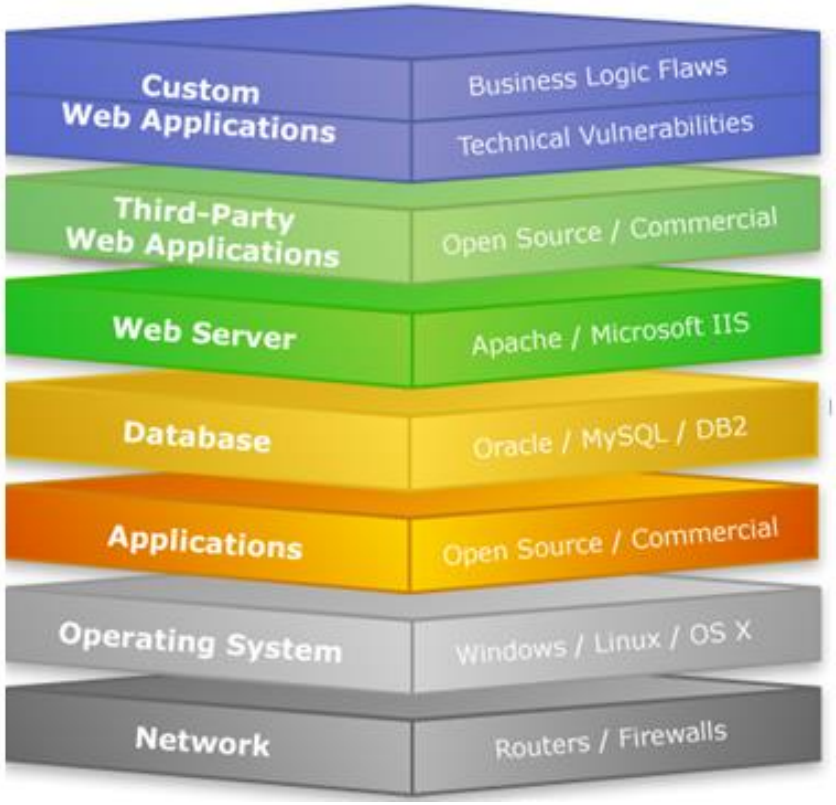
Ataques más comunes

CY-203 Hackeo Ético

fidélitas
Universidad

Servidores Web y sus tipos de ataques

Los sitios *web* están alojados en servidores *web*. Los servidores *web* son en sí mismos computadoras que ejecutan un sistema operativo; conectado a la base de datos *back-end*, ejecutando varias aplicaciones. Cualquier vulnerabilidad en las aplicaciones, Base de Datos, Sistema Operativo o en la red dará lugar a un ataque al servidor *web*. La pila de vulnerabilidades de un servidor *web* se proporciona a continuación.



Inyección SQL

SQL fue desarrollado en la década de 1970, es un lenguaje de consulta estructurado (*structured query language*), que se ha transformado en el lenguaje estándar para la gestión de base de datos.

Cuando un sitio web requiere acceder a la base de datos que tiene en su servidor para buscar o editar información, emplea SQL para procesar esa consulta o solicitud.

La inyección SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio de un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, toma control de la base de datos del sitio web y secuestra la información de los usuarios.

fidélitas
Universidad

Inyección SQL

Si un desarrollador web no está pendiente, al crear un sitio podría dejar una vulnerabilidad. Alguien con malas intenciones podría utilizarla para provocar efectos inesperados en sus bases de datos.

Las inyecciones de SQL se producen cuando el hacker introduce o inyecta en el sitio web código SQL malicioso, un tipo de *malware* que se conoce como la carga útil, de esta manera enviando su código a su base de datos como si de una consulta autentica se tratara.

Los hackers recurren a los ataques de inyección SQL con la finalidad de acceder a la base de datos de un sitio web. En ocasiones buscan editar la base de datos, generalmente en el caso de sitios web financieros.

fidélitas
Universidad

Efectos de la Inyección SQL

Los hackers recurren a los ataques de inyección de SQL, con la finalidad de introducirse a la base de datos de un sitio web. Buscan editar la base de datos, especialmente en el caso de sitios web financieros. En el instante en el que el hacker ha logrado el control de la base de datos, ya es posible interferir en los saldos de las cuentas de los clientes y enviar dinero a su propia cuenta.

Sin embargo, lo que el ciberdelincuente busca son los datos de usuario guardados en el sitio web, como credenciales de inicio de sesión.

Estos datos de inicio de sesión robados pueden emplearlos para realizar acciones en nombre de los usuarios afectados o reunirlos en una gran lista que luego venderán a otros ciberdelincuentes en la oscura red.

¿Cómo se produce un ataque de Inyección SQL?

Si un sitio *web* no toma las precauciones para asegurar la introducción de datos, un *hacker* puede inyectar el código malicioso que quiera. De esta manera, el sitio *web* envía el código del *hacker* (la carga útil) a su servidor. Cuando llega a la base de datos del sitio *web* ubicada en su servidor, la carga útil del *hacker* entra en acción e interfiere en la base de datos, de esta manera el *hacker* cumple su objetivo.

Debido a que son relativamente fáciles de implementar y que la posible recompensa es grande, los ataques de inyección de SQL son comunes. Las estadísticas varían, pero se estima que los ataques de inyección de SQL constituyen la mayoría de los ataques en las aplicaciones de software. Según el Open Web Application Security Project (Proyecto abierto de seguridad de aplicaciones web), los ataques de inyección, que incluyen las inyecciones de SQL, fueron el tercer riesgo de seguridad más grave en las aplicaciones web en 2021.

fidélitas
Universidad

Ejemplo de ataque de Inyección SQL

Puede editar un email de una cuenta de usuario:

```
Y'; UPDATE table SET email = 'atacante@ejemplo.com' WHERE email =
'usuario@ejemplo.com';
```

Después de la Y hay una comilla y un punto y coma, lo que permite al atacante cerrar la sentencia y ejecutar otra.

fidélitas
Universidad

Impacto de los ataques de Inyección SQL

Exponer datos sensibles

Los atacantes pueden extraer datos, lo que pone en riesgo la exposición de datos sensibles almacenados en el servidor SQL

Comprometer la integridad de los datos

Los atacantes pueden alterar o eliminar información del sistema

Comprometer la privacidad de usuarios

En función de los datos almacenados en el servidor SQL, un ataque puede exponer información sensible del usuario, como direcciones, números de teléfonos y detalles de tarjetas de crédito.

fidélitas
Universidad

Impacto de los ataques de Inyección SQL

Otorgar acceso de administrador

Si un usuario de la base de datos tiene privilegios de administrador, un atacante puede acceder al sistema a través de un código malicioso.

Otorgar acceso general

Si usa comandos SQL débiles para verificar nombres de usuario y contraseñas, un atacante podría acceder a su sistema sin conocer las credenciales del usuario y causar problemas al acceder a información sensible y manipularla.

fidélitas
Universidad

Tipos de inyección SQL

Según la forma de acceso a los datos de *backend* y la extensión del posible daño provocado, las inyecciones de SQL se pueden dividir en las siguientes tres categorías:

- **SQL en banda:** este tipo de ataque SQL es sencillo para los atacantes, porque usan el mismo canal de comunicación para lanzar ataques y obtener resultados. Este tipo de ataque SQL tiene dos subvariantes:
  - ✓ **SQL basado en errores:** la base de datos genera un mensaje de error por las acciones del atacante. El atacante obtiene información sobre la infraestructura de la base de datos en función de los datos que generaron estos mensajes de error.
  - ✓ **SQL basado en unión:** el atacante usa el operador *UNION* SQL para obtener los datos deseados mediante la fusión de varias declaraciones *Select* en una única respuesta *HTTP*.

fidélitas
Universidad

Tipos de inyección SQL

- **SQL inferencial (también conocida como inyección de SQL ciega):** En este tipo de SQL, los atacantes usan patrones de respuesta y comportamiento del servidor después de enviar cargas útiles de datos para obtener más información sobre su estructura. Los datos no se transfieren de la base de datos del sitio web al atacante, así que el atacante no ve la información sobre el ataque en banda (por eso se usa el término "SQL ciega"). La SQL inferencial se puede clasificar en dos subtipos:
  - ✓ **SQL basado en el tiempo**: los atacantes envían una consulta de SQL a la base de datos, esto hace que la base de datos espere unos segundos antes de responder si la consulta es verdadera o falsa.
  - ✓ **SQL booleana:** los atacantes envían una consulta de SQL a la base de datos, así permiten que la aplicación responda mediante la generación de un resultado verdadero o falso.

fidélitas
Universidad

Tipos de inyección SQL

- **SQL fuera de banda:** Este tipo de ataque de SQL se puede llevar a cabo en las siguientes dos situaciones:
  - ✓ Cuando los atacantes no pueden usar el mismo canal para lanzar el ataque y compartir información.
  - ✓ Cuando un servidor es demasiado lento o inestable para realizar estas acciones.

¿Cómo prevenir los ataques de inyección de SQL?

Para las empresas interesadas en la prevención de la inyección de SQL, los principios clave para ayudar a proteger los sitios y las aplicaciones *web* son los siguientes:

- **Capacitar al personal:** Concientizar al equipo responsable de la aplicación *web* sobre los riesgos relacionados con la SQLi y brindar la capacitación necesaria para todos los usuarios en función del puesto
- **Mantener el control de la entrada de usuarios:** Cualquier entrada de usuario utilizada en una consulta de SQL genera un riesgo. Aborda las entradas de los usuarios autenticados o internos de la misma manera que las entradas públicas hasta que se verifiquen. Otórgales a las cuentas que se conectan a la base de datos SQL solo los privilegios mínimos necesarios. Utilice listas blancas como práctica estándar en lugar de listas negras para verificar y filtre la entrada de los usuarios.

fidélitas
Universidad

¿Cómo prevenir los ataques de inyección de SQL?

- **Utilizar las versiones más recientes:** Es importante usar la versión más reciente del entorno de desarrollo para maximizar la protección, ya que es posible que a las versiones anteriores les falten funciones de seguridad. Asegúrese de instalar el *software* y los parches de seguridad más recientes cuando estén disponibles.
- **Analizar de forma continua las aplicaciones web:** Use herramientas integrales de administración del rendimiento de las aplicaciones. Analizar regularmente las aplicaciones *web* permite identificar y abordar posibles vulnerabilidades antes de que provoquen daños graves.
- **Usar un firewall:** El *firewall* de una aplicación *web* (WAF) a menudo se usa para filtrar SQLi, así como otras amenazas en línea. Un WAF confía utiliza una extensa lista de firmas que se actualiza con frecuencia y le permite filtrar consultas de SQL maliciosas. Por lo general, la lista tiene firmas para abordar vectores de ataque específicos y se corrige con regularidad en respuesta a vulnerabilidades recientemente descubiertas.

fidélitas
Universidad

Casos reales de vulnerabilidades

- ***Fornite***, 2019: *Fornite* es un juego en línea con más de 350 millones de usuarios. En 2019, se descubrió una vulnerabilidad de inyección de SQL que les permitía a los atacantes acceder a las cuentas de los usuarios. La vulnerabilidad se corrigió.
- ***Cisco***, en 2018, se encontró una vulnerabilidad de inyección de SQL en *Cisco Prime License Manager*. La vulnerabilidad permitía que los atacantes tuvieran acceso *shell* a los sistemas en los que estaba implementado el administrador de licencias. Cisco ya corrigió la vulnerabilidad.
- ***Tesla***, 2014, investigadores de seguridad anunciaron que podían quebrantar el sitio *web* de *Tesla* con una inyección de SQL, lo que les permitiría obtener privilegios de administrador y robar datos de los usuarios en el proceso.

fidélitas
Universidad

¡Gracias!

fidélitas
Universidad