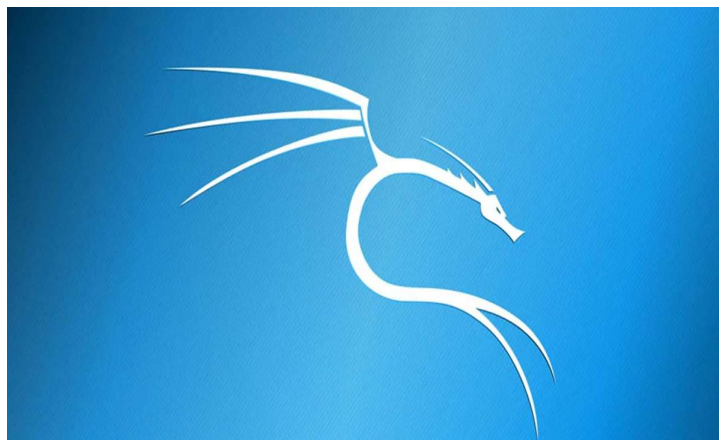


Curso 2021/2022

# Introducción a la Ciberseguridad Práctica 3



Marta Pérez Rodríguez

Luis Ortiz Fernández

Curso 1º Ingeniería de la Ciberseguridad





## Índice

Ejercicio 1	3
Ejercicio 2	3
Ejercicio 3	4
Ejercicio 4	6
Ejercicio 5	7
Ejercicio 6	9
Ejercicio 7	10
Ejercicio 8	12
Ejercicio 9	21
Ejercicio 10	23
Bibliografía	24

## Ejercicio 1

**Empleando como referencia al organismo IANA, averigua el nombre del puerto 993, su protocolo de transporte, su descripción y la fecha de la última modificación en su definición.**

Su nombre es imaps. El protocolo de transporte es tcp. Como descripción nos encontramos: IMAP over TLS protocol. Su última modificación fue el 22 de febrero de 2021.

Service Name	Port Number	Transport Protocol	Description	Assignee	Contact	Registration Date	Modification Date	Reference
imap	143	tcp	Internet Message Access Protocol	[IESG]	[IETF_Chair]		2021-02-22	[RFC3501][RFC9051]
imap3	220	tcp	Interactive Mail Access Protocol v3	[James_Rice]	[James_Rice]			
imap3	220	udp	Interactive Mail Access Protocol v3	[James_Rice]	[James_Rice]			
imaps	993	tcp	IMAP over TLS protocol	[IESG]	[IETF_Chair]		2021-02-22	[RFC3501][RFC8314][RFC9051]
imap2			Interim Mail Access Protocol version 2					

Figura 1: 'Datos obtenidos en IANA'

## Ejercicio 2

**¿Qué es el localhost? ¿A qué dirección IP corresponde este nombre? ¿Qué es un loopback?**

Localhost es el nombre que se le da al equipo que estamos utilizando, siendo la traducción servidor o dispositivo local, estando localizado en el propio equipo. Por ejemplo, si ejecutamos un programa en nuestro ordenador, éste es el localhost. Por tanto cuando realizamos una petición a un localhost. Realmente para lo que sirve es emular conexiones de red cuando no hay ninguna red activa o disponible, conectando el dispositivo consigo mismo.

Corresponde a la IP 127.0.0.1

Un loopback es la dirección IP invariable asignada a localhost. En IPv4 es 127.0.0.1, cuyo único propósito consiste en redirigir el tráfico de vuelta al equipo actual.

## Ejercicio 3

Tras averiguar la dirección IP asignada a tu máquina, prueba a realizar un escaneo con “nmap”. Puedes escanear también la dirección privada de tu router y la pública, a ver qué diferencias observas.

```
(kali㉿kali)-[/]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe43:73bc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:43:73:bc txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 1240 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 2798 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 28 bytes 1440 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 1440 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 2: ‘Averiguar dirección IP’

La IP pública asignada es 10.0.2.15, averiguada con “ifconfig”.

Posteriormente realizamos el escaneo con nmap seguido de nuestra IP pública:

```
(kali㉿kali)-[/]
$ nmap 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-23 07:59 EST
Nmap scan report for 10.0.2.15
Host is up (0.00020s latency).
All 1000 scanned ports on 10.0.2.15 are closed
```

Figura 3: ‘Escaneo de IP’

La IP pública se corresponde con 10.0.2.15 mientras que la IP privada se corresponde con 192.168.56.1. La IP privada es la dirección que asigna el router a cada dispositivo a la hora de conectarse a él, mientras que la IP pública es la dirección común que asigna el router a todos los dispositivos conectados a él que quieren conectarse a Internet.

```
Adaptador de Ethernet VirtualBox Host-Only Network:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . . : fe80::7cb4:a864:e081:9caa%9
Dirección IPv4. . . . . : 192.168.56.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
```

Figura 4: 'IP privada obtenida con ifconfig en Windows'

**Menciona alguna página web que puedas consultar para averiguar y geolocalizar la dirección IP pública de tu router doméstico.**

Algunas de las páginas web que podemos consultar son:

<https://www.cualesmiip.com/localizar-ip>

<https://www.cual-es-mi-ip.net/>

## Ejercicio 4

Con ayuda del manual de nmap (man nmap), investiga qué comando o comandos necesitarías para extraer la versión utilizada en el servicio SSH de tu máquina virtual. ¿Qué comando te ha servido para realizar esta tarea? ¿Qué información, aparte de la versión del servicio SSH, has conseguido extraer?

El comando utilizado ha sido nmap -sV

Se ha obtenido, además de la versión del servicio SSH, información del sistema operativo.

```
(kali@kali)-[~]
$ nmap -sV 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-25 06:03 EST
Nmap scan report for 10.0.2.15
Host is up (0.000046s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
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 0.30 seconds
```

Figura 5: 'Servicio SSH'

## Ejercicio 5

**¿Qué significado tienen los valores de entrada de la función socket “familia”, “tipo” y “protocolo”? Identifica esta llamada en el código proporcionado. Explica los valores concretos que se emplean en el código.**

Un socket no es más que un "fichero" que se abre de una manera especial, por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada.

```
int sockfd = socket(int familia, int tipo, int protocolo)
```

int socket (consiste en crear el fichero)

type: permite decidir el tipo de socket, ya sea, socket de flujo (“SOCK\_STREAM”[Conexión bidireccional confiable con el flujo de datos ordenado]) o un socket de datagramas (“SOCK\_DGRAM”[Mensajes no confiables, sin conexión, con una longitud máxima fija]), además de existir SOCK\_SEQPACKET: Conexión bidireccional confiable con el flujo de datos ordenados y datagramas de longitud máxima fija. El resto de parámetros se pueden fijar a “AF\_INET” para el dominio de direcciones, y a “0”, para el protocolo (de esta manera se selecciona el protocolo automáticamente).

Entonces, lo correcto es usar AF\_INET en su estructura sockaddr\_in y PF\_INET en su llamada a socket (). Pero prácticamente hablando, puedes usar AF\_INET en todas partes. Esto es debido a que AF\_INET es una familia de direcciones que se utiliza para designar el tipo de direcciones con las que su socket puede comunicarse (en este caso, direcciones de Protocolo de Internet v4).

**¿Qué significado tiene cuando la función devuelve un -1? ¿Qué significa si devuelve un valor distinto de -1?**

El valor devuelto es un entero:  $\geq 0$  si el socket es creado correctamente;  $< 0$  si se produce un error en la creación, y debería aparecer -1 y no ningún otro valor negativo.

Si el valor devuelto es 0 significa que el otro extremo ha cerrado la conexión

Cualquier otro número positivo supondrá el número de bytes recibidos.



Completa el código para hacer funcional tu escáner de puertos. Una vez completado el código en C, compílalo (`gcc Practica3_myportscanner.c -o myportscanner`), pruébalo (`./myportscanner`) y comenta los resultados. Compara con los que obtuviste con nmap.

estado de los puertos en nmap (ejercicio 4):

```
(kali@kali)~$ nmap 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-30 07:51 EST
Nmap scan report for 10.0.2.15
Host is up (0.000046s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Figura 6: 'Escáner de puertos en nmap'

Previamente abiertos los puertos 22 (ssh) y 80 (apache2); podemos ver como ambos scanners nos detectan los mismos puertos abiertos por lo tanto comprobamos que nuestro scanner funciona correctamente.

```
(urjc@ETSIICTF)~/Escritorio/Ciberseguridad$ ./myportscanner
Introduce hostname o dirección IP : 127.0.0.1

Puerto de inicio: 1

Puerto de salida: 100
Doing inet_addr ... Hecho
Comienza el escaneo de puertos ...
22    open
80    open

(urjc@ETSIICTF)~/Escritorio/Ciberseguridad$ nmap 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-02 11:57 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

Figura 7: 'Escáner de puertos creado'

## Ejercicio 6

Una vez instalado y configurado LAMP, muestra, mediante un pantallazo, el resultado de acceder a la página <http://localhost/info.php>.

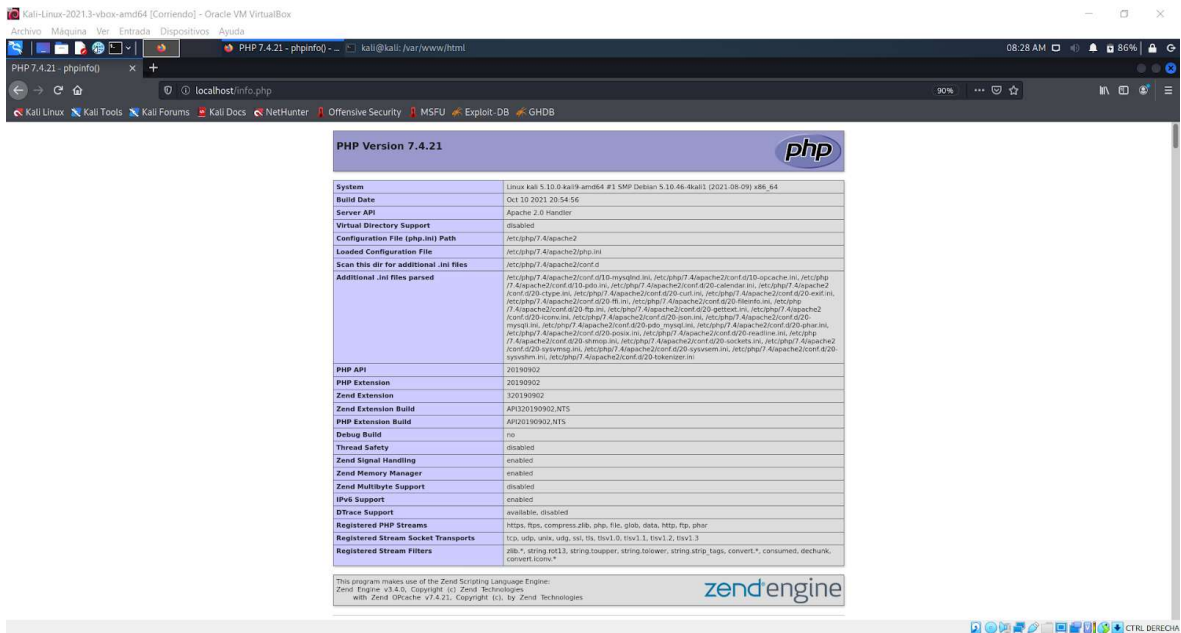


Figura 8: ‘PHP’

## Ejercicio 7

Tras finalizar con la instalación y configuración de LAMP, debes crear una base de datos (BBDD) sencilla y un usuario de MySQL con las características que se muestran en la Tabla:

Nombre de la BBDD	accesos
Nombre de la tabla	user_pass
Campos de la tabla	user; password
Usuario	app
Permisos del usuario	ALL PRIVILEGES (sobre la tabla "user_pass" de la BBDD "accesos")

Figura 9: 'Tabla para la creación de la BBDD'

```
(kali@kali)~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.5.12-MariaDB-1 Debian 11

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

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

MariaDB [(none)]> CREATE DATABASE accesos;
Query OK, 1 row affected (0.004 sec)

MariaDB [(none)]> CREATE TABLE user_pass (user varchar (30), password varchar (45));
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> USE accesos;
Database changed
MariaDB [accesos]> CREATE TABLE user_pass (user varchar (30), password varchar (45));
Query OK, 0 rows affected (0.018 sec)

MariaDB [accesos]> CREATE USER app@localhost IDENTIFIED by ciber;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'ciber' at line 1
MariaDB [accesos]> CREATE USER 'app'@'localhost' IDENTIFIED by 'ciber';
Query OK, 0 rows affected (0.007 sec)

MariaDB [accesos]> GRANT ALL PRIVILEGES ON accesos.user_pass TO 'app'@'localhost';
Query OK, 0 rows affected (0.004 sec)

MariaDB [accesos]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)

MariaDB [accesos]> exit;
Bye
```

Figura 10: 'Base de datos creada'

Una vez creada la base de datos y la tabla con los campos requeridos (véase la Figura 9), inserta mediante comandos (con “INSERT INTO”), dos usuarios con sus correspondientes contraseñas. ¿Qué comando o comandos has utilizado?

```
(kali@kali)-[~]
└─$ mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.12-MariaDB-1 Debian 11

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

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

MariaDB [(none)]> SHOW DATABASES
+-----+
| Database |
+-----+
| accesos  |
| information_schema |
| mysql    |
| performance_schema |
+-----+
4 rows in set (0.005 sec)

MariaDB [(none)]> USE accesos;
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
MariaDB [accesos]> INSERT INTO user;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' at line 1
MariaDB [accesos]> INSERT INTO user_pass(user,password) VALUE ('marta','ciber');
Query OK, 1 row affected (0.013 sec)

MariaDB [accesos]> INSERT INTO user_pass(user,password) VALUE ('luis', 'ciber');
Query OK, 1 row affected (0.004 sec)

MariaDB [accesos]>
```

Figura 11: 'Usuarios creados'

Hemos utilizado los comandos INSERT INTO y VALUE

## Ejercicio 8

**Crea la página web sencilla indicada en la Tabla 1 y verifica que funcione. Muestra un pantallazo al acceder a ella desde un navegador web.**



Figura 12: 'Página web creada'

Añade una tabla a la página web dentro de la etiqueta (véase el ejemplo de la Tabla 2). En ella, deben incluirse tres filas y tres columnas. Las columnas corresponden a los campos “Profesor”, “Despacho” y “Edificio”. Las filas corresponden a la siguiente información:

- Marta Beltrán | 122 | Departamental II
- Isaac Martín | 167 | Departamental II
- Miguel Calvo | S/N | Departamental II



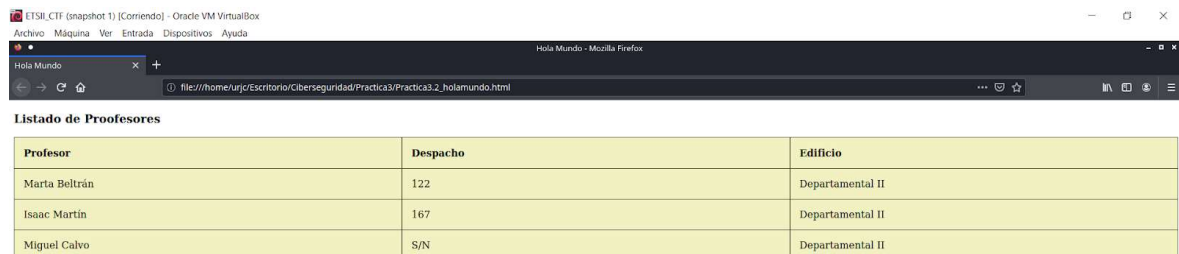
Figura 13: ‘Tabla añadida’

Investiga sobre las etiquetas “h” de HTML y añade una cabecera con el título “Listado de profesores” a la página web.



Figura 14: ‘Cabecera añadida’

**Cambia el estilo de la tabla utilizando el código CSS de la Tabla 3. ¿Qué has tenido que modificar o añadir en la tabla para que se muestre en color amarillo?**



The screenshot shows a web browser window with the address bar displaying a file path. Below the browser window, there is a table titled 'Listado de Profesores'. The table has three columns: 'Profesor', 'Despacho', and 'Edificio'. The background of the table is yellow.

Profesor	Despacho	Edificio
Marta Beltrán	122	Departamental II
Isaac Martín	167	Departamental II
Miguel Calvo	S/N	Departamental II

Figura 15: 'Estilo de tabla'

En el código hay que cambiar **table#01 por th,td** como aparece en las anteriores al abrir paréntesis o mover el background color al apartado de arriba (table, th, td) y añadirlo también en el último apartado (table#01) el color de background

**Modifica el CSS que acabas de insertar para que el borde de la tabla (véase la Figura 1) se muestre del mismo color que tiene la corona del logotipo de la Universidad Rey Juan Carlos. Para descubrir el código de color puedes utilizar GIMP, la extensión para Google Chrome "ColorZilla" o alguna herramienta similar. ¿Qué línea has añadido y dónde para realizar este cambio? Haz un pantallazo del resultado.**



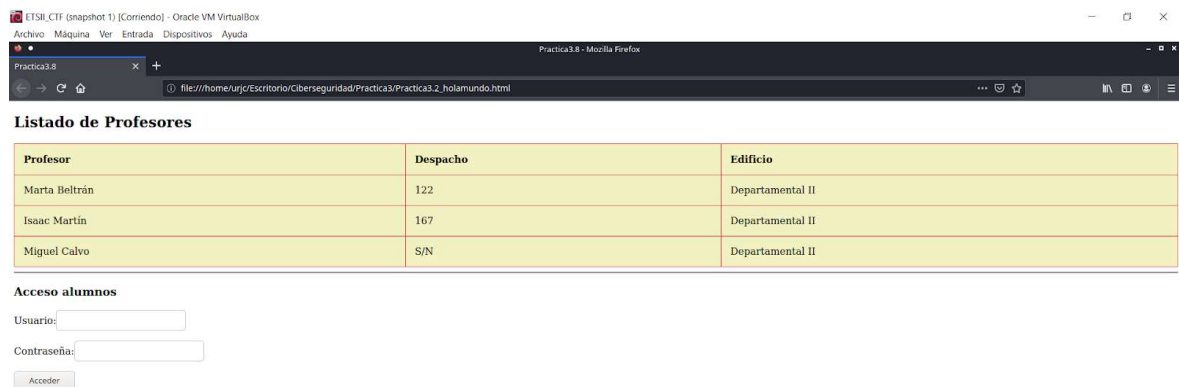
The screenshot shows the same web browser window as before, but the table now has a red border. The background remains yellow.

Profesor	Despacho	Edificio
Marta Beltrán	122	Departamental II
Isaac Martín	167	Departamental II
Miguel Calvo	S/N	Departamental II

Figura 16: 'Borde de tabla'

Utilizando la herramienta ColorZilla conseguimos el color de la corona (#E90129) y este lo he cambiado en la línea: **border: 1px solid black** por **border: 1px solid #E90129** o añadiendo **border-color:**

Añade un formulario a la web. Dicho formulario ha de solicitar un nombre y una contraseña (oculta cuando se escribe, sustituida por “\*”). Si das al botón “Acceder” del formulario, la petición de acceso será enviada a una página llamada “Practica3.2\_control\_de\_accesos.php” (esta página de momento no tendrá ninguna funcionalidad, se escribirá en próximos apartados de la práctica). Además, añade una cabecera al formulario que diga “Acceso alumnos”, (de tamaño menor que la anterior “Listado de Profesores”). El resultado debe ser similar al de la Figura 2. ¿Qué código has utilizado?



The screenshot shows a web browser window with the address bar displaying a local file path. The page content includes a table titled 'Listado de Profesores' and a login form titled 'Acceso alumnos'.

Profesor	Despacho	Edificio
Marta Beltrán	122	Departamental II
Isaac Martín	167	Departamental II
Miguel Calvo	S/N	Departamental II

Below the table, the 'Acceso alumnos' section contains the following form elements:

- Label: 'Usuario:' followed by a text input field.
- Label: 'Contraseña:' followed by a password input field.
- A button labeled 'Acceder'.

Figura 17: 'Usuario y contraseña'

Código:

```
<form method="post" action="Practica3.2_control_de_accesos.php">
```

```
<h2>Acceso alumnos</h2>
```

```
<label for="usuario">Usuario:</label><br>
```

```
<input type="text" id="usuario" name="usuario"/><br>
```

```
<label for="password">Contraseña:</label><br>
```

```
<input type="password" id="password" name="password"/><br><br>
```

```
<input type="submit" name="submit" value="Acceder"/>
```





**En este ejercicio, se debe añadir una lista a la web. Esta lista debe incluir una cabecera (de tamaño aún menor que la cabecera del formulario de acceso) de color azul que diga “Listado de prácticas”. Para ello, investiga sobre las etiquetas “ul” y “li” de HTML y lee la ayuda que te proporcionamos. El resultado debe ser similar al de la Figura 3. Pega el código utilizado para cambiar el color de la cabecera (tanto el CSS como la etiqueta HTML de la propia cabecera).**

---

## Listado de Profesores

Profesor
Marta Beltrán
Isaac Martín
Miguel Calvo

## Acceso alumnos

Usuario:

Contraseña:

## Listado de Prácticas

- Práctica 1
  - Memoria 1
- Práctica 2
  - Examen tipo test
- Práctica 3
  - Memoria 3.1
  - Memoria 3.2

Figura 18: 'Listado de prácticas'

Código:

```
<h3 style="color:#00F">Listado de Prácticas</h3>
```

```
<ul>
```

  
`<li>Práctica 1</li>``<ul>``<li>Memoria 1</li>``</ul>``<li>Práctica 2</li>``<ul>``<li>Examen tipo test</li>``</ul>``<li>Práctica 3</li>``<ul>``<li>Memoria 3.1</li>``<li>Memoria 3.2</li>``</ul>``</ul>`

Después de añadir el listado de elementos y buscando un resultado similar al de la Figura 4, añade un nuevo apartado en tu web con una cabecera que diga “Enlaces externos” y una sub-cabecera que diga “Enlaces de interés”. En este apartado, debes incluir un enlace a la web de la URJC, otro al de la ETSI y otro al Aula Virtual. El color de los enlaces debe ser (investiga sobre “CSS Links”):

- Verde cuando no haya sido visitado.
- Rosa cuando haya sido visitado.
- Subrayado y rojo cuando esté activo.
- Azul cuando se tenga el ratón encima.

¿Qué código CSS has utilizado? Adjuntar un pantallazo del resultado.

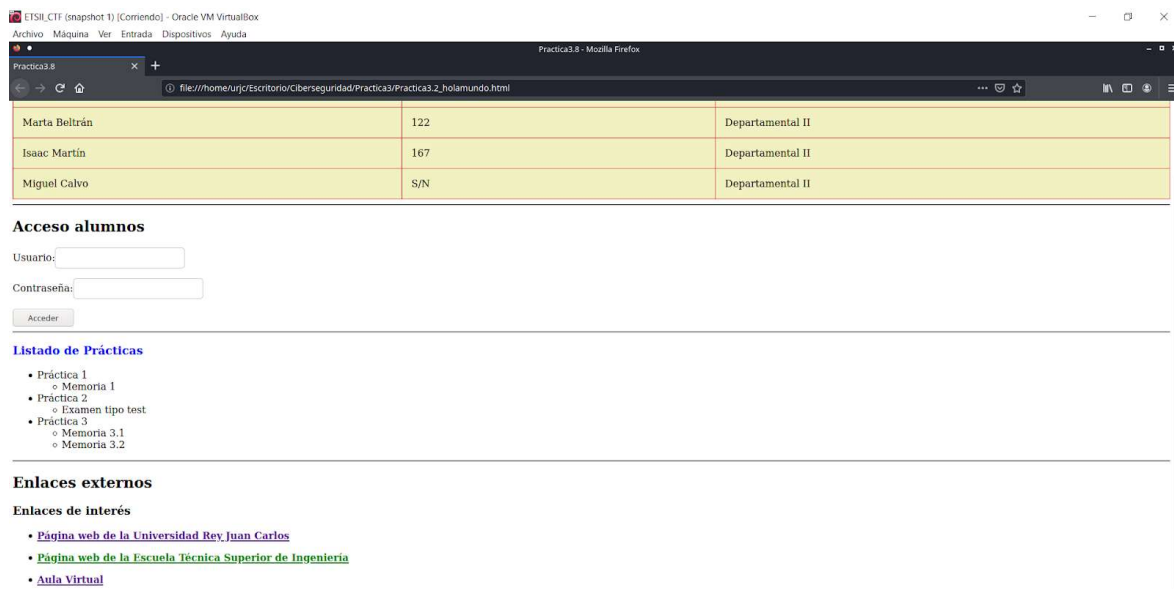


Figura 19: 'Enlaces externos'

Código:

**<h2>Enlaces externos</h2>**

**<style>**

**a:link {**

**color: green;**

**}**

**a:hover {**

**color:blue;**

**}**

```

a:active{
color:red;
}

</style>

<h3>Enlaces de interés</h3>

<ul>

<li><p><b><a href="https://www.urjc.es/" target="_blank">Página web de la Universidad Rey
Juan Carlos</a></b></p></li>

<li><p><b><a href="https://www.urjc.es/etsii" target="_blank">Página web de la Escuela
Técnica Superior de Ingeniería</a></b></p></li>

<li><p><b><a href="https://www.aulavirtual.urjc.es/moodle/login/index.php"
target="_blank">Aula Virtual</a></b></p></li>

</ul>

```

Graba un audio con la herramienta de grabación de tu ordenador (por ejemplo, “Grabadora de voz” en Windows, “Audio Recorder” en Ubuntu, etc.). En este audio, todos los integrantes del grupo debéis presentaros (diciendo vuestro nombre, la carrera que estáis haciendo y el nombre de la asignatura). Después, incluye el audio dentro de la página web (con cabecera “Presentación”), apoyándote en la etiqueta “audio” de HTML5. El resultado debe ser similar al de la Figura 5. ¿Qué código has utilizado para incluir tu audio en el HTML?

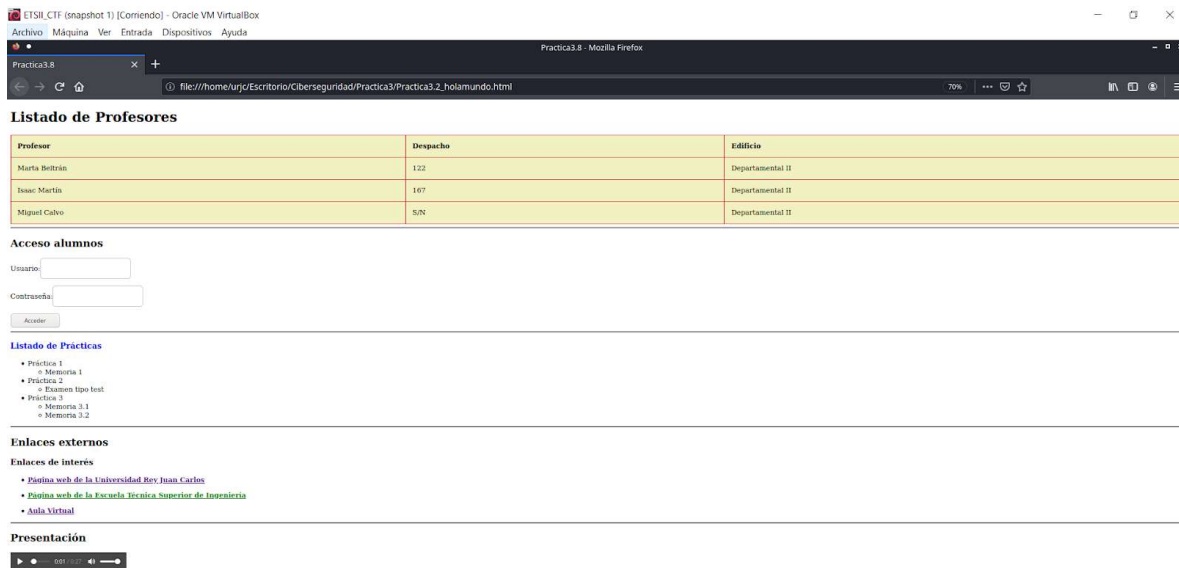


Figura 20. 'Audio'

Código:

```
<h2>Presentación</h2>
```

```
<audio controls="controls">
```

```
<source src="Practica3.2_EjemploAudio.mp3" type="audio/mpeg">
```

```
</audio>
```

Quando los estilos se van complicando, como ha ocurrido en esta web tan sencilla ¿cómo suelen gestionarse? ¿Se dejan en el HTML como hemos hecho en esta primera página o se separan de los contenidos de alguna manera? Hazlo en tu web y llama al nuevo fichero “Practica3.2\_styles.css”.

Se suele gestionar creando un fichero externo css, separando los estilos del contenido.

## Ejercicio 9

¿Qué hay que modificar en el código HTML de la página “Practica3.2\_holamundo.html” para que al dar al botón “Acceder” del formulario se procese el control de accesos

(“Practica3.2\_control\_de\_accesos.php”) contra la base de datos de usuarios y contraseñas que tenemos en MySQL?

Añadiendo en `<form method="post" action="Practica3.2_control_de_accesos.php"`

Y en el botón acceder `<input type="submit" value="Acceder"/>`

¿Cómo debe programarse la página “Practica3.2\_control\_de\_accesos.php”? Escríbela completando el esqueleto de la Tabla 4 y comprueba que funciona correctamente en todos los casos posibles.

**USUARIOS:**

**USER: PASSWORD:**

**LUIS LUIS**

`<?php`

```
if(isset($_POST['usuario']) && isset($_POST['password']) && !empty($_POST['usuario']) &&
!empty($_POST['password'])){
```

```
    $user=($_POST['usuario']);
```

```
    $pass=($_POST['password']);
```

```
    $conn = new mysqli('localhost','app','password-usuario','accesos')
```

```
    if ($conn->connect_error){
```

```
        die("FALLÓ LA CONEXIÓN A BBDD: ".$conn->connect_error);
```

```
    }
```

```
$resultado = $conn->query("SELECT * FROM accesos.user_pass WHERE  
usuario='$user' AND password='$pass';");
```

```
if ($resultado->num_rows !=0){
```

```
    echo 'Usuario encontrado: Puedes acceder a la zona privada';
```

```
} else {
```

```
    echo 'Usuario no encontrado: Vuelve a intentarlo';
```

```
}
```

```
$conn->close();
```

```
} else {
```

```
    echo 'Introduce un usuario y una contraseña.';
```

```
}
```

```
?>
```



## Ejercicio 10

**Sabiendo que el adversario no tiene cuenta en nuestra aplicación y, por lo tanto, no está en la base de datos, ¿Qué podría escribir en el campo del formulario de la contraseña para ganar acceso a la zona privada? ¿Qué daría siempre un resultado TRUE al lanzar la consulta SQL contra la base de datos? Este patrón de ataque se denomina inyección SQL.**

La inyección de SQL es un tipo de ciberataque en el cual un hacker inserta código propio en un sitio web con el fin de acceder a datos protegidos.

Para acceder necesitamos que el usuario y contraseña nos devuelvan verdadero.

La forma que se utiliza para saber si un formulario es vulnerable es añadiendo una comilla simple en algún campo. Por ejemplo: si insertamos como usuario mar'ta, todo lo que vaya después de la comilla simple se ha quedado fuera de código y formaría parte de la sentencia SQL.

Por lo tanto, si introducimos como usuario y contraseña una condición booleana que siempre sea TRUE podríamos acceder con datos incorrectos. Por ejemplo: 'asdf' OR 'a' = 'a' como usuario y contraseña devuelve siempre un TRUE

1. usuario = 'asdf' OR 'a'='a' AND password = 'asdf' OR 'a'='a'
2. FALSE OR TRUE AND FALSE OR TRUE
3. FALSE OR FALSE OR TRUE
4. TRUE

**¿Cómo tendría que mejorarse la página “Practica3.2\_control\_de\_accesos.php” para evitar este tipo de inyecciones? Propón al menos dos alternativas y explícalas (no hace falta que las implementes).**

Para evitar inyecciones SQL, se pueden emplear distintas estrategias. Por ejemplo estas tres opciones:

- Validar la entrada del usuario mediante una lista de admisión para evitar que se envíen datos no deseados a la base de datos
- Limitar los privilegios del administrador de la base de datos
- Almacenar datos confidenciales de forma segura para limitar el impacto en caso de una fuga de datos

## Bibliografía

[https://www.cloudcenterandalucia.es/blog/localhost-que-es-conceptos-basicos-y-como-crearlo/#Que es un localhost y para que se usa](https://www.cloudcenterandalucia.es/blog/localhost-que-es-conceptos-basicos-y-como-crearlo/#Que_es_un_localhost_y_para_que_se_usa)

<https://forums.virtualbox.org/viewtopic.php?f=2&t=69429#p331107>

[http://www.chuidiang.org/clinix/sockets/sockets\\_simp.php](http://www.chuidiang.org/clinix/sockets/sockets_simp.php)

<https://stackoverflow.com/es/q/447653/is-0-or-1-valid-return-values-for-socket-function-call>

<https://programmerclick.com/article/64541915707/>

▷ Crear Tablas en MYSQL Workbench 【Create Table】 (codigosql.top)

Tipos de datos en MYSQL para emplear en base de datos ▷  VidaBytes ▷ 

<https://bit.ly/3DTjoqj>

<https://www.tutorialspoint.com/How-can-we-set-up-a-MySQL-User-account-by-using-INSERT-INTO-statement>

[https://protecciondatos-lopd.com/empresas/direccion-ip-privada-publica/#Direccion\\_de\\_IP\\_publica\\_Que\\_es](https://protecciondatos-lopd.com/empresas/direccion-ip-privada-publica/#Direccion_de_IP_publica_Que_es)

<https://kinsta.com/es/blog/inyeccion-sql/>

<https://datadome.co/es/gestion-y-proteccion-contrabots/como-prevenir-ataques-de-inyeccion-de-sql-llevados-a-cabo-por-bots/#strategies>

<https://www.avast.com/es-es/c-sql-injection#topic-3>

<https://www.securityartwork.es/2013/11/21/evasion-de-autenticacion-con-inyeccion-sql/>