

VishwaCTF-2021

CHALLENGES' WRITE-UPS



13-14 MARCH 2021

Team Kali Billi



Contents

WEB.....	4
Inspect the un-Inspected	4
Redeeem	5
bot not not bot.....	5
Is Js Necessary?	6
My Awesome YouTube recommendation	7
Time is an illusion.....	8
UwU Steps:.....	9
General.....	10
BiGh Issue	10
Prison Break	11
Good Driver Bad Driver	12
Secret Service	13
Treasure Hunt	14
Front Pages.....	15
Pub	16
Find the room	17
Git Up and Dance	17
Magician	19
Findthepass.....	20
Warmup	21
Flag Format	21
Discord-bot	21
Networking	22
Commenting is the key	22
Invalid	23
Cryptography	24
Mosha	24
A typical day at work	24
Weird Message.....	25
Can you see??	25
From the FUTURE	26
Reverse Engineering	27



Apollo 11	27
Rotations	27
Misleading Steps	28
Facile	28
Give it to get it	29
Suisse	29
Forensics	30
Barcode Scanner	30
Peace	31
Sherlock	32
Comments	33
Bubblegum	34
Remember	35
Dancing LEDs	36



WEB

Inspect the un-Inspected

Challenge 63 Solves x

Inspect the un-Inspected

479

Home is the only place where you can practice and frequently ask questions! maybe..?

Flag Submit

Steps:

- From questions I picked up word Home, Practice and FAQs.
- Flag was divided into three parts.
 - 1/3 flag: `vishwaCTF{EvEry_` at Home (<https://vishwactf.com/>) source code.
 - 2/3 flag: `C0iN_ha$` in Practice-Flag (<https://play-vishwactf-mini.ml/flag>) source code in hidden (black) format "`<p style="color: black;">C0iN_ha$</p>`"
 - 3/3 flag: `_3_s1Des}` in GitHub repository FAQ file.

FLAG: **vishwaCTF{EvEry_C0iN_ha\$__3_s1Des}**



Redeeem

Challenge 148 Solves ×

Redeeem
385

One of our seller has the flags. and it seems you don't have enough money to buy the same. The only way to get money is by redeeming the coupon code. TRY UR LUCK ! <https://redeeeem.vishwactf.com/>

Steps:

- Opened [BurpSuite](#) and Intercepted the request.
- Changed the wallet money to 6969.
- It passed the request and showed the flag.

FLAG: **vishwaCTF{@DDed_T0_C@rT}**

bot not not bot

Challenge 185 Solves ×

bot not not bot
322

Ain't Much, But It's Honest Work!!! <https://bot-not-not-bot.vishwactf.com/>

Steps:

- Parts of flag were hidden in few links from the 500 different links which were present on this website <https://bot-not-not-bot.vishwactf.com/>
- Made a custom script for web scraping
- Then found the Flag

FLAG: - **vishwaCTF{r0bot_15_t00_OP}**



Is Js Necessary?

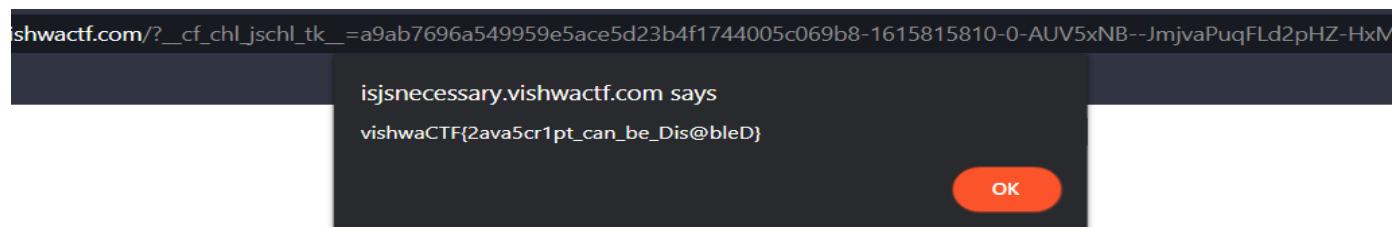
Challenge 152 Solves X

Is Js Necessary?
380
<https://isjsnecessaryvishwactf.com>

Flag Submit

Steps:

- Click the challenge a popup will come with link.
- After clicking the link, it will redirect to google.com in fractions of seconds
- To check why this is happening click the link and trap the request in burpsuit and send it to burp repeater then you will see a JS function is causing this redirection in about 200 ms
- To stop this function being executed block the scripts from browser's setting
- First click the link then cloudflare will do some authentication for 5 sec after
- That 5 sec block the JS from browser setting after blocking the link will not redirect to google.com instead it will stay on original website
- When original website will not redirect then unblock scripts
- On original website one question was given after answering (answer was 10) the Question flag will be popup



Save me!

I don't wanna go back!!!

how many days did Brendan take to develop this language?
 submit

FLAG: - **vishwaCTF{2ava5cr1pt_can_be_Dis@bleD}**



My Awesome YouTube recommendation

Challenge 48 Solves

My Awesome Youtube recommendation

487

Hey there, I made my first Flask app which recommends youtube videos for your search. Hope you like it.

<https://yt-search.vishwactf.com/>

Flag Submit

Steps:

- Open the challenge and go to given [link](#) in the challenge

During pandemic, everyone has been bored. So we have created this search system, where you'll search something and it'll recommend videos on youtube!

Hear us out, not affiliated by youtube

Hello From the other sideeeeeee

Hello From the other sideeeeeee

- Type vishwactf or anything in the input box and trap the request in burpSuite and then forward the request to burp repeater and change the Query of URL to “{{ config }}” which is payload to get flag from the website
 - After changing the query, you will be prompted to website where you will get the flag

FLAG: - vishwaCTF{th3_f14q_ln_c0nflq}



Time is an illusion

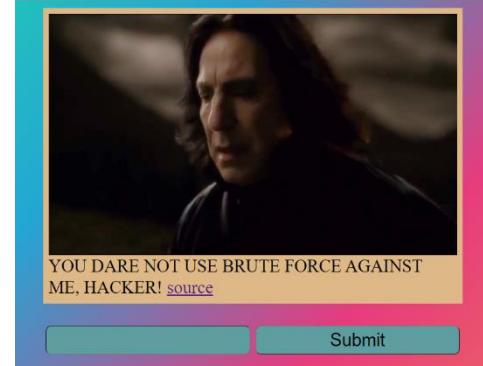
Challenge 34 Solves X

Time is an illusion
493

The source should convey it all <https://time-is-an-illusion.vishwactf.com/>

Flag

Submit



Steps:

- First let's visit to the source.
- Looking at the source it seems like we'll have to brute force.
- As it says that the key is 5 characters long including numbers and characters both capital and small, so we prepared a script to brute force it.
- After some time, the script gave us the output as "KuKa9".
- Entering it in the input box we get

vishwaCTF{PhP_h@\$_iTs_0wN_PErK\$}

the flag.

- Flag = **vishwaCTF{PhP_h@\$_iTs_0wN_PErK\$}**

```
<?php
include "env.php";
set_time_limit(0);
if(isset($_GET['key'])){
    $your_input = $_GET['key'];
    if(strlen($your_input)!=5){
        die("It's five characters long, and may or may not contain numbers or characters or small letters or");
    }
    for($i=0; $i<strlen($your_input);$i++){
        $let_check=$_ENV['our_input'];
        if($your_input[$i]!=$let_check[$i]){
            die("VERY VERY VERY INCORRECT");
        }
        usleep(100000);
    }
    echo getenv('THE_THING_YOU_ARE_LOOKING_FOR');
}
>>
```



UwU

Challenge 98 Solves X

UwU
448

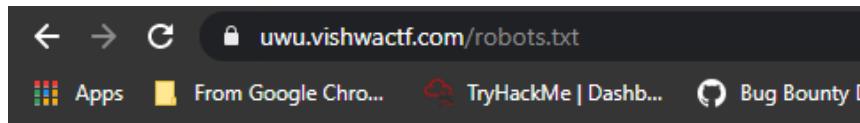
when php, anime and robots come together. they make hell of a challenge. <https://uwu.vishwactf.com/>

Flag

Submit

Steps:

- When you open the challenge link, there is some anime site where a video is playing. Nothing useful in that site, I guess.
- But then as the challenge suggest "robots" so that make me go to robots.txt.



- So as robots.txt suggest, there is a directory named "robots", which when visited looks something like this.

Here, we find some source code which is in php with a preg_replace function in it.

- Read more about preg_replace over [here](#).
- So, using preg_replace function and a little brainstorming we edited the URL of the challenge to this GET request

```
<!DOCTYPE HTML>
<?php
require("cyberflagster.php");
$try; //1
$function; //5
if (isset($_GET['showThem'])) {
    highlight_file(__FILE__);
    die();
}
$reach; //3
if (isset($_GET['php_is_hard'])) {
    $you_enter = $_GET['php_is_hard'];
    $we_enter = 'suzuki_harumiya';
    $the_final_one = preg_replace(
        "/$we_enter/", '', $you_enter);
    if ($the_final_one === $we_enter) {
        open_up();
    }
    $to; //2
    $open_up; //4
?>
```

https://uwu.vishwactf.com/robots/?php_is_hard=suzuki_suzuki_harumiyaharumiya

- There we got the flag.

great, here it is what your looking for=> vishwaCTF{well_this_was_a_journey}

- Flag = **vishwaCTF{well_this_was_a_journey}**



General

BiGh Issue

Challenge 30 Solves

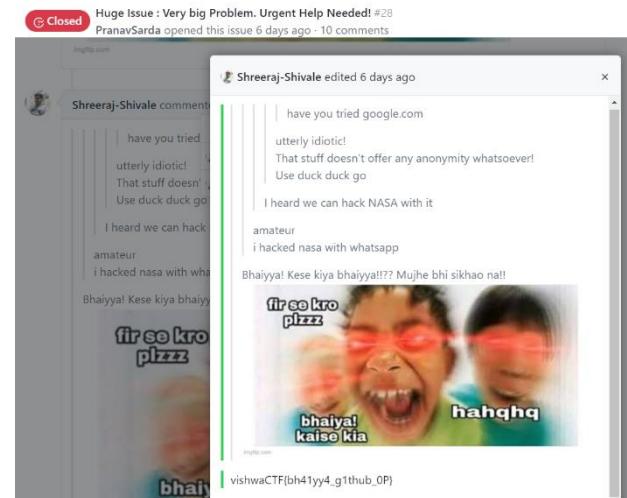
BiGh Issue
496

Our team recently faced a very big issue while making the frontpage website for vishwaCTF'21. Thankfully, it got resolved later and we closed the discussion off. But I guess someone accidentally posted a flag there, and had to take a lot of hearing from our guide.

Flag Submit

Steps:

- Found the GitHub repository of VishwaCTF2021 (<https://github.com/CybercellVIIIT/vishwaCTFWebsite21/issues/28>)
- Found "[Huge Issue : Very big Problem. Urgent Help Needed!](#)" closed issues in insights.
- There people were talking about the "Big Issue"
- In last there was a post that was edited
- Found bug by seeing the edited history of that post
-



FLAG: - **vishwaCTF{bh41yy4_g1thub_0P}**



Prison Break

Challenge 86 Solves X

Prison Break
463

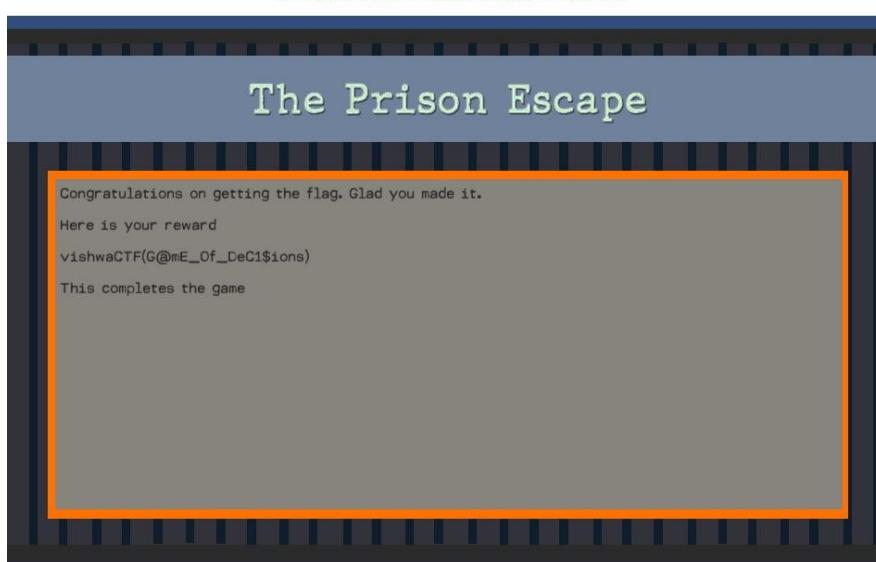
Please help yourself, Get out of the prison! and YES,
every move matters. <https://prisonbreak.vishwactf.com/>

Flag Submit

Step:

- I followed the story line and found the flag.

This game has the flag in it! Play the game to find the flag



- Flag = **vishwaCTF{G@mE_Of_DeC1\$ions}**



Good Driver Bad Driver

Challenge 31 Solves

Good Driver Bad Driver
496

We are starting a new service company providing on-rent good drivers, by the name BBDDrivers. We already have 3600 drivers that we have classified as Good=0, Average=1 or Bad=2 and also have their scores on particular tests. We have received 400 more applications for drivers, but reviewing them will be a loss of time and money. Can you please let me know what kind of drivers these guys are? I'll even give you the old driver's data in case you need it.

Test your results here (Follow instructions shown on the website): <https://drivervishwactf.com/>
Enter the results only in a string as mentioned on the website. You will get a flag only if you have an accuracy of 1.0 in predicting the classes.

Designer : <http://www.antrixacademy.com/>

[drivert...](#) [driverte...](#)

Steps:

- I figured out the pattern of grading.
- Found out
 - If Distance_feature < 100 ; Rating = Average =1
 - If Distance_feature > =100
 - Speeding_Feature <50 ; Rating = Good=0
 - Speeding_Feature >=50 ; Rating = Bad=2
- Sorted out list of drivertestunlabeled and ranked them according to the above. Later I used MS Excel functions to unsort.

S21	A	B	C	D
22	60.75	30	1	
23	49.16	4	1	
24	34.81	8	1	
25	179.26	79	2	
26	32.9	16	1	
27	100.49	4	1	
28	193.05	11	0	
29	82.03	6	1	
30	40.49	5	1	
31	130.83	24	1	
32	59.66	9	1	
33	44.18	5	1	
34	55.56	4	1	
35	42.81	6	1	
36	102.42	7	1	
37	57.65	8	1	
38	58.38	5	1	
39	46.51	6	1	
40	153.53	2	1	
41	30.45	7	1	
42	169.24	4	0	
43	42.86	24	1	
44	56.42	6	1	
45	109.59	6	1	
46	177.29	10	0	
47	50.05	8	1	
48	58.98	6	1	
49	200.58	5	0	
50	166.1	18	0	
51	58.03	24	1	
52	70.59	2	1	
53	65.82	6	1	
54	130.34	16	0	
55	153.45	1	0	
56	48.47	3	1	
57	55.72	5	1	
58	200.21	18	0	
59	54.89	3	1	
60	58.46	5	1	
61	54.89	6	1	
62	166.51	15	0	
63	183.67	9	0	
64	52.12	5	1	
65	51.97	2	1	

- Made a string of the rankings and submitted.

FLAG: vishwaCTF{d4t4_5c13nc3_15_n3c3554ry}



Secret Service

Challenge 16 Solves ×

Secret Service
499

Hello.
We are looking for highly intelligent individuals. To find them, we have devised a test. There is a url hidden in the image. Find the 3 prime numbers and it will lead you on a road to find us.
Good Luck
3301

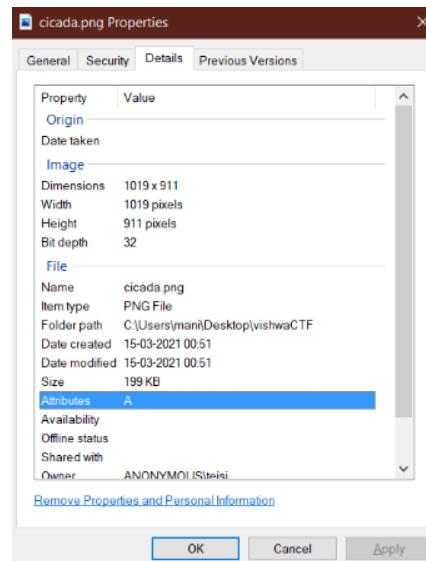
note -> The url is the flag and just input the number string in [www.\(string\).com](http://www.(string).com)

cicada.p...

Flag Submit

Steps:

- I opened the description of the image and found 2 prime number in description (width-1019 and breadth-911) and third prime number was in



question – 3301

- I multiplied all these three prime numbers which came out-3064348009

FLAG: **vishwaCTF{www.3064348009.com}**



Treasure Hunt

Challenge 126 Solves ×

Treasure Hunt
421

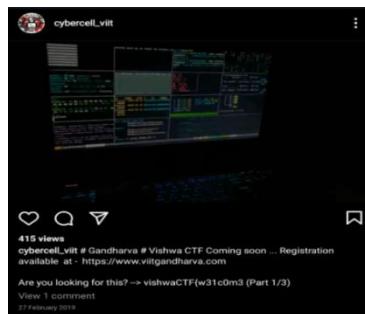
Instagram, Twitter and LinkedIn are the steps to Social Success. And, I'm sure I put the flag somewhere on our posts here, but I can't remember if it was the caption or comment or retweet. Can you help me find it? Go sequentially

[Instagram](#)
[LinkedIn](#)
[Twitter](#)

Flag

Steps:

- On 1st post of Instagram (<https://www.instagram.com/p/BuY2bhkhboO/?igshid=1bxmneomcaevr>) I found 1st part of flag.



- On LinkedIn post (https://www.linkedin.com/posts/cybercell-viit_cybersecurity-security-cyber-activity-6705436186833387521-aghB) I found 2nd part of flag



- On twitter post (<https://twitter.com/cybercellviit/status/1299671113039970305>) I found 3rd part of the flag.



FLAG:

vishwaCTF{w31c0m3_t0_v1shw4ctf}



Front Pages

Challenge 39 Solves X

Front Pages
493

Cover pages or front pages of newspapers and magazines contain the biggest news stories and are designed to grab a person's attention. BTW, did you know that the internet has a front page too?
Flag Format is same : vishwaCTF{}

Flag Submit

Steps:

- Reddit is the front page of internet so searched VishwaCTF on reddit and found a post but something was deleted from it.
- So, checked it through "Wayback Machine" and got this.

Well, so I'm just gonna drop the flag here, and I certainly hope no hackers get access to this.

So here goes:

vishwaCTF{0\$dVI_1z_kFV3g_0a3mT0graD}

But hang on, this text doesn't make sense, does it?

Oh well, it is what it is I guess.

Good luck for rest of the challenges!

P.S. 18th century French scholars deserve more recognition!

- Using [vignere cipher decoder](#) we encoded flag (i.e 0\$dVI_1z_kFV3g_0a3mT0graD). In "text to decode" block and enter "VISHWACTF" as key in **Key block** and got the flag in the output.

Flag: **vishwaCTF{0\$int_1s_oft3n_0v3rl0oked}**

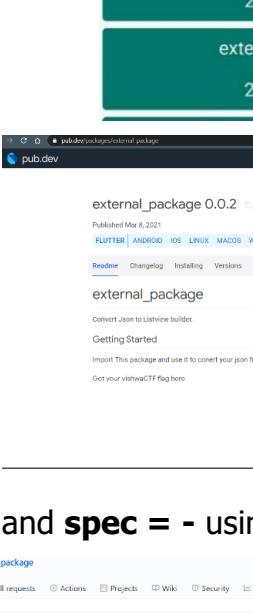


Pub

Challenge	14 Solves
pub 500	
This Flutter app lists some popular marvel movies. Go through the movie list.	
Unlock Hint for 200 points	
 pub.apk	
Flag	Submit

Steps:

- Downloaded the given "pub.apk" and searched the contents of file.
 - It had a long list of Marvel Movies but one odd file named "external_package"
 - I searched for "pub flutter" and got a website (<https://pub.dev/>) where I searched for this "external_package" which made me land on (https://pub.dev/packages/external_package)
 - It had a GitHub repo link on right. On navigating there (https://github.com/anilChouhan-sh/external_package) I found a file "pubspec.yaml" which had editing history and encoded flag.

 - After analysing these edits we figured out **pub = .** and **spec = -** using which we converted whole flag to morse code.
 - Then using the online converter we converted the morse code and got the flag

List of Marvel Movies
2016-10-25
Guardians of the Galaxy Vol. 2
2017-04-19
external_package
2017-07-05

pub.dev/packages/external package

The screenshot shows the details page for the `external_package` package on the Flutter package page. The package name is at the top, followed by its version `0.0.2`. Below the name is a link to the package's GitHub repository. The page includes tabs for `FLUTTER`, `ANDROID`, `IOS`, `LINUX`, `MACOS`, `WEB`, and `WINDOWS`. A progress bar indicates the package is 11% complete. Below the tabs are sections for `Readme`, `ChangeLog`, `Installing`, `Versions`, and `Scores`. The `Installing` section contains a button to "Convert JSON to ListView builder". Below this is a "Getting Started" section with a "Import" instruction and a link to "Get your vishvawCTF flag here". On the right side, there are sections for `1`, `90`, and `11%` labeled `LIKES`, `PUBS`, and `POPULARITY` respectively. Below these are links for `MetricData`, `This is a flutter package`, `GitHub`, `Issues`, `Repository (GitHub)`, `View report issues`, `Documentation`, `API Reference`, and `Uploader` (with an email address). At the bottom, there are links for `Licenses` and `BSD (LICENSE)`.

pub - : and spec - - using which

anilChouhan-sh / external_package

Code Issues Pull requests Actions Projects Wiki Security Insights

Update pubspec.yaml

update 3

master

anilChouhan-sh committed 3 days ago Verified

Showing 1 changed file with 1 addition and 1 deletion.

pubspec.yaml

```
35 # To add custom fonts to your package, add a fonts section here.
36 # In this section, font names can be mapped to a "fontFamily" value.
37 # For example, the font "My Font" can be accessed as "myFont" using
38 # <img>#font myFont>.
39 # pubsubspec pubsubpub pubsubpubpubpubpubspec pubpubpubspec
40 # pubsubpubspecspec pubsubspec pubspecspecpub pubsubpubspecspecpub
41 # pubsubpubspecspecpub spec specpub specpubspecspecpub
42 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
43 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
44 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
45 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
46 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
47 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
48 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
49 # specpubspecspecpub specpubspecspecpub specpubspecspecpub
50 # list giving the asset and other descriptors for the font. For
51 # example:
52 # fonts:
```

F1 AG: vishwaCTE{US3FU1 F1UTT3R P@CKAGE}



Find the room

Challenge 55 Solves ×

Find the room
486

Studying in VIIT(FV5M+VH) is one of the best experiences in my life... You need to be street smart in order to survive... I got called to the principals office one day, and couldn't find the room number(Yes!! am not very smart! and Nope!! don't belong here!) Can you help me find it? Maybe the room number is a flag

Flag Submit

Steps:

1. Googled “FV5M+VH,pune” and zoomed google map
2. Changed to street view and found the room



FLAG: **vishwaCTF{A 003}**

Git Up and Dance

Challenge 61 Solves ×

Git Up and Dance
480

You gotta git up and maybe dance a little back and forth to get the desired result

git_up_and_d...

Flag Submit

Steps:

- Extract the zip file from the question.
- You can see that this folder contains many files and an index file.



- We use “git log -p | grep -i vishwa” to see the log and find the flag from it.

```
root@kali:/media/sf_Shared_with_VM/git up and dance# git log -p | grep -i vishwa
-          // This is not the flag vishwaCTF{d4nc3ing_4nd_gitup}
+      // This is not the flag vishwaCTF{d4nc3ing_4nd_gitup}
+      // This is not the flag vishwaCTF{d4nc3ing_4nd_gitup}
-          // This is the flag vishwaCTF{d4nc3_4nd_giitupp}
-          // This is not the flag vishwaCTF{d4nc3ing_4nd_gitup}
-          // This is the flag vishwaCTF{d4nc3_4nd_giitupp} [Flag]
-          // This not the flag vishwaCTF{d4nc3ing_4nd_gitup}
+      // This is not the flag vishwaCTF{d4nc3ing_4nd_gitup}
-          // This not the flag vishwaCTF{d4nc3ing_4nd_gitup}
+      // This is the flag vishwaCTF{d4nc3_4nd_giitupp}
+      // This not the flag vishwaCTF{d4nc3ing_4nd_gitup}
+      // This not the flag vishwaCTF{d4nc3ing_4nd_gitup}
+      <meta name="keywords" content="matias martinez, vishwactf, ditto, konga, conga, shake your body">
root@kali:/media/sf_Shared_with_VM/git up and dance#
```

- Flag = **vishwaCTF{d4nc3_4nd_giitupp}**



Magician

Challenge 44 Solves X

Magician
491

I'll show you a cool magic trick. check it out:
<https://magician.vishwactf.com/>

Flag

Submit

Steps:

- The site gives us one letter of a flag at a time and it takes 20-25 minutes for the next letter but do we have time?
- We automate the task using a script.

```
import requests, re
flag = []
for i in range(40):
    flag.append("")
while(True):
    s = requests.Session()

    html = s.get('https://magician.vishwactf.com/%27).text

    symbol = re.search("<body>\s*<h1>\s([a-zA-Z0-9_])\s</h1>",html).group(1)
    pos = re.search("(\\d+)+\\s</h1>\\s<h3>", html).group(1)
    flag[int(pos)] = symbol
    print("".join(flag))
```

- Now we get the flag as **vishwaCTF{cr0nj0bs_m4k3_l1f3_s1mp13}**



Findthepass

Challenge 42 Solves X

findthepass
492

You have been provided with a vm of a linux os, find the password of the root
https://drive.google.com/file/d/14FnXZ1DiHgCFPKQF_hIZdAU, usp=sharing

Steps:

- Install the vm given in the file.
- There's a dump of with 10 passwords.
- Convert the hash and try each with admin you will the right password that is "password"
- Flag = **vishwaCTF{password}**



Warmup

Flag Format

Challenge 362 Solves X

Flag Format 25

The Flag Format is : vishwaCTF{} The Flag for all challenges would follow this format unless specified otherwise in the challenge. The Flag for this challenge is : vishwaCTF{welcome_to_vishwaCTF}

Flag Submit

Flag: **vishwaCTF{welcome_to_vishwaCTF}**

Discord-bot

Challenge 168 Solves X

Discord-bot 354

Try communicating with the VishwaCTFbot on our discord... it may respond with a flag...

Syntax:\$

Flag Submit

Steps:

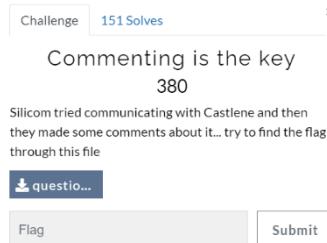
- Messaged “\$flag” to VISHWACTFBOT and it gave the flag.

Flag: **vishwaCTF{d15c0rd_5p1ll3d_th3_b34n5}**



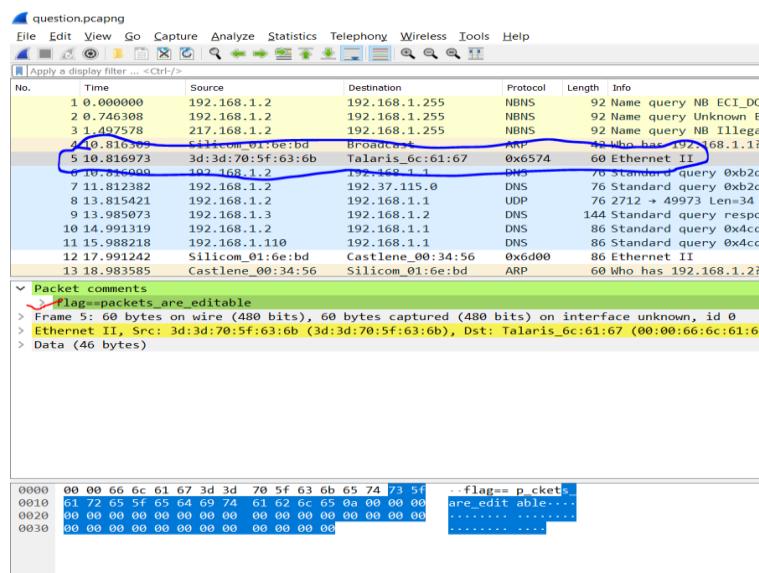
Networking

Commenting is the key



Steps:

- open the challenge and download the file given in challenge
- Open the file in wireshark then go through each packets
- Flag was hidden in the packets comments of 5th packet



Flag: **vishwaCTF{packets_are_editable}**



Invalid

Challenge 142 Solves X

Invalid
394

In the previous challenge's file, what was the ip of the person who entered the wrong credentials?

Flag

Submit

Steps:

- Open the pcap file in wireshark
- Search for SIP protocol and you will find the IP address of the user who input the wrong password.

No.	Time	Source	Destination	Protocol	Length	Info
29	49.418608	192.168.1.1	192.168.1.2	UDP	105	9587 → 156 [BAD UDP LENGTH 199 > IP PAYLOAD LENGTH] Len=191
30	49.420564	Silicom_01:6e:bd	Castlrene_00:34:56	0x2800	722	Ethernet II
31	49.566655	208.242.33.35	192.168.1.2	SIP	348	Status: 100 Trying
32	49.616489	212.242.33.35	192.168.1.2	SIP	388	Status: 403 Wrong password
33	49.736731	192.168.1.2	192.168.1.255	NBNS	92	Name query NB ECI DOMAIN\1c>
34	54.257334	192.168.1.2	192.168.1.251	NBDS	243	Direct group datagram [Malformed Packet]

- Flag = **212.242.33.35**



Cryptography

Mosha

Challenge 40 Solves ×

Mosha
492

My friend created a font and sent me a message. I cant quite understand it.
Help me decode it. He has posted the font on a social media under the name mosha font or something.

moshat...

Flag Submit

- The language given in the image was weird but we had to find it on some social media platform to decode it.
- Found the Mosha font on Instagram with username `@mosha_font` and it had 2 posts with the font script.
- Compared the font with the image and got the flag

Flag: - **vishwaCTF{Y0u4rem05hAnoW}**

A typical day at work

Challenge 57 Solves ×

A typical day at work
484

The manager at mcgronalds seemed very happy today, after a tedious day at work, he shed tears of joy and said this "yonvkahj_on_jeyonx_jeajon"... can you tell us what he said?

Flag Submit

Steps:

1. We searched "mcgronalds" and found anime reference of 'hataraku'.
2. Figured out the "Entean language" is used in anime which is a substitution cypher with the help of this blog (<https://hataraku.fandom.com/f/p/3009718557606080307>)
3. Decoded the statement "yonvkahj_on_jeyonx_jeajon"

FLAG: **vishwaCTF{congrats_on_second_season}**



Weird Message

Challenge 22 Solves X

Weird Message
498

My friend sent me this file containing a damn long string.
He told me to find the message to prove I'm worthy of
his friendship XD. Please help me do it!
Something about the length is bothering me. Also, he
told me to remember this short message for our next
meeting. Is this really rememberable?

Steps:

1. Opened the file given in notepad and zoomed out.
2. It seemed to us like something is drawn.
3. Figured out it was a binary image
4. Used <https://www.dcode.fr/binary-image> to decode it and got the flag.

FLAG: **vishwaCTF{pr1m35_4r3_w31rd}**

Can you see??

Challenge 5 Solves X

Can you see??
500

Steps:

- Used Braille Notation to decode the content of the given file, were 1=upper dots and 0=lower dots

FLAG: **vishwaCTF{vvho n33ds 3y3s 7o 5ee}**



From the FUTURE

Challenge 141 Solves X

From the FUTURE
400

Accidentally frozen, pizza-deliverer Fry wakes up 1,000 years in the future and finds himself surrounded by cyclops, robots, flying cars and crazy scientists. He is given a note but he can't understand it. Can you help him??

 note.png

Flag Submit

Steps:

- We searched terms from question like "frozen", "pizza-delivery Fry" by which we got to know about Futurama.
- Decoded the given file using Futurama Decoder (<https://www.dcode.fr/futurama-alien-alphabet>) and got the flag.

FLAG: **vishwaCTF{WEARENOTALONE}**



Reverse Engineering

Apollo 11

Challenge 129 Solves X

Apollo 11
412

Apollo's next mission is put on hold owing to a backdoor passkey. I'm pretty sure some rival countries have a hand in this. Hope you find it...

Apollo11.iso

Flag

Submit

Steps:

- Strings Apollo11.iso to find the flag.
- Use “*strings Apollo11.iso | grep Vishwa*”
- Flag: **vishwaCTF{I50_1s_A_MEs5}**

```
root@kali:~/Downloads# strings Apollo11.iso | grep vishwa
vishwaCTF{I50_1s_A_MEs5}
root@kali:~/Downloads#
```

Rotations

Challenge 98 Solves X

Rotations
450

Rotations make you dizzy...don't they?

mm

Flag

Submit

Steps:

- Check file type by “file mm”. It is a ELF file.
- “strings mm” and we see some format which is similar to our flag format. ivfujnP GS{s1Nt_1f_e0g4gRq_Ol_!3}.
- Not the challenge name hints about it being ROT encoded.
- We decoded it using ROT13 and got the flag.
- Flag: **vishwaCTF{f1Ag_1s_r0t4tEd_By_!3}**

```
u+UH
ivfujnP GS{s1Nt_1f_e0g4gRq_Ol_!3}
S{1Nt_1f_e0g4gRq_Ol_!3}
JTHGFEDCH
```



Misleading Steps

Challenge 78 Solves X

Misleading Steps

468

Misleading Steps often lead you to unexpected places...

mislead

Flag

Submit

Steps:

- Used strings to find it lol, it was a mislead vishwaCTF{1_0ft3n_M1sl3ad_pPl}.
 - Now used Ghidra and saw the function main.
 - There was some hex code with it
“7669736877614354467b556d4d5f77336952446f6f6f305f416d5f7468335f723
3346c5f306e337d”
 - Decoded it and got the flag.
- ```
root@kali:/media/sf_Shared_with_VM# echo 7669736877614354467b556d4d5f77336952446
f6f6f305f416d5f7468335f723346c5f306e337d | xxd -p -r
vishwaCTF{UmM_w3iRDooo0_Am_th3_r34l_0n3}root@kali:/media/sf_Shared_with_VM#
```
- Flag: **vishwaCTF{UmM\_w3iRDooo0\_Am\_th3\_r34l\_0n3}**

## Facile

Challenge    47 Solves    X

### Facile

489

Mr Bingo has hidden something secretive inside...

**s1mple.gzf**

Flag

Submit

Steps:

- Use binwalk to extract the file “binwalk -e s1mple.gzf”
- There is a file names “FOLDER\_ITEM”.
- Strings it and you get the flag.

```
root@kali:/media/sf_Shared_with_VM/_s1mple.gzf-0.extracted# strings FOLDER_ITEM | grep -i vishwa
vishwaCTF{r3v_1t_1s5s5s}
root@kali:/media/sf_Shared_with_VM/_s1mple.gzf-0.extracted#
```

- Flag: **vishwaCTF{r3v\_1t\_1s5s5s}**



## Give it to get it

Challenge 27 Solves ×

Give it to get it  
497

vishwaCTF{f14g\_1s\_Wh3r3\_Th3\_h3aRt\_L1Es} HEHE THIS  
Ain't the flag. You'll have to give it something so that it splits  
out this flag. The "something" is the flag.

[a.out](#)

Flag

Submit

Steps:

```
a = 'vishwaCTF{f14g_1s_Wh3r3_Th3_h3aRt_L1Es}'
a = [hex(ord(i))[2:] for i in a]
print(''.join(a))
```

- This code will take the text from the flag given in the question of the challenge and will give us a hex output.
- Now we have a hex number and that is the flag.
- **7669736877614354467b663134675f31735f57683372335f5468335  
f68336152745f4c3145737d0**
- This hex is the flag.

## Suisse

Challenge 21 Solves ×

Suisse  
498

Let's Uno His Name and reduce 3 from each uno you found.  
Admin suffers from cardiovascular disorders. So do obtain  
the flag accordingly.

Note: Do not include whitespaces in the flag if you find any.  
and your flag should be of the format vishwaCTF{flagtext}.

[a.out](#)

Flag

Submit

Steps:

- Using Ghidra to open a.out file, you will find a hex code in main function “111 88 107 81 113 93 52 118 56 104 102 88 85 104” and convert it to string “oXkQq]4v8hfXUh”
- Now Convert this in ASCII Number
- And then reduce 3 from each number.
- Then convert this again to text you will get this “IUhNnZ1s5ecURe”
- Flag: **vishwaCTF{ IUhNnZ1s5ecURe }**

|     |    |     |    |     |    |    |     |    |     |     |    |    |     |
|-----|----|-----|----|-----|----|----|-----|----|-----|-----|----|----|-----|
| 111 | 88 | 107 | 81 | 113 | 93 | 52 | 118 | 56 | 104 | 102 | 88 | 85 | 104 |
| 108 | 85 | 104 | 78 | 110 | 90 | 49 | 115 | 53 | 101 | 99  | 85 | 82 | 101 |



## Forensics

### Barcode Scanner

Challenge    103 Solves    X

### Barcode Scanner

446

My phone is not recognizing this barcode. Can you give it a try?

Flag

Submit

Steps:

- This was the given barcode.



- Download any barcode scanner app from Google play store/Apple store and scan it
- Flag: **vishwaCTF{5oo\_3asY}**



## Peace

Challenge    89 Solves    X

peace  
460

commando1(radio)- ive tapped into enemy frequency and got  
a shocking news here's the message...over n out commando2  
(radio)- roger ....

**morse.rar**

Flag

Submit

Steps:

- We have a .rar file here which is password protected. What's the password? We don't have any hint on that.
- Here we could do 2 things, to use an online rar password cracker or run rockyou.txt to bruteforce the password.
- <https://www.lostmypass.com/file-types/rar/> Used this site to crack the password of morse.rar and the password came out to be "india".
- After we unrar the morse.rar file we get an audio file which has some morse code in it.
- Let's again use this online morse decoder and upload the file here. <https://morsecode.world/international/decoder/audio-decoder-adaptive.html>
- We get some hex values  
" 76 69 73 68 77 61 63 74 66 7B 37 68 33 79 5F 34 72 45 5F 46 30 72 33 66 65 37 31 6E 67 7D "
- After converting it to text we get the flag as  
**vishwactf{7h3y\_4rE\_F0r3fe71ng}.**



## Sherlock

Challenge    81 Solves    X

### Sherlock

468

Sherlock found a green envelope on its door step and this image.

 decode.jpg

Flag

Submit

#### Steps:

- Since it is a png image, we used zsteg to find whats inside it and found the flag.

```
root@kali:/media/sf_Shared_with_VM# zsteg -a decode.png
b2,rgba,lsb,xy .. text: ["?" repeated 14 times]
b2,abgr,msb,xy .. text: ["?" repeated 14 times]
b4,abgr,msb,xy .. file: MPEG ADTS, layer I, v2, Monaural
b5,rgb,msb,xy .. file: MPEG ADTS, layer II, v1, Monaural
b5,bgr,msb,xy .. file: MPEG ADTS, layer II, v1, Monaural
b5,rgba,msb,xy .. file: MPEG ADTS, layer II, v1, Monaural
b5,abgr,lsb,xy .. file: MPEG ADTS, layer II, v1, Monaural
b6,rgb,msb,xy .. file: MPEG ADTS, layer I, v2, Monaural
b6,bgr,msb,xy .. file: MPEG ADTS, layer I, v2, Monaural
b6,rgba,msb,xy .. file: MPEG ADTS, layer I, v2, Monaural
b7,rgb,lsb,xy .. file: , Monaural
b7,bgr,lsb,xy .. file: , Monaural
b7,rgba,lsb,xy .. file: , Monaural
b8,r,msb,xy .. text: ["?" repeated 14 times]
b8,g,msb,xy .. file: RDI Acoustic Doppler Current Profiler (ADCP)
b8,abgr,msb,xy .. file: ddis/ddif
b2,r,lsb,xy,prime .. file: AIX core file fulldump
b1,g,lsb,yx .. text: "vishwaCTF{@w3s0Me_sh3Rl0cK_H0m3s}"
b3,abgr,msb,xy .. file: AIX core file 64-bit
```

- Flag: **vishwaCTF{@w3s0Me\_sh3Rl0cK\_H0m3s}**



## Comments

Challenge      65 Solves      X

### Comments

478

Changing the contents of file will result in loosing the flag. So I repeat dont change its contents

Comments.d...

Flag

Submit

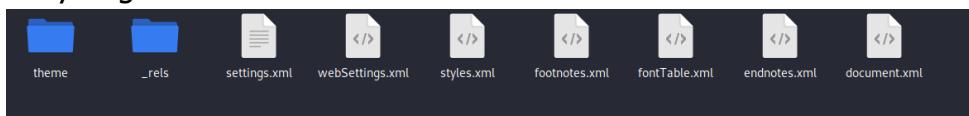
Steps:

- There was a word file named Comments.docx which at first was not suspicious at all
- When opened it contained this false flag.
- 
- Now we did some basic recon o the .docx file by using "file Comments.docx"

vishwaCTF{f@ls3\_fl@g}

and it came out that this is a OOXML file which is a zip file containing various files in it.

- Extract it using "unzip Comments.docx" in Linux.
- Now you get a bunch of files in extracted



- When you open "settgis.xml" file you will find the flag.

```
<!--vishwaCTF{comm3nts_@r3_g00d}-->
-<w:settings mc:Ignorable="w14 w15 w16se w16cid">
----- "100"-----
```

- Flag: **vishwaCTF{comm3nts\_@r3\_g00d}**



## Bubblegum

Challenge    42 Solves    X

Bubblegum  
491

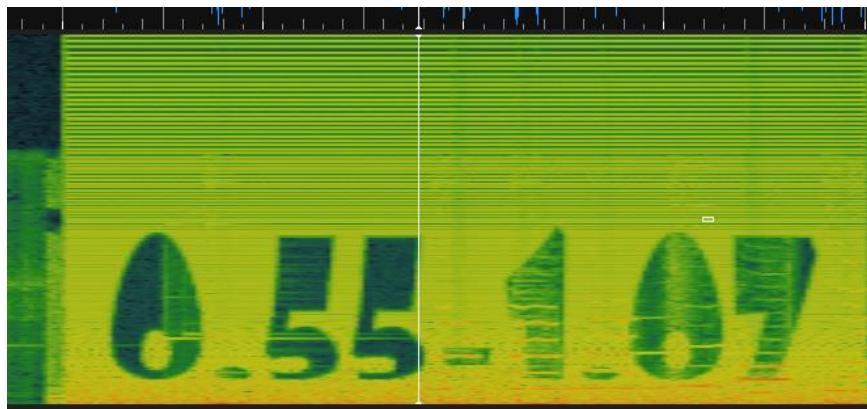
My sister loves a particular phrase of this songs. But i don't seem to guess it, can you make it simple for me?  
Note: only lowercase letters and no punctuation marks  
ex. He's the guy, right? -> vishwaCTF{hes the guy right}

Flag

Submit

Steps:

- When you listen to bkk.wav in any music player at a certain point of time you will find some distortion in the music.
- Evaluate it in Sonic Visualizer and enable the spectrogram view there we find something written there.



- ( 0.55 – 1.07 ) What could this be? The question said that the guy need the lyrics then this can be the timestamp of the lyrics in this music but we can't find lyrics in this audio.
- Simple OSINT on Bubblegum music on YouTube gives us various options but then the name of audio file suggests "bkk.wav" which means bubblegum by kk.
- Found the video there (<https://www.youtube.com/watch?v=5x441jo1-sg>). It had lyrics and at 0.55 to 1.07 we found the flag which was needed.
- Flag: vishwaCTF{oh bubble gum dear im yours forever i would never let them take your bubblegum away}



## Remember

Challenge    38 Solves    X

### Remember

494

Shreyas forgot when did he changed his Laptop's password. He has provided some files , can you tell when he changed his password ? flag format : vishwaCTF{day\_month\_date\_hour\_minutes\_seconds\_year} ex: vishwaCTF{saturday\_march\_13\_15\_30\_03\_2021} Ps: all lower case and also the month is january

[file1](#)    [file2](#)

Flag

Steps:

- 2 files were given to analyse.
- Using Registry Viewer from access data to analyse the files.
- File2 has a SAM directory we open it.
- We find the flag in SAM/Domains/Accounts/Users/000003E9.

The screenshot shows the Registry Viewer interface with the following details:

**File Structure:**

- file2
- SAM
  - Domains
    - Account
      - Aliases
      - Groups
      - Users
        - 000001F4
        - 000001F5
        - 000001F7
        - 000003E9
      - Names
    - Builtin
    - LastSkuUpgrade
    - RXACT

**Key Properties:**

| Property                  | Value                   |
|---------------------------|-------------------------|
| Last Written Time         | 10-01-2013 08:24:36 UTC |
| RID unique identifier     | 1001                    |
| User Name                 | Shreyas Gopal           |
| Logon Count               | 5                       |
| Last Logon Time           | 10-01-2013 08:24:36 UTC |
| Last Password Change Time | 10-01-2013 08:24:36 UTC |
| Expiration Time           | Never                   |
| Invalid Logon Count       | 0                       |
| Last Failed Login Time    | Never                   |

- Flag: **vishwaCTF{thursday\_january\_10\_08\_24\_36\_2013}**



## Dancing LEDs

Challenge    20 Solves    X

### Dancing LEDs

498

The creator is communicating in American Standard Code for Information Interchange.

[Download Video58.mp4](#)

Flag

Submit

Steps:

- Video with 7 blinking LEDs was given named "Video58.mp4"
- LED's blinking patterns were Binary Codes where one can see ON LED = 1 and OFF LED = 0
- 0110100 1101001 1110000 1011010 1001010 1001000 1111010 1111000 0110100 0110001 were the binary numbers the LEDs showed us.
- Decoded this to ASCII and got "4ipZJHzx41". Now this is Base58 as the video name also suggested us "58". Decode this in CyberChef and we get the flag.
- Flag: **vishwaCTF{b1!nk3r}**