UNIVERSIDAD LATINA DE COSTA RICA
LAUREATE INTERNATIONAL UNIVERSITIES®

Facultad de Tecnologías de la Información y Comunicación.

Escuela de Ingeniería de Sistemas Informáticos.

# Tipos de ataquen en código EJECT y XSS.

Programación III (BSI-090).

Profesor: Lic. Jorge Isaac Vásquez Valenciano.

Estudiante: Anthony Quirós Alfaro.

(20160111305).

Universidad Latina San Pedro.

25 mayo de 2018.

Índice

# Ataque en código XSS:

El Cross Site Scripting o XSS es un tipo de ciberataque por el cual se buscan vulnerabilidades en una aplicación web para introducir un script dañino y atacar su propio sistema. Los scripts son archivos de comandos o programas escritos en lenguajes de programación −como JavaScript− que se ejecutan en el navegador web. En su versión más inocua se ejecutan ventanas emergentes y, en el peor de los casos, son utilizados por atacantes para acceder a información sensible o al equipo del usuario. Siempre que una aplicación web transfiera datos de usuario no validados al navegador, habrá riesgo de un ataque por Cross Site Scripting o XSS, ya que este es el camino por el que los archivos dañinos van a parar al cliente o navegador. Una vez aquí, las aplicaciones infectadas manipulan scripts propios de la página tales como formularios de registro y, mientras que para el usuario todo indica que se trata de una página protegida, en realidad los datos están siendo transferidos a otro sitio sin ningún tipo de filtro. Pero no todos los ataques de XSS tienen como objetivo robar información privada o dañar al cliente afectado. Hay scripts muy extendidos que manipulan al cliente para convertirlo en iniciador de tácticas de phishing y de ataques de malware, o que cambian el contenido de una página afectándolo negativamente. Los causantes del ataque permanecen la mayor parte de las veces en el anonimato.

## Ataque en código Eject:

Consiste en la inserción de código SQL por medio de los datos de entrada desde la parte del cliente hacia la aplicación. Es decir, por medio de la inserción de este código el atacante puede modificar las consultar originales que debe realizar la aplicación y ejecutar otras totalmente distintas con la intención de acceder a la herramienta, obtener información de alguna de las tablas o borrar los datos almacenados, entre otras muchas cosas. Como consecuencias de estos ataques y dependiendo de los privilegios que tenga el usuario de la base de datos bajo el que se ejecutan las consultas, se podría acceder no sólo a las tablas relacionadas con la aplicación, sino también a otras tablas pertenecientes a otras bases de datos alojadas en ese mismo servidor. Lo comentado anteriormente es posible gracias a que el uso de ciertos caracteres en los campos de entrada de información por parte del usuario, ya sea mediante el uso de los campos de los formularios que son enviados al servidor mediante POST o bien por medio de los datos enviados mediante GET en las urls de las páginas web, posibilitan coordinar varias consultas SQL o ignorar el resto de la consulta, permitiendo al hacker ejecutar la consulta que elija, de ahí que sea necesario realizar un filtrado de esos datos enviados para evitar problemas.