JULIO ANTHONY ENGELS RUIZ COTO - 1284719

Laboratorio 8: Pruebas manuales de seguridad

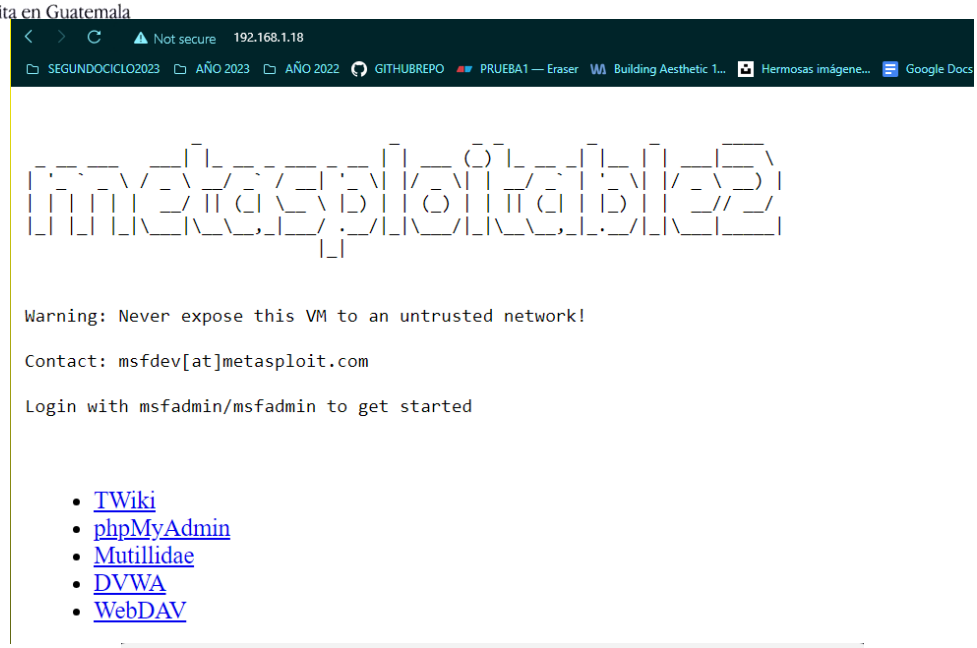
Para esta práctica necesitará:

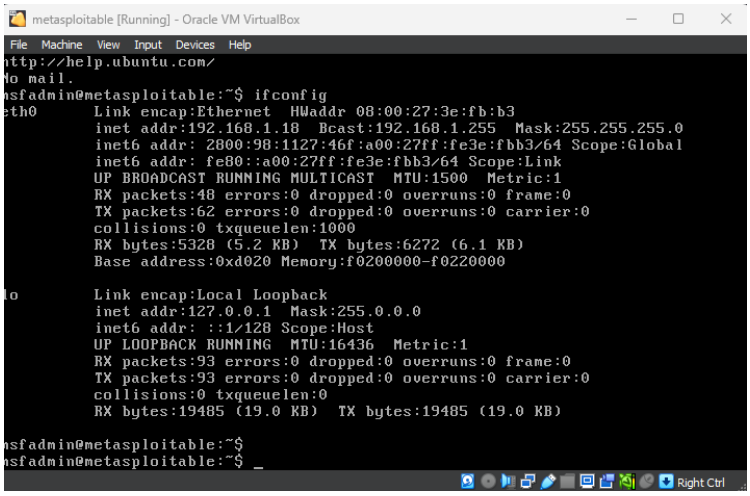
- Máquina virtual Metasploitable versión 2, la máquina debe acceso solamente a la máquina física.

Utilizando la aplicación instalada DVWA ya instalada por defecto en la máquina metasploitable, deberá realizar los ataques que a continuación se presentan.

Por referencia, el usuario y contraseña de la máquina es: msfadmin, utilizarlo para obtener la IP

Una vez consultando la IP en nuestro navegador (máquina host)

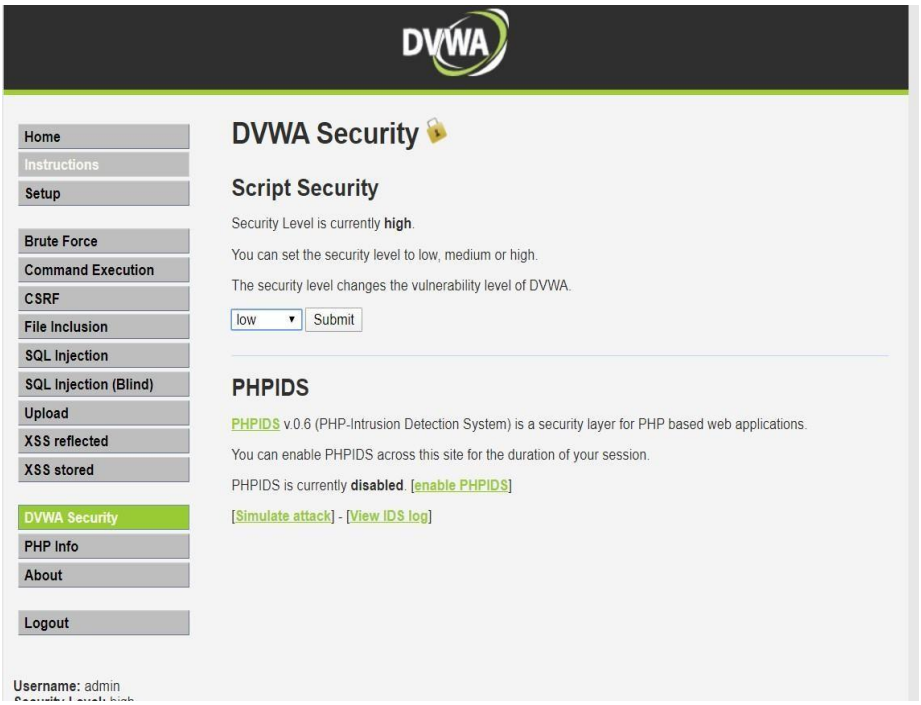




Seleccionamos DVWA y estamos listos, el login para DVWA es:

- Usuario: admin
- Contraseña: password

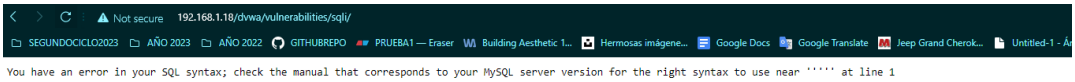
Navegar hasta DVWA Security y seleccionar low como nivel de seguridad:



Parte 1: SQL Injection

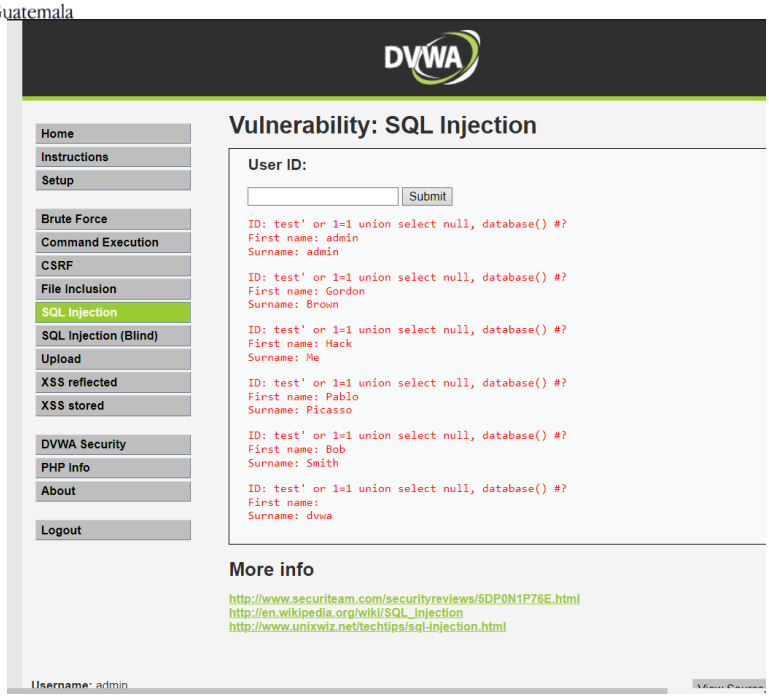
Navegar hasta la opción de SQL Injection y realice lo siguiente:

1. Ingrese el apóstrofe en el formulario de usuarios, es decir el símbolo ` ¿Qué error de obtiene? ¿Qué nos indica este error?



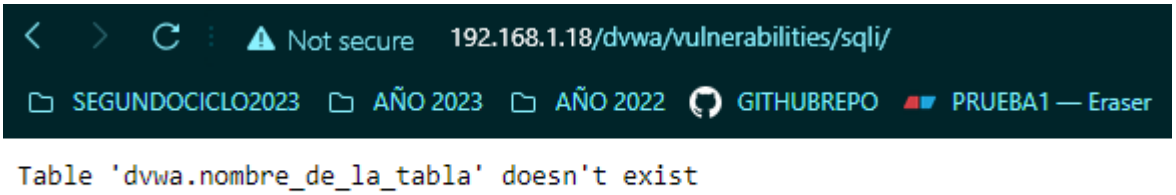
Lo que indica el presente error de entrada del usuario ya que no se está validando o desinfectando adecuadamente antes de ser utilizada en una consulta SQL, dado esto puede un atacante puede inyectar comandos SQL maliciosos.

2. ¿Qué información se obtiene ingresando **test' or 1=1 union select null, database() #**?



test' or 1=1: La parte 1=1 siempre será verdadera devuelve todos los registros
union select null, database(): UNION para combinar los resultados de dos o más consultas SELECT, null se utiliza para garantizar que la cantidad de columnas seleccionadas en la consulta inyectada coincida con la cantidad en la consulta original.
#: comentario en sql, útil para cancelar el resto de la consulta original.

3. Realice una acción más desde SQL explicando cómo ha llegado a esto y cuál era el objetivo.
   test' UNION SELECT username, password FROM nombre_de_la_tabla #

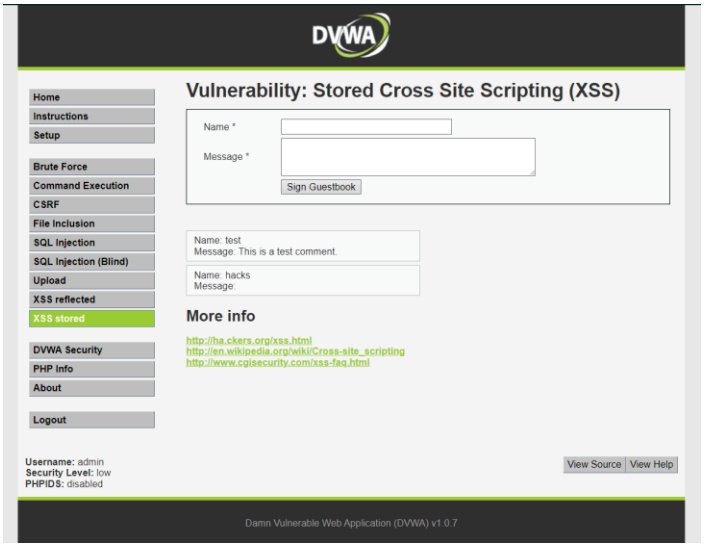


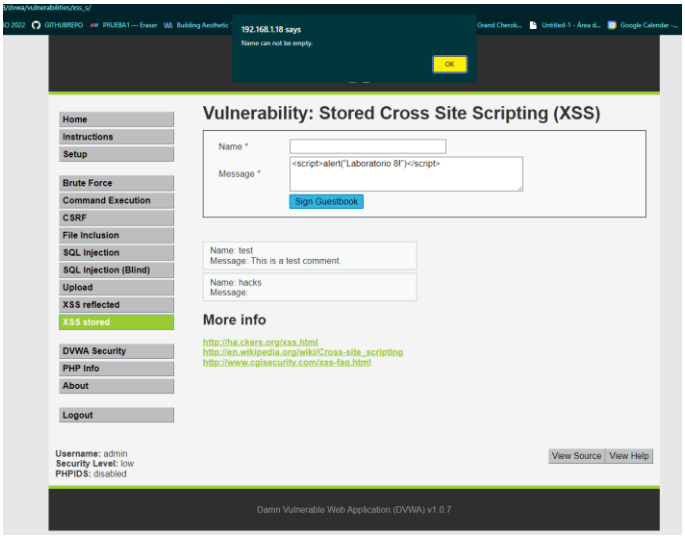
objetivo aquí es obtener información sensible o valiosa ya que, en el mundo real, este sería uno de los pasos finales en un ataque de inyección SQL, ya que el atacante ha obtenido lo que quería: datos reales, la consulta lo que intenta es extraer datos específicos, en este caso, username y password de una tabla la cual hay que especificar, luego se reemplazar 'nombre_de_la_tabla' con el nombre de una tabla que se identificó previamente y que se sospeche que contiene información de usuarios. Si el sistema es vulnerable, esta consulta proporcionará una lista de nombres de usuario y contraseñas, se pueden poner otros datos, de la tabla específica.

Parte 2: XSS

En la misma aplicación, DVWA, ingrese a la opción de XSS Stored y realice lo siguiente:

1. En el mensaje ingrese el siguiente texto: **<script>alert("Laboratorio 8!")</script>** ¿Qué ocurre al hacer submit?



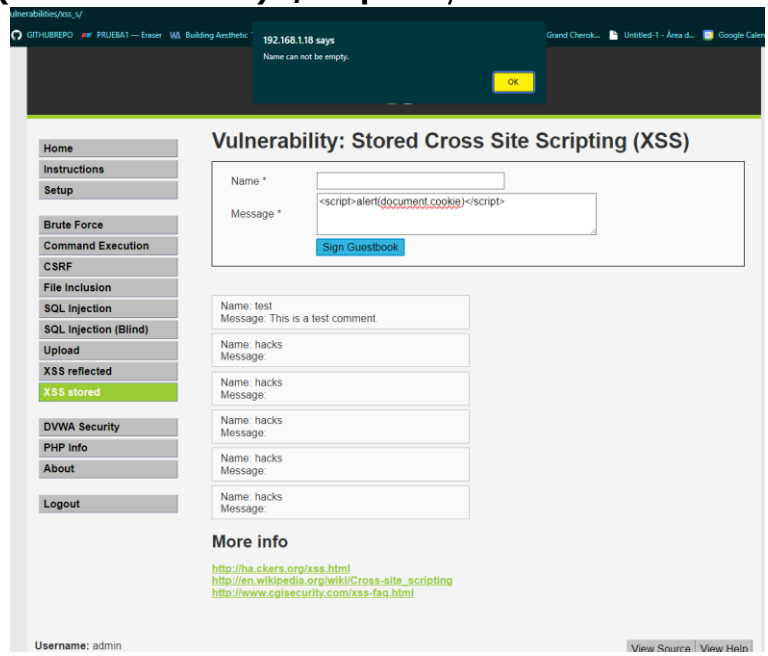


Al momento de aplicar un clic en sign, ejecutará el script. Por qué es un script que muestra una ventana de alerta, se despliega un mensaje emergente que dice "Laboratorio 8!" indica que el sitio es vulnerable a ataques de XSS almacenados, ya que está permitiendo que se ejecute código JavaScript arbitrario que ha sido almacenado en la base de datos.

2. ¿Qué ocurre si se refresca el Sitio?

Se observa otra vez el mensaje emergente "Laboratorio 8!", ya que es un ataque de XSS almacenado, este código malicioso se guarda en la base de datos del servidor y por cada vez que un usuario acceda a esa página, el código se ejecutará, afectando a cualquier usuario que visite la web.

3. Ahora pruebe con el siguiente código **<script>alert(document.cookie)</script>** y Describa el resultado.



Al dar click en sign intentará acceder a las cookies del navegador para el sitio web en cuestión y mostrará su contenido en una ventana emergente, se presenta una alerta con el contenido de una cookie, se analiza que un atacante podría explotar esta vulnerabilidad para robar cookies de sesión, y esto podría llevar a cosas como la toma de control de cuentas de usuario.