**¿Qué hacer después de explotar un SQli?**

Esta es una pregunta que me han hecho más de una vez y también hay que reconocer de que muchas veces los papers sobre SQLi explican como explotar la vulnerabilidad pero no van más allá de eso.

Para responder la pregunta, luego de explotar un SQLi, **obviamente hay que reportarlo al administrador del sitio.**

Todos aquellos que tenemos un sitio web, sabemos lo que cuesta mantenerlo y la cantidad de horas que hay que dedicarle para tenerlo activo, destacando también de que hay mucha gente que vive de su sitio web, y es de muy mal gusto que alguien encuentre una vulnerabilidad y la explote, tirando a la basura tanto tiempo dedicado en el sitio. Es por ello que lo más humano sería y lo que yo recomiendo es reportarlo para que esto no ocurra.

Más allá de esto, veremos el daño que se puede hacer explotando esta vulnerabilidad.

Para evitar todo el rodeo de inyectar en la URL, usaré directamente sqlmap para obtener las credenciales. Aún así, acá les dejo el link de uno de los talleres de Underc0de que justamente es para explotar esta falla desde cero:

**Taller de Seguridad Web #2: SQLi desde cero**: You are not allowed to view links. [Register](https://underc0de.org/foro/index.php?action=register) or [Login](https://underc0de.org/foro/index.php?action=login)

Como se puede ver, en la captura, he obtenido las credenciales de una tabla llamada tb\_usuario. Cabe aclarar que en este caso, la password no estaba con ningun tipo de hash, es decir, estaba en texto plano.

El paso siguiente es encontrar un panel para podernos loguear con estas credenciales obtenidas. Para ello debemos utilizar algun tipo de scanner, crawler o panel finder para encontrarlo.

Yo les dejaré dos links que son bastante útiles:

Por un lado este panel finder online: You are not allowed to view links. [Register](https://underc0de.org/foro/index.php?action=register) or [Login](https://underc0de.org/foro/index.php?action=login)

Como se puede ver en la imagen, solo ponemos la URL a analizar y comenzará a probar distintas combinaciones.

Y por otro lado también pueden utilizar un Crawler, el cual recopila todas las URL y paths que tiene el sitio web como por ejemplo este: You are not allowed to view links. [Register](https://underc0de.org/foro/index.php?action=register) or [Login](https://underc0de.org/foro/index.php?action=login)

Es un generador de Sitemaps, pero justamente recolecta todas las urls que tiene el sitio web

Otros tips útiles es ver el robots.txt del sitio, o usar los comodines de Google como por ejemplo “site:sitio.com” y ver todo lo indexado.

Existen miles de herramientas similares, es cuestión de probar y quedarse con la que más cómoda nos resulte.

Una vez ubicado el panel, probaremos las credenciales obtenidas:

Y como podemos ver, pudimos ingresar. Aparentemente como administradores ya que podemos agregar y ver varias cosas dentro del panel.

El paso siguiente será explorar un poco el sitio y ver si logramos encontrar algún uploader para poder subir una shell.

**¿Qué es una Shell?**

Para los que no sepan lo que es una Shell, lo explicaré brevemente diciendo que es un fragmento de código escrito en PHP, JS, Python, Perl, etc que tiene como finalidad “manipular” el sitio web como si fuesemos administradores.

Es decir, podemos descargarnos toda la web, ejecutarle comandos al servidor o incluso borrar todo y subir un index como que el sitio ha sido defaceado. Es un daño muy grande el que se puede hacer con esta falla de seguridad que es el SQLi.

Pueden encontrar una buena cantidad de shells y herramientas en nuestra colección: You are not allowed to view links. [Register](https://underc0de.org/foro/index.php?action=register) or [Login](https://underc0de.org/foro/index.php?action=login)

Para este ejemplo usaré una llamada C99.php que es una muy conocida y que pueden descargar del link que les he dejado.

**Subiendo la Shell**

Explorando el sitio web, me topé con un formulario para agregar “versiones de autos” y que tiene un uploader (Para subir archivos al servidor)

Probaremos completando todo el formulario y subiendo la shell por ese uploader y veremos si verdaderamente lo sube o no.

Completamos todos los datos y damos en guardar y veremos si nos deja subir la shell.

Al parecer todo marcha bien! Hemos podido salvar los cambios sin recibir ningún error diciendo que el archivo subido es inválido ni nada de eso.

lo siguiente será ver en donde quedó subido y si verdaderamente quedó guardado como PHP para poderse ejecutar cuando la abramos.

Volvemos al listado y damos en editar, para saber si tenemos algo extra de información de donde puede estar la shell.

Como se puede ver, en donde dice “Archivo actual” me ha cambiado el nombre de la shell, le ha agregado el img\_2017…. Pero si vemos abajo en la izquierda, lo ha guardado como PHP, esto quiere decir, que si abrimos esa URL, podremos ver la shell.

Y efectivamente ahí esta la shell y todos los archivos listados de la web. Como se puede ver, podemos editarlos, descargarlos, borrarlos, etc.

Tiene opción de hacer brute force al FTP, ver bases de datos, etc.

Con esto ya estaría explotada la falla al 100%, pero como bien dije antes, yo recomiendo reportarlo al administrador, tal como lo hice yo con este sitio web. **El administrador ya fue notificado del fallo y le comenté la gravedad del mismo.**

Espero que les haya gustado a modo educativo y no destructivo.