MUTILLIDAE SQLi

Version 2.1.19

Dificultad low:

Vamos a la página de MUTILLIDAE y a la sección de SQL Injection de OWASP10 User Info

En el apartado username escribimos el comando admin'-- (y un espacio al final.)
y una contraseña cualquiera.

Dificultad media:

Hacemos lo mismo y nos saldrá el resultado.

Dificultad Alta:

Para la dificultad alta vemos que hacer un simple admin'-- no funciona.
Tendremos que hacer otras técnicas para intentar acceder al usuario admin.

Analizando la página vemos que cuando cambiamos la dificultad de low a hard el boton de "Toggle hints" desaparece.

Para poder verla en la dificultad hard haremos lo siguiente:

Burp Suite

Usamos Burp como proxy entre la página web.

Navegamos hasta la página en cuestión (User info)

Haremos click en "Toggle Hints" y nos saltará una pestaña de Burp.

En ella tendremos que observar los datos a los que hace referencia las hints.

"Cookie: showhints=1; PHPSESSID=63276e7949cb64ee3ba9ed35ddcefcae"

En este caso nos muestra que en la cookie se encuentra showhints=1.

Si cambiamos a la seguridad alta seguramente nos lo marque en 0.

Comprobamos.

"Cookie: showhints=0; PHPSESSID=63276e7949cb64ee3ba9ed35ddcefcae"

Como vemos showhints ahora tiene valor 0, por lo cual no aparece en pantalla.

Solución.

Ponemos la página en dificultad alta y utizamos la consola de DevTools.

y ejecutamos document.cookies
/*

document.cookie
"showhints=0; PHPSESSID=63276e7949cb64ee3ba9ed35ddcefcae"
*/

Introduciremos el siguiente código para habilitar las hints:

document.cookie="showhints=1"

Volvemos a ejecutar el comando document.cookie para ver si se han producido cambios en el showhint.

Si se han hecho ahora deberemos de poder ver el botón Toggle Hint en la dificultad alta.

Para ello tendremos que refrescar la página para que surtan los efectos.

SQLMAP-

Para utilizar SQLMAP en MUTILLIDAE tendremos que hacer lo siguiente:

En una consola de kali ejecutaremos el comando:
sqlmap ="192.168.1.24/mutillidae/index.php page=user-info.php" --current-db

Con el siguiente comando veremos las tablas que contiene nuestra base de datos obtenida:

```
sqlmap -url="http://192.168.1.24/mutillidae/index.php?page=user-info.php&username=joaking&password=12345&user-info-php-submit-button=View+Account+Details" -D owasp10 --tables
```

Obtenemos todos las cuentas de la database con el comando:

```
sqlmap -url="http://192.168.1.24/mutillidae/index.php?page=user-info.php&username=joaking&password=12345&user-info-php-submit-button=View+Account+Details" -D owasp10 -T accounts --dump
```

Usamos --dump para que nos salte los resultados en la consola.

Accedemos como admin en la página gracias al dump.