SEGURIDAD DEL SITIO WEB

La seguridad eficaz de sitios web requiere de esfuerzos de diseño a lo largo de todo el sitio web: en la aplicación web, en la configuración del servidor web, en las políticas para crear y renovar contraseñas, y en el código del lado cliente. Aunque lo anterior podría sonar inquietante, la buena noticia es que si está usando un framework web de lado servidor, es casi seguro que habilitará por defecto mecanismos de defensa robustos y bien pensados contra gran cantidad de los ataques más comunes. Otros ataques pueden mitigarse por medio de la configuración de su servidor web, por ejemplo habilitando HTTPS. Finalmente, hay herramientas de escaneo de vulnerabilidades disponibles públicamente que pueden ayudarle a saber si ha cometido algún error obvio.

Amenazas contra la seguridad de sitios web. Las amenazas tienen éxito cuando la aplicación web, ¡o confía o no es lo suficientemente acerca de los datos que vienen del explorador web!

CROSS-SITE SCRIPTING (XSS)

XSS es un tipo de ataque que permite inyectar scripts de lado cliente, a través del sitio web, hasta los exploradores de otros usuarios. Las vulnerabilidades XSS han sido históricamente más comunes que las de cualquier otro tipo.

La mejor defensa contra las vulnerabilidades XSS es eliminar o deshabilitar cualquier etiqueta que pueda contener instrucciones para ejecutar código. En el caso del HTML ésto incluye etiquetas como <script>, <object>, <embed>, y <link>.

INYECCIÓN SQL

Las vulnerabilidades de Inyección SQL habilitan que usuarios maliciosos ejecuten código SQL arbitrario en una base de datos, permitiendo que se pueda acceder a los datos, se puedan modificar o borrar, independientemente de los permisos del usuario. La manera de evitar esta clase de ataque es asegurar que cualquier dato de usuario que se pasa a un query SQL no puede cambiar la naturaleza del mismo. Una forma de hacer ésto es eludir ('escape') todos los caracteres en la entrada de usuario que tengan un significado especial en SQL.

UCR

CROSS SITE REQUEST FORGERY (CSRF)

Los ataques de CSRF permiten que un usuario malicioso ejecute acciones usando las credenciales de otro usuario sin el conocimiento o consentimiento de éste. . El explorador del usuario almacena esta información, y la incluye automáticamente en todas las peticiones al servidor asociado.

Una manera de prevenir este tipo de ataque por parte del servidor es requerir que la petición POST incluya una palabra secreta específica del usuario generada por el sitio (la palabra secreta podría proporcionarla el servidor cuando envía el formulario web que se usa para hacer transferencias).

OTROS ATAQUES/VULNERABILIDADES INCLUYEN:

- **CLICKJACKING** El usuario malicioso secuestra las pulsaciones de ratón dirigidas a un sitio visible por encima de los demás y las redirige a una página escondida por debajo. Como defensa, tu sitio puede protegerse de ser embebido en un iframe de otro sitio configurando las cabeceras HTTP apropiadamente.

- **DENEGACIÓN DE SERVICIO**, (Denial of Service, DoS) se consigue normalmente inundando el sitio objetivo con peticiones espúreas de manera que se interrumpa el acceso a los usuarios legítimos. Las defensas contra DoS normalmente trabajan mediante la identificación y el bloqueo de tráfico "malo" permitiendo sin embargo que atraviesen los mensajes legítimos.

- **SALTO DE DIRECTORIOS/REVELACIÓN DE FICHEROS** En este tipo de ataque un usuario malicioso intenta acceder a partes del sistema de ficheros del servidor web a los que no debería tener acceso.. La solución es desinfectar la entrada antes de usarla.

- **INCLUSIÓN DE FICHEROS** En este ataque un usuario es capaz de especificar, para mostrar o ejecutar, un fichero "no intencionado para ello" en los datos que le pasa al servidor. La solución es desinfectar la entrada antes de usarla.

- **INYECCIÓN DE COMANDOS** Los ataques de inyección de comandos permiten a un usuario malicioso ejecutar comandos del sistema arbitrarios en el sistema operativo del host. La solución es desinfectar la entrada de usuario antes de que pueda ser usada en llamadas al sistema.

  Para un listado completo de amenazas, ver Category:Web security exploits (Wikipedia) y Category:Attack (Open Web Application Security Project).

central 2511-1800
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
CI
Centro de **Informática**