WEB安全-SQL注入之宽字节注入

西安电子科技大学网络与信息安全学院
网络行为研究中心

崔艳鹏
ypcui@mail.xidian.edu.cn

写在前面

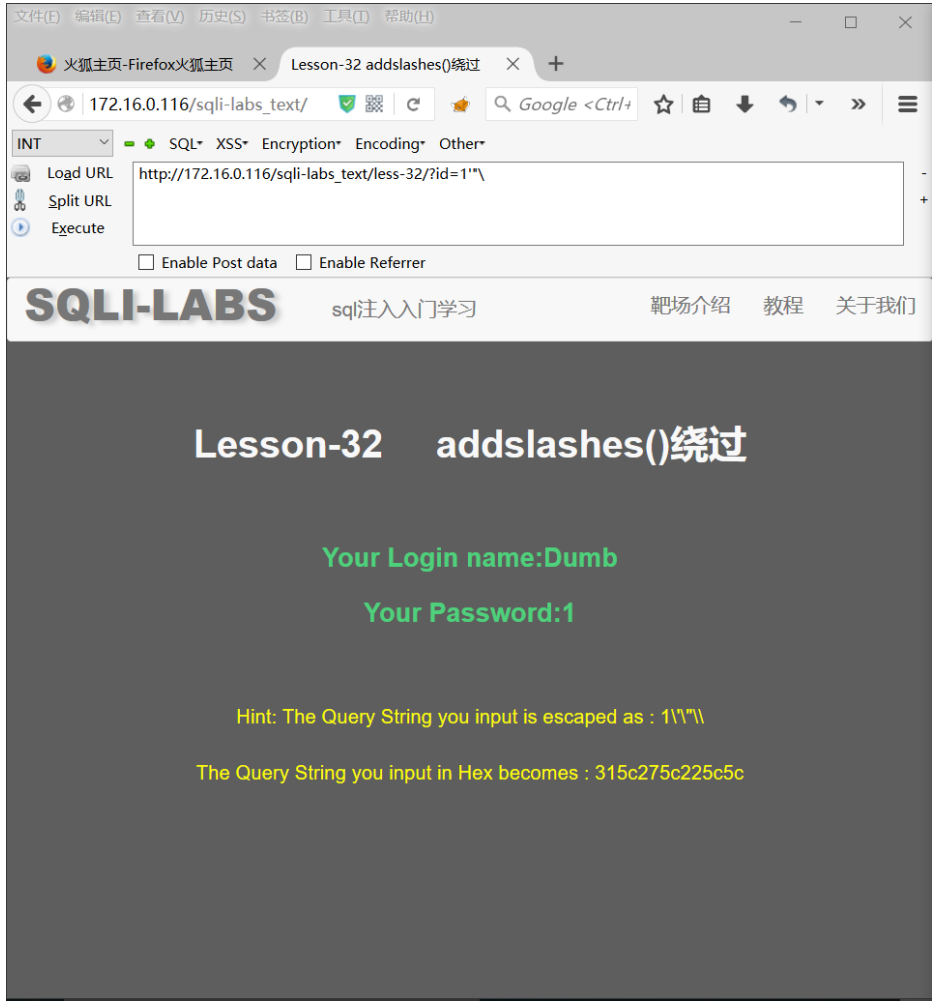
1. WEB安全问题以SQL注入、XSS攻击为最，因此，本课程主要授课内容实施以网络行为研究中心靶场Sqli-labs_nbrc靶场为对象，进行原理介绍和实践练习 。
2. Lesson-1将详细讲解第一个SQL注入例子，给初学者一个初步思路的引导，后面的课程尽量只给出提示。
3. 推荐使用火狐浏览器，非必需，但火狐的一些插件会大大提高注入的效率，以下教程默认使用火狐浏览器.
4. 教程难免会有的纰漏和局限，欢迎指正和讨论。联系方式微信号wwwbird520。

本课程的主要知识点：

- PHP的Addslashes()函数
- 宽字节编码
- 宽字节注入

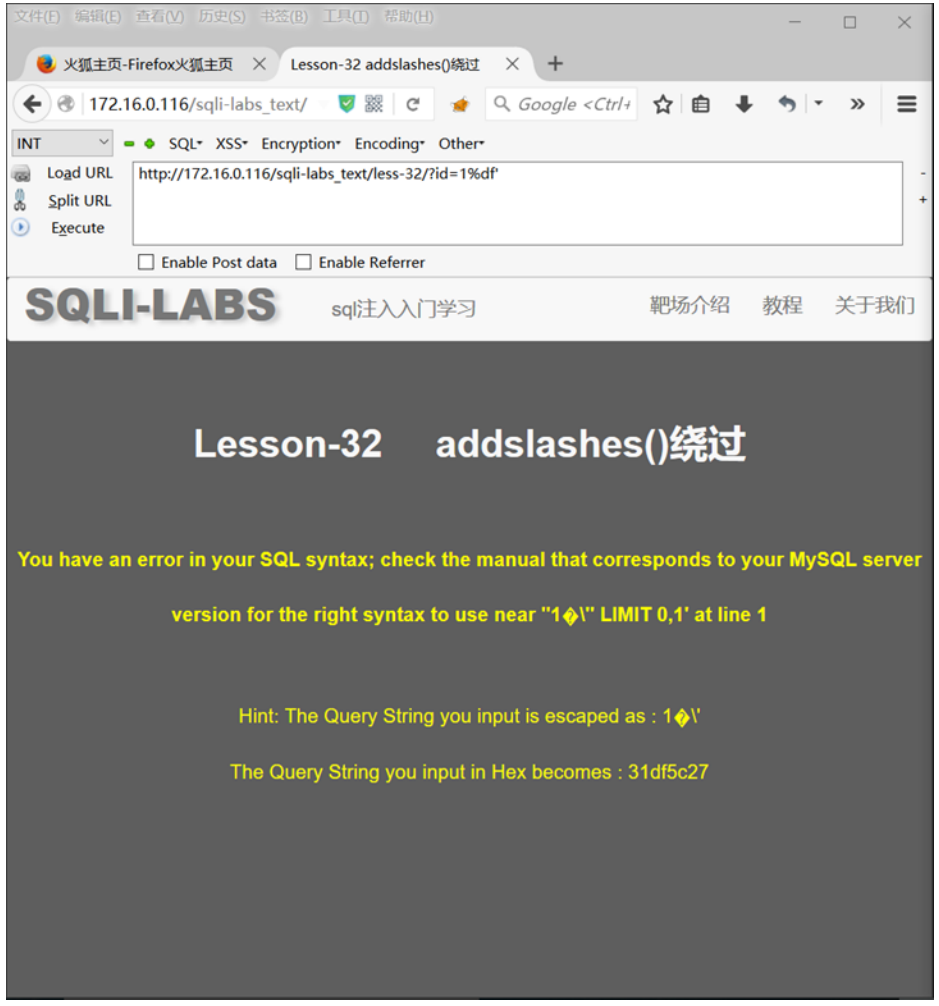
1. Addslashes()函数

- addslashes()函数会在预定义的字符前添加反斜杠，预定义的字符有 ”，’，\。
- 例如输入***?id=1“"***,执行后页面会显示处理后的结果。如图。
- 转义后就无法正常闭合，但如果php采用宽字节编码，就可以采用宽字节注入。



2. 宽字节注入方法

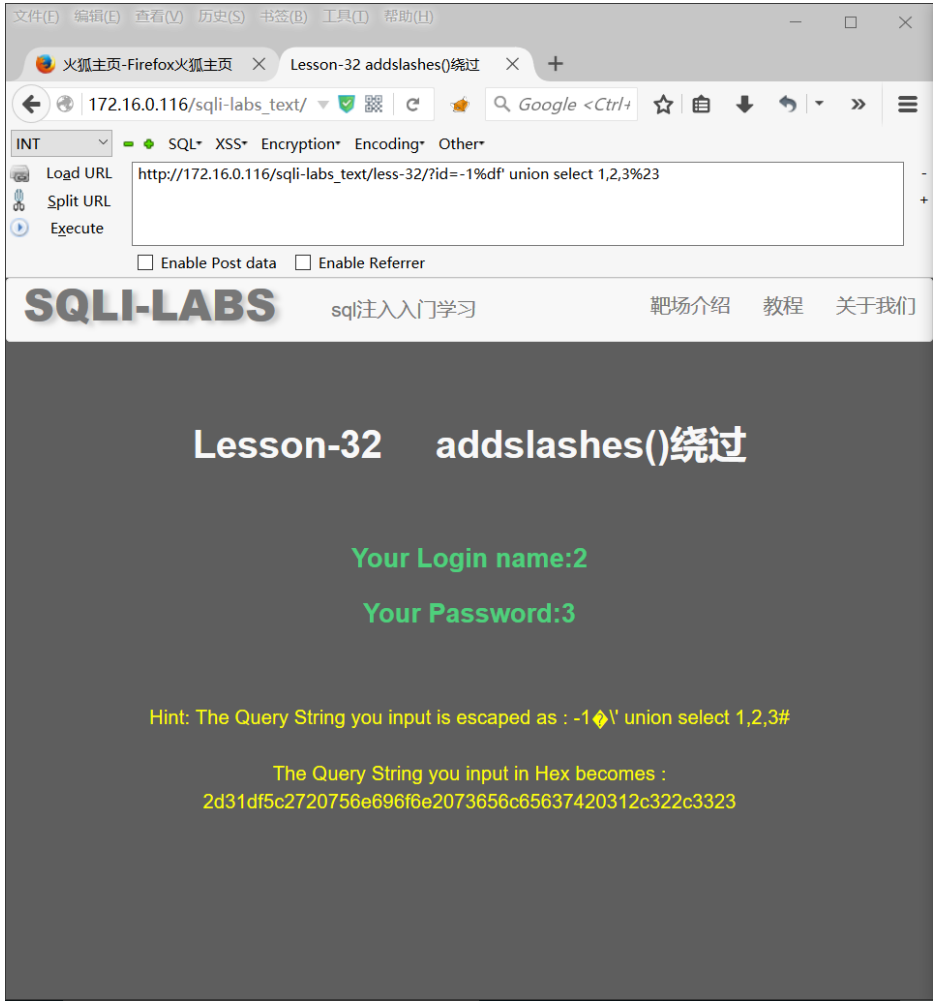
- 一般的宽字节有GBK，GB2312等，只有两个字节。也就是说宽字节会把两个字符一起解析。
- 注入时，在会被转义的字符前添加一个特殊字符%df，转义后这个特殊字符和反斜杠\编码后在mysql解析为一个中文字符。就可以使这次转义无效。
- 输入***?id=1%df'***,执行结果如图。



0X20. lesson-32 addslashes()绕过

- 引发报错说明单引号并没有被转义。
- 根据错误报告闭合语句，构造注入语句：

  ?id=-1%df' union select 1,2,3%23
- 执行后回显成功如图。说明绕过成功。



Thanks!

卓越品质 ，我们到追求！

崔艳鹏

微信：*******

微博：*******

扫一下，有更多惊喜！