



[academy](#)

>Cerrar

[Para el hogar](#) Para el hogar Productos para la protección de PC y teléfonos móviles

[Para empresas](#) Para empresas Proteja su negocio con Avast

[Para socios](#) Para socios Asóciase con Avast e impulse su negocio

[Quiénes somos](#) Quiénes somos Carreras, inversores, medios, contacto

Blogs Academia, Blog, Decoded, Foro



España

Avast Academy > Seguridad > Hackeo > ¿Qué es la inyección de SQL y cómo funciona?



HACKEO

¿Qué es la inyección de SQL y cómo funciona?

La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios. Le explicamos cómo funcionan los ataques de inyección de SQL, cómo combatirlos y cómo una herramienta antivirus potente lo puede

proteger contra las consecuencias.



2022
**Avanzado en la Prueba
Wild Malware Test**



2022
**Producto Mejor
Valorado**



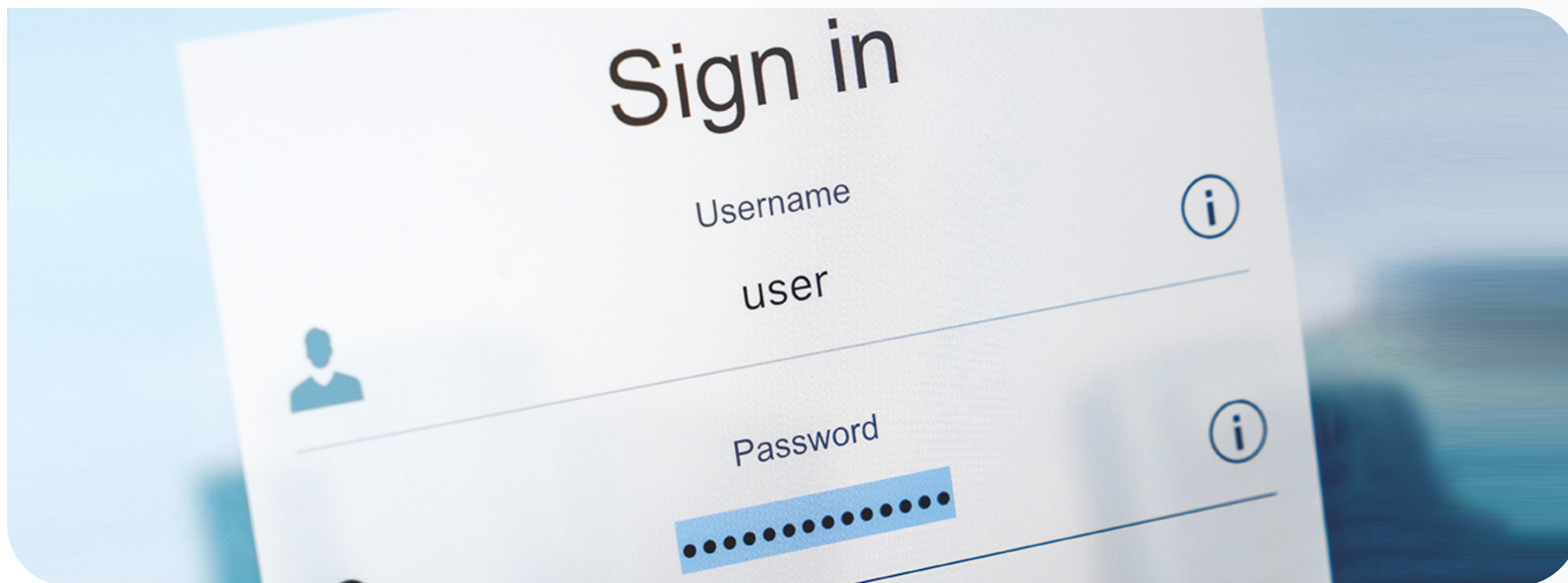
2022
**La Mejor
Protección**

Muy bueno



13.480 opiniones en

★ Trustpilot





Escrito por [Ivan Belcic](#)

Fecha de publicación septiembre 22, 2020

¿Qué es la inyección de SQL? ¿Y qué es el SQL?

Antes de empezar a hablar de la inyección, primero vamos a aclarar qué significa SQL. El SQL, desarrollado en la década de 1970, es un lenguaje de consulta estructurado («Structured Query Language») que se ha convertido en **el lenguaje estándar para la gestión de bases de datos**. Cuando un sitio web necesita acceder a la base de datos que tiene en su servidor para buscar o editar información, utiliza SQL para procesar esa «consulta» o solicitud.

El SQL es un lenguaje amplio y flexible que ofrece a los diseñadores de bases de datos infinidad de posibilidades. Casi todos los diseñadores crean bases de datos con su propio conjunto de normas SQL, aquellas que mejor se adaptan a sus necesidades particulares. No se puede copiar y pegar sin más el SQL de una base de datos en otra, puesto que cada una puede haberse creado de una forma totalmente distinta.

Este artículo contiene:



Tan



¿Qué es el malware y cómo protegerse de los ataques?

¿Qué es el spyware Pegasus? ¿Ha infectado su teléfono?

¿Qué es la botnet Mirai?

El troyano Zeus: qué es, cómo funciona y cómo protegerse

Cómo eliminar un virus del router

¿Qué es un malware troyano? Guía definitiva

¿Y dónde entra la parte de la inyección?

Si un desarrollador web no es meticuloso, al crear un sitio podría dejar un resquicio que alguien con malas intenciones podría usar para provocar efectos inesperados en su base de datos. Las inyecciones de SQL (o SQLI) 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*, y consigue subrepticamente que envíe ese código a su base de datos como si de una consulta legítima se tratara.



Los hackers recurren a los ataques de inyección de SQL con el fin de introducirse en la base de datos de un sitio web. A veces solo quieren eliminar datos para provocar el caos y, en otras ocasiones, lo que buscan es editar la base de datos, especialmente en el caso de sitios web financieros.



Los ataques de inyección de SQL únicamente son viables cuando un sitio web carece de un *saneamiento de entrada* adecuado: el proceso que vela por que la información que introducen los usuarios finales no pueda colarse por ningún resquicio y funcionar

como código ejecutable en el servidor. Esto requiere más trabajo por parte del desarrollador, pero, en última instancia, protege frente a la inyección de SQL, las [secuencias de comandos en sitios cruzados](#) y otras clases de ataques a sitios web.

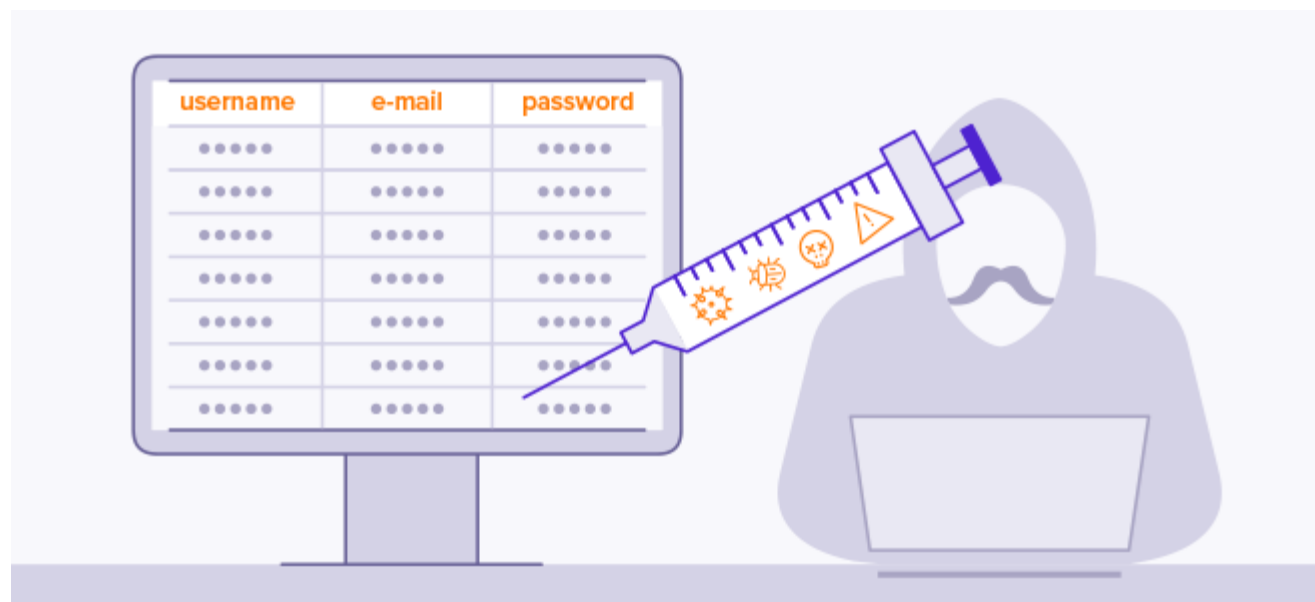
¿Qué efecto tienen los ataques de inyección de SQL?

Los hackers recurren a los ataques de inyección de SQL con el fin de introducirse en la base de datos de un sitio web. A veces solo quieren eliminar datos para provocar el caos y, en otras ocasiones, lo que buscan es editar la base de datos, especialmente en el caso de sitios web financieros. En el momento en que el hacker ha logrado el control de la base de datos, ya es fácil interferir en los saldos de las cuentas de los clientes y mandarse dinero a su propia cuenta.

Sin embargo, a menudo lo que **el ciberdelincuente quiere son los datos de usuario guardados en el sitio web**, como las credenciales de inicio de sesión. Estos datos de inicio de sesión robados puede emplearlos para realizar acciones en nombre de los usuarios afectados o reunirlos en una gran lista que luego venderá a otros [ciberdelincuentes](#) en la [red oscura](#). Las personas que compran información robada lo hacen, frecuentemente, con la finalidad de [robar identidades](#) y cometer fraudes.

¿Cómo se produce un ataque de inyección de SQL?

Si un sitio web no toma las medidas adecuadas para [sanear la introducción de datos](#), un hacker puede inyectar el código SQL que quiera. De este modo, 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 modo que el hacker puede cumplir sus objetivos.



Los hackers recurren a los ataques de inyección de SQL con el fin de introducirse en la base de datos de un sitio web.

Así es como se inyecta SQL: ¡no lo intente en casa!



Inyección de SQL mediante la introducción de datos del usuario

La inyección de SQL mediante la introducción de datos del usuario es la forma más sencilla de perpetrar un ataque de inyección de SQL. Hay un montón de sitios web que recopilan las entradas del usuario y las transmiten al servidor. Eso quiere decir que si hace un pedido por Internet y pone su dirección, este dato se recopila. Y

ocurre lo mismo en un apartado de comentarios o de reseñas de usuario. Sin un saneamiento de entrada seguro, un formulario con campos para rellenar o un recuadro para poner comentarios constituyen una vulnerabilidad flagrante en cuanto a la inyección de SQL.

En lugar de cumplimentar estos formularios con contenido y respuesta normales y corrientes, los hackers que utilizan la inyección de SQL hacen algo muy diferente: introducir una secuencia de comandos de código SQL. **Cuando un sitio web con un saneamiento de entrada deficiente envía el contenido del formulario a su servidor, el código del hacker se ejecuta.** Así es como los hackers usan la SQLI para robar los datos de los usuarios o trastocar el funcionamiento de un sitio web.

Veámoslo con un ejemplo real: una situación en la que una persona va a solicitar un empleo. El nombre del candidato es Juan González, pero en la solicitud escribe «Contratar a Juan González». Cuando el director de contrataciones lee el nombre del candidato en voz alta, el equipo de RR. HH. le oye decir «Contratar a Juan González», así que le envían a Juan una oferta de empleo formal.

En lugar de indicar su nombre real, Juan ha enviado una carga útil de SQL que, al ejecutarla la base de datos (el director de contrataciones), hace que Juan consiga el trabajo.



Inyección de SQL mediante la modificación de cookies

Las [cookies](#) son archivos pequeños que residen en el navegador y facilitan a los sitios web información sobre el usuario. Algunas veces son útiles, por ejemplo, cuando recuerdan sus credenciales de inicio de sesión o sus preferencias; es cómodo. Otras veces dan miedo: muchos sitios emplean cookies para [seguir las actividades del usuario en Internet](#) y en sus páginas. Utilizan la información obtenida con el seguimiento para llevar a cabo investigaciones de mercado y con fines publicitarios. Este segundo tipo de cookie es una herramienta de seguimiento web habitual.

Los ciberdelincuentes son capaces de manipular o «envenenar» las cookies de manera que, cuando transmitan información al servidor del sitio web, envíen código SQL a la base de datos.



Inyección de SQL mediante variables de servidor

Al introducir la URL de un sitio web en el navegador, tiene lugar una rápida secuencia de comunicaciones cuya finalidad es ofrecer el sitio al usuario. Dentro de este proceso, el navegador solicita una lista de datos denominada «variables de servidor» que sirve para que el sitio se renderice correctamente.

Un hacker astuto puede meter sigilosamente código SQL en las solicitudes del navegador, las cuales, si no se sanean debidamente, se inyectarán en la base de datos del sitio web, que se encuentra en el servidor.



Inyección de SQL mediante herramientas de hackeo automáticas

Si esto parece demasiado complicado, existe una opción más sencilla. Hay **herramientas automáticas de inyección de SQL, como SQLMAP, que detectan y aprovechan las vulnerabilidades en la inyección de SQL** presentes en un sitio web determinado y en su base datos.

[SQLMAP](#) es una herramienta de código abierto muy popular entre los gestores de bases de datos y los desarrolladores de sitios web que quieren parchear sus sitios para protegerlos contra la inyección de SQL. Pero no hay nada que impida a las personas utilizar SQLMAP con malas intenciones.



Ataques SQL de segundo orden

La inyección de SQL de segundo orden va un poco más lejos, ya que emplea un método mucho más sofisticado. Dado que muchos sitios web se sanean para evitar la introducción de datos directa por parte los usuarios, los hackers inyectan SQL diseñado para ejecutarse únicamente en las visitas posteriores. Al implantar unas medidas preventivas básicas de saneamiento de entrada, el sitio web en cuestión bloquearía un ataque normal de SQLI, también denominado ataque de «primer orden». Sin embargo, **un ataque de inyección de SQL de segundo orden es una bomba de relojería**. Lo que sucede es lo siguiente:

Un hacker inyecta un fragmento de código en la base de datos que, por sí mismo, no hace nada. Pero este código está diseñado para alterar el funcionamiento de la base de datos al interpretarlo como una entrada más de todas las que contiene. Así, cuando el SQL de la base de datos incluye el código del hacker entre sus propias funciones, se lanza el ataque.

Vamos a ilustrar este concepto con un clásico de la literatura, el poema épico de Homero: *La Odisea*. En esta historia, un cíclope de nombre Polifemo captura a Ulises, el héroe. Tratando de escaparse, Ulises emborracha a Polifemo. Cuando el cíclope le pregunta cuál es su nombre para darle las gracias por el vino ofrecido, Ulises responde que se llama «Nadie».

Esta es la primera fase de un ataque de SQL de segundo orden: **Ulises, el taimado hacker, inyecta la aparentemente benigna carga útil «Nadie» en la base de datos de Polifemo.**

Más tarde, Ulises ciega a Polifemo. El enfurecido cíclope corre a relatar a sus hermanos que «Nadie» lo ha engañado y lo ha dejado ciego. La respuesta de ellos es reírse. En lugar de vengarse, Polifemo es humillado y Ulises logra escapar.

Esa es la segunda fase. **La carga útil de SQL «Nadie» es inofensiva por sí sola, pero cuando Polifemo (la base de datos) intenta usarla, se pone al descubierto el ataque.**

Como al principio es indetectable, la **inyección de SQL** permite a los ciberdelincuentes burlar, de manera indirecta y eficaz, los procedimientos básicos de saneamiento de la introducción de datos.

La repercusión de los ataques de inyección de SQL

Los ataques de inyección de SQL pueden tener muy diversas consecuencias. Un solo ataque de SQLI puede tener unos efectos devastadores tanto en los usuarios afectados como en la empresa o el negocio atacados.

Efectos de las SQLI en las personas

Aunque los blancos de una SQLI no son las personas, si usted utiliza un sitio web donde se haya perpetrado un ataque de este tipo, el impacto podría ser considerable. Tener una cuenta en un sitio web que sufra un ataque o enviar datos personales a este sitio permitiría a los hackers hacer muchas cosas, no solo conseguir sus datos personales.

Los ataques de inyección de SQL pueden tener consecuencias graves para las personas, a saber:

- **Pérdida de dinero:** un hacker puede usar una SQLI en la página de una entidad bancaria u otra institución financiera a fin de transferir dinero desde la cuenta de un usuario.
- **Robo de identidad:** cuando un hacker controla una base de datos, puede hacerse con la información que contiene y venderla en la red oscura. Otros ciberdelincuentes pueden comprar estos datos y utilizarlos para robar identidades.

[Avast BreachGuard](#) le permite aislarse contra posibles ataques de robo de identidad. Esta prestación busca sus datos en la red oscura y le avisa si alguno de los sitios web que utiliza ha sufrido el ataque de algún hacker u otros ataques a la seguridad.

Efectos de las SQLI en las empresas

Como los verdaderos blancos de los ataques de SQLI son las empresas, estas se enfrentan a una [serie de amenazas](#) mucho más diversas. Cuando un hacker se introduce en una base de datos, puede realizar varias acciones y, una vez que el suceso se divulga, la empresa afectada se ha de preparar para hacer frente a los perjuicios a su imagen pública y minimizarlos.

A continuación, detallamos algunos de los daños que pueden sufrir las empresas en un ataque de SQLI:

- **Sabotaje:** un hacker puede sembrar el caos fácilmente en una empresa borrando su base de datos o destrozando el sitio web.
- **Robo de datos:** muchos ataques de SQLI tienen por objeto robar datos confidenciales tales como secretos comerciales, información privilegiada, propiedad intelectual protegida y, a menudo, información de los usuarios o clientes.
- **Filtraciones de seguridad:** un hacker podría usar el contenido de una base de datos quebrantada para acceder a otras partes de la red interna de una empresa. Al final, toda la red puede estar en riesgo.
- **Pérdida de reputación:** tras sufrir los efectos de un ataque de SQLI, puede resultar difícil que una empresa recupere la confianza de sus clientes y del público en general.

Posibles costes de los ataques de SQLI

Teniendo en cuenta todo lo que un hacker puede llegar a hacer con una SQLI, los costes pueden llegar a ser sustanciales. Un estudio llevado a cabo en 2014 reveló que la subsanación del *más leve* [ataque de inyección de SQL puede costar en torno a 200 000 dólares](#), y esto solo considerando las consecuencias financieras.

En un artículo de *Ars Technica* publicado en el mismo año, se informó de que [la Marina de EE. UU. gastó más de medio millón de dólares](#) en responder a un solo ataque de inyección de SQL. A causa del ataque, más de 70 miembros en servicio pasaron varios meses sin poder resolver las solicitudes pendientes de traslado.

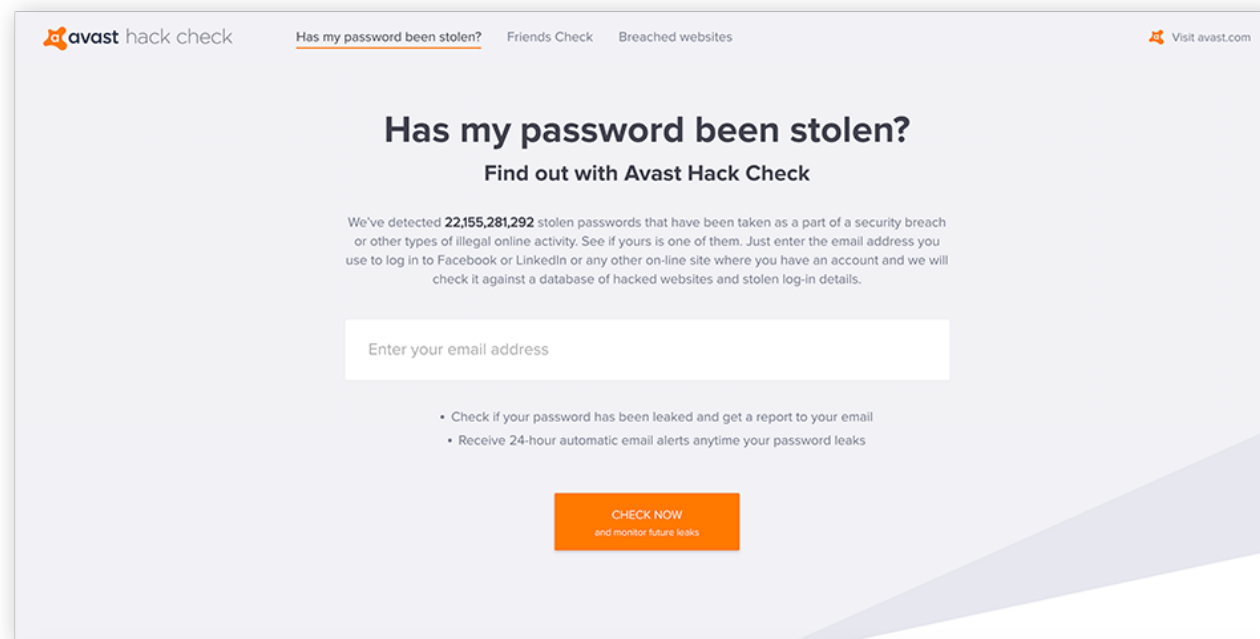
Aparte de los costes económicos que supone hacer frente a un ataque, el daño que se inflige a largo plazo en la reputación de una empresa puede resultar irreversible.

¿Cómo puedo evitar los ataques de inyección de SQL?

A menos que se dedique al desarrollo web, no tiene forma de hacerlo. **La inyección de SQL no va dirigida directamente a usted como usuario, así que no puede detectar, contrarrestar ni bloquear un ataque.** Además, no sabrá si está usando un sitio que

haya sufrido un ataque hasta que los efectos salgan a la luz tiempo después.

Prevenir los ataques de inyección de SQL es responsabilidad de las personas que gestionan los sitios web que usted utiliza. No obstante, sí puede hacer algo para combatir las SQLI. Hágalo ahora mismo: vaya a nuestra herramienta gratuita [Avast Hack Check](#) para ver si las credenciales de inicio de sesión de los sitios que utiliza se han filtrado. En caso afirmativo, cambie la contraseña de ese sitio de inmediato.

The image shows the Avast Hack Check website. At the top, there's a navigation bar with the Avast logo, 'hack check', and links for 'Has my password been stolen?', 'Friends Check', and 'Breached websites'. A 'Visit avast.com' link is in the top right. The main heading is 'Has my password been stolen?' with the subtext 'Find out with Avast Hack Check'. Below this, a paragraph states: 'We've detected 22,155,281,292 stolen passwords that have been taken as a part of a security breach or other types of illegal online activity. See if yours is one of them. Just enter the email address you use to log in to Facebook or LinkedIn or any other on-line site where you have an account and we will check it against a database of hacked websites and stolen log-in details.' There is a text input field labeled 'Enter your email address'. Below the field, two bullet points list the benefits: 'Check if your password has been leaked and get a report to your email' and 'Receive 24-hour automatic email alerts anytime your password leaks'. At the bottom, there is an orange button that says 'CHECK NOW and monitor future leaks'.

Utilice Avast Hack Check para averiguar si sus credenciales de inicio de sesión se han filtrado.

Como muchos ataques de inyección de SQL se cometen para robar datos de usuario,

Hack Check es una forma de reducir el riesgo de que sus datos se filtren.

¿Entonces qué hago para evitar una inyección de SQL?

Si bien no puede impedir que un ataque de inyección de SQL se produzca, sí *puede* reducir la posibilidad de verse afectado y mitigar los efectos si alguna vez se ve involucrado. Siga siempre estos hábitos de navegación segura al utilizar Internet:

- **No proporcione información personal en sitios web sospechosos.** Al introducir datos confidenciales, asegúrese de hacerlo solo en [sitios web de confianza](#) que cuenten con fuertes medidas de seguridad. Ni siquiera esto es garantía infalible para evitar ser víctima de un ataque de este tipo, pero es un comienzo.
- **Manténgase informado de las noticias sobre seguridad tecnológica.** Cuando se producen ataques de hackers y filtraciones en sus bases de datos, las empresas lo anuncian. Esté al tanto de las noticias sobre los sitios web que utiliza y, si ve algo en referencia a una SQLI, cambie sus credenciales de inicio de sesión sin demora.
- **Acostúmbrese a crear contraseñas seguras.** Si utiliza una contraseña distinta para cada cuenta, reducirá el riesgo. Siga las prácticas recomendadas de [creación de contraseñas](#) para ir siempre un paso por delante de los hackers.
- **Utilice un administrador de contraseñas.** Muchos [administradores de](#)

[contraseñas](#) alertan al usuario cuando un sitio web que utiliza ha sufrido un ataque. Si es el caso, podrá cambiar rápidamente una contraseña difícil de averiguar por otra igual de segura. Busque un administrador que proporcione funcionalidad en varias plataformas para poder usar las contraseñas en todos sus dispositivos.

Disfrute de una seguridad digital completa con Avast Free Antivirus

Su navegador no sabrá si ha visitado un sitio web en riesgo por una inyección de SQL, pero usted no tiene por qué batirse solo en la constante lucha contra los ciberdelincuentes. Es la hora de llamar a la caballería.

[Avast Free Antivirus](#) lo dota de ciberseguridad en tiempo real en varios frentes para protegerlo frente a toda clase de amenazas virtuales. Supervisa su dispositivo en busca de posibles vulnerabilidades, incluidas las redes Wi-Fi no seguras, los programas de software desactualizados, las aplicaciones sospechosas, los intentos de phishing y, no podía faltar, cualquier rastro de malware.

Lleve la seguridad digital al nivel siguiente con el antivirus en el que confían más de 400 millones de usuarios de todo el mundo.



Artículos más recientes sobre seguridad

También podría gustarle...

¿Qué es el malware y cómo protegerse de los ataques?

¿Qué es el spyware Pegasus? ¿Ha infectado su teléfono?

¿Qué es la botnet Mirai?

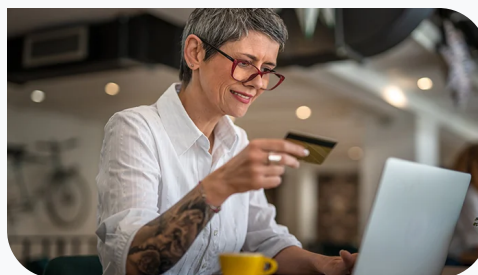
El troyano Zeus: qué es, cómo funciona y cómo protegerse

Cómo eliminar un virus del router

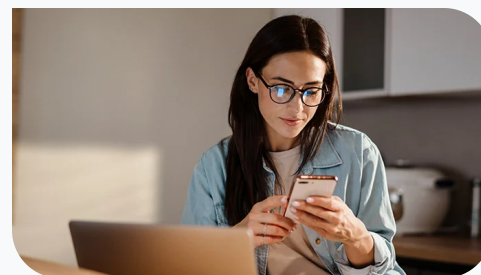
¿Qué es un malware troyano? Guía definitiva



¿Qué es un ataque de gemelo malvado y cómo actúa?



¿Han hackeado mi cuenta de Amazon?



¿Puede alguien hackear su teléfono llamándole o enviándole un mensaje de texto?



Para El Hogar

Soporte

Seguridad

Privacidad

Rendimiento

Para Empresas

Soporte empresarial

Productos para empresa

Socios empresariales

Blog empresarial

Para Socios

Mobile Carriers

Empresa

Contacte con nosotros

Investors

Empleo

Centro de prensa

[Blog](#)

[Afiliados](#)

[Responsabilidad](#)

[Forum](#)

[Tecnología](#)

[Política de privacidad](#)

[Información legal](#)

[Informar de una vulnerabilidad](#)

[Contactar con seguridad](#)

[Declaración sobre la esclavitud moderna](#)

[Preferencias de cookies](#)

Gen © 2024 Gen Digital Inc. Todos los derechos reservados.