Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico Matemáticas

Licenciatura en Seguridad en Tecnologías de Información

Diseño Orientado a Objetos

Maestro: Miguel Salazar

Ensayo: riesgos/vulnerabilidades

Nombre: Daniel de la Rosa Rodríguez

Matrícula: 1666385

4 de septiembre de 2017, Cd. Universitaria, San Nicolás de los Garza, Nuevo León

El ***Cross Site Scripting (XSS)*** o ejecución de comandos en sitios cruzados es una de las vulnerabilidades más habituales.

Tiene la funcionalidad que los atacantes explotan la confianza del usuario que le tiene a un sitio web. Esta puede ser explotada de dos maneras:

- Reflejada: consiste en modificar los valores del sitio web para pasar variables entre dos páginas. El atacante podría robar las cookies para luego robar la identidad del usuario, para esto se necesita que la víctima ejecute un determinado comando dentro del sitio web. Para esto se usa phishing, ya sea en correos o algún otro medio, para que este parezca fidedigno y la victima pueda caer.
- Almacenada: esta consiste en inserta un código HTML peligroso en sitios que lo permitan; de esta forma la información de los usuarios será visible y podrá ser modificada.

Para evitar esto se debe tener con soluciones de seguridad instaladas y actualizadas para que estas bloqueen automáticamente el malware o exploits. Además de que detecta phishing con antivirus y bloquea esto de los navegadores.

Es importante mirar la URL del sitio al que ingresas, pues puede haber redirecciones de páginas fidedignas, tal como lo es el phishing.

Una recomendación es usar navegadores alternativos que no sean tan populares, de esta manera los atacantes están forzados a saber las vulnerabilidades de este navegador que no es tan conocido

De este modo, para los desarrolladores de sitios web es un gran reto, pues se necesita saber del tema para poder evitarlo en sus proyectos. Para esto es recomendable repasar cuidadosamente el código que hay detrás del sitio y verificar si no es vulnerable a este tipo de ataques. Se podrían hacer tests de seguridad antes de lanzar la página y tener el menor riesgo posible.

Y para el usuario es recomendable verificar bien los sitios en donde se navega, pues puede haber en cualquiera de estos. También verificar el URL de la página para así darse una idea si es fidedigna o no. Pues si algo está fuera de lo común dentro de los sitios que son frecuentes puede que seas víctima de estos ataques.