



---

# HACKING ÉTICO

---

Unidad 1. Actividad 6




11 DE OCTUBRE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD









## Índice

Actividad 6.....	2
Basico .....	2
Básica: red .....	6
Básica: web.....	9


## Actividad 6

Nos creamos una cuenta en atenea





### Ajustes de perfil



Email

Apodo

País

## Basico

### Actividad 1

Realizamos distintas actividades de hash:

#### Hash (1pts)

**Dificultad:** ☆☆☆☆☆

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

La contraseña para superar este reto es **LearnTheHashFunction**


Tendrás que calcular su hash md5 y ponerla en el formato de la plataforma, esto es: flag(md5)

Por ejemplo: flag{378041508fcb2574e1724f8917369be9}

Referencias:  
<https://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales>  
<https://askubuntu.com/questions/53846/how-to-get-the-md5-hash-of-a-string-directly-in-the-terminal>

```
(kali㉿kali)-[~]  
$ echo -n "LearnTheHashFunction" | md5sum  
b2f2d6b27b264d83fe1abe0169b7613e -
```

## Felicidades!



Flag correcto, eres increíble!

Yay!

### Actividad 2

La frase **ThisIsAMoreSecureHashFunction** la pasamos a sha512, después el resultado ese lo pasamos a md5.

Hash 2 (1pts)

Dificultad: ☆☆☆☆☆

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Existen diferentes algoritmos para calcular estas funciones resumen o hash, siendo los más extendidos md5 y sha256.

La contraseña para superar este reto es **ThisIsAMoreSecureHashFunction**

Tendrás que calcular su hash sha256 y posteriormente calcular su md5 para poder poner la solución en el formato de la plataforma, esto es: flag{md5}

Por ejemplo: flag{378041508fcb2574e1724f8917369be9}

### Actividad 3

Buscamos un conversor de md5 a texto, ponemos el md5 (54f662a095fa3d5fbbdaac72d176701b) y desde una pagina lo convertimos:

Hash 3 (2pts)

Dificultad: ☆☆☆☆☆

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Estas funciones son de un único sentido. Es decir, que a partir de un hash no es posible obtener su valor original de manera directa.

La única forma de calcular el valor correspondiente a un hash es mediante ataques de fuerza bruta, esto es, calcular el hash de

### Actividad 4

Ponemos el contenido en ASCII en texto, despues lo pasamos a mayúsculas y pasamos ese texto en md5:

ASCII (3pts)

Dificultad: ☆☆☆☆☆

El código ASCII es una representación numérica de un carácter. Como otros códigos de formato de representación de caracteres, el ASCII es un método para una correspondencia entre cadenas de bits y una serie de símbolos (alfanuméricos y otros), permitiendo de esta forma la comunicación entre dispositivos digitales así como su procesamiento y almacenamiento.

El código ASCII reserva los primeros 32 códigos (numerados del 0 al 31 en decimal) para caracteres de control: códigos no pensados originalmente para representar información imprimible, sino para controlar dispositivos (como impresoras) que usaban ASCII.

Los códigos del 33 al 126 se conocen como caracteres imprimibles, y representan letras, dígitos, signos de puntuación y varios símbolos.

Para pasar este reto deberás encontrar los caracteres correspondientes a la siguiente codificación ASCII:

080 097 115 115 119 111 114 100 032 112 097 114 097 032 115 117 112 101 114 097 114 032 101 108 032 114 101 116 111 058 032 084 104 101 065 083 067 073 073 084 097 098 108 101 033

### Actividad 5

Descodificamos el fichero, nos saldrá un texto y ese texto hay que pasarlo a md5:

## Base64 (3pts)



**Dificultad:** ☆☆☆☆☆

Base64 es un grupo de esquemas de codificación de binario a texto que representa los datos binarios mediante una cadena ASCII, traduciéndolos en una representación radix-64. El término Base64 se origina de un sistema de codificación de transmisión de contenido MIME específico.

Los esquemas de codificación Base64 son comúnmente usados cuando se necesita codificar datos binarios para que sean almacenados y transferidos sobre un medio diseñado para tratar con datos textuales. Esto es para asegurar que los datos se mantienen intactos y sin modificaciones durante la transmisión. Base64 es comúnmente usado en muchas aplicaciones, incluyendo la escritura de emails vía MIME y el almacenamiento de datos complejos en XML.

Para superar este reto tendrás que decodificar el fichero adjunto y poner la contraseña en el formato de la plataforma, esto es: flag{md5}

Por ejemplo: flag{378041508fcb2574e1724f8917369be9}

Referencia:

[https://developer.mozilla.org/es/docs/Web/API/WindowBase64/Base64\\_codificando\\_y\\_decodificando](https://developer.mozilla.org/es/docs/Web/API/WindowBase64/Base64_codificando_y_decodificando)

base64.txt `c6d8efd649ad94af23eb2bd2af63edd0`

## Actividad 6

Pasamos de Hexadecimal a ASCII, despues de ASCII a md5:

Paste hex numbers or drop file

50617373776f72643a2044346d7054686548337821

Character encoding

ASCII

Convert Reset Swap

Password:

## Hex (3pts)



**Dificultad:** ☆☆☆☆☆

El sistema hexadecimal es el sistema de numeración posicional que tiene como base el 16. En principio, dado que el sistema usual de numeración es de base decimal y, por ello, sólo se dispone de diez dígitos, se adoptó la convención de usar las seis primeras letras del alfabeto latino para suplir los dígitos que nos faltan.

El conjunto de símbolos es el siguiente:



$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$

Siendo A = 10, B = 11, C = 12, D = 13, E = 14 y F = 15. Para su representación se pueden utilizar tanto letras minúsculas como mayúsculas.

Para pasar este reto deberás decodificar la siguiente cadena hexadecimal:

50617373776f72643a2044346d7054686548337821

## Actividad 7

[XOR](#) (4pts)  

**Dificultad:** ★☆☆☆☆

En criptografía, el cifrado XOR es, como su nombre indica, un algoritmo de cifrado basado en el operador binario XOR:



$$A \text{ xor } 0 = A$$
$$A \text{ xor } A = 0$$
$$(B \text{ xor } A) \text{ xor } A = B$$

Una cadena de texto puede ser cifrada aplicando el operador de bit XOR sobre cada uno de los caracteres utilizando una clave. Para

## Actividad 8

Muestro la entropía de cada imagen:

```
Archivo Edición Formato Ver Ayuda
air = 7.970380436428385 no
Blue = 7.956819811378534 no
cello = 7.978027860280588
chess = 7.912812270142892 no
chestnut = 7.972698675368137 no
fire = 7.970070565599005 no
fly = 7.968972890840315 no
seemed = 7.972985827100437 no
waffle = 7.972985827100437 no
|
```

[Entropía](#) (5pts)  

**Dificultad:** ★☆☆☆☆

En el ámbito de la teoría de la información la entropía mide la incertidumbre de una fuente de información. La entropía también se puede considerar como la cantidad de información promedio que contienen los símbolos usados. Los símbolos con menor probabilidad son los que aportan mayor información. Llevando este concepto al campo informático, podemos decir que un fichero tiene una entropía alta (yendo ésta de 0 a 8), cuando sus bytes son más heterogéneos entre sí. Esto es especialmente interesante en seguridad informática porque los ficheros con una entropía muy alta (cerca de 8) suelen ser ficheros cifrados o comprimidos.

Teniendo en cuenta esto, para pasar este reto deberás encontrar cuál de las imágenes adjuntas tiene la mayor entropía. La solución al reto es el nombre del fichero de la imagen (incluyendo la extensión) en el formato habitual de la plataforma (por ejemplo: imagen25.jpg).

## Actividad 9

## Básica: red

### Actividad 1

La capa de internet se encuentra en la dos, simplemente ponemos el numero 2 en md5:

#### Modelo TCP/IP (1pts)

Dificultad: ☆☆☆☆☆

TCP/IP es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. La sigla TCP significa Protocolo de control de transmisión/Protocolo de Internet. Proviene de los nombres de dos protocolos importantes incluidos en el conjunto TCP/IP, es decir, del protocolo TCP y del protocolo IP.

Este modelo incluye cuatro capas. Para superar el reto indica el número de capa (en formato numérico, por ejemplo: 15) correspondiente a la capa de Internet.

### Actividad 2

Ponemos la dirección valida (212.271.123.45) en md5:

#### Dirección IP (2pts)

Dificultad: ☆☆☆☆☆

La dirección IP es un conjunto de números que identifica a un equipo dentro de una red que utilice el protocolo Internet Protocol (IP) o que corresponde al nivel de red del modelo TCP/IP.

La versión 4 de la dirección IP (IPv4) utiliza un formato de 4 números separados por un punto entre ellos.

Para superar este reto, indica cuál es una IPv4 válida:

45.2.6..1  
192.1t8.32.8  
8.8.8.8.8  
3:4:5:6  
212.27.123.45  
00.25.350.56  
128.76.64.258

### Actividad 3

Ponemos la dirección valida (2001:0aa8:13ed:0000:0000:ff7a:98ff:0001) en md5:

#### Dirección IPv6 (2pts)

Dificultad: ☆☆☆☆☆

IPv6 es el sucesor del primer protocolo de direccionamiento de Internet, Internet Protocol versión 4 (IPv4). A diferencia de IPv4, que utiliza una dirección IP de 32 bits, las direcciones IPv6 tienen un tamaño de 128 bits. Por lo tanto, IPv6 tiene un espacio de direcciones mucho más amplio que IPv4.

Una dirección IPv6 (128 bits) se representa mediante ocho grupos de cuatro dígitos hexadecimales, cada grupo representando 16 bits (dos octetos). Los grupos se separan mediante dos puntos (:).

Para superar este reto, averigua la IPv6 válida:

192.168.1.1  
80.40.32.112.0.0.1.12  
ab00.12cd.4eef.2100.4e11.0a22.3333.1f44  
2001:0aa8:13ed:0000:0000:ff7a:98ff:0001  
2ae3::0:0233:1  
8.8.8.8  
1aad:3aaa:13ej:0000:0000:ff7a:98ff:0001

#### Actividad 4

Ponemos la dirección válida (172.25.0.3) en md5:

Direcciones IP privadas y públicas (2pts)

**Dificultad:** ☆☆☆☆☆

Una dirección IP puede ser privada o pública. Las IPs privadas se utilizan para las comunicaciones de los equipos dentro de una red local, mientras que las IPs públicas se utilizan para las comunicaciones a través de Internet.

Por ejemplo, en una red doméstica, en la que se tiene un router ADSL o de fibra, los equipos conectados a él mediante wifi o cable tendrán una dirección IP privada, pero saldrán a Internet usando la misma dirección IP pública.

Los rangos de IPs privadas están definidos dentro del RFC1918.

Para superar este reto, indica cuál de las siguientes IPs es una IP privada:

- 8.8.8.8
- 192.178.1.1
- 172.25.0.3
- 85.32.11.0
- 172.0.0.1
- 12.10.25.4
- 11.22.33.44
- 0.0.0.0

#### Actividad 5

Descargamos el archivo y buscamos la ip que le da al cliente, después lo pasamos a md5:

3	0.070031	0.0.0.0	255.255.255.255	DHCP	314 DHCP Request	- Transaction ID 0x
4	0.070345	192.168.0.1	<u>192.168.0.10</u>	DHCP	342 DHCP ACK	- Transaction ID 0x

DHCP (3pts)

**Dificultad:** ☆☆☆☆☆

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes. En todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido, etc.

En el fichero adjunto, el servidor DHCP asigna una IP privada a un equipo. Indica cuál es.

Referencias:  
[https://es.wikipedia.org/wiki/Protocolo\\_de\\_configuraci%C3%B3n\\_din%C3%A1mica](https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica)  
<https://www.wireshark.org/>

 [dhcp.pcap](#) 350a4a71b742023fcfed000c5f664fd6



## Actividad 6

La mascara de red es 24, despues lo pasamos a md5:

### Máscara de red (3pts)

**Dificultad:** ☆☆☆☆☆

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Para superar este reto, indica la equivalencia en el formato CIDR de esta máscara de red (por ejemplo: 37):

255.255.255.0

## Actividad 7

/20 en decimal es 255.255.240.0, despues lo pasamos a md5:

### Máscara de red 2 (3pts)

**Dificultad:** ☆☆☆☆☆

La máscara de red se puede representar en diversos formatos.

Para superar este reto, indica la equivalencia en formato decimal de la máscara de red /20.

Referencias:

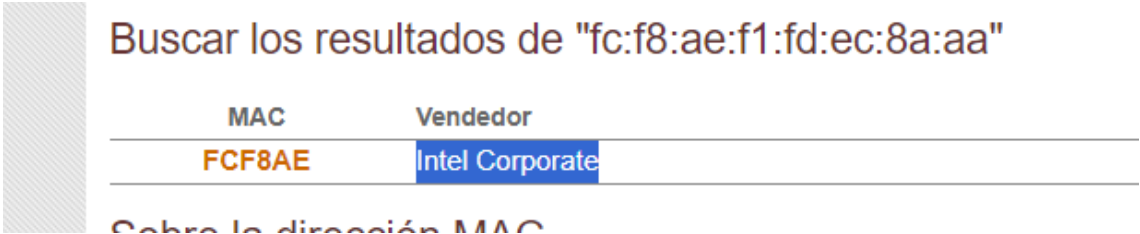
[https://es.wikipedia.org/wiki/M%C3%A1scara\\_de\\_red](https://es.wikipedia.org/wiki/M%C3%A1scara_de_red)

<https://en.wikipedia.org/wiki/Subnetwork>

[https://es.wikipedia.org/wiki/Classless\\_Inter-Domain\\_Routing](https://es.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

## Actividad 8

Buscamos el fabricante de la MAC en internet:



Buscar los resultados de "fc:f8:ae:f1:fd:ec:8a:aa"

MAC	Vendedor
FCF8AE	Intel Corporate

Sobre la dirección MAC

### MAC (4pts)

**Dificultad:** ☆☆☆☆☆

La dirección MAC (Media Access Control) es un identificador único para cada dispositivo de red. Se la conoce también como dirección física, y su valor depende del fabricante.

Para superar este reto, indica el fabricante (primera letra en mayúsculas) de la tarjeta de red con la siguiente dirección MAC:

fcf8aef1fddec8a:aa

Referencias:

### Actividad 9

El puerto http es el 80

#### Puerto (4pts)

**Dificultad:** ☆☆☆☆☆

En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de trans aplicaciones que se pueden conectar al mismo host, o puesto de trabajo.

Aunque muchos de los puertos se asignan de manera arbitraria, ciertos puertos se asignan particulares o servicios de carácter universal.

Para superar este reto, indica el puerto asignado por convenio para HTTP.

Referencias:

[https://es.wikipedia.org/wiki/Puerto\\_\(inform%C3%A1tica\)#Puertos\\_de\\_Internet](https://es.wikipedia.org/wiki/Puerto_(inform%C3%A1tica)#Puertos_de_Internet)

### Actividad 10

El puerto https es el 443:

#### Puerto 2 (4pts)

**Dificultad:** ☆☆☆☆☆

En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transport aplicaciones que se pueden conectar al mismo host, o puesto de trabajo.

Aunque muchos de los puertos se asignan de manera arbitraria, ciertos puertos se asignan, por particulares o servicios de carácter universal.

Para superar este reto, indica el puerto asignado por convenio para HTTPS.

Referencias:

### Actividad 11

## Básica: web

### Actividad 1

Ponemos TITLE en md5:

Tag HTML (1pts)

**Dificultad:** ☆☆☆☆☆

Para superar este reto, deberás indicar cuál es el tag que se utiliza en HTML para establecer el título de una página web. (Deberás poner la solución en mayúsculas, por ejemplo: DATA)

Referencias:  
<https://www.w3schools.com/TAGS/default.ASP>

## Actividad 2

Descargamos el archivo y lo abrimos en whreshark, despues nos vamos a la sección de Hypertext transfer protocol y nos saldrá el nombre del servidor:

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 5846
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 01 Nov 2021 08:54:46 GMT\r\n
    Server: Microsoft-IIS/8.0\r\n
    Last-Modified: Mon, 03 Dec 2018 18:36:22 GMT\r\n
    ETag: "22688-57c226cf0b580-gzip"\r\n
    Accent-Range: hvtes\r\n
```

Servidor web (2pts)

**Dificultad:** ☆☆☆☆☆

El fichero adjunto contiene el tráfico intercambiado contra un servidor web. Identifica de qué servidor web se trata (por ej Apache/1.2.7)

Referencias:  
<https://www.wireshark.org/>  
<http://www.steves-internet-guide.com/http-basics/>  
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers>

📎 http.pcap 2d1f610aa9773de1c096e32cb09b1b25

## Actividad 3

Descargamos el archivo y lo abrimos en whreshark, despues nos vamos a la sección de Hypertext transfer protocol y nos saldrá el nombre del navegador (Firefox/93.0):

Servidor web 2 (2pts)

**Dificultad:** ☆☆☆☆☆

Indica el navegador que se ha usado para realizar la navegación al servidor web (por ejemplo: Chrome/95.0)

Referencias:  
<https://www.wireshark.org/>  
<https://developer.mozilla.org/es/docs/Web/HTTP/Headers/User-Agent>  
<https://developers.whatismybrowser.com/useragents/parse/>

## Actividad 4

Descargamos el archivo y lo abrimos en whreshark, despues nos vamos a la sección de Hypertext transfer protocol y nos saldrá el lenguaje (zh-CN):

**Pais de origen** (3pts)

**Dificultad:** ☆☆☆☆☆

A partir de la captura de tráfico adjunta, deduce cuál es el idioma que habla la persona que está realizando la navegación web. La solución a este reto es el país donde más se habla dicho idioma (introduce el país con la primera letra en mayúsculas y en inglés. Por ejemplo: Spain)

Referencias:  
<https://www.wireshark.org/>  
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Accept-Language>  
[https://docs.oracle.com/cd/E13214\\_01/wli/docs92/xref/xqisocodes.html](https://docs.oracle.com/cd/E13214_01/wli/docs92/xref/xqisocodes.html)

Descargamos el archivo y lo abrimos en whire shark, buscamos el archivo unknow.jpg y miramos su código (404):

550 HTTP/1.1 404 Not Found (text/html)

376 GET /img/gallery/img\_02.jpg HTTP/1.1


[Código HTTP](#) (4pts)

**Dificultad:** ☆☆☆☆☆

Indica cuál es el código devuelto por el servidor web cuando el usuario intenta acceder al recurso unknown.jpg (por ejemplo: 501)

Referencias:

- <https://www.wireshark.org/>
- <https://www.restapitutorial.com/httpstatuscodes.html>

 [http3.pcapi">@fcef3f43e4d753ca493c80d64232883](#)

Descargamos el archivo y lo abrimos en whireshark, despues nos vamos a la sección de Hypertext transfer protocol y nos saldrá el Cookie:

## Cookie (5pts)

**Dificultad:** ☆☆☆☆☆

Identifica el nombre de la cookie que se está utilizando en la captura de tráfico adjunta.

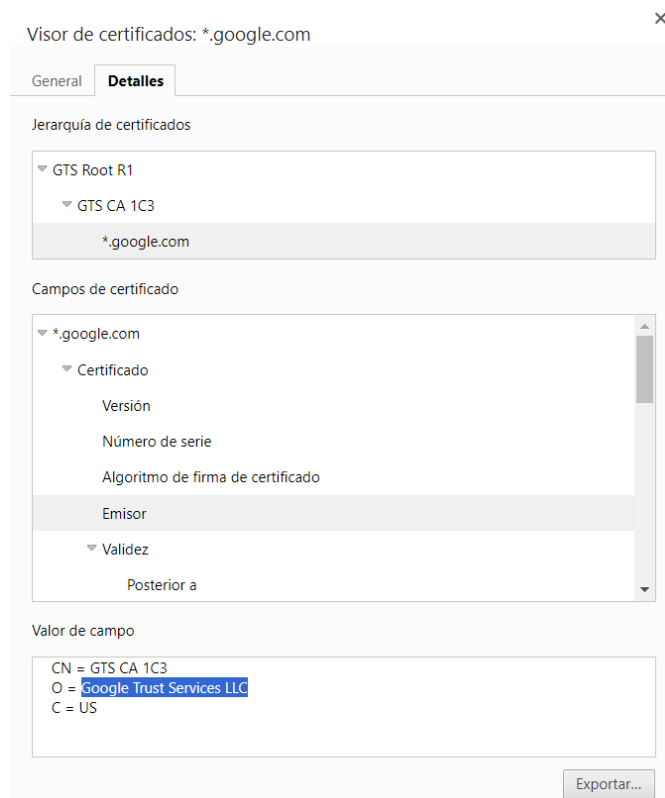
Referencias:

<https://www.wireshark.org/>

<https://developer.mozilla.org/es/docs/Web/HTTP/Headers/Cookie>

## Actividad 7

Para ver el certificado de Google podemos buscarlo desde cualquier navegador:



## Certificado SSL (6pts)

**Dificultad:** ☆☆☆☆☆

Indica el valor del campo organización del certificado de la web de Google:

<http://www.google.com>

Referencias:

<https://www.google.com>

<https://www.venafi.com/education-center/ssl/how-to-check-ssl-certificate>

<https://securitytrails.com/blog/extract-ssl-data>

## Actividad 8

Buscamos en el código fuente de la página flexslider.css:

← → ↺ view-source:https://www.ccn-cert.cni.es

Ajuste de línea

flexslider.css

```
1 <!DOCTYPE html>
2 <html xmlns="http://www.w3.org/1999/xhtml"
3   xml:lang="es-es" lang="es-es" >
4
5 <head>
6   <base href="https://www.ccn-cert.cni.es/" />
7   <meta http-equiv="content-type" content="text/html; charset=utf-8" />
8   <meta name="description" content="Bienvenido al portal de CCN-CERT" />
9   <meta name="generator" content="Joomla! - Open Source Content Management" />
10  <title>CCN-CERT</title>
11  <link href="/?format=feed&type=rss" rel="alternate" type="application/rss+xml" title="RSS 2.0" />
12  <link href="/?format=feed&type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0" />
13  <link href="https://www.ccn-cert.cni.es/" rel="alternate" hreflang="es-ES" />
14  <link href="https://www.ccn-cert.cni.es/gl/" rel="alternate" hreflang="gl-ES" />
15  <link href="https://www.ccn-cert.cni.es/ca/" rel="alternate" hreflang="ca-ES" />
16  <link href="https://www.ccn-cert.cni.es/eu/" rel="alternate" hreflang="eu-ES" />
17  <link href="https://www.ccn-cert.cni.es/en/" rel="alternate" hreflang="en-GB" />
18  <link href="/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />
19  <link href="/modules/mod_reslider/assets/css/flexslider.css" rel="stylesheet" type="text/css" />
20  <link href="/media/mod_languages/css/template.css?09f37ba290759df5a6ab750c49c072d6" rel="stylesheet" type="text/css" />
```

Ruta (6pts)

Dificultad: ☆☆☆☆☆

Encuentra la ruta completa donde se encuentra la hoja de estilos flexslider.css de la web:

<https://www.ccn-cert.cni.es>

Por ejemplo: /styles/css/flexsilder.css

Referencias:

<https://www.ccn-cert.cni.es>

<https://www.dummies.com/web-design-development/site-development/how-to-view-source-code-on-a-web-page/>

[https://www.w3schools.com/html/html\\_css.asp](https://www.w3schools.com/html/html_css.asp)

## Actividad 9

Copio el código y lo pongo en javascript, el resultado lo pongo en md5:

Menú Añadir framework JavaScript

HTML CSS JavaScript Console

HTML

```
<html>
<body>
<script>
  var contador;
  var result = 0;
  for (contador = 1; contador <= 10; contador++)
  {
    if (contador % 5 == 0)
      result += contador;
  }
  document.write(result);
</script>
</body>
</html><!DOCTYPE html>
<html>
<head>
<meta charset=utf-8 />
<title>Editor JavaScript online - www.cubicfactory.com</title>
</head>
<body>

</body>
</html>
```

Resultado

15

13

## JavaScript (7pts)

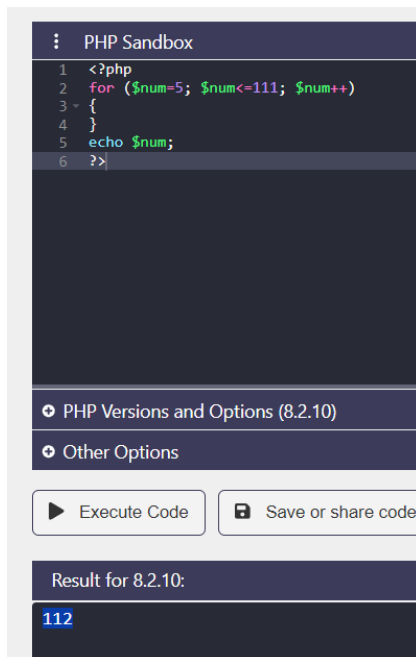
Dificultad: ☆☆☆☆☆

Indica el resultado tras ejecutar el siguiente código JavaScript:

```
<html>
<body>
<script>
  var contador;
  var result = 0;
  for (contador = 1; contador <= 10; contador++)
  {
    if (contador % 5 == 0)
      result += contador;
  }
  document.write(result);
</script>
```

### Actividad 10

Copio el código y lo pongo en php, el resultado lo pongo en md5:



The screenshot shows a web-based PHP Sandbox. At the top, it says "PHP Sandbox". Below that is a code editor with the following code:

```
1 <?php
2 for ($num=5; $num<=111; $num++)
3 {
4 }
5 echo $num;
6 ?>
```

Below the code editor are two expandable sections: "PHP Versions and Options (8.2.10)" and "Other Options". At the bottom, there are two buttons: "Execute Code" and "Save or share code". Below the buttons, it says "Result for 8.2.10:" and displays the output "112" in blue text.

## PHP (7pts)

Dificultad: ☆☆☆☆☆

PHP es un lenguaje de código abierto muy popular especialmente adecuado para el HTML. En lugar de usar muchos comandos para mostrar HTML (como en C o en Perl) código incrustado, encerrado entre las etiquetas especiales de comienzo y final <?ph

Lo que distingue a PHP de algo del lado del cliente como Javascript es que el código y enviándolo al cliente. El cliente recibirá el resultado de ejecutar el script, aunque no

Indica el resultado de ejecutar el siguiente código PHP:

```
<?php
```