Round 1 report

tcs HackQuest
Season 9

Contest Date: - 25th January 2025

CT/DT ID	
Name	
College/University	
City	
Challenges solved & the total score	
Anything else that you want us to know	

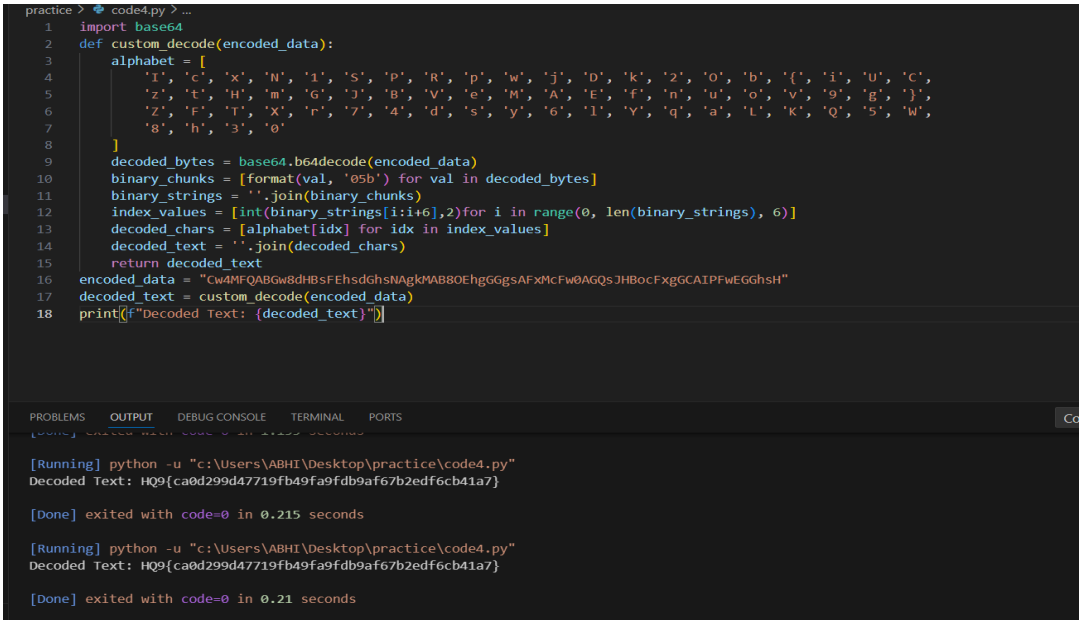
(Copy & paste the table x times if you solved x challenges and fill in the steps)

Challenge Title: Stranger Things
Points-500

Flag: HQ9{ca0d299d47719fb49fa9fdb9af67b2edf6cb41a7}
HQ9FLAG{e626f35e23bccd0498d04adb8b7d65280e325a2c}

Approach (Step by Step):

1. Decode base64: Decode the encoded string into bytes using base64.
2. Convert bytes to binary: Each byte is converted into a 5-bit binary string.
3. Concatenate binary strings: Join all the 5-bit binary strings into one long binary string.
4. Split into 6-bit chunks: Group the long binary string into 6-bit segments.
5. Convert to decimal indices: Convert each 6-bit chunk into its decimal equivalent.
6. Map indices to custom alphabet: Use the decimal indices to look up characters from the custom alphabet.
7. Join characters: Combine the characters to form the decoded message.
8. Done question by using Python Code.



```
practice > code4.py > ...
1   import base64
2   def custom_decode(encoded_data):
3       alphabet = [
4           'I', 'c', 'x', 'N', '1', 'S', 'P', 'R', 'p', 'w', 'j', 'D', 'k', '2', 'O', 'b', '{', 'i', 'U', 'C',
5           'z', 't', 'H', 'm', 'G', 'J', 'B', 'V', 'e', 'M', 'A', 'E', 'f', 'n', 'u', 'o', 'v', '9', 'g', '}',
6           'Z', 'F', 'T', 'X', 'r', '7', '4', 'd', 's', 'y', '6', 'l', 'Y', 'q', 'a', 'L', 'K', 'Q', '5', 'W',
7           '8', 'h', '3', '0'
8       ]
9       decoded_bytes = base64.b64decode(encoded_data)
10      binary_chunks = [format(val, '05b') for val in decoded_bytes]
11      binary_strings = ''.join(binary_chunks)
12      index_values = [int(binary_strings[i:i+6],2)for i in range(0, len(binary_strings), 6)]
13      decoded_chars = [alphabet[idx] for idx in index_values]
14      decoded_text = ''.join(decoded_chars)
15      return decoded_text
16  encoded_data = "Cw4MFQABGw8dHBsFEhsdGhsNAgkMAB8OEhgGGgsAFxMcFw0AGQsJHBocFxgGCAIPFwEGGhsH"
17  decoded_text = custom_decode(encoded_data)
18  print(f"Decoded Text: {decoded_text}")

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

[Running] python -u "c:\Users\ABHI\Desktop\practice\code4.py"
Decoded Text: HQ9{ca0d299d47719fb49fa9fdb9af67b2edf6cb41a7}

[Done] exited with code=0 in 0.215 seconds

[Running] python -u "c:\Users\ABHI\Desktop\practice\code4.py"
Decoded Text: HQ9{ca0d299d47719fb49fa9fdb9af67b2edf6cb41a7}

[Done] exited with code=0 in 0.21 seconds
```

Challenge Title: Garbalator
Points-200

Flag: HQ9{craiostlrarsnlhrlege}
HQ9FLAG{41ffc8051aa2611614aa97d4d6fa4fc89f44f07e}

Approach (Step by Step):

1. Read the file: Load the file content into memory.
2. Remove lowercase words: Use regular expressions to remove any words consisting entirely of lowercase letters.
3. Clean up spaces: Normalize spacing by removing extra spaces and ensuring a clean, consistent format.
4. Split the content: Break the remaining content into individual words.
5. Character mapping: Create a dictionary that maps specific characters to new characters.
6. Decode words: Replace each character in the remaining words with its mapped counterpart from the dictionary.
7. Extract 4th characters: For each decoded word, extract the 4th character, if the word is long enough.
8. Form the flag: Combine the 4th characters into a string enclosed in HQ9{} to create the final flag.
9. Output: Display the filtered content, decoded words, and the final flag.
10. Done Using Python Code.

practice > code4.py > ...

```python
import re
file_path = "C:/Users/ABHI/Desktop/TCS_Hackquest/garbalator/Garbalator_7DCF2839479BDF3E/file.txt"
with open(file_path, 'r') as f:
    file_content = f.read()
filtered_content = re.sub(r'\b[a-z]+\b', '', file_content)
filtered_content = re.sub(r'\s+', ' ', filtered_content).strip()
remaining_words = filtered_content.split()
mapping = {
    "L": "a", "v": "b", "0": "c", "V": "d", "R": "e", "9": "f", "I": "g", "z": "h",
    "8": "i", "4": "j", "q": "k", "c": "l", "Z": "m", "b": "n", "1": "o", "y": "p",
    "X": "q", "P": "r", "U": "s", "7": "t", "K": "u", "w": "v", "t": "w", "d": "x",
    "k": "y", "S": "z", "A": "A", "C": "B", "x": "C", "i": "D", "D": "E", "6": "F",
    "a": "G", "F": "H", "J": "I", "e": "J", "O": "K", "5": "L", "H": "M", "f": "N",
    "p": "O", "n": "P", "o": "Q", "B": "R", "3": "S", "W": "T", "l": "U", "T": "V",
    "Y": "W", "j": "X", "s": "Y", "2": "Z", "N": "0", "g": "1", "m": "2", "G": "3",
    "Q": "4", "r": "5", "u": "6", "h": "7", "M": "8", "E": "9"
}
decoded_words = [
    "".join(mapping.get(char, char) for char in word) for word in remaining_words
]
fourth_chars = [word[3] for word in decoded_words if len(word) > 3]
flag = f"HQ9{{{''.join(fourth_chars)}}}"
print("Filtered Content (No Lowercase-Only Words):")
print(filtered_content)
print("\nRemaining Words:", remaining_words)
print("\nDecoded Words:", decoded_words)
print("\nExtracted 4th Characters:", fourth_chars)
print("\nFinal Flag:", flag)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
Final Flag: HQ9{craiostlrarsnlhrlege}

[Done] exited with code=0 in 0.411 seconds
```

Challenge Title: Code Pool
Points-100

Flag: HQ9{everyloquaciousdeadpoolhasapeter}
HQ9FLAG{ed3d1q9fbt35f4790d7e237e6a675340b0t9d46c}

Approach (Step by Step):

1. Identify using dcode identifier.
2. Then using Affine Cipher decode the code.

Challenge Title: Captain Atom
Points-100

Flag: HQ9{5f1216cf2bd259b59abe5ddcbd4509e8}
HQ9FLAG{bfe7cfce861267c7af5f41c1892bf4b40f93fe24}

Approach (Step by Step):

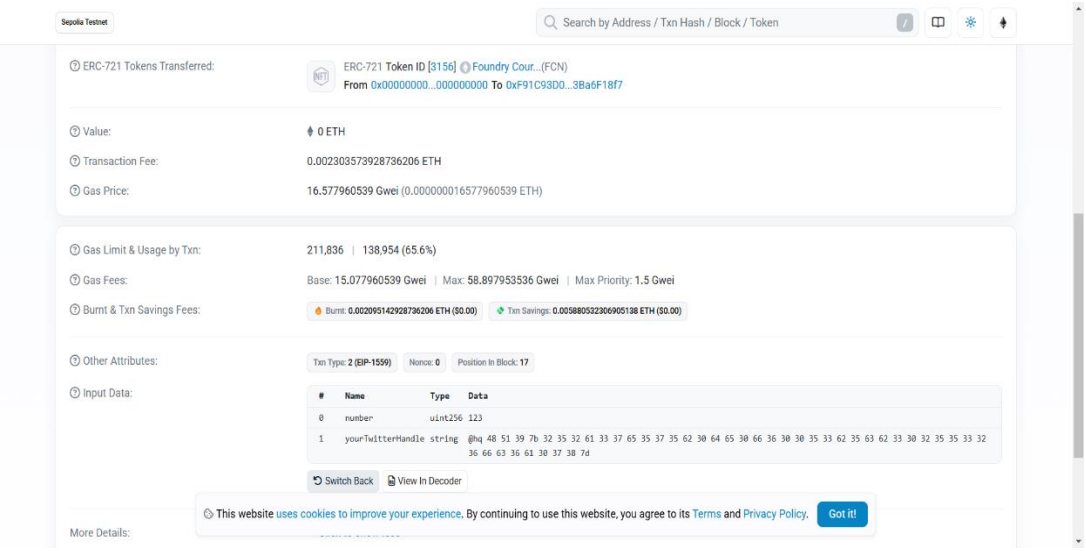
1. Just Decode the given code using all base 64 variant decoder using dcode.

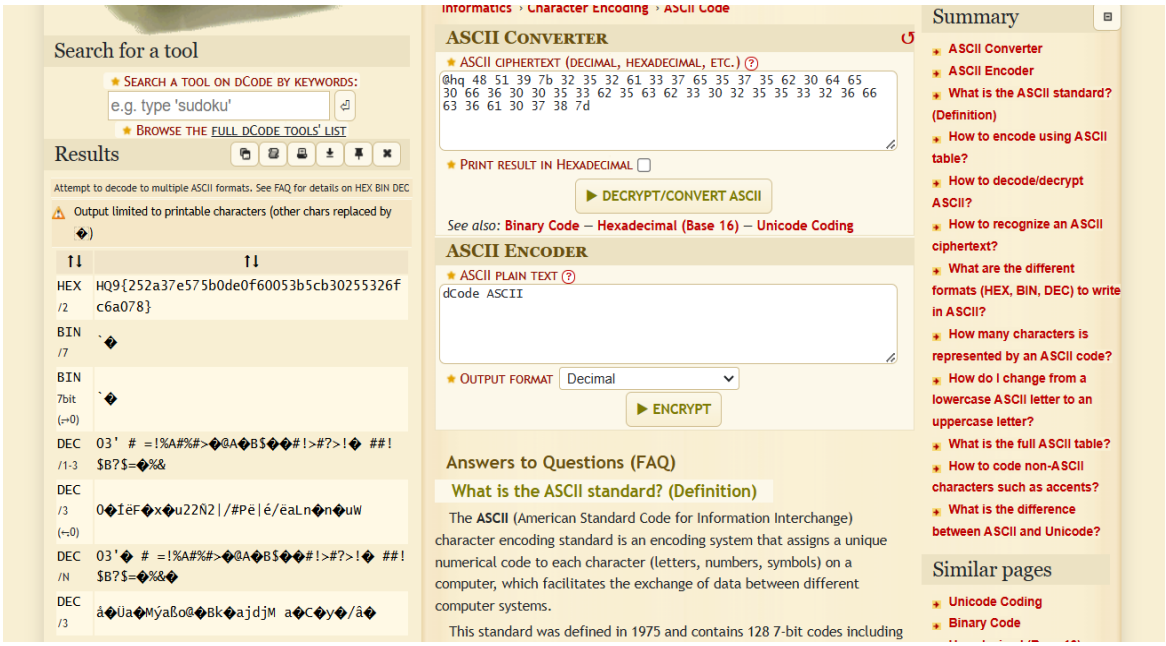
Challenge Title: Crypto Conundrum
Points-200

Flag: HQ9{252a37e575b0de0f60053b5cb30255326fc6a078}
HQ9FLAG{f03268de58d3eef92e5813b29985c6e1117e0da4}

Approach (Step by Step):

1. According to the question go to sepolio.etherscan.io then paste the hash.
2. Decode the input data.
3. Copy and paste it on ASCII Convertor dcode.



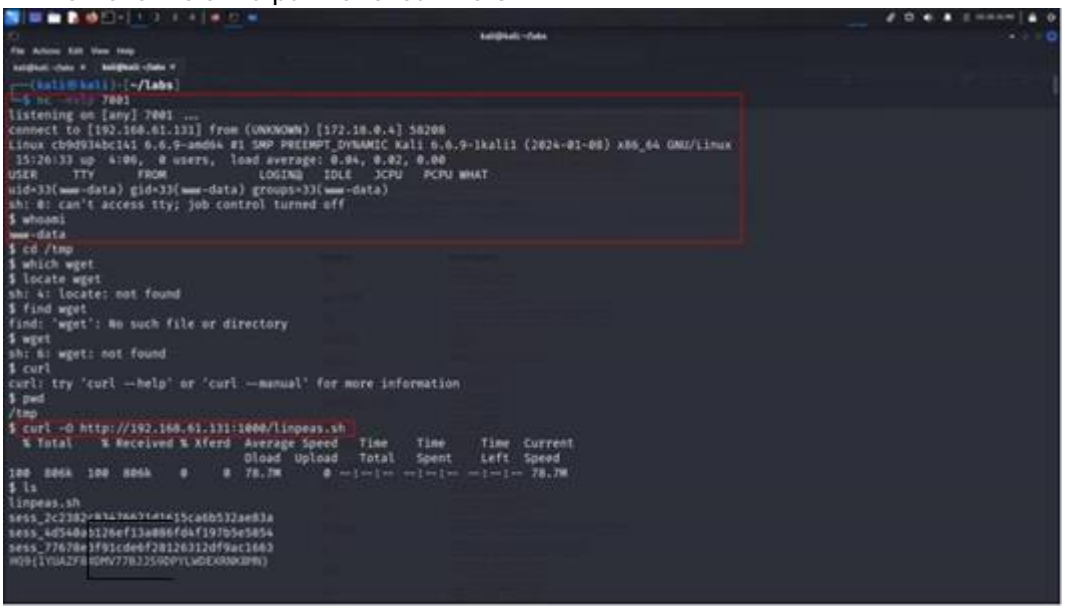


Challenge Title: The Mask
Points-200

Flag: HQ9{1YUAZF84DMV77BJJS9DPYLWDEXRNK8MN}
HQ9FLAG{0c8270dedc7e8165d46c6decf9b01ff4c2957b68}

Approach (Step by Step):

1. Unlock By using PDF Unlocker Online tool.
2. Go to the HQ9 contain page.
3. Using Microsoft word to edit the PDF.
4. Remove the extra part to reveal the CTF.

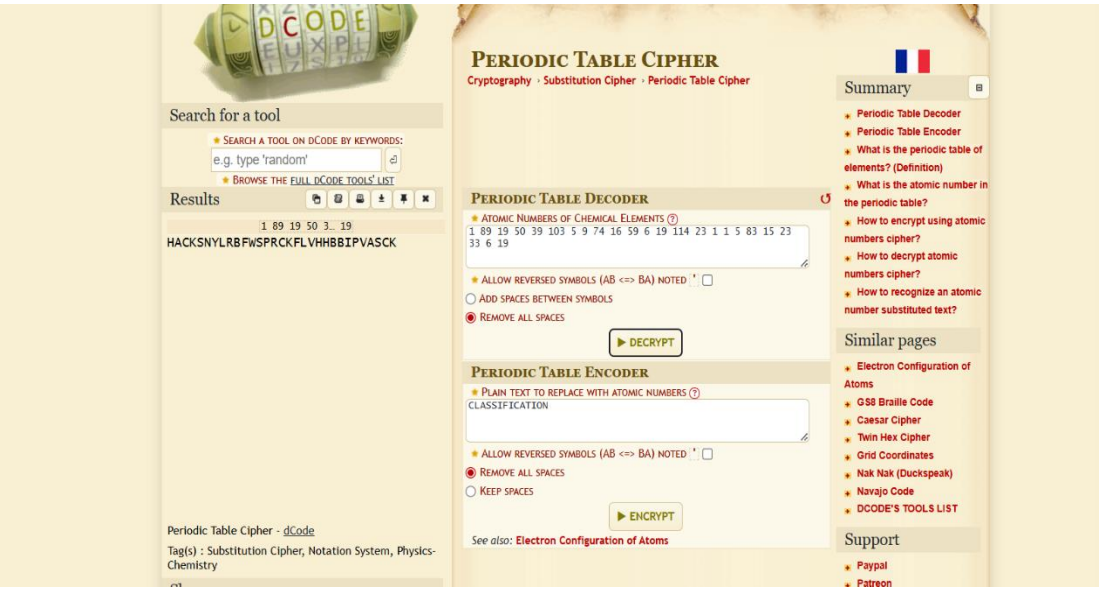


Challenge Title: Breaking Bad
Points-100

Flag: HQ9{HACKSNYLRBFWSPRCKFLVHHBBIPVASCK}
HQ9FLAG{ec7c86662416231da2e2e0768fe60e10fa768729}

Approach (Step by Step):

1. Using Periodic Table Cipher to decode the given code according to question.

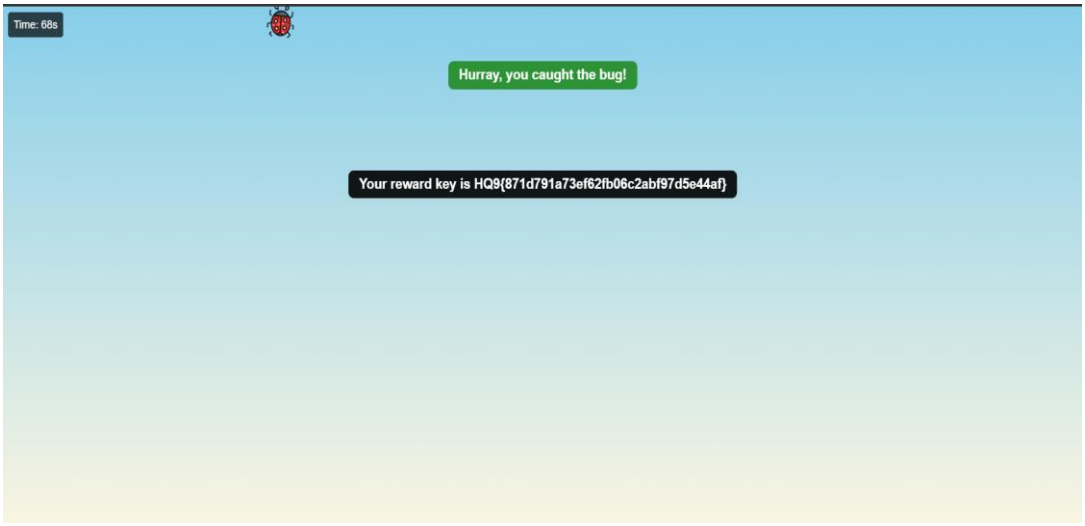


Challenge Title: The Bug's Life
Points-100

Flag: HQ9{871d791a73ef62fb06c2abf97d5e44af}
HQ9FLAG{878ce322c56450aa062c88ed6b593d7e4ca26038}

Approach (Step by Step):

1. Minimize the Window.
2. Catch the Bug with speed.
3. Then automatically it will reveal the flag.



Challenge Title: Dussahas Dice
Points-200

Flag: HQ9{bebd9d1f9fb52044040b4aa4c09d6b82}
HQ9FLAG{dba13cef45048193073a904c831f1e140a07a207}

Approach (Step by Step):

1. JavaScript Deoxyfecate to find function checkRolls.
2. Run Console with checkRolls(6,6);.