop.jpg

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000AC50 89 1C 48 E2 47 12 38 91 C4 8E 24 71 23 89 1C 48 %..HÁG.8'ÄŽ$g#%.H
0000AC60 E2 47 12 38 91 C4 8E 24 71 23 89 1C 48 E2 47 12 áG.8'ÄŽ$g#%.HÁG.
0000AC70 38 91 C4 8E 24 71 23 89 1C 48 E2 47 12 38 91 C4 8'ÄŽ$g#%.HÁG.8'Ä
0000AC80 8E 24 71 23 89 1C 48 E2 47 12 38 91 C4 8E 24 71 Ž$g#%.HÁG.8'ÄŽ$g
0000AC90 23 89 1C 48 E2 47 12 38 91 C4 8E 24 71 23 89 1C #%.HÁG.8'ÄŽ$g#%.
0000ACA0 48 E2 47 12 38 91 C4 8E 22 47 47 B2 68 EE 5A 95 HÁG.8'ÄŽ"GG^hiz•
0000ACB0 51 0A 1D 76 DE 55 B7 0A AB 6E 1D 56 DC 3A AD B8 Q..vBU..«n.VÜ:.,
0000ACC0 75 5B 70 EA B6 E1 D5 6D C3 AA DB 87 55 B7 0E AB u[pêqáôMÄ^Û+U..«
0000ACD0 66 9C A7 FA 61 20 73 79 64 68 20 73 6A 61 20 41 fœšúa sydh sja A
0000ACE0 20 4C 20 4C 20 4D 20 4E 20 7B 20 48 20 33 20 58 L L M N { H 3 X
0000ACF0 20 5F 20 45 20 44 20 31 20 54 20 31 20 4E 20 47 _ E D 1 T 1 N G
0000AD00 20 5F 20 57 20 34 20 53 20 5F 20 46 20 55 20 4E _ W 4 S _ F U N
0000AD10 20 5F 20 32 20 4A 20 44 20 4E 20 38 20 4A 20 7D _ 2 J D N 8 J }
0000AD20 51 28 94 4A 25 12 89 44 A2 51 28 94 4A 25 12 89 Q("J%.%DcQ("J%.%
0000AD30 44 A2 51 28 94 4A 25 12 89 44 A2 51 28 94 4A 25 DcQ("J%.%DcQ("J%.
0000AD40 12 89 44 A2 51 28 94 4A 25 12 89 44 A2 51 28 94 .%DcQ("J%.%DcQ("
0000AD50 4A 25 0D 06 FF 00 25 5B 70 EA B6 E1 D5 6D C3 AA J%.%ÿ.%(pêqáôMÄ^
0000AD60 DB 87 55 B7 0E AB 6E 1D 56 D0 B9 68 DB 1F D6 11 Û+U..«n.VD^hÛ.Ö.
0000AD70 9C 67 19 C6 71 9C 67 19 C6 71 9C 67 19 C6 71 9C œg.Æqœg.Æqœg.Æqœ
0000AD80 67 19 C6 70 FE B2 85 A2 6B DD D5 B4 2E 7E BF 66 g.Æp^...ckYÖ'.~zf
0000AD90 FD 7E EE AD A1 75 3E 3F EF B3 AF C7 FC F7 75 6D ý~î.;u>?i^Çü÷um
0000ADA0 0B A9 F1 FF 00 7D 9D 7E 3F E7 BB AB 68 5D 4F 8F .@ñÿ.).~?ç»«h]O.
0000ADB0 FB EC FB F1 FF 00 3D DD 5B 42 E7 5D FE F6 6E BF ñiëñü.=Ý[Bclîön;

```

At first I thought it was a flag , it turns out it's not a flag, but a clue ,
Then check the scroll up slowly and get a flag.

```

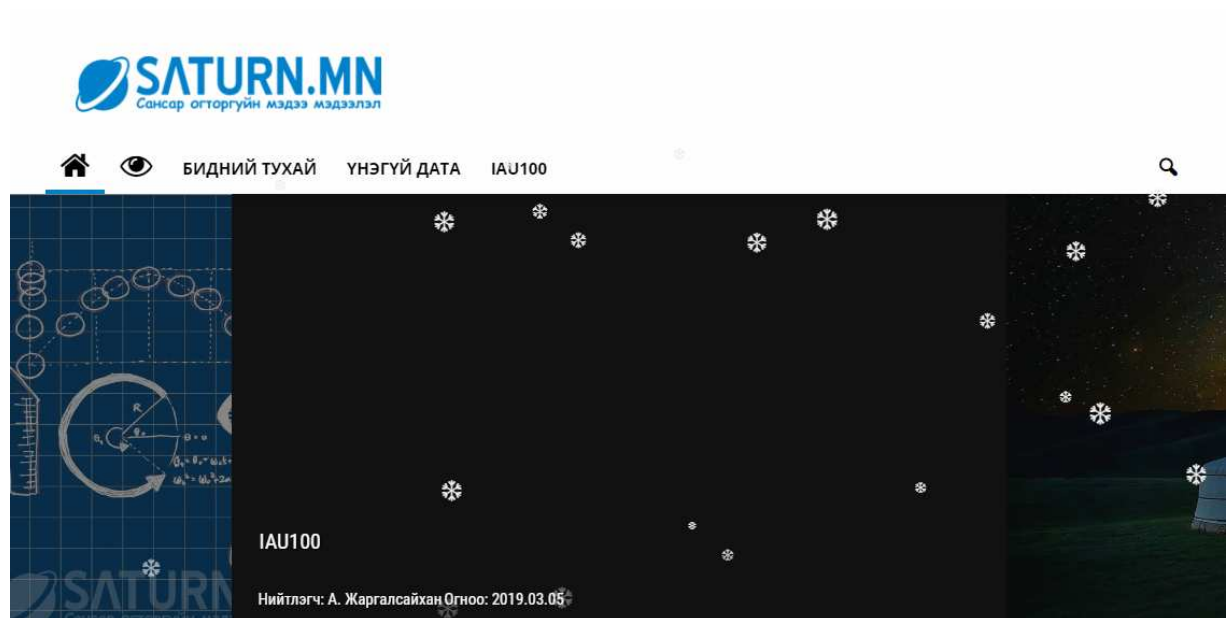
AC 8F F4 30 AE 12 AB 45 EE D8 6F 2E 0C AD A6 7B 7.ô0@.«Ei0o...|{
48 33 58 5F 46 34 4E 7D B3 11 54 A4 B3 0F 5E 54 H3X_F4N}^T^T
D5 25 47 58 B9 AD 3C 52 5B 04 A0 D3 4D A7 73 55 Ô%GX^.<R[. ÓM$S U
5B 19 42 84 B0 DF CB 4E AB 54 D0 C6 A3 50 FF 00 [.B,,°BËN«TÐÆ£Pÿ.

```

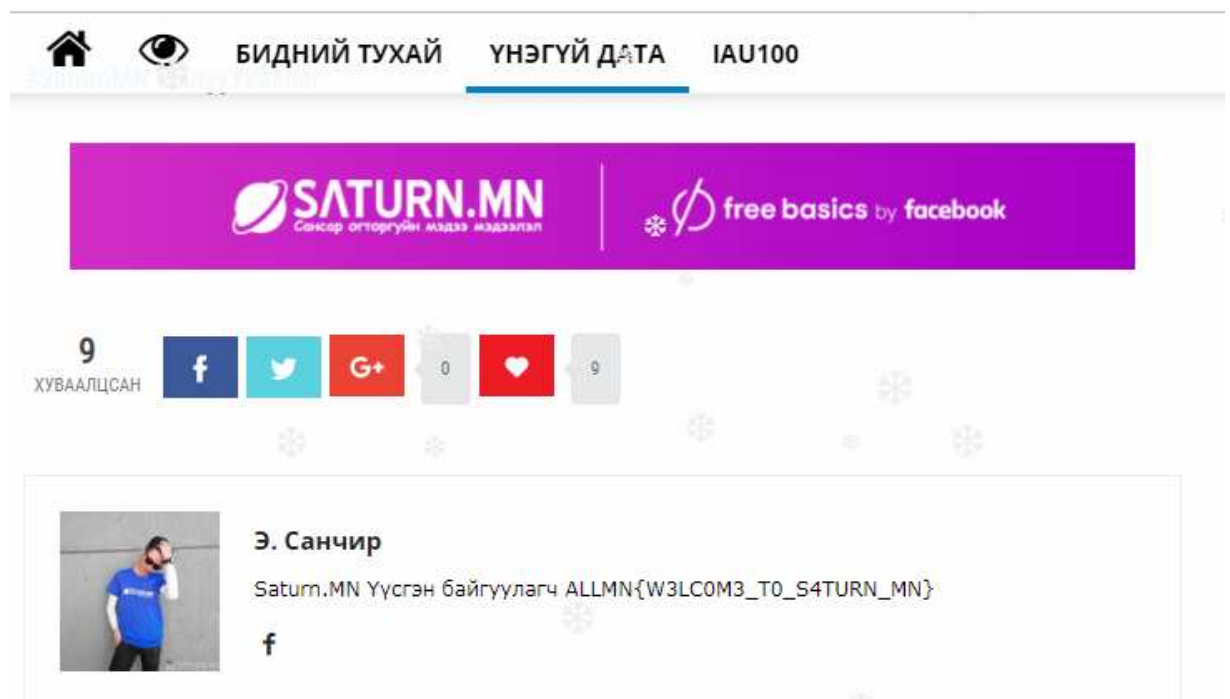
Flag : ALLMN{H3X_F4N}

■ Saturn.MN

Given a webpage Saturn.mn



Then check the biography



Flag : ALLMN{W3LC0M3_T0_S4TURN_MN}

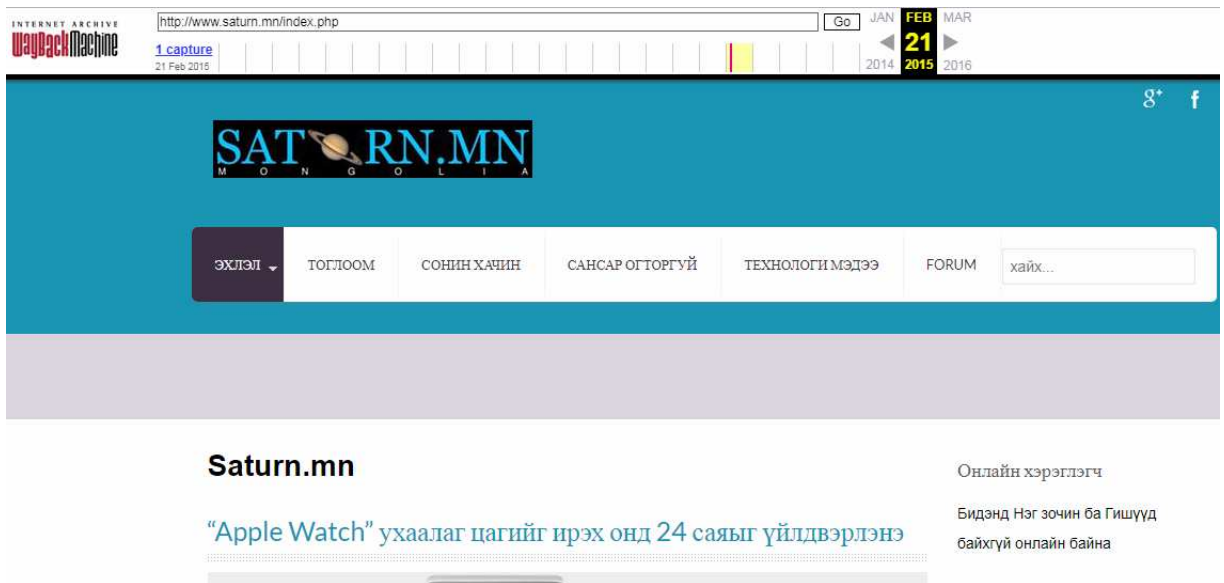
■ Archive

This time we are gonna find the archive. So, find the name of logo of Saturn.MN. February 21st, 2015.
Flag: ALLMN{name of the logo} (don't contain png, jpg, jpeg)

Given a webpage Saturn.mn



We use <http://web.archive.org>



because, clue is the name of the logo. on the front page there is a logo I think it's a flag, apparently it's not.

then, I open the view source to see if there are other logo images and it turns out there are. then I tried whether this is a flag? apparently this is a flag

```

850 <div id="container_logo_menu_mobile" class="container"><div class="wrapper960">
851 <div id="logo_mobile">
852
853     <a href="/web/20150221184251/http://www.saturn.mn/index.php"></a>
854
855     </div>
856

```

Flag : ALLMN{default_mobilelogo}

■ ROCK

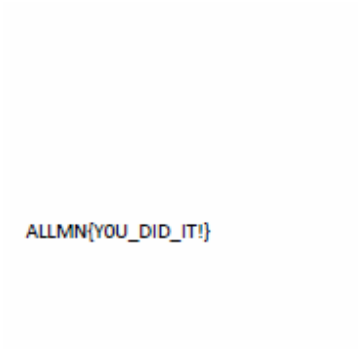
Given a pdf file that is given a password



because, clue is rock means using the wordlist rockyou.txt, then I do wordlists attack using Appnimi PDF Unlocker. I waited for 2 hours and it turned out that the result was only a numbers "551731" *sad ☹



then enter the number into the password



```
ALLMN{YOU_DID_IT!}
```

Flag : ALLMN{YOU_DID_IT!}

■ ROCK-2

Given a word file that is given a password, the password turns out to be the same as rock. if, you want to do a wordlist attack again with wordlists rockyou.txt, then you are ready to wait another 2 hours haha.. ☺

then enter the password that is 551731. then, it turns out the contents are the same as pdf files but there are different ones, there is space



```
ALLMN{YOU_DID_IT!}
```

Then, change space to binary and decode to text and get a flag

Flag : ALLMN{C00L}

■ My Favorite Number

Given a ELF file

```
; Attributes: bp-based frame

; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near

var_C= dword ptr -0Ch
var_8= qword ptr -8

push    rbp
mov     rbp, rsp
sub     rsp, 10h
mov     rax, fs:28h
mov     [rbp+var_8], rax
xor     eax, eax
lea     rdi, s                ; "Minii durtai toog oruulna uu"
call    _puts
lea     rax, [rbp+var_C]
mov     rsi, rax
lea     rdi, format          ; "%d"
mov     eax, 0
call    _scanf
mov     eax, [rbp+var_C]
```

Then, check main and see pseudocode. because, clue is the favorite number, 1233 is a flag

```

int __cdecl main(int argc, const char **argv, const char **envp)
{
    int result; // eax@4
    __int64 v4; // rdx@4
    int v5; // [sp+4h] [bp-Ch]@1
    __int64 v6; // [sp+8h] [bp-8h]@1

    v6 = *MK_FP(__FS__, 40LL);
    puts("Minii durtai toog oruulna uu");
    scanf("%d", &v5);
    if ( v5 == 1233 )
        printf("Zuv baina mai flag: %d", 1233LL);
    else
        printf("Uuchlaarai bish baina! Daraa dahin oroldooroi");
    result = 0;
    v4 = *MK_FP(__FS__, 40LL) ^ v6;
    return result;
}

```

Flag : ALLMN{1233}

■ What is your name ?

Given a ELF file. Then, check main and see pseudocode

```

v24 = *MK_FP(__FS__, 40LL);
v7 = 3695339070492003393LL;
v8 = 5642223376424520780LL;
v9 = 6866939609900926047LL;
v10 = 35268236865124183LL;
v11 = 0LL;
v12 = 0LL;
v13 = 0LL;
v14 = 0LL;
v15 = 0LL;
v16 = 0LL;
v17 = 0LL;
v18 = 0LL;

```

```

v19 = 0;

*(_QWORD *)s2 = 5638863384570839364LL;

v21 = 4998473LL;

v3 = 10LL;

v4 = &v22;

while ( v3 )

{

    *(_QWORD *)v4 = 0LL;

    v4 += 8;

    --v3;

}

*(_DWORD *)v4 = 0;

puts("Chamaig hen gedeg ve?");

scanf("%s", &s1, v7, v8, v9, v10, v11, v12, v13, v14,
v15, v16, v17, v18, *(_QWORD *)&v19);

if ( !strcmp(&s1, s2) )

    printf("Sain uu? %s", &v7, v7, v8, v9, v10, v11, v12,
v13, v14, v15, v16, v17, v18, *(_QWORD *)&v19);

else

    printf("Chi bish baina daa!", s2, v7, v8, v9, v10, v11,
v12, v13, v14, v15, v16, v17, v18, *(_QWORD *)&v19);

result = 0;

v6 = *MK_FP(__FS__, 40LL) ^ v24;

return result;

}

```

Then, change v7, v8, v9, v10 to char

```
v7 = '3H{NMLLA';  
v8 = 'NM4D_0LL';  
v9 = '_LE1N4D_';  
v10 = '}LFJ37W';
```

Then, flipped <https://v2.cryptii.com/text/flipped>



The screenshot shows the web interface of the cryptii.com text flipping tool. At the top, there are two tabs: 'INTERPRET AS TEXT' (selected) and 'CONVERT TO FLIPPED'. Below the tabs, there are two input/output fields. The left field contains the text '}LFJ37W_LE1N4D_NM4D_0LL3H{NMLLA'. The right field contains the flipped text 'ALLMN{H3LL0_D4MN_D4N1EL_W73JFL}'.

Flag : ALLMN{H3LL0_D4MN_D4N1EL_W73JFL}

NB : Special thanks to mxtmvn and fredrica for supported