



El futuro digital  
es de todos

MinTIC



UNIVERSIDAD  
EL BOSQUE

Mision  
TIC2022

Ciclo 4A

## Semana 5

*Seguridad en aplicaciones Web y bases de datos NO-SQL*

Lectura 1 - Amenazas de seguridad a aplicaciones Web

## Amenazas de seguridad a aplicaciones Web


Los múltiples ataques a servidores y aplicaciones en Internet constituyen el día a día de muchas organizaciones alrededor del mundo, las cuales deben invertir una importante cantidad de recursos financieros, humanos, logísticos y técnicos para tareas de ciberseguridad.

La seguridad de una aplicación Web ha de abordarse desde múltiples aspectos, a saber:

- **Disponibilidad:** Asegurar que los clientes de la aplicación tengan acceso cuando así lo requieran.
- **Autenticidad:** Asegurar que tanto los clientes como los servidores involucrados en una transacción sean quienes dicen ser y no un caso de suplantación.
- **Integridad:** Asegurar que la información almacenada e intercambiada por las aplicaciones no ha sido indebidamente alterada.
- **Confidencialidad:** Asegurar que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Trazabilidad:** Asegurar que se cuenta con toda la información real sobre quién o qué exactamente realizó algún tipo de operación sobre los datos o componente de un sistema.

Cada uno de los aspectos mencionados antes, puede ser atacado a través de múltiples técnicas usadas por los ciberdelincuentes, o incluso, pueden fallar sin que necesariamente se trate de un ataque, sino tal vez un error o descuido en el desarrollo. A continuación, se relacionan algunas de las amenazas más conocidas:

- **Ataque de secuencia de comandos en sitios cruzados o Cross-site scripting – XSS**




Esta técnica le permite al atacante inyectar código HTML y JavaScript en las páginas Web visitadas por la víctima. Este código le permitirá robar información delicada, secuestrar sesiones de usuario y comprometer el navegador. Para el ataque, pueden utilizarse etiquetas `<iframe>` o `<script>`.



## Semana 5

Seguridad en aplicaciones Web  
y bases de datos No-SQL

## • Ataque de Inyección SQL



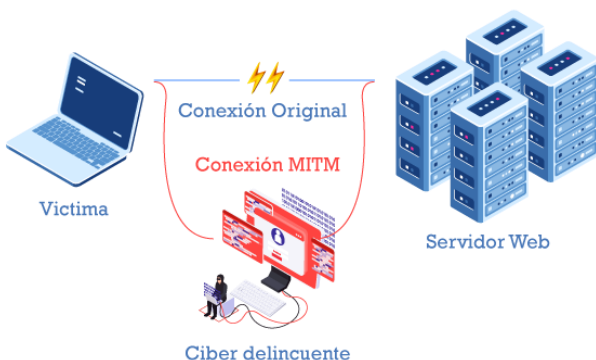
La inyección SQL es la colocación de código malicioso en declaraciones SQL, a través de la entrada de una página web. La inyección de SQL generalmente ocurre cuando se le pide a un usuario una entrada, como su nombre de usuario, y en lugar de un nombre, el atacante le da una instrucción SQL que, sin saberlo, se ejecutará en la base de datos.

## • Ataque de denegación de servicio



Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. La forma más común consiste en “inundar” el sitio Web con un gran número de peticiones, hasta que el servidor agote sus recursos y no pueda atender más peticiones.

## • Ataque de hombre en el medio




El ataque de MITM por sus siglas en inglés (Man in the middle), consiste en intervenir la comunicación que establecen dos partes entre ellas, sin que éstas puedan percibir la intromisión, el atacante puede estar ubicado de forma física o lógica. Como medidas preventivas para este tipo de ataque se recomienda a los usuarios el empleo de claves públicas de cifrado, cifrado de la información, uso de certificados y firmas digitales.

Semana 5

Seguridad en aplicaciones Web  
y bases de datos No-SQL

- Falsificación de Petición en Sitios Cruzados (CSRF)




CSRF

Cookie

CSRF (falsificación de petición en sitios cruzados) es una vulnerabilidad en un sitio web que permite a los atacantes forzar a las víctimas a ejecutar acciones sensibles en el sitio sin su conocimiento. Al igual que en XSS, CSRF está en capacidad de abusar de conexiones confiables. En CSRF el servidor ejecuta acciones sensibles porque este contenido fue enviado por un cliente que en el que servidor confía.

- Pérdida de la autenticación



Ocurre cuando las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).