Piscine Discovery de Ciberseguridad

Gecko 02

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 nos ayudan. En este proyecto tendrás que averiguar cómo funcionan y cómo romperlos.

Versión: 2.00

Índice general

Capítulo I

Bienvenidx a la Piscina Discovery de Ciberseguridad

Hola!

Bienvenid@ a esta Piscine Discovery de ciberseguridad, un reto donde aprenderás los fundamentos de la ciberseguridad ofensiva mientras experimentas el modelo educativo único de 42. Aquí no encontrarás clases tradicionales ni una única solución correcta; el aprendizaje es colaborativo, práctico y centrado en tí.

Queremos que te sumerjas en el código que forma parte del software que usas cada día, desarrollando habilidades que van más allá de lo técnico: pensamiento lógico, resolución de problemas y aprendizaje autónomo. La programación no se trata de memorizar reglas, sino de ensamblar bloques de manera creativa para resolver problemas de forma única.

Durante esta experiencia, abordarás temas clave de la ciberseguridad:

- Manejo de la terminal: Aprende a navegar y operar con soltura en un sistema operativo utilizando comandos.
- OSINT (Open Source Intelligence): Descubre cómo recopilar información pública para identificar amenazas.
- Seguridad web: Comprende las vulnerabilidades más comunes de los sitios web y cómo se explotan.
- Criptografía: Familiarízate con los principios básicos de la protección de datos y comunicaciones.

En este proceso, la evaluación y el aprendizaje entre pares jugarán un papel crucial. Compartirás ideas, discutirás soluciones y descubrirás perspectivas diferentes al interactuar con tus compañeros. Esto no solo enriquecerá tu aprendizaje, sino que también te permitirá forjar conexiones y desarrollar habilidades clave para resolver desafíos futuros.

Recuerda que esta experiencia es tan única como tú: cada participante seguirá su propio camino, validará proyectos distintos y enfrentará retos únicos. Lo importante es lo que aprendas, tanto de tus aciertos como de tus errores.

¡Buena suerte! Esperamos que disfrutes este viaje hacia el mundo de la ciberseguridad y el aprendizaje colaborativo.

Capítulo II

Introducción

La criptografía está en el corazón de la protección de datos y comunicaciones en el mundo digital. Aunque a menudo se percibe como un campo reservado para matemáticos y expertos en seguridad, en realidad, muchas de las técnicas que la sustentan son herramientas que usamos (y dependemos de) todos los días, como cuando protegemos nuestras contraseñas, enviamos mensajes cifrados o verificamos la integridad de un archivo.

Entender cómo funcionan los principios básicos de la criptografía te permitirá no solo proteger mejor tu información, sino también reconocer las debilidades de los sistemas mal implementados. Desde los hashes y las codificaciones hasta los cifrados más complejos, este módulo te enseñará cómo se utilizan estas técnicas en el mundo real y cómo, si no se aplican correctamente, pueden ser explotadas.

Los hashes son otro concepto común en criptografía. Una vez que algo se "hashea", no se puede determinar su contenido original, ya que las funciones hash no son reversibles. La única forma de verificar un hash es hashear la misma entrada y comparar los resultados. Los hashes se utilizan principalmente para almacenar contraseñas de forma segura, verificar la integridad de los datos y más. En este ejercicio, utilizarás fuerza bruta y una lista de contraseñas comunes para descifrar un hash.

Qué aprenderás en este ejercicio:

- Cómo funcionan los hashes y sus usos principales.
- Técnicas de fuerza bruta para descifrar hashes.
- La importancia de políticas de contraseñas fuertes para resistir ataques de fuerza bruta.

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.
- 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 leer la documetación y 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

Ejercicio 02

	Ejercicio: 02
Basic	
Directorio de entrega: *ex*02/	
Archivos de entrega: `flag.txt`	
Funciones prohibidas: `Ninguna`	

En este ejercicio, no estás tratando con codificaciones, sino con hashes. ¿Ya conoces la diferencia?
Una vez más, te damos un texto y tendrás que descubrir el flag, que es el texto que sirve como base para crear lo siguiente:

```
629cf0d815ccb448a2c7a4d3d9cc3989
```

Got it? Tienes que "deshashear.^es^te texto, excepto que acabo de inventarme el verbo y la noción de "deshashear", jejeje ;)

`hashcat`

Capítulo V

Entrega y evaluación entre pares

- Has encontrado la flag? Cuando la tengas debes escribirla en un archivo `flag.txt`.
- El archivo `flag.txt` debe estar situado en `/gecko/ex02`.

Por favor, ten en cuenta que durante la evaluación lo que queremos comprobar es que has entendido lo que has hecho. Debes sabes explicarlo y argumentar las decisiones tomadas.