SEGURIDAD, CONTROL Y ACCESO

Autenticación y gestión de sesiones

El software principal administra las cuentas de usuario y la autenticación, y los detalles como la ID de usuario, el nombre y la contraseña se administran en el lado del servidor, así como las cookies de autenticación. Las contraseñas están protegidas en la base de datos utilizando técnicas estándar de salado y estiramiento. Las sesiones existentes se destruyen al cerrar sesión.

Cross Site Scripting (XSS)

Proporciona una variedad de funciones que pueden ayudar a garantizar que los datos proporcionados por el usuario estén seguros. Los usuarios de confianza, es decir, administradores y editores pueden publicar HTML o JavaScript sin filtrar según lo necesiten, como dentro de una publicación o página. Los usuarios no confiables y el contenido enviado por los usuarios se filtra de manera predeterminada para eliminar entidades peligrosas, utilizando la biblioteca KSES.

Exposición de datos sensibles

Las contraseñas de las cuentas de usuario se procesan con sal en base al Marco de Hashing de Contraseña El sistema de permisos se utiliza para controlar el acceso a la información privada, como la PII de los usuarios registrados, las direcciones de correo electrónico de los comentaristas, el contenido publicado de forma privada, etc.

Control de acceso al nivel de función

Se verifica la autorización y los permisos adecuados para cualquier solicitud de acceso a nivel de función antes de ejecutar la acción. El acceso o la visualización de URL administrativas, menús y páginas sin una autenticación adecuada está estrechamente integrado con el sistema de autenticación para evitar el acceso de usuarios no autorizados.

Falsificación de solicitud de sitios cruzados (CSRF)

Se usan tokens criptográficos, llamados nonces13, para validar las solicitudes de intención de acción de los usuarios autorizados para proteger contra posibles amenazas de CSRF.

Contraste de datos en formularios

Los datos se recogen desde la plataforma (donde previamente se han registrado) y al hacer click en el botón de acceso/registro al curso, donde el botón será una url con parámetros del estilo url&Parametro1=valor&Parametro2=valor, la url estará preparada para coger esos parámetros y realizar las validaciones siguientes:

- Al usuario, en registro previo, le aparece un formulario de registro del curso, donde deberá rellenar todos sus datos y su número de colegiado y especialidad. Posteriormente, si cumple con estos requisitos, se le da acceso. Se contrasta si el profesional nuevo que se registra está colegiado en España y es el especialista que se incluye dentro del target de especialistas a los que va dirigido el curso. Si no es así, se procede a denegarle el acceso.
- El campo de la contraseña viene encriptado.