

Решение Reverse-11 Тайна эндермена

Описание

В крепости Края ты нашел книгу, которую писал эндермен. Но эндермен постоянно телепортировался во время написания, поэтому книга полна хаотичных записей и повторений! Среди всего этого беспорядка спрятано истинное заклинание, которое закодировано особыми эндер-рунами. Найди его среди хаоса и расшифруй послание из Края!

Решение

Обфусцированный код на C. Программа собирает флаг из закодированных частей и выводит в base64.

Анализ

"Мусорные" функции

Отвлекающие функции: `teleport_*`, `chaos_generator_*`, `enderman_scream()` и др.

Значимые функции

Находим 4 функции с частями флага:

1. `get_portal_coords()` → `"vsosh{"` (plaintext)
2. `calculate_dimension_offset()` → XOR с ключом `0x42`
 - `{0x71, 0x2c, 0x26}` → `"3nd"`
 - `"\x71\x30\x1d"` → `"3r_"`
3. `decode_pearl_data()` → ROT13
 - `"pu40f"` → `"ch40s"`
4. `generate_stronghold_key()` → ASCII shift (-3)
 - `{0x62, 0x70, 0x37, 0x76, 0x77, 0x36, 0x75, 0x80}` → `"_m4st3r}"`

Сборка

Флаг: `vsosh{ + 3nd3r_ + ch40s + _m4st3r} = vsosh{3nd3r_ch40s_m4st3r}`

Решение

Анализируем исходный код и декодируем части флага:

```
import base64

def decode_xor(data, key):
    return bytes([b ^ key for b in data]).decode()

def decode_rot13(text):
    result = []
    for c in text:
        if 'a' <= c <= 'z':
            result.append(chr((ord(c) - ord('a') + 13) % 26 + ord('a')))
        elif 'A' <= c <= 'Z':
            result.append(chr((ord(c) - ord('A') + 13) % 26 + ord('A')))
        else:
            result.append(c)
    return ''.join(result)

def decode_ascii_shift(data, shift):
    return bytes([b - shift for b in data]).decode()

# Декодируем части флага
part1 = "vsosh{"
part2 = decode_xor(bytes([0x71, 0x2c, 0x26]), 0x42) +
decode_xor(b"\x71\x30\x1d", 0x42)
part3 = decode_rot13("pu40f")
part4 = decode_ascii_shift(bytes([0x62, 0x70, 0x37, 0x76, 0x77, 0x36, 0x75,
0x80]), 3)

flag = part1 + part2 + part3 + part4
print(f"Флаг: {flag}")
```

Флаг

`vsosh{3nd3r_ch40s_m4st3r}`