**SecDevOps**

**1. Idea de la aplicación**

Página web para vender productos de ropa. Incluye sección de tienda, portal de usuario y carrito de la compra, pero no el proceso de pago.

También he incluido un formulario de inicio de sesión básico (login.html).

**2. Tecnología de la aplicación**

Esta aplicación web se desarrolla en Visual Studio Code, utilizando lenguajes HTML, CSS y JavaScript.

**3. Vulnerabilidad a subsanar**

La página web redirecciona a una página de login al hacer clic en “portal de usuario”, aceptando todo tipo de redireccionamientos. Spammers y phishers utilizan los redireccionamientos abiertos de un sitio web para redireccionar a los usuarios desde la web original a su página web maliciosa, lo cual supone un problema de seguridad y confianza en los usuarios de tu sitio web.

Esta es la parte de mi código que redirecciona al portal de login.

Existe un botón en la sección de Portal de Usuario que no verifica el redireccionamiento.

Texto

Descripción generada automáticamente

Posteriormente, el botón redirecciona a una URL absoluta e independiente de mi sitio web.

Texto

Descripción generada automáticamente

**4. Vulnerabilidad ya subsanada**

Hay dos maneras de subsanar esta vulnerabilidad.

La primera opción es utilizar URLs relativos. En la sección del portal de usuario se puede incluir un enlace relativo que redirija a la página de inicio de sesión (/login).

**Interfaz de usuario gráfica, Texto

Descripción generada automáticamente**

La segunda opción es validar los redireccionamientos. Antes de redireccionar a una página, se realiza una validación para asegurarse de que la URL de destino es segura y está permitida.

La función esURLSegura verifica si el path de la URL es relativo, es decir, verifica si la URL no empieza con http:// o htpps://. Además, para aumentar la seguridad del sitio web, se puede incluir una lista de paths permitidos, que no permite que el sitio web redireccione a otros paths. Si cumple los requisitos, el sitio web redireccionará a la URL de destino. Si no es así, mostrará una alerta de URL no segura.

**Texto

Descripción generada automáticamente**

Aquí se define la función mostrarMensajeNoSeguro, la cual impide que el usuario entre a la URL de redireccionamiento y muestra por pantalla que el sitio web al que accedes no es seguro.

**Texto

Descripción generada automáticamente**

Si en la constante urlDestino ponemos la url https://www.ejemplo.com/login, el sitio web mostrará un mensaje de error (index2.html).

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**

Si por el contrario, se pone una url relativa, redireccionará a la página de login (index.html).



Interfaz de usuario gráfica

Descripción generada automáticamente

**5. Subida del código a un repositorio de github nuevo (no git101)**

https://github.com/marteag/pag-web

**6. Subida del documento con capturas de pantalla del proceso**

https://github.com/marteag/pag-web