WARMUPS

TOO MANY BITS

What do all these ones and zero's mean!?! We are in the **Warmups** category after all...

```
01100110 01101100 01100001 01100111 01111011 01100100 00110000
00110001 00110100 00110111 00110001 00110111 00110000 00110010
01100001 00110001 00110000 00110001 00110011 00110100 01100011
01100100 01100001 01100100 00110001 01100100 01100100 01100100
01100101 00110000 00110110 00110110 00110111 00111000 01100110
00110010 01100110 01111101
```

Solution: Throw the binary into cyberchef

Flag: flag{d01471702a10134cdad1ddde06678f2f}

CATTLE

I know it's an esoteric challenge for a Capture the Flag, but could you herd these cows for me?

Text file: variations of ‘MOo’ ‘MoO’ ‘moO’ ‘MMM’

https://huntress.ctf.games/files/59342f87e9fdecd17a4204cbad0bfbf3/cattle?token=eyJ1c2VyX2lkIjo0NTgsInRlYW1faWQiOjE5NiwiZmlsZV9pZCI6MjB9.ZwARJA.fna3VbyP_m4xdlVn4Bkf4NoWwKE

Solution: Asked ChatGPT what it thought based on the contents of the text file and the challenge description. One of its suggestions was moo code. Searching the web, I found COW code https://www.cachesleuth.com/cow.html. Decrypting the text file gave the flag.

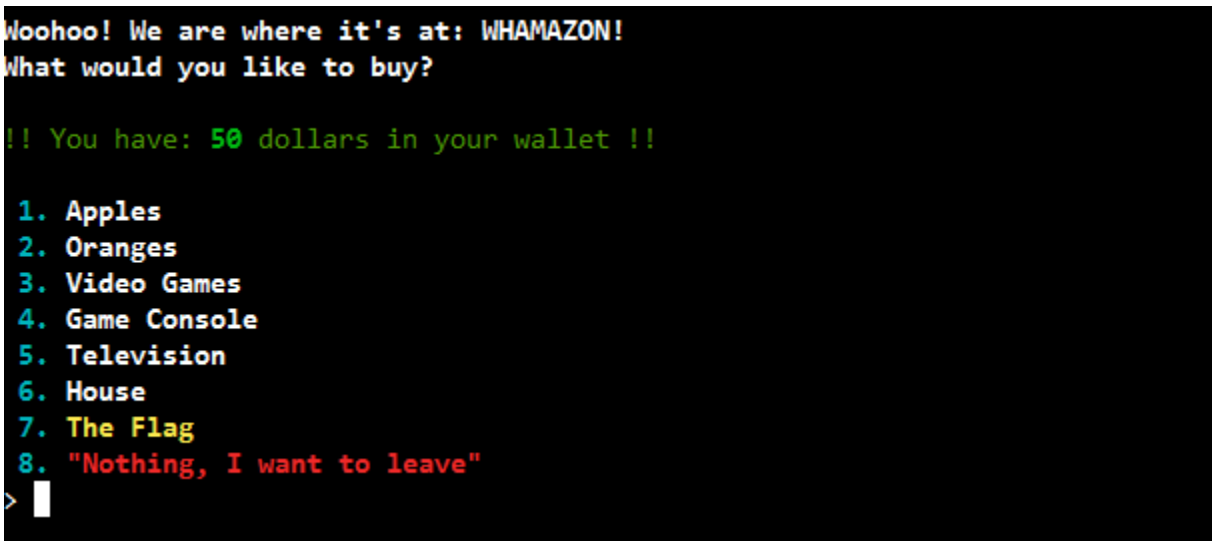
Flag: flag{6cd6392eb609c6ae4c332ef6a321d9dd}

WHAMAZON

Wham! Bam! Amazon is entering the hacking business! Can you buy a flag?

Solution: Connecting to the webserver displays the WHAMAZON shell with a few options.

Choosing to buy from whamazon moves us to the options to buy and we see that we have $50 in our wallet



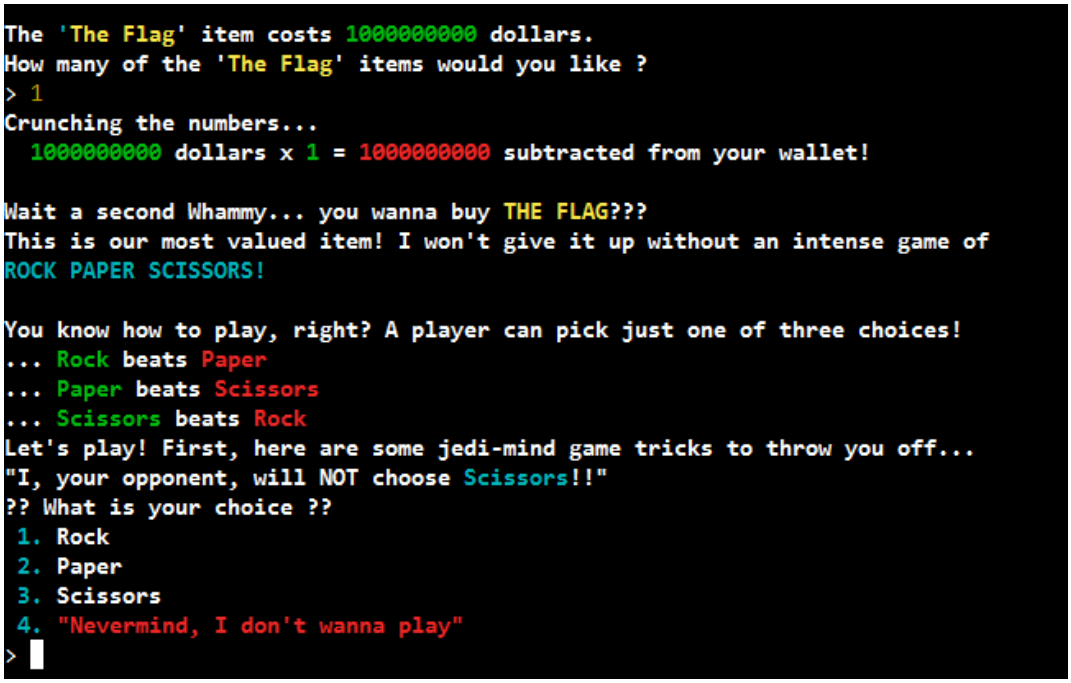
The flag costs too much

```
The 'The Flag' item costs 1000000000 dollars.
This costs you 1000000000 dollars but you only have 50 in your wallet!
We're sorry Whammy, but you can't afford this!!

!! You have: 50 dollars in your wallet !!


 1. Apples
 2. Oranges
 3. Video Games
 4. Game Console
 5. Television
 6. House
 7. The Flag
 8. "Nothing, I want to leave"
> 
```

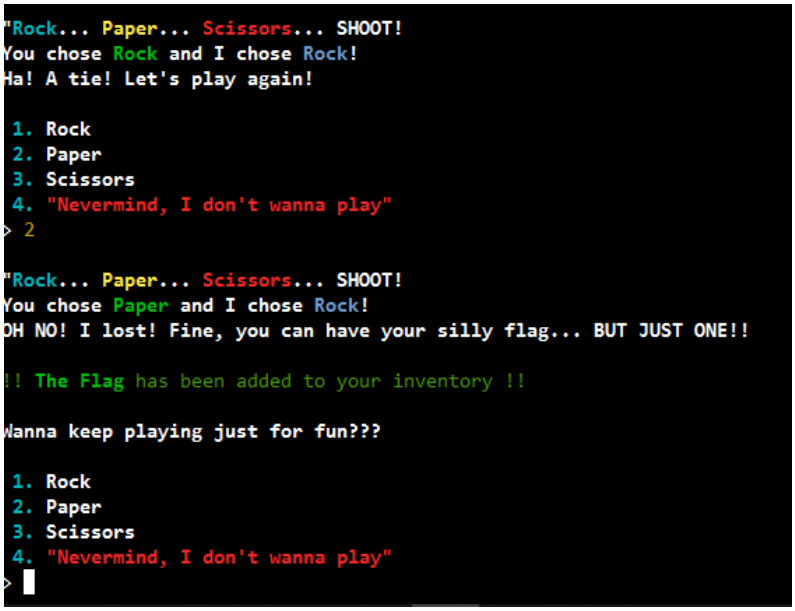
But apples are affordable, and I seem to be able to buy a negative number of them!

```
The 'Apples' item costs 3 dollars.
How many of the 'Apples' items would you like ?
> -10000000000000000000
Crunching the numbers...
  3 dollars x -10000000000000000000 = -30000000000000000000 subtracted from your wallet!

!! You have: 30000000000000000050 dollars in your wallet !!


 1. Apples
 2. Oranges
 3. Video Games
 4. Game Console
 5. Television
 6. House
 7. The Flag
 8. "Nothing, I want to leave"
> 
```

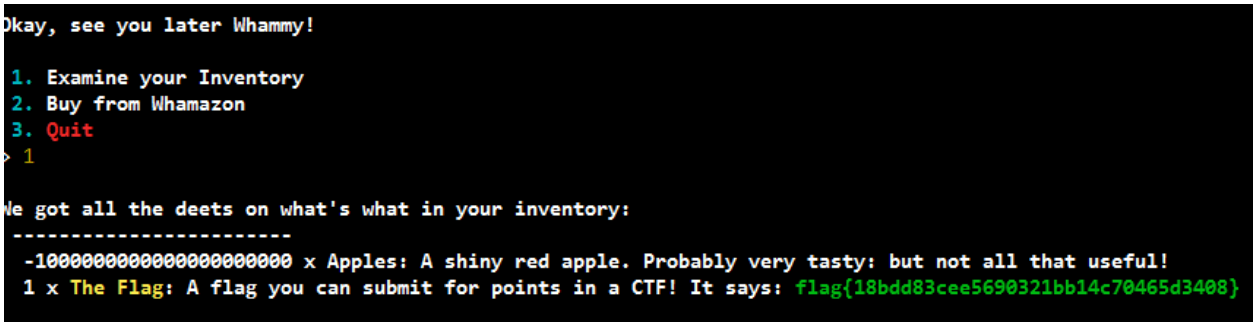
Now I can buy a flag:



I'll choose rock, assuming it's lying about not choosing scissors. It wasn't lying. Choosing paper next:



Leaving and checking the inventory shows the flag!



UNBELIEVABLE

Don't believe everything you see on the Internet!

Anyway, have you heard this intro soundtrack from Half-Life 3?

Solution: The file included is named Half-Life_3_OST.mp3, but it won't play. Running the command 'file Half-Life_3_OST.mp3' shows that it is in fact an .png file. Changing the extension and opening the file gives the flag.

Flag: flag{a85466991f0a8dc3d9837a5c32fa0c91}

TXT MESSAGE

Hmmm, have you seen some of the strange DNS records for the ctf.games domain? One of them sure is odd…

Solution: A dns lookup at dnschecker.org turns up a TXT record with the following values:

146 154 141 147 173 061 064 145 060 067 062 146 067 060 065 144 064 065 070 070 062 064 060 061 144 061 064 061 143 065 066 062 146 144 143 060 142 175

The clue for the challenge "od" references octal dump. Using the following command, I find all values for characters commonly used in flags:

```
echo "abcdefghijklmnopqrstuvwxyz{}_1234567890" | od -cb

0000000   a   b   c   d   e   f   g   h   i   j   k   l   m   n   o
p
        141 142 143 144 145 146 147 150 151 152 153 154 155 156 157
160
0000020   q   r   s   t   u   v   w   x   y   z   {   }   _   1   2
3
        161 162 163 164 165 166 167 170 171 172 173 175 137 061 062
063
0000040   4   5   6   7   8   9   0  \n
        064 065 066 067 070 071 060 012
0000050
```

Comparing these to the values found in the dns record reveals the flag:

Flag: flag{14e072f705d45882401d141c562fdc0b}

SCRIPTING

BASE64BY32

Download the text file containing Base64 encoded text. It's just the flag base64 encoded 32 times. Use cyberchef to decode.

Flag: flag{8b3980f3d33f2ad2f531f5365d0e3970}

CRYPTO

NO NEED FOR BRUTUS

A simple message for you to decipher:

squiqhyiiycfbudeduutvehrhkjki

Submit the original plaintext hashed with MD5, wrapped between the usual flag format: flag{}

Solution: The message appears to be a caesar cipher. Using the online caesar cipher decoder https://www.dcode.fr/caesar-cipher, and rotating the message 10 places right, the message caesarissimplenoneedforbrutus can be found. Hashing that with MD5, we get c945bb2173e7da5a292527bbbc825d3f.

Flag: flag{c945bb2173e7da5a292527bbbc825d3f}

MISC

RED PHISH BLUE PHISH

You are to conduct a phishing excercise against our client, Pyrch Data.

We've identified the Marketing Director, Sarah Williams (swilliams@pyrchdata.com), as a user susceptible to phishing.

Are you able to successfully phish her? Remember your OSINT ;)

NOTE: The port that becomes accessible upon challenge deployment is an SMTP server. Please use this for sending any phishing emails.

You will not receive an email/human response as the mail infrastructure for this challenge is emulated.

Solution: Doing a quick google search for pyrch data shows the following result:

https://pyrchdata.com

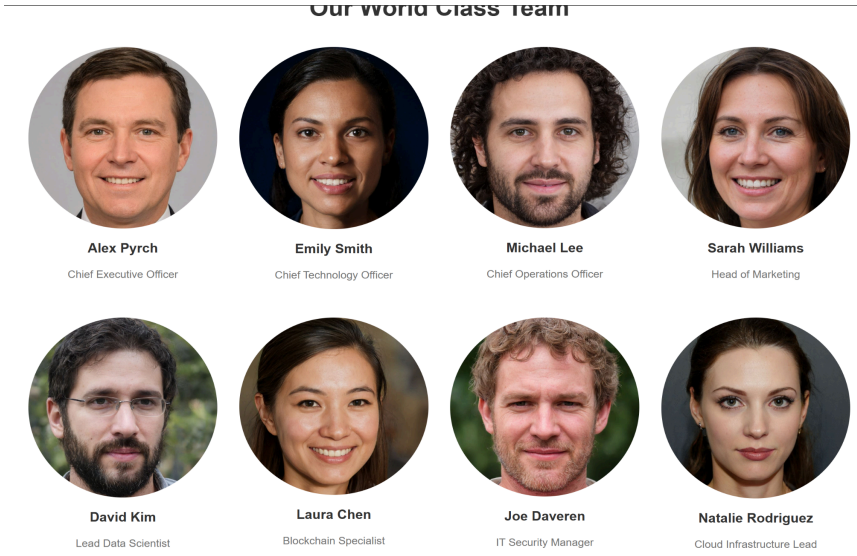
Pyrch Data Solutions

Pyrch Data Solutions. Home; About; Meet the Team; Innovative Solutions for a **Data**-Driven World. Leveraging AI, Blockchain, and Cloud technologies to drive seamless automation and intelligence. Learn More. What We Offer. AI & Machine Learning. Transforming businesses with cutting-edge AI...

Meet the Team

This site was created for the Huntress Cybersecurity Awareness Month...

Checking this site, we find a team page:



For some reason, nc doesn't work for this challenge, but telnet does. Crafting an email impersonating Joe from IT gives the flag.

```
└─$ telnet challenge.ctf.games 30114
Trying 35.193.148.143 ...
Connected to challenge.ctf.games.
Escape character is '^]'.
220 red-phish-blue-phish-6543a74491650bee-74d6b88bfb-t6dd6 Python SMTP 1.4.6
HELO local.domain.name
250 red-phish-blue-phish-6543a74491650bee-74d6b88bfb-t6dd6
MAIL FROM: jdaveren@pyrchdata.com
250 OK
RCPT TO: swilliams@pyrchdata.com
250 OK

500 Error: bad syntax
DATA
354 End data with <CR><LF>.<CR><LF>

SUBJECT: flag

Hello Sarah,

This is Joe from IT. Do you have that flag I gave you?

Thanks.

.
250 OK. flag{54c6ec05ca19565754351b7fcf9c03b2}
```

OSINT

RAN SOMEWHERE

Thanks for joining the help desk! Here's your first ticket of the day; can you help the client out?

NOTE, this challenge uses a non-standard flag format. Enter the human-readable name of the location.

File: ran_somewhere.eml

Email: Opening the .eml presents an email with three attachments and the following message:

Help Me IT!! My USB was stolen! I was headed into town for some work

and stopped by a client's coffee shop to get work done. Everything was fine; I was working and drinking coffee. I got up to use the restroom; when I returned, I saw that my computer had been tampered with! All my work was closed out, and my flash drive with my projects was gone! I can't lose this; there was very important work on it! I thought the security tools you put in place would stop something like this!!

When I was looking at the desktop, I noticed three new files that were not there before. I opened one to see if they were my files, but they are a jumbled mess. I can't make any sense of it. I think it is that "ran somewhere" that your team keeps warning us about. I still don't know what it is, but please reverse this and get my USB back. I can't believe this happened!

I am attaching those files so you can fix them.

-Mack Eroni

President

Attached Text File: Hex Encoded. Decoding the message we get:

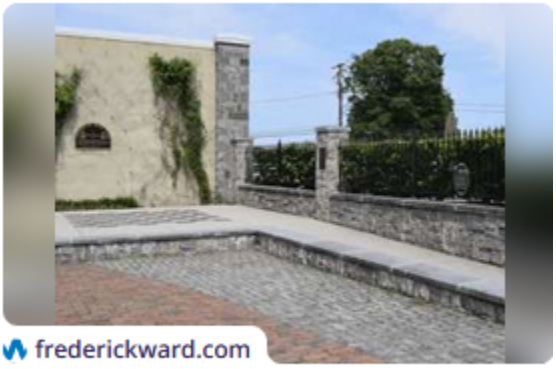
Hey There! You should be more careful next time and not leave your computer unlocked and unattended! You never know what might happen. Well in this case, you lost your flash drive. Don't worry, I will keep it safe and sound. Actually you could say it is now 'fortified'. You can come retrieve it, but you got to find it. I left a couple of files that should help.

- Vigil Ante

Two attached .dat files

Opening in the notepad, we can see JFIF at the top of the file, meaning these are in fact .jpeg files. Changing the extensions to .jpeg we get two images.

Solution: Using reverseimagesearch.com gives several options for reverse image searches. Google didn't turn up much, but using Lenso.ai, I was able to find the second image.



Flag: Reckord Armory