

# Round 1 report

# **tcs HackQuest**

## Season 10

**Contest Date: - 13th December 2025**

CT ID	REDACTED
Name	Pranay Pawar
College/University	REDACTED
City	REDACTED
Challenges solved & the total score	4 (700)
Anything else that you want us to know	

## Challenge Title: Area 64

Flag: HQX{70c5d525ca34df3cabaff1a49bf4ccf8}

### Approach (Step by Step):

#### 1. Decode the Base64

The screenshot shows the CyberChef interface with the following details:

- Operations:** base
- From Base:** Base64
- Input:** A long Base64 encoded string: Mw01J3J1I6luc2lkZS8BcmVhIDY0L1BIZXJlJ3MgeW9ic1BrZXk@0iBIVh7N2bjNwQ1MjVjYTm02GYZy2F1YwZmMe80WJmGNJZjh9
- Alphabet:** A-Za-z0-9+=
- Options:** Remove non-alphabet chars (checked)
- Output:** The decoded output: You're inside Area 64. Here's your key : HQX{70c5d525ca34df3cabaff1a49bf4ccf8}

## Challenge Title: Small-E

Flag: HQX{36b8682966c5dabfbac72d3f687a77ff}

### Approach (Step by Step):

- Made the script for RSA low exponent attack: with small public exponent ( $e=3$ ) and no padding, ciphertext equals plaintext<sup>3</sup>, so attacker recovers the message by taking the integer cube root
- [Code: <https://termbin.com/af21> ]

```

solve.py — Kate
File Edit Selection View Go Projects LSP Client Sessions Tools Settings Help
File New Open Save Save As Undo Redo
< home bugaddr Downloads Firefox 2 solve.py
File Home Downloads Firefox 2 solve.py
From Crypto.Util.number import long_to_bytes
def Integer_ntb_root(n):
    """Calculates the integer part of the nth root of n using binary search."""
    if n < 0:
        result = -1
    else:
        low = 0
        high = n
        while low <= high:
            mid = (low + high) // 2
            power = mid ** e
            if power == n:
                result = mid
                break
            elif power < n:
                low = mid + 1
            else:
                high = mid - 1
        else:
            raise ValueError("Root not found")
    return result
# Given values
e = 3
n = 465212109071469908709921594873996116436591247123513352211939893952881627800038194216529980720613892862288671236335822327612575623109632815732951867841619611075251237456945377771
# Calculate the cube root
m = Integer_ntb_root(e, n)
# Verify it's a perfect cube
if pow(m, e) != n:
    print(f"Error: {n} is not a perfect cube root!")
# Convert to bytes and decode
raw_bytes = long_to_bytes(m)
flag = raw_bytes.decode('utf-8', errors='ignore').split('\\00')[0]
print(f"Message ({n}): {flag}")
print(f"Flag: {flag}")

```

- Run the script and got flag

```

2 — Dolphin
/ > home > bugaddr > Downloads > Firefox 2
Places
  Home
  Desktop
  Documents
  Downloads
  Music
  Pictures
  Videos
  Trash
  Network
Recent
  Recent Files
  Recent Locations
Devices
  500.0 GiB Internal Drive (dm-0)
  Basic data partition
  500.0 GiB Encrypted Drive
  1 folder, 3 files (3.3 KiB)

bugaddr@arc ~/Pictures/Screenshots $ cd /home/bugaddr/Downloads
bugaddr@arc ~/Downloads $ cd /home/bugaddr/Downloads/Firefox 2
bugaddr@arc ~/Downloads/Firefox 2 $ cd /home/bugaddr/Downloads/Firefox/1
bugaddr@arc ~/Downloads/Firefox/1 $ cd /home/bugaddr/Downloads/Firefox/1/2
bugaddr@arc ~/Downloads/Firefox/1/2 $ cd /home/bugaddr/Downloads/Firefox
bugaddr@arc ~/Downloads/Firefox $ cd /home/bugaddr/Downloads/Firefox/1
bugaddr@arc ~/Downloads/Firefox/1 $ cd /home/bugaddr/Downloads/Firefox
bugaddr@arc ~/Downloads $ cd /home/bugaddr/Downloads/Firefox
bugaddr@arc ~/Downloads/Firefox $ cd /home/bugaddr/Downloads/Firefox/2
bugaddr@arc ~/Downloads/Firefox/2 $ ls
cryptot1_1fce059d.py DT20257381363_Small-E-1fce059da.zip solve.py venv
bugaddr@arc ~/Downloads/Firefox/2 $ python solve.py venv
bugaddr@arc ~/Downloads/Firefox/2 $ python solve.py
Message (n): 35965300646197725772811086666699081780146331795547973191319384558085423884234016581245
Flag: HQX{36b8682966c5dabfbac72d3f687a77ff}
bugaddr@arc ~/Downloads/Firefox/2 $ 

```

## **Challenge Title: Hidden Layers**

**Flag:** HQX{24c0ce09e08bcb246d09c1439d1d48f0}

## **Approach (Step by Step):**

1. **LSB steganography**: hidden data extracted from the least significant bits of image pixels using zsteg, revealing an embedded text/flag without altering visible image quality.

## **Challenge Title: Seeds of Time**

**Flag:** HQX{c126bb454bf27489a1583af0729fbd08}

## **Approach (Step by Step):**

1. Built this script for **time-based PRNG seed brute-force attack** and tried to attack last 30days PRNG [Code: <https://term-bin.com/zqza> ]

## 2. The flag

Places

- Home
- Desktop
- Documents
- Music
- Pictures
- Videos
- trash

Recent

- Recent Files
- Recent Locations

Devices

- 500.0 GiB Internal Drive (dm-0)
- Basic data partition
- 500.0 GiB Encrypted Drive

/ > home > bugaddr > Downloads > Firefox > \$

DT20257381363, Seeds Of Time-SdC73D749.zip output.SdC73D749.txt solve.py .output.SdC73D749.txt.kate-swp

```
bugaddr@arc ~$ cd /home/bugaddr/Pictures/Screenshots
bugaddr@arc ~$ cd /home/bugaddr/Downloads/Firefox/3
[*] Starting attack on a 259200 second window around 2025-12-13 16:19:57...
[!] FILE FOUND !(!)
[*] Recovered Seed: 1765680208 (2025-12-13 16:08:00)
[*] Decrypted Flag: H0X(C12bb545af27489a1583af2729fb008)
bugaddr@arc ~$ cd /Downloads/Firefox/3
bugaddr@arc ~$ cd /home/bugaddr/Pictures/Screenshots
bugaddr@arc ~$ cd /home/bugaddr/Downloads/Firefox/3
bugaddr@arc ~$ cd /home/bugaddr/Pictures/Screenshots
bugaddr@arc ~$ cd /home/bugaddr/Downloads/Firefox/3
bugaddr@arc ~$ cd /home/bugaddr/Downloads/Firefox/3
[*] Starting attack on a 259200 second window around 2025-12-13 16:19:57...
[!] FILE FOUND !(!)
[*] Recovered Seed: 1765680208 (2025-12-13 16:08:00)
[*] Decrypted Flag: H0X(C12bb545af27489a1583af2729fb008)
bugaddr@arc ~$ cd /Downloads/Firefox/3
bugaddr@arc ~$ cd /home/bugaddr/Pictures/Screenshots
bugaddr@arc ~$ cd /home/bugaddr/Downloads/Firefox/3
bugaddr@arc ~$ cd /home/bugaddr/Pictures/Screenshots
bugaddr@arc ~$ cd /home/bugaddr/Downloads/Firefox/3
bugaddr@arc ~$ cd /home/bugaddr/Downloads/Firefox/3
```