VULNERABILIDADES Y RECOMENDACIONES

Vulnerabilidad Nº1

- **SQL INYECTION**: Estos ataques hacen uso de los métodos *GET* y *POST* para alterar y/o borrar nuestra información de las bases de datos mediante la introducción instrucciones en Lenguaje SQL.

Vulnerabilidad Nº2

- **XSS o Cross Site Scripting:** Estos ataques también hacen uso de los métodos *GET* y *POST* para alterar nuestra información mediante la introducción de código *PHP* o *JavaScript*.

Vulnerabilidad Nº3

- **Robots / XSF (Ataques de fuerza bruta / Cross Site Forgery):** El objetivo de estos ataques es acceder a los sitios registrados y sensibles de la aplicación o sitio web a través del uso de distintas combinaciones de las contraseñas

Vulnerabilidad Nº4

- **Defectos en Cross-Site Scripting (XSS):** Mostrar información de fuentes exteriores sin haberla filtrado antes.

  RECOMENDACIÓN

  Herramientas para filtrar la información.

  ```
  htmlspecialchars().
  strtr().
  strip_tags().
  utf8_decode()
  ```

Vulnerabilidad Nº5

- **Problemas de la gestión del error:** Los mensajes de error no deben contener ninguna información descriptiva del sistema.

  RECOMENDACIÓN

  Configura PHP para poner los mensajes de error en el registro de errores de tu servidor en vez de mostrarlos:

  ```
  log_errors = On
  display_errors = Off
  ```

RECOMENDACIONES:

1. Restringir el acceso a carpetas y archivos sensibles de nuestra aplicación haciendo uso del archivo *.htaccess*.
2. Validar datos de los formularios antes que estos se envíen al servidor.
3. Para evitar los ataques de fuerza bruta XFS
    - Encriptar las contraseñas.
    - Restringir la cantidad de intentos permitidos para acceder a zona restringida con Usuario-Password.
    - Introducir '*captchas*' a los formularios

4. Validar la información una vez que esta se encuentra en el servidor.
5. Crear copias de seguridad (*Backup*) de todo nuestro código de programación.
6. Crear *Backups* periódicos de nuestras BBDD

FUENTES:

http://blog.escuelactec.com/seguridad-informatica-en-php/

http://www.tufuncion.com/5_vulnerabilidades

https://www.capitanseo.es/2011/04/seguridad-web-formularios-web-y-urls-parte-1/