**# `02` Identification & authentication failures - Broken Authentication**

La autenticación rota es una vulnerabilidad de seguridad crítica que surge cuando las aplicaciones web no gestionan adecuadamente la autenticación de los usuarios. Puede permitir a los atacantes comprometer cuentas, robar credenciales o acceder a información sensible sin autorización.

**## \*\*Formularios de login inseguros\*\***

1. Selecciona la vulnerabilidad **\*\*Broken Authentication/Insecure Login Forms\*\*** y "Hack". Serás redirigido a una vista de formulario donde puedes probar ingresar cualquier dato, pero te dará un mensaje de `Invalid credentials!`.

A close-up of a white background

Description automatically generated

A white square with red text

Description automatically generated

2. Haz clic derecho en la página y selecciona **\*\*Ver código fuente de la página\*\*** en el menú. Esto abrirá una nueva pestaña con el archivo HTML.

3. Localiza el formulario de inicio de sesión y revisa los valores, donde verás que el nombre de usuario es `tonystark` y la contraseña es `I am Iron Man`, lo que inicialmente resulta en un mensaje de "Credenciales inválidas".

A screenshot of a computer code

Description automatically generated

4. Usa estas credenciales (usuario: `tonystark`, contraseña: `I am Iron Man`) si hay un problema de autenticación rota, el sistema te dirá que el usuario ha iniciado sesión con éxito y te mostrará un mensaje.

A white background with black text

Description automatically generated

A close up of a text

Description automatically generated

Las credenciales están incrustadas directamente en el código fuente HTML de la página de inicio de sesión, es una vulnerabilidad importante ya que al visualizar el código fuente, un atacante puede explotar las credenciales incrustadas, acceder al sistema y, potencialmente, obtener acceso no autorizado a información sensible o cuentas de usuario. Esto ilustra cómo una mala implementación de los mecanismos de autenticación puede llevar a brechas de seguridad.

**## Gestión de cierre de sesión.**

1. Selecciona la vulnerabilidad **\*\*Broken Authentication/Logout Management\*\*** y "Hack". Serás redirigido a una vista donde aparece un mensaje que dice **\*\*"Click to Logout"\*\***.

A screenshot of a computer

Description automatically generated

2. Haz click en este mensaje. Te pedirá una confirmación para cerrar sesión.

A close up of a logo

Description automatically generated

Haz clic en `OK` y serás redirigido a un formulario de inicio de sesión, lo que indica que aparentemente has cerrado sesión correctamente.

A screenshot of a computer

Description automatically generated

Sin embargo, si usas la opción de regresar a la página anterior (presionando la flecha de "atrás" en tu navegador), verás que vuelves a la página en la que estabas antes de cerrar sesión, con acceso completo a la cuenta autenticada, lo que demuestra que el cierre de sesión no fue exitoso.

A screenshot of a computer

Description automatically generated

Cuando el sistema no invalida correctamente la sesión del usuario después de cerrar sesión, encontraremos vulnerabilidades críticas; ya que aunque el usuario aparentemente cierra sesión, el servidor no invalida la sesión de manera efectiva y esto expone a los atacantes la posibilidad de acceder a una cuenta sin autorización, especialmente si utiliza un dispositivo compartido donde el usuario anterior no haya cerrado sesión correctamente.