Seguridad de *Cripto-altramuz*

En este apartado se exponen los puntos más relevantes respecto a la seguridad de nuestra web, y distinguiremos entre la seguridad integrada de nuestro gestor de contenido, Wordpress, y otros métodos de seguridad externos.

Respecto a la seguridad integrada de Wordpress, se exponen concretamente 10 puntos entre los que se encuentran la protección contra inyecciones de código, la exposición de datos sensibles y el *Cross Site Scripting*,entre otros:

1. Protección contra inyecciones de código: WP incluye múltiples APIs que se aseguran de sanitarizar todos los datos

2. Rotura de autenticación y manejamiento de sesiones: WP guarda todos los datos de autenticación en el servidor así como las cookies de autenticación. Las contraseñas se guardan cifradas y las sesiones caducan a partir de WP 4

3. Cross Site Scripting: WP se asegura que esto no afecte limitando la ejecución de scripts por los niveles de acceso del usuario. Los administradores y demás pueden ejecutarlos, pero lo que envían los usuarios es filtrado previamente.

4. Referencias directas a objetos inseguros (IDOR): WP utiliza como urls y acceso muchos elementos que podrían ser identificativos, sin embargo, el acceso a cualquiera de los elementos está restringido por su nivel de acceso.

5. Configuración de seguridad: la configuración de seguridad solo la puede realizar el administrador y aun así el núcleo de WP evalúa la configuración y avisa de los peligros.

6. Exposición de datos sensibles: las contraseñas de los usuarios no solo están cifradas sino que utilizan una semilla de cifrado para aumentar el nivel de seguridad de las contraseñas. El sistema de permisos y propietarios de Wordpress hace que solo el propietario de los datos privados, al igual que los posts privados, solo los pueda ver el propietario de los mismos.

7. Falta de petición de permisos: en el caso de que se lance una función o procedimiento de cualquier tipo que solicite acceso a recursos protegidos, primero se comprueba si quien la lanza tiene permiso para hacerlo. Si en la función no se ha añadido la petición de comprobación de permisos, Wordpress rechazará ejecutar la función automáticamente.

8. Cross-Site Request Forgery (CSRF): para evitar que a través de otro sitio se utilice una sesión abierta, o un token de acreditación de acciones, Wordpress usa un sistema de cifrado de tokens donde identifica: quien, como, donde, cuando y que se quiere hacer con ese token y son de un único uso. Así que incluso aunque se robasen, serían de una acción ya realizada y no podrían usarse de nuevo. Además de esto, al acabar la sesión caducan todas las tokens.

9. Componentes con vulnerabilidades conocidas: el equipo del núcleo de Wordpress monitoriza muy de cerca todos los componentes esenciales integrados en Wordpress. Tanto es así que ante vulnerabilidades han colaborado con terceros para solucionar problemas de seguridad que podrían poner en peligro Wordpress o su funcionamiento.

10. Redirecciones no válidas y envíos no deseados: gracias al control interno de acceso de Wordpress no se puede enviar a los usuarios a destinos a los que no tiene acceso, no se pueden hacer tampoco las redirecciones automáticas a destinos a los que no tienen acceso.

Por otro lado tenemos la seguridad externa (seguridad no integrada), dentro de la cual destacan los servicios *captcha* para impedir el acceso a bots que hemos integrado en la página de registro e inicio de sesión usando los servicios de Google reCaptcha.

El servicio de reCaptcha que utilizaremos es reCaptcha v3 de Google. Este servicio funciona analizando el comportamiento del usuario en nuestra web y asignando puntuación a cada una de las acciones. Las acciones “naturales” obtienen puntuación positiva y las acciones “automatizadas” obtienen puntuación negativa.

Dependiendo de la puntuación, reCaptcha tomará diferentes medidas. En caso de puntuación alta, reCaptcha será completamente transparente al usuario y no requerirá de ningún paso adicional.

En el caso de que la puntuación sea baja, requerirá que el usuario resuelva dos puzles captcha de Google.

En casos de puntuación negativa, reCaptcha bloqueará los botones de redes sociales, requerirá solucionar dos puzles captcha de Google, un email y confirmación de email para poder continuar con la acción.