## 2021ISCC 部分web writeup

## 原创

版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接:<u>https://blog.csdn.net/Destiny\_one/article/details/116538667</u>

版权



ctf 专栏收录该内容

7 篇文章 0 订阅 订阅专栏 1.ISCC客服冲冲冲(一)

在这道题目中让左边的票数超过右边的票数,我第一反应是写一个脚本刷票,而且看起来没有限制ip多次投票,所以写了一个比 较简单的python自动点击投票

from selenium import webdriver

```
driver = webdriver.Chrome("C:\Program Files (x86)\Google\Chrome\Application\chromedriver.exe")
driver.get("http://39.96.91.106:7020/test.html")
```

for i in range(3000):
 driver.find\_element\_by\_id('left\_button').click()

当20秒过后左边票数比右边多的话就出来flag了

2.这是啥

打开页面显示的是这是啥,f12打开发现有一个js的代码块

这只是一小部分,剩下的没复制。想起来以前看的一个小例子,用js骂人,直接复制打开console控制台粘贴运行,弹出flag

3.web01

点开场景是让我们看robots.txt文件,查看发现Disallow: /src/code/code.txt,我们查看这个文件,

```
<?php
code.txt
if (isset ($_GET['password'])) {
if (preg_match ("/^[a-zA-Z0-9]+$/", $_GET['password']) === FALSE)
 {
 echo 'You password must be alphanumeric';
   }
  else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
 {
 if (strpos ($_GET['password'], '*-*') !== FALSE)
 {
  die('Flag: ' . $flag);
 }
 else
 {
  echo('*-* have not been found');
 }
 }
 else
 {
 echo 'Invalid password';
 }
?>
```

让我们进行正则匹配绕过,主要看 strlen(\$\_GET['password']) < 8 && \$\_GET['password'] > 99999999 这个条件,然后使用科 学计数法2e9就绕过了,再往后面加个\*-\*就出来了 构造playload: ?password=2e9\*-\*

4.登录

打开场景是一个登录界面,我是尝试弱口令登录,admin123,123456,结果登录成功,我看其他的大佬说反序列化的字符串逃逸,不太懂...下来多学习,登录成功以后就会有一张图片,进行检查,图片是用base64表

示,  3Jvb3QnOwokY29uZmlnWydwYXNzd29yZCddID0gJ3F3ZXJ0eXVpb3AnOwokY29uZmlnWydkYXRhYmFzZSddID0gJ2NoYWxsZW5nZXMnOwokZmxhZ yA9ICdJU0NDe3doYXRfaXNAdGhlJ19uaWNrbmFtZSo/MTExMjIzNH0nOwo/Pgo=

```
用base64解码 <?php $config['hostname'] = '127.0.0.1'; $config['username'] = 'root'; $config['password'] = 'qwertyuiop'; $config['database'] = 'challenges'; $flag = 'ISCC{what_is@the&_nickname*?1112234}'; ?>
```