# Tema: Websites Input Validation and Input Misuse Based Attacks

## Síntesis:

Las aplicaciones WEB tienen un peso muy importante en nuestra forma de vida hoy en día, ya que de ellas dependen muchas cosas de nuestro día a día, por lo que estas deben estar necesariamente verificadas y protegidas. En este artículo se nos muestra como es que la mala validación en la entrada de datos en una página web puede causar graves daños, y hoy en día el índice de actos ilícitos es bastante mayor debido a que hay más piratas informáticos que están a la orden del día descubriendo nuevas vulnerabilidades.

Desde una perspectiva de seguridad, la validación de la entrada del usuario también es importante. Los usuarios pueden, intencional o involuntariamente, ingresar valores de entrada incorrectos si se ejecutan o procesan en las bases de datos de back-end y causarán graves problemas o intrusiones, por lo cual es importante dar a entender que el desarrollador de la página web debe tener muy buenas prácticas de programación, además de realizar las pruebas para evitar que su sistema se vuelva vulnerable.

Un ataque muy popular hacia las bases de datos de las páginas web es la **inyección SQL**, en la cual los atacantes intentan manipular el texto de entrada que puede romper los procedimientos de SQL y acceder a bases de datos en el back-end. Se requieren de declaraciones SQL diseñadas que permitan exponer información relacionada con la base de datos; por ejemplo, tablas, nombres de columnas, etc. La inyección de SQL se puede utilizar para la **exposición de datos o la corrupción de datos.**

Las técnicas que se nos mencionan para mitigar este enorme problema son la **ejecución simbólica** y las **pruebas de mutación**, estas tienen por objetivo general evaluar las vulnerabilidades de sitios web, con el fin de saber si sí son vulnerables o no. Cabe mencionar que no todas las vulnerabilidades provienen del mismo sitio, sino que pueden venir de enlaces externos, por ejemplo tener en una página web el enlace a un sitio de un tercero, y este sea vulnerable a los ataques, esto generaría una puerta trasera para ingresar al sitio principal, por eso es necesario tener en cuenta esta información para poder implementar técnicas de mitigación lo más posible.

Referencia: Alsmadi, I., Alazzam, I., “Websites Input Validation and Input Misuse Based Attacks”, Cybersecurity and Cyberforensics Conference CPS, 2016, pp. 113 - 116