



Piscine Discovery de Ciberseguridad

Weasel 02

by @alrodri2

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

Versión: 2.00

Índice general

I.	Bienvenidx a la Piscina Discovery de Ciberseguridad	2
II.	Introducción	3
III.	Instrucciones generales	4
IV.	Ejercicio 02	5
V.	Entrega y evaluación entre pares	6

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

Cuando visitas una página web, es fácil asumir que todo está a simple vista, funcionando de manera segura y confiable. Sin embargo, detrás de cada botón, formulario y ruta, hay una compleja estructura de código y configuraciones que, si no se gestionan adecuadamente, pueden convertirse en puertas de entrada para atacantes.

La seguridad web no es solo cuestión de proteger información; se trata de comprender cómo los usuarios interactúan con una página, cómo los datos son procesados y qué vulnerabilidades pueden surgir. Aprender a identificar y explotar errores en aplicaciones web te permitirá ver el mundo digital desde otra perspectiva, preparándote para diseñar sistemas más seguros y resilientes.

Confiar ciegamente en que las entradas de los usuarios no serán maliciosas puede dar lugar a serias vulnerabilidades en las aplicaciones web. Este ejercicio se centra en cómo una entrada manipulada puede revelar rutas o datos que deberían permanecer protegidos, mostrándote la importancia de una validación adecuada.

Qué aprenderás en este ejercicio:

- Identificación de vulnerabilidades relacionadas con entradas de usuario.
- Análisis de cómo las entradas maliciosas pueden ser procesadas de manera insegura.
- Implementación de buenas prácticas para validar datos de entrada.

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 documentación 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
Desvíos	
Directorio de entrega: <i>ex02/</i>	
Archivos de entrega: flag.txt	
Funciones prohibidas: Ninguna	

Aquí tienes la URL del sitio web que vas a explotar:

`http://cybersec.[campus].[tld.]:3319.`

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



Path traversal.



El objetivo del ejercicio es descubrir la vulnerabilidad, no la URL.
Si no funciona, pide al staff del campus la URL válida.

Capítulo V

Entrega y evaluación entre pares

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



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