



# Piscine Discovery de Ciberseguridad

Cell 2 - 2 - Gecko

by @alrodri2

*Resumen: Las codificaciones se pueden revertir. Esto hace que no sean muy seguras para enviar información sensible, o siquiera almacenarla. Y aquí es precisamente donde los hashes -o funciones resumen- salen a la ayuda. En este proyecto tendrás que averiguar cómo funcionan y cómo romperlos.*

*Versión: 1.0*

# Índice general

I.	Unas palabras sobre la Piscine Discovery de Ciberseguridad	2
II.	Introducción	3
III.	Instrucciones generales	4
IV.	Instrucciones comunes	5
V.	Ejercicio 02: Basic	6
VI.	Entrega y evaluación entre pares	7

# Capítulo I

## Unas palabras sobre la Piscine Discovery de Ciberseguridad

¡Te damos la bienvenida!

Vas a comenzar la primera celda de esta Discovery de Ciberseguridad. Queremos mostrarte el código que compone el software que usas todos los días, y al mismo tiempo experimentar el aprendizaje entre pares, un modelo educativo de 42.

La programación implica lógica (no matemáticas). Te proporciona los bloques elementales, que ensamblas como desees. No existe LA solución a un problema. Existe tu solución, existe la de cada uno de tus compañeros.

Lenta o rápida, fea o bonita, si hace el trabajo, ¡eso es todo lo que se necesita! este conjunto de bloques constituirá una serie de órdenes (cálculo, visualización, ...) que el ordenador realizará, en el orden que hayas elegido.

En lugar de darte un curso con una sola solución para cada problema, y que probablemente esté desactualizado en unos años, hemos elegido ponerte en una situación de aprendizaje entre pares. Vas a buscar los elementos que podrían servirte para tu desafío, seleccionar los que realmente te interesan probándolos y manipulándolos, y crear tu propio programa. Para hacer esto, discute con otros, intercambia puntos de vista, encuentra nuevas ideas en grupo, y finalmente compruébalo tu mismo hasta convencerte de que funciona.

La evaluación entre pares es un momento clave para descubrir otras formas de hacer las cosas, así como casos especiales que no has pensado y que podrían socavar tu programa (piensa en tu grado de nerviosismo con el software que se bloquea).

Al igual que diferentes clientes que no prestan atención a las mismas cosas, cada evaluador será diferente al anterior. Y quién sabe, podrías acabar forjando nuevas amistades para futuras colaboraciones.

Al final de esta piscina, no habrás hecho las mismas cosas que los demás participantes, no habrás validado los mismos proyectos, habrás elegido hacer un desafío en lugar de otro... ¡y eso es normal! Es una experiencia tanto colectiva como personal. Todos se beneficiarán de lo que experimenten durante este tiempo.

¡Buena suerte a todo el mundo! Esperamos que os guste esta experiencia.

# Capítulo II

## Introducción

Qué aprenderás en este proyecto:

- Trabajar con funciones hash.

# Capítulo III

## Instrucciones generales

Salvo que se especifique explícitamente, las siguientes reglas se aplicarán cada día de esta Piscine Discovery.

- Este enunciado es la única fuente confiable. No confíes en ningún rumor.
- Este enunciado puede ser actualizado hasta una hora antes de la fecha límite de entrega.
- Las tareas en un enunciado deben hacerse en el orden indicado. Las tareas posteriores no serán calificadas a menos que todas las anteriores estén perfectamente ejecutadas.
- Ten cuidado con los permisos de acceso de tus archivos y carpetas.
- Tus tareas serán evaluadas por tus compañeros de Piscine.
- Todas las tareas de shell deben ejecutarse usando `/bin/bash`.
- No debes dejar en tu entrega ningún archivo que no sea explícitamente solicitado por los enunciados.
- ¿Tienes una pregunta? Pregúntale a tu vecino de la izquierda. De lo contrario, prueba suerte con tu vecino de la derecha.
- Cualquier respuesta técnica que puedas necesitar está disponible en el `man` o en Internet.
- ¡Recuerda usar el foro de la Piscine de tu intranet y también Slack!
- Debes leer detenidamente los ejemplos. Pueden revelar requisitos que no son obvios en la descripción del enunciado.
- ¡Por Thor, por Odin! ¡Usa tu cerebro!


# Capítulo IV

## Instrucciones comunes

- El uso de herramientas automáticas está prohibido a menos de que se especifique lo contrario en el enunciado.
- Si no se indica otra cosa, el formato de flag será `42BCN{esto_es_una_prueba_flag}`
- La evaluación entre pares comprobará si has entendido cómo resolver cada reto, así que tendrás que poder explicar claramente todo lo que has hecho, y la persona que te evalúe tendrá que poder entender tu explicación.
- Los ejercicios dentro de este proyecto tienen un orden estricto. No podrás seguir haciendo ejercicios posteriores si no has completado los anteriores (por ejemplo, no podrás hacer el ejercicio 3 sin completar el 2).

# Capítulo V

## Ejercicio 02: Basic

	Ejercicio: 02
Ejercicio 02: Basic	
Directorio de entrega: <i>ex02/</i>	
Archivos de entrega: <b>flag.txt</b>	
Funciones prohibidas: None	

En este proyecto no vas a trabajar con codificaciones sino con hashes. Y, al contrario que las codificaciones, los hashes no pueden revertirse.

La única forma de conocer el texto que ha sido pasado por una función hash -o resumenes encontrar un texto que sabes que al pasarlo por la función hash se obtiene el mismo resultado. Así que quizá quieras investigar esto para resolver el desafío.

Debes entregar el texto original que fue pasado por la función hash. Ten en cuenta que tendrás que entregarlo en el formato flag. Por ejemplo, si el texto original era “barcelona” deberías entregar 42BCN{barcelona}

Hash:

629cf0d815ccb448a2c7a4d3d9cc3989



hashcat

Tu tarea es acceder al contenido de esta cadena de texto. Cuando lo hayas logrado debes escribirlo en un archivo flag.txt.

Tendrás que preparar el archivo **flag.txt**, guardarlo en el directorio indicado y pasar la evaluación entre pares.

# Capítulo VI

## Entrega y evaluación entre pares

- Navega hasta la carpeta `cybersec_discovery` en la raíz de tu directorio de usuario.
- Crea una nueva carpeta `cell102` y navega hasta ella.
- Desde ahora en adelante, todos los ejercicios deberían estar en el directorio de entrega correcto. Ejercicio 00 en el directorio `ex00`, Ejercicio 01 en el directorio `ex01`, etc.



Por favor, ten en cuenta que durante tu defensa, cualquier cosa que no esté presente en la carpeta de entrega no será evaluado.