

LambdaMamba / CTFwriteups

Code Issues Pull requests Actions Projects Security Insights

Files

main Go to file

- 1337UP_2022
- UTCTF_2022
- VishwaCTF_2022
- Cryptography
- Forensic
- Misc
- OSINT
- Platypus_Perry**
- files
- img
- README.md
- Rocket Raccoon
- The_Library
- README.md
- solved.png
- picoCTF_2022
- .gitignore
- README.md

CTFwriteups / VishwaCTF_2022 / OSINT / Platypus_Perry /

Add file ...

LambdaMamba Update challengenew.png 8b47e9f · 2 years ago History

Name	Last commit message	Last commit date
..		
files	Added writeup for VishwaCTF Platypus Perry	2 years ago
img	Update challengenew.png	2 years ago
README.md	Merge branch 'main' of https://github.com/LambdaMamba/CTFwriteups	2 years ago

README.md

Platypus Perry (Category: OSINT)

This challenge was an emotional rollercoaster, where I experienced the downs of multiple incorrect submissions and the highs of being the first to solve the challenge.

The challenge is the following,

Challenge 7 Solves **Challenge** 7 Solves

Platypus Perry

500

Agent John got some information that a group of people hid a bag of LSD on a dog. He needs to find the dog before it reaches the dealer.

Flag format: vishwaCTF{Firstname_Lastname}

Hint : David is Linked IN with some "Russian Hacks"

Hire-me.mp3

Flag **Submit**

Here, we are given the file [Hire-me.mp3](#). The challenge description says Agent John got some information that a group of people hid a bag of LSD on a dog. He needs to find the dog before it reaches the dealer., which is a pretty ambiguous challenge description but tells us that we should be looking for a dog .

When I listened to [Hire-me.mp3](#), I couldn't make out anything meaningful, so I opened it up on Audacity.

It sounded like it was in reverse, so I reversed the audio and amplified it.



This processed audio file can be found in [Hire-me-rev.mp3](#).

I listened to the audio and wrote down the letters, which gave me,

nierbrustiushcihwgnihemolletthgimlabmobdivadyugruo

Since the audio was in reverse, I assumed this text might also be in reverse, so I went ahead and reversed the text,

ourguydavidbombalmighttellusomethingwhichsuitsurbrain

And I added spaces to the text,

our guy david bombal might tell u something which suits ur brain

Now we know the next step would involve [David Bombal](#), who is a well-known guy in the infosec community and has a lot of websites and accounts associated with him.

The hint in the challenge says Hint : David is Linked IN with some "Russian Hacks" , which hints to looking up [his LinkedIn](#), and find something related to Russian Hacks .

His LinkedIn looks like the following,

David Bombal posted this • 1d
 Move and the way will open.
...show more

eco 183 2 comments

David Bombal posted this • 2d
Interview: Hackers Arise to hack Russia
...show more

 Interview: Hackers Arise to hack Russia // Ukraine Cyberwar
youtube.com
4 comments

Show all activity →

If we look closely, there is indeed a post related to [Russian Hacks](#).

 **David Bombal** • 3rd+
Author, Instructor and YouTuber - I've now reached 30,...
2d • 

[Interview: Hackers Arise to hack Russia](#)

Ukraine Cyberwar: <https://lnkd.in/gHkRvZrV> ...see more


HACKERS ARISE TO HACK RUSSIA

[Interview: Hackers Arise to hack Russia // Ukraine Cyberwar](#)
youtube.com

 **eco** 85 5 comments • 5 shares

And in the comments, I saw the following comment.

 **Atharva Pande** • 3rd+
EnTc Engineer at VIIT 
1d • ...
Yeh bugs here !

```
++++++[>+>++++>++++++>+++++++
<<<<-]>>>+++++.+++++++.----.+++.<-----.
----,>++++...<.----.----.----.----.----.
-.+++++.----.----.----.----.----.----.
<+,>----.----.----.----.----.----.----.
-<----,>----.----.----.----.----.----.
----.----.----.----.----.----.----.----.
-.+++++.----.----.----.----.----.----.
-.+++++.----.----.----.----.----.----.
-----.<-,>+++++++.----.----.----.----.
-----.<+,>-----.----.----.----.----.
```

[Like](#) | [Reply](#)

 **Eduardo Castellini Dourado** (He/Him) • 3rd+
Linux Administrator LPIC-1 (In process). Cloud Architect Oracle (O...
2d • ...
-Great interview with Professor David Bombal....!!!
-It's a digital war happening in parallel with the real war and guys working on a non government company's is the target of Russian

I went ahead and checked [Atharva Pande's LinkedIn](#),



Atharva Pande
EnTc Engineer at VIIT 
Pune, Maharashtra, India · [Contact info](#)

500+ connections

[+ Follow](#) [Message](#) [More](#)

About

Engineering Student
Philosopher
Thinker
Logo De: ...see more

Activity

539 followers

[+ Follow](#)

Atharva Pande commented on a post • 1d
Yeh bugs here !

++++++>+>++++>+++++>++++++<<<->>>+++++.+++++++,---.++-.-->...show more

 85 5 comments · 5 shares

This person was from Vishwakarma Institute of Information Technology, which is a [gold sponsor for VishwaCTF](#) so I assumed the comment this person made was one of the clues to this challenge.

I isolated the cipher-like section of [Atharva Pande's](#) comment, and put it into [brainfk.txt](#)



I wasn't exactly sure what type of cipher it was using, so I copied and pasted it into Google to get some hints.

Google

++++++[>+>++++>++++++>++++++><<<-]>>>++++.++++++ X |  

All Maps Videos Images Shopping More Tools

About 196,000,000 results (0.65 seconds)

<https://www.dcode.fr/brainfuck-language> :: Brainfuck Language - Online Decoder, Translator, Interpreter
decrement the byte in the memory cell where the pointer is located, ... The characters + and - are the most common and usually appear to +++ group or --- .

<https://en.wikipedia.org/wiki/Brainfuck> :: Brainfuck - Wikipedia
Cell #2 has value 72 which is 'H' >---. Subtract 3 from Cell #3 to get 101 which is 'e'
++++++..+++. Likewise for 'lo' from Cell #3 >>.

<https://www2.gvsu.edu/miljours> :: Analysis of the Programming Language Brain*ck
You can increment or decrement, by one, the byte at the pointer, ... +++,>> +++++++
[<++++++>]<+,-----,<++++++>,-----+++-----,> ...

So apparently, it was using Brain F*ck, so I went ahead to a Brain F*ck Decoder

Results

Console

<https://www.mediafire.com/file/q7ka3dhesrzftcd/bkchd.rar/file>

Memory:

```
[1] = (10)
[2] = (30)
[3] = / (47)
[4] = e (101)
```

BRAINFUCK INTERPRETER

★ BRAINFUCK CODE TO INTERPRET

```
-.-.+++++.+++.+++++++.-----.<.>-.+++++++.--.
<.>-.>----.++.----.<.>----.+++++++.<+++++++.>----.
----.----.<.>----.+++.----.++.
```

★ ARGUMENT

▶ EXECUTE

See also: [Leet Speak 1337](#) – [Spoon](#) – [Ook!](#)

Decoding this gave me the following URL:

<https://www.mediafire.com/file/q7ka3dhesrzftcd/bkchd.rar/file>

Accessing this [Media Fire Link](#) gave me the following:



bkchd.rar
Compressed Archive (RAR)

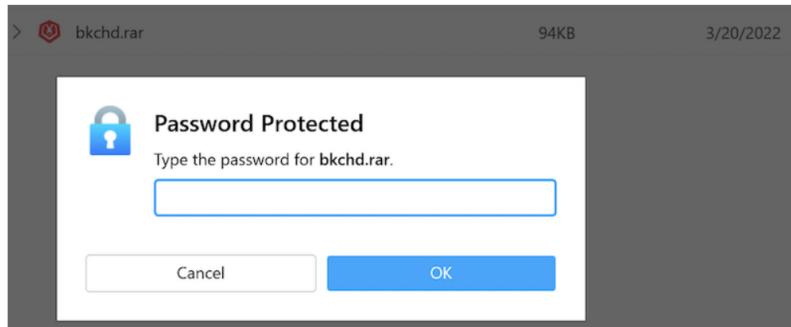
File size: 94.11KB

Uploaded: 2022-03-14 10:01:42

About Compressed Archive Formats

Compressed archives combine multiple files into a single file to make them easier to transport or save on diskspace. Archiving software may also provide options for encryption, file spanning, checksums, self-extraction, and self-installation. Zip is the most-widely used format, used by the Windows operating system and more recently by OSX as well. RAR is also a very popular and flexible format. Unix uses the tar file format, while Linux uses the tar and gz format.

I went ahead and downloaded [bkchd.rar](#), but unfortunately, it was password protected.



I tried to crack this .rar file using John the Ripper. A couple of hours passed, but no password candidate was found.

At this time, a new hint was added,

Challenge hints

Platypus Perry and Foggy has some password encrypted rar files and the bruteforcing pwd is 5 letter alphabets. Hope this helps

March 20th, 8:16:24 PM

Now I know that the password length is 5 characters, which drastically reduces the brute-forcing time.

So I downloaded `rockyou.txt` from [here](#), unzipped it, and isolated all the 5 character passwords into `rock5.txt` with,

```
$ grep -E '^.{5}$' rockyou.txt > rock5.txt
```

So now I just needed to use `rock5.txt` as the wordlist for John the Ripper.

I went ahead and made the hash using

```
$ sudo rar2john bkchd.rar > rarhash
```

And crack with John using [rock5.txt](#) as

```
$ john --wordlist=rock5.txt rarhash
```

After a few minutes, John has found the password, which is

```
[idgaf] [root@kali]~[home/kali/Desktop]
# sudo rar2john bkchd.rar > rarhash
! file name: bkchd.png

[root@kali]~[home/kali/Desktop]
# john --wordlist=rock5.txt rarhash
Using default input encoding: UTF-8
Loaded 1 password hash (rar, RAR3 [SHA1 256/256 AVX2 8x AES])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
idgaf          (bkchd.rar)
ig 0:00:07:03 DONE (2022-03-21 10:44) 0.002360g/s 383.0p/s 383.0c/s 383.0C/s
ifndri
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

[root@kali]~[home/kali/Desktop]
#
```

I went ahead and opened `bkchd.rar` with the password `ideaf`, and inside was the following picture.





I checked for steganographic messages using [Steganography Online](#)

Input



As shown above, some text was contained in this image, which I put into [decodedsteg.txt](#).



I didn't know what this was supposed to mean and assumed it was saying that this guy's pet, more specifically, the dog is what we're supposed to look for.

So I did a reverse image on Google using [bkchd.png](#).

Q All  Images  Maps  Shopping  More Tools

About 269 results (0.24 seconds)



Image size:
320 × 320

No other sizes of this image found.

Possible related search: **temporary tattoo**

Possible related search: ***temporary tattoo***

<https://www.amazon.co.jp> › Temporary-Tattoos

Results 1 - 12 of 10000+ — Online shopping for Temporary Tattoos from a great selection of brands.

Clothing ... tuzuru **Temporary Pregnancy Tattoos, Tattoo Stickers, ...**

Tattoos for now - Inkbox™

Lasts 1-2 weeks. Looks real. Not your

Lasts 1-2 weeks. Looks real. Not your average temporary tattoo. ... Want personalized tattoo recommendations? ... How long does an Inkbox tattoo last?

Visually similar images



However, nothing much came up except for other men with tattoos. So I went [Yandex](#) to do a reverse image search.

Vandex Uploaded image ×

Search Register

Web **Images** Video News Translate Disk Mail Ads



Размер изображения: 320x320 Select crop area

Image appears to contain

брutalnye borodatye kabanы brutalnyy zhuchina v shlyape

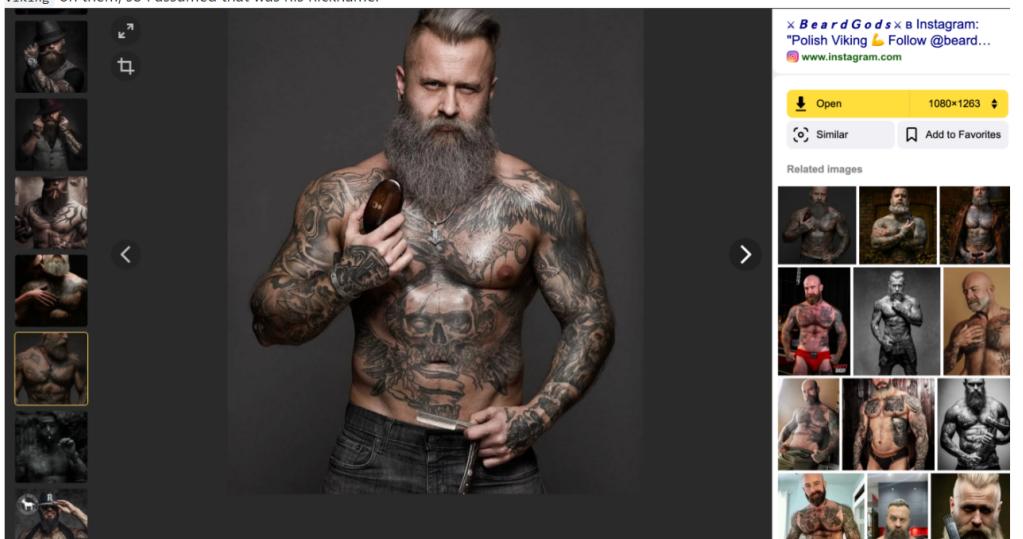
...
Similar images



Bad Guy

Similar images

By looking for his distinctive beard and tattoo through the reverse image search results, I noticed that most of them had the name **Polish Viking** on them, so I assumed that was his nickname.

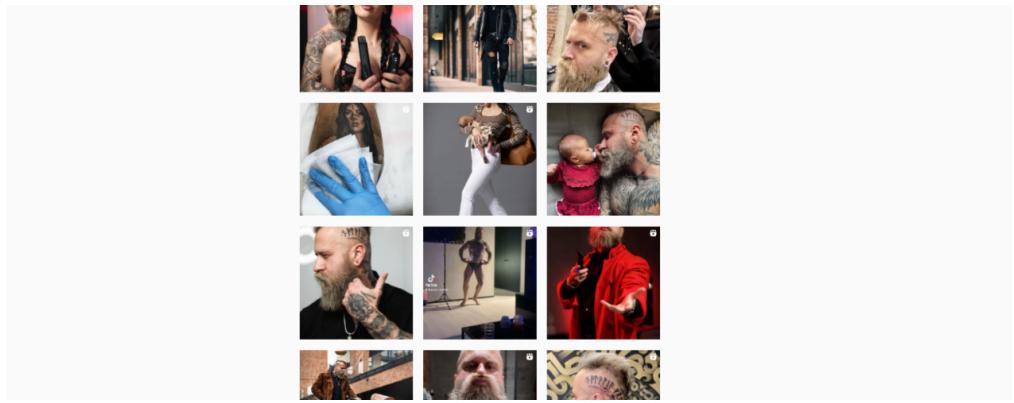


So I looked up Polish Viking,

Google polish viking X |

https://www.instagram.com/pavel_ladziak ::
Polish Viking (@pavel_ladziak) • Instagram photos and videos
462k Followers, 622 Following, 531 Posts - See Instagram photos and videos from Polish
Viking (@pavel_ladziak)

and found his Instagram and name, which was pavel_ladziak .



I went to Google and changed the language settings to Polish to get the most out of the results, and looked up `pavel ladziak dog`, which showed me that his dog was a toy dog with white and beige coloration.

Google

Q Wszystko **Grafika** Filmy Wiadomości Zakupy Więcej Narzędzia

vacchi gianluca gianluca vacchi pawel ladziak wife tattoo gym polish

Cover photos m.facebook.com Pavel Ladziak - We got t... facebook.com Pavel Ladziak - I found ... m.facebook.com Pavel Ladziak - My best vi... m.facebook.com Discover pavel ladziak ... tiktok.com Polish Viking Pavel Lad... pinterest.ca

Pavel Ladziak - Bearde... m.facebook.com Pavel Ladziak - Bearde... m.facebook.com Pavel Ladziak - Are you... m.facebook.com Pavel Ladziak - Please ... m.facebook.com Polish bodybuilder Pay... reddit.com Paweł Ladziak - Polish Vikin... pinterest.com

I dug through his Instagram, and found a [few pictures with his dog](#),

pavel_ladziak • Follow Warsaw, Poland

pavel_ladziak Love at first sight 🐶. We both care for our beards the same, you know 😊 @thebeardstruggle 20% off use my code „pavel” if you want 46 w

robertbyzantinos Ale jesteś czaderskim facetem. Podziwiam. Wspaniałe filmy i fotografie z Twoim udziałem. Super. Szacun..★★★★★★★★★★★★★★★★★★

cottage_living_dk @lulu_hansen84 32 w Reply View replies (1)

zainabali937_rz Nice pic 😍 40 w 1 like Reply

tinkkrbell 😍 40 w Reply

arita.kundu.3 ❤️ 43 w Reply

thorids_gewandung I'm in love 🔥 44 w Reply

terence.bosc @mortifera8 44 w Reply

However, I could not find the name of his dog. I was thinking to look through his followings list to find his dog, but I assumed that his wife might be more likely to tag their dog in the pictures.

531 posts 462k followers 622 following



Polish Viking

Photographer

My photo portfolio [@pavel_ladziak_foto](#)

♥[@natalia.zieicina](#) +++++ PRM+†

@bodyengineers code „BEVIKING” 15% off

@thebeardstruggle -20% code „Pavel”

tbs.discount/pavel

So I went ahead to [his wife's](#) account.

natalia.zieicina Follow ...

66 posts 25.9k followers 1,670 following

Natalia Ziecina •
Honey, beauty
last post 15h ago at @elvercosmetics

•
@pavel_ladziak
@pavel_ladziak
owner:
@natalia_zieicina_narczyna

26 photos 28 Reels 0 Videos 0 Tagged

grid of 18 photos showing various shots of Natalia Zieicina, including a baby, her in lingerie, and her with a dog.

So I dug through her pictures with their dog in it, and came across [this picture](#).

natalia.zieicina • Follow Tarnów

natalia.zieicina 📸 [@pavel_ladziak_foto](#) [@iamthemisio](#)

#photo #photomodel #polishgirl
#polish #instaphoto #instagirl
#polskadjewczyna #brunettegirl
#photoshoot #sunglasses
#sunglassesfashion #street
#streetphoto #tarnow

42 w

+

militarygymwear.official Super stylówka🔥 pozdrawiamy, dobrego dżonka💪

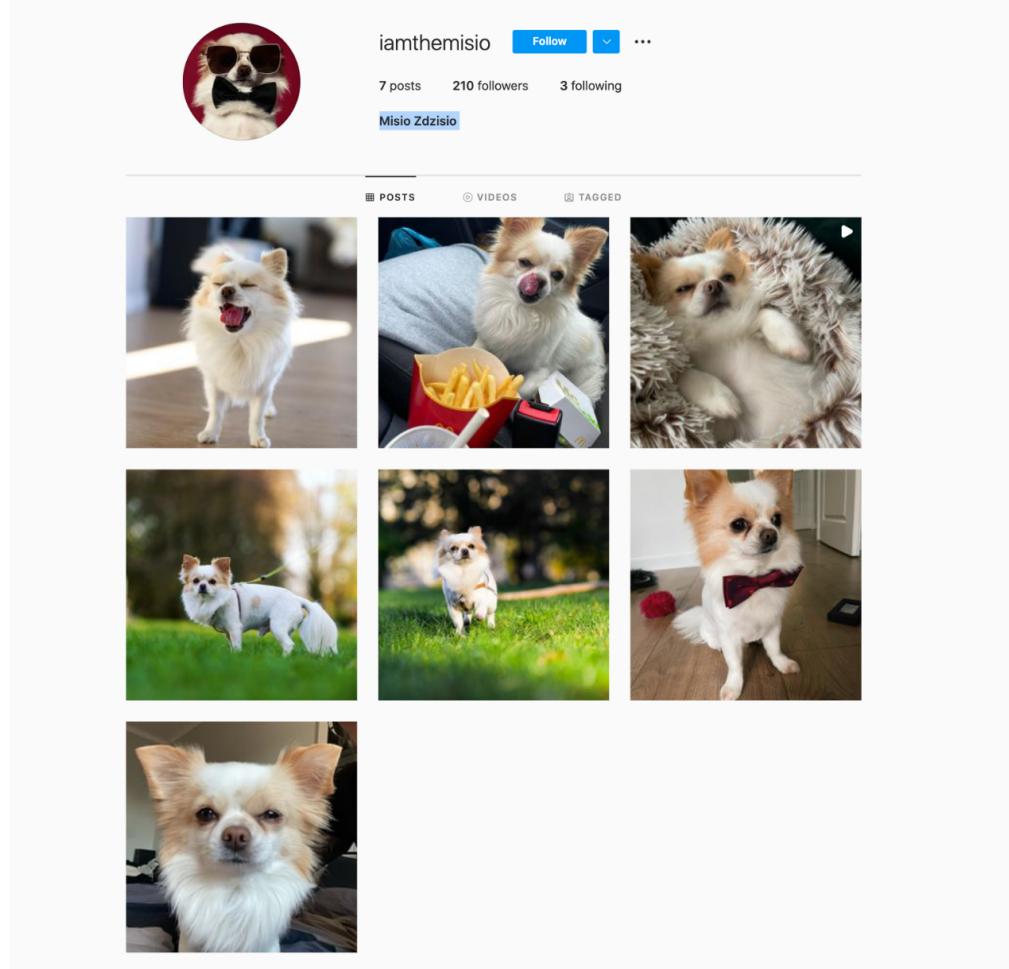
heart search share

Liked by brandonperez7532 and others

MAY 29, 2021

I saw that she tagged her dog in that picture, which has the Instagram username [iamthemisio](#)

I went to the dog's account and saw the following.



The dog's name is `Misio_Zdzisio`, and as the challenge was to find a dog and the flag format was `vishwaCTF{Firstname_Lastname}`, the flag for this challenge would be,

`vishwaCTF{Misio_Zdzisio}`

I cried tears of joy when I inputted this flag and finally got `correct`, because I failed multiple times with flags like `vishwaCTF{David_Bombal}`, `vishwaCTF{Atharva_Pande}` and `vishwaCTF{Pavel_Ladziak}`.

Challenge 1 Solves X

Platypus Perry

500

Agent John got some information that a group of people hid a bag of LSD on a dog. He needs to find the dog before it reaches the dealer.

Flag format: `vishwaCTF{Firstname_Lastname}`

Hint : David is Linked IN with some "Russian Hacks"

[Hire-me.mp3](#)

Flag

Submit

Correct

This challenge was an emotional rollercoaster. Every time I thought I got the flag, it turns out it wasn't the flag, but rather only a step in obtaining the flag. Thus, finally getting `correct` was extremely satisfying, especially because I was the first to solve the challenge.

I experienced an important life lesson while doing this challenge, which is to keep trying even if you fail because those failures will lead your way to success.