Proyecto final de curso

Paola Gatta, Azrael , Michael Zambrana, Jose Reche

Máquinas virtuales:

**VM 1:**

Introducción:

Esta máquina virtual consiste de una vulnerabilidad vía web que se llama pérdida de control de acceso.

La vulnerabilidad Brocken Access Control se da cuando hay un fallo o simplemente no existe el control de acceso. En estos casos los usuarios podrán acceder a recursos que están fuera de los permisos previstos. Es una de las vulnerabilidades más comunes y la podemos encontrar en la posición N 1 de OWASP TOP 10.

Arrancar la máquina:

Para la ejecución de la primera máquina hay un script con el nombre de run.sh en la ubicación {ruta} y se le habrá de dar permisos para ejecutar.

Para comprobar que esté levantado accedemos a la web por <http://pino-php.local/>

Walkthrough:

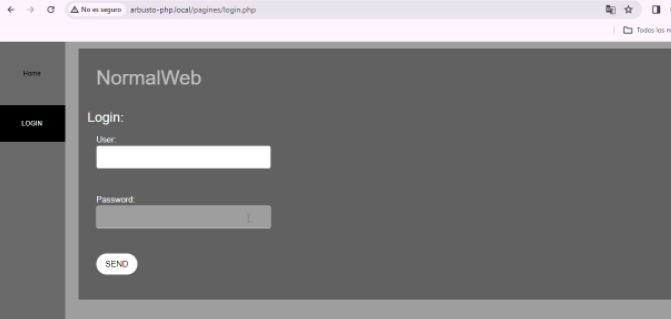
Revisando la web en la parte de contactos el dominio de contacto no es el mismo que el de la web por lo que se cree que existe otra web con ese dominio.

Como podemos ver a continuación:

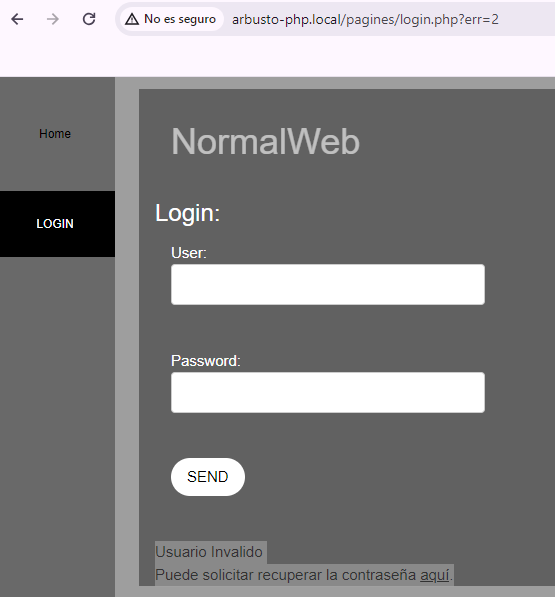


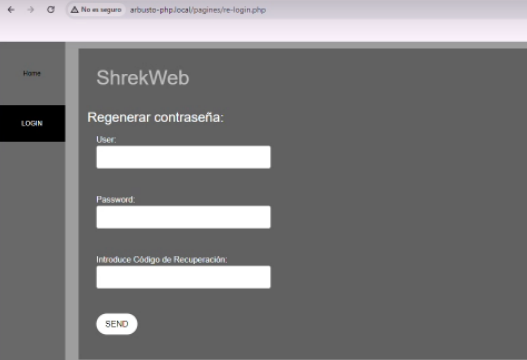
Accederemos a ese dominio y tendremos un login.

Intentaremos entrar con cualquier credencial y veremos que saldrá un error y un link al que podremos acceder para restablecer nuestra contraseña.

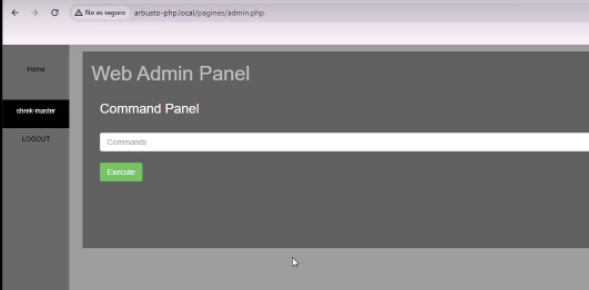


Haremos clic en ‘aquí’





Nos inventaremos las credenciales y volverá a la página anterior pero podemos ver que nos hemos logueado.



Lo siguiente que haremos aquí será añadir mejoras para la CTF.

Añadir reverseshell para poder ejecutarla desde el Command Panel

CTF 1:

Montar servidor web en máquina atacante, donde se creará un fichero para hacer una reverse shell.

Descargar el fichero que se encuentra en la vm del atacante, esto lo haremos haciendo un ‘Curl’ desde el panel de control.

Este fichero se descargará en la ruta ‘var/www/html/web2/páginas’.

**VM2:**

Introducción:

Esta VM se basa en la vulnerabilidad de fallos criptográficos. Esta vulnerabilidad se encuentra en la posición N 2 del TOP 10 DE OWASP.

Un fallo criptográfico es un fallo de seguridad que se produce cuando una entidad expone datos sensibles a causa de un mal uso o de un descuido completo de la criptografía.

Challenge\_1.py

Uso inseguro de un modo de operación de cifrado de bloque. El reto consistirá en descifrar un mensaje que ha sido cifrado incorrectamente debido a un error en la implementación del modo ECB (Electronic Codebook)

El mensaje ha sido cifrado utilizando AES en modo ECB, lo cual es inseguro. Tu tarea es descifrar el mensaje cifrado y encontrar el mensaje secreto. Considera las propiedades del modo ECB y cómo podrías explotarlas para descifrar el mensaje.

challege\_2.py

Uso inseguro de la función hash en la generación de contraseñas

El objetivo del desafío es que los participantes encuentren una palabra que, al ser hasheada con MD5, resulte en el mismo hash que la ‘contraseña’ dada

Challenge\_4.py

Desafío CTF: Decodificación Secreta de Base64

Parte 1: Desafío para los Participantes

El desafío consiste en decodificar un mensaje que ha sido codificado en Base64. Se proporciona a los participantes el mensaje codificado y deben decodificarlo para revelar la bandera oculta.

Mensaje codificado en Base64:

Q1RGe2Jhc2U2NF9kZWNvZGluZ19pc19mdW59

Instrucciones:

Investiga qué es la codificación Base64 y cómo funciona. Utiliza una herramienta de decodificación de Base64 para convertir el mensaje codificado en texto plano. El texto plano revelará la bandera del CTF.

Challenge\_5.py

Desafío CTF: El Misterio del Mensaje Oculto

Parte 1: Desafío para los Participantes

El desafío consiste en identificar un patrón en una serie de números y letras para descubrir un mensaje oculto. Se proporciona a los participantes una cadena de caracteres que parece aleatoria, pero contiene una bandera oculta siguiendo un patrón específico.

Cadena de caracteres:

9a8b7c6d5e4f3g2h1iCTF{p4ttern\_rec0gniti0n\_1s\_k3y}

Instrucciones:

Examina la cadena de caracteres para identificar cualquier patrón o secuencia. Una vez identificado el patrón, extrae la bandera del CTF. La bandera estará en el formato típico CTF{...}.

Arrancar la máquina:

Para la ejecución de la primera máquina hay un script con el nombre de run.sh en la ubicación {ruta} y se le habrá de dar permisos para ejecutar.

Para comprobar que esté levantado accedemos a la web por <http://pino-php.local/>

Walkthrough: