



Piscine Discovery de Ciberseguridad

Cell 1 - 2 - Weasel

by @alrodri2

Resumen: Aquí tenemos otra mala configuración que se puede explotar. Tendrás que exfiltrar alguna información...

Versión: 1.0

Índice general

| | | |
|------|--|---|
| I. | Unas palabras sobre esta Piscine Discovery | 2 |
| II. | Intrucciones Generales | 3 |
| III. | Instrucciones comunes | 4 |
| IV. | Ejercicio 2: Desvíos | 5 |
| V. | Entrega y evaluación entre compañeros | 6 |

Capítulo I

Unas palabras sobre esta Piscine Discovery

¡Te damos la bienvenida!

Vas a comenzar la siguiente 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

Instrucciones Generales

Salvo que esté explícitamente especificado, las siguientes reglas se aplicarán todos los días de esta Piscine:

- 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 III

Instrucciones comunes

- El uso de herramientas automatizadas está prohibido a menos que se especifique en el enunciado del ejercicio.
- Si no se especifica ningún otro formato, la bandera tendrá el siguiente aspecto: 42BCN{esto_es_una_bandera_de_prueba}
- Las evaluaciones entre compañeros medirán tu entendimiento de cómo resolver cada desafío, por lo que debes ser capaz de explicar claramente todo lo que hiciste, y tu compañero debe ser capaz de entender tu explicación.
- Los ejercicios dentro de este enunciado tienen un orden estricto y no podrás hacer ejercicios posteriores si no completaste los anteriores (por ejemplo: No puedes hacer el ejercicio 3 sin haber hecho el ejercicio 2).

Capítulo IV

Ejercicio 2: Desvíos

| | |
|---|---------------|
|  | Ejercicio: 02 |
| Ejercicio 2: Desvíos | |
| Directorio de entrega: <i>ex02/</i> | |
| Archivos de entrega: flag.txt | |
| Funciones prohibidas: None | |

Este sitio web sufre de una vulnerabilidad que permite ver el contenido de archivos a los que no deberíamos tener acceso.

Tu objetivo es encontrar el flag oculto en el sistema de archivos del sitio web

El sitio web: `http://cybersec.[campus].[tld.]:3319`
Pide al staff del campus la URL válida.



Path traversal o desvío de ruta

Deberás enviar el **flag.txt** en la carpeta correcta y pasar por tus compañeros.

Tu tarea es encontrar la URL real utilizada. Cuando hayas tenido éxito, debes escribirla en un archivo **flag.txt**.

Deberás enviar el **flag.txt** en la carpeta correcta y evaluarlo con tus compañeros.

Capítulo V

Entrega y evaluación entre compañeros

- Crea una carpeta `cybersec_discovery` en la raíz de tu carpeta de inicio, y muévete a ella.
- Crea una nueva carpeta `cell102` y navega a ella.
- De ahora en adelante, todos los ejercicios deben estar en la carpeta correcta para que se puedan evaluar. El ejercicio 00 en la carpeta `ex00`, el ejercicio 01 en la carpeta `ex01`, etc. ... ya entiendes la lógica.



Por favor, recuerda que durante tu defensa, todo lo que no esté presente en tu carpeta de entrega no será evaluado.