|  |
| --- |
| Redes populares |
| Activistas en Red |
| Vulnerabilidades de seguridad |

|  |
| --- |
| Alejandro Sanchez  02/09/2009 |

**Vulnerabilidades encontradas**

1) Hay un ataque llamado “SQL Injection”, se trata introducir frases especiales en los campos los formularios tales como nombre de usuario, contraseña, etc. Estas frases son interpretadas por el servidor como sentencias de código lo que permite al hacker ejecutar código propio dentro del servidor web, logrando por ejemplo, que ignore las validaciones de verificación de usuario, lo que le permitiría entrar al sistema sin necesidad de autenticación.

Si colocas la siguiente dirección podrás ver que estoy en el área de miembros sin haber colocado mi email y mi contraseña.  
  
[http://activistasenred.com/verif/miembro/home.php?enc=si&log=a1e60f8a&user=%27%20or%200=0%20#](http://activistasenred.com/verif/miembro/home.php?enc=si&log=a1e60f8a&user=%27%20or%200=0%20)

Otros ejemplos de inyección de código permitirían de manera muy fácil eliminar todas las tablas de la base de datos, eliminar la data, etc.

**Soluciones**

Una validación exhausta de la información introducida por el usuario, la aplicación de store procedures, hibérnate y/o la utilización de la función [**mysql\_escape\_string**](http://www.php-es.com/function.mysql-escape-string.html) antes de utilizar los datos dentro del código.

En esta página encuentras mas información al respecto: <http://www.governmentsecurity.org/SQLinjectionBasicTutorial> o en el siguiente video sencillo <http://www.youtube.com/watch?v=dDQ8oXWt58w>

**2)** Puedo leer una noticia que estaba restringida para miembros, quitando 'verif/miembro'

http://www.activistasenred.com/verif/miembro/noti\_des.php?id\_noti=56

Si intentas poner esta dirección de esta noticia en tu navegador, te va a decir que debes registrarte, ósea, de acceso restringido. Pero si remueves la parte que dice 'verif/miembro' entonces ya vas a poder leerla perfectamente.

**Solución**

Implementación de variables de sesión dentro del sistema para controlar el acceso a las páginas privadas. De esta manera el hacker no tiene acceso a los datos que se utilizan para bloquear una noticia.

**3)** La evolución de los ataques de internet ha dado cabida a un nuevo tipo de ataque donde unos robots especiales se hacen pasar por humanos y llenan los formularios web de manera masiva alrededor del mundo. Para evitar esto la comunidad web ha desarrollado un concepto llamado “CAPTCHA” donde se le pregunta al usuario que interprete las figuras que ve en una imagen mostrada, de esta manera se verifica que es realmente humano dada la inferior capacidad para la interpretación de imágenes que tienen las computadoras hoy en día.

El formulario de registro de la página no tiene captcha, es decir, me puedo registrar mil veces con un robot, además con cualquier IP. Eso podría generar registros masivos de una manera muy sencilla, ataques de denegación de servicio similares a los ocurridos en twitter en los días anteriores, explosión de usuarios en la base de datos, etc.

Lo mismo ocurre en el proceso de login, puedo intentar registrarme cientos de veces probando diferentes combinaciones hasta lograr entrar. Este tipo de ataque es llamado diccionario o fuerza bruta.

**4) Puedo realizar transacciones simulando cualquier IP**

<form method="POST" action="enviador.php">

<p>

<input type="hidden" name="nombre" size="19" value="Alejandro Sanchez">

<input type="hidden" name="email" size="19" value="alesanchezr@hotmail.com">

<input type="hidden" name="ip" value="190.200.6.213" />

Contáctanos<br>

<textarea rows="9" name="mensaje" cols="50"></textarea>

<br>

Escribe el código de seguridad

<br>

<img src="captcha.php" /><input type="text" name="CAPTCHA" style="width: 50px;" />

<p style="padding-top: 5px;">

<input type="submit" value="Enviar" name="Enviar">

</form>

Si verificas este formulario web, puedes ver que la dirección IP del usuario se envía como un campo más del formulario, es decir, yo lo puedo modificar de manera muy sencilla y suplantar mi identidad a otra IP que yo quiera. Incluso hay un programa llamado **firebug** que te permite hacer estas modificaciones mientras estas visualizando la página en el navegador. La detección del IP del usuario debería hacerse del lado del servidor para que el cliente no tenga acceso. TODOS los formularios de la página tienen el IP del lado del cliente, es decir, modificable.

**Solución**

Obtener el IP del cliente del lado del servidor y justo antes de registrarlo en la base de datos. De esta manera el hacker no tiene acceso a los datos.

**5) Sobre exposición de información**

Si analizamos la barra de dirección del navegador podemos obtener demasiada información de manera sencilla, por ejemplo:

<http://activistasenred.com/verif/miembro/home.php?enc=si&log=f6b8a265&user=ef4b1d94b5&verific=pass&md5=9gndbwufbgfiendcjfidncifoencfjfri>

En este caso podemos conocer por ejemplo, que el id del usuario actual es ef4b1d94b5 y la clave encarapitada es “*9gndbwufbgfiendcjfidncifoencfjfri*”. Faltaría empezar a descifrar esa clave con algún servidor o programa especializado.

**Solución**

Replantear la transferencia de información entre las páginas dejando la menor cantidad de información útil para el hacker en el URL de la página. Se puede plantear pasar las variables por sesión y por POST.

6) **Utilización de MD5:**

La utilización de md5 ha dejado de utilizarse dentro del mundo de seguridad informática. No sólo por que utiliza claves más pequeñas que sha1. Sino porque al ser, durante muchos años el más implementado, en la mayoría de aplicaciones web y de otros ámbitos las contraseñas podría estar comprometidas.

**Solucion**

Utilización de sha1 de 128 bits.