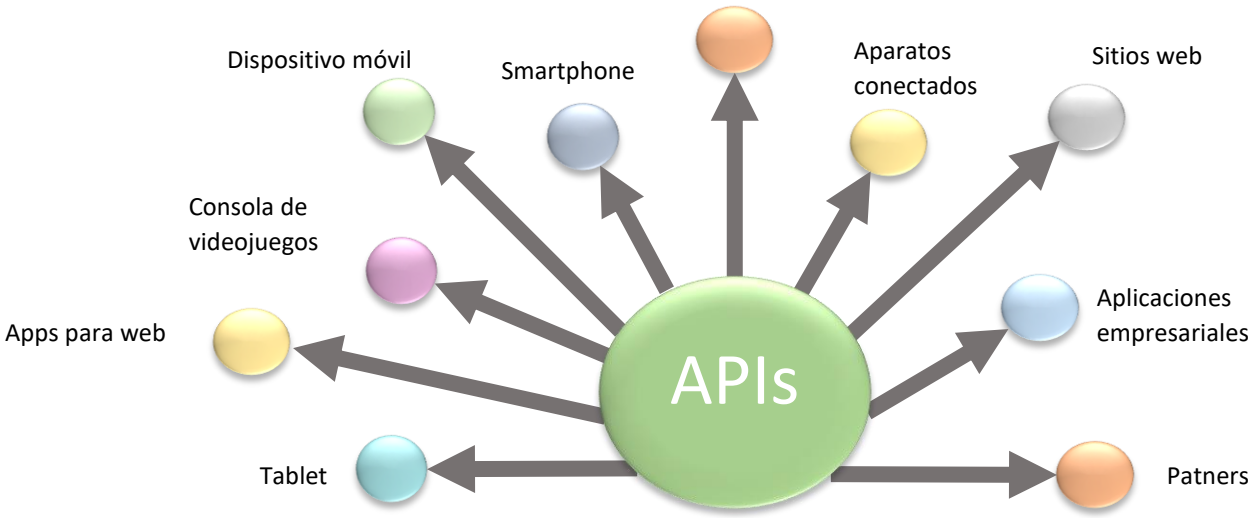
SEGURIDAD EN LAS API´S

Top 10 de OWASP

@BUMANSEC



Contenido

1. ¿Por qué es necesario aplicar una Prueba de Seguridad en las API's?
2. Top 10 de OWASP aplicado a la Seguridad en las API´s.

¿POR QUÉ ES NECESARIO APLICAR UNA PRUEBA DE SEGURIDAD EN LAS API´S?

¡¡¡ANALICEMOS!!!

Ataques contra la seguridad en las API´s durante los últimos años:

SEP 2018

- Un grupo de hackers explotaron una vulnerabilidad hallada en el desarrollador de API´s, con un solo objetivo: exponer la información de millones de usuarios.

2019

- Un estudiante de Ciencias de la Computación acaparó 7 millones de transacciones de la cartera digital Venmo con un solo objetivo: demostrar que la actividad pública de los usuarios aún puede ser obtenido fácilmente.
- Desarrolladores de Starbacks dejaron la clave de su API (API Key) en un repositorio público de GitHub. La API permite el intercambio de datos entre aplicaciones, por lo que si un hacker hubiera violado la seguridad de la API, tendría acceso a información sensibles almacenada en su Sitio Web.

ACTUAL

- FUGA DE INFORMACIÓN DE CLIENTES: Generalmente estos datos son ofertados en el mercado negro.
- DESCONFIGURACIÓN DEL SITIO WEB DEL NEGOCIO: Generalmente afectan con alto nivel de gravedad a la reputación de la marca de las empresas en el mercado.

TOP 10 DE OWASP APLICADO A LA SEGURIDAD DE LAS API´S

¿¿¿CUÁLES SON ACTUALMENTE???

1. API1:2019 – Autorización a Nivel Objeto Interrumpida
2. API2:2019 – Autenticación de Usuario Interrumpida
3. API3:2019 – Exposición Excesiva de Datos
4. API4:2019 – Falta de Recursos y Velocidad Limitada
5. API5:2019 – Autorización a Nivel Función Interrumpida
6. API6:2019 – Asignación Masiva
7. API7:2019 – Configuración Errónea de Seguridad
8. API8:2019 – Inyección
9. API9:2019 - Gestión Inadecuada de Activos
10. API10:2019 – Monitoreo e Registros Insuficientes.

- NOTA: Actualmente continua vigente el TOP10 del año 2019 por OWASP.ORG.

¿¿¿¿PERO, COMO ES QUE SE ESTABLECE ESTE TOP10???

Aquí se muestra como es la ponderación del riesgo de seguridad en las API´s:

Agente Amenaza	Depende de la API	Depende de la API	Depende de la API
Explotabilidad	Fácil: 3	Promedio: 2	Difícil: 1
Prevalencia de la debilidad	General: 3	Común: 2	Difícil: 1
Detectabilidad de la debilidad	Fácil: 3	Promedio: 2	Difícil: 1
Impacto técnico	Severo: 3	Moderado: 2	Mínimo: 1
Impacto al negocio	Depende del negocio	Depende del negocio	Depende del negocio

API1:2019 – Autorización a Nivel Objeto Interrumpida

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por 3 razones:

1. La Autorización a Nivel Objeto (en inglés OLA) es un mecanismo de control de acceso que es implementado a nivel de código para validar que un usuario solamente puede ingresar objetos que deberían tener un legítimo acceso.

2. La API recibe un identificador único de un objeto y ejecuta cualquier tipo de acción con ese objeto, por lo que debe implementar comprobaciones de autorización a nivel Objeto. Las comprobaciones deben ser validadas para que el usuario que ha iniciado sesión tenga acceso a realizar la acción cualquier acción que solicite sobre el objeto que haya seleccionado.

3. Esta vulnerabilidad conduce a la divulgación no autorizada de información, así como la modificación o destrucción de todos los datos.

EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza ——— **Vectores de Ataque**	3	Los atacantes pueden explotar los endpoints de las API´s a través de manipulación del ID de un objeto que es enviado dentro de la solicitud.
Debilidad de Seguridad	2	La detección del control de acceso no suele ser susceptible a pruebas estáticas o dinámicas automatizadas.
Impactos	3	Divulgación de datos a partes no autorizadas, pérdida o manipulación de datos. Control total de la cuenta.

API2:2019 – Autenticación de Usuario Interrumpida

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por 5 razones:

1. Esta vulnerabilidad permite el ataque “Credential Stuffing” que busca robar las credenciales y contraseñas validas del usuario.

2. Permite a los atacantes realizar un ataque de fuerza bruta contra la misma cuenta de usuario, ni que se genere captcha o mecanismo de bloqueo de la cuenta. Esto permite que se ingresen contraseñas débiles.

3. Envía detalles sensibles de autenticación, como tokens de autenticación y contraseñas, en una URL. Esto permite que no sea validada la autenticidad de los tokens.

4. Acepta tokens JWT sin firma digital o débilmente firmados (“alg”:”none”), además no valida su fecha de expiración. Esto permite que se utilice contraseñas en texto plano, no cifradas o con un hash débil.

5. Usa llaves con un débil cifrado.

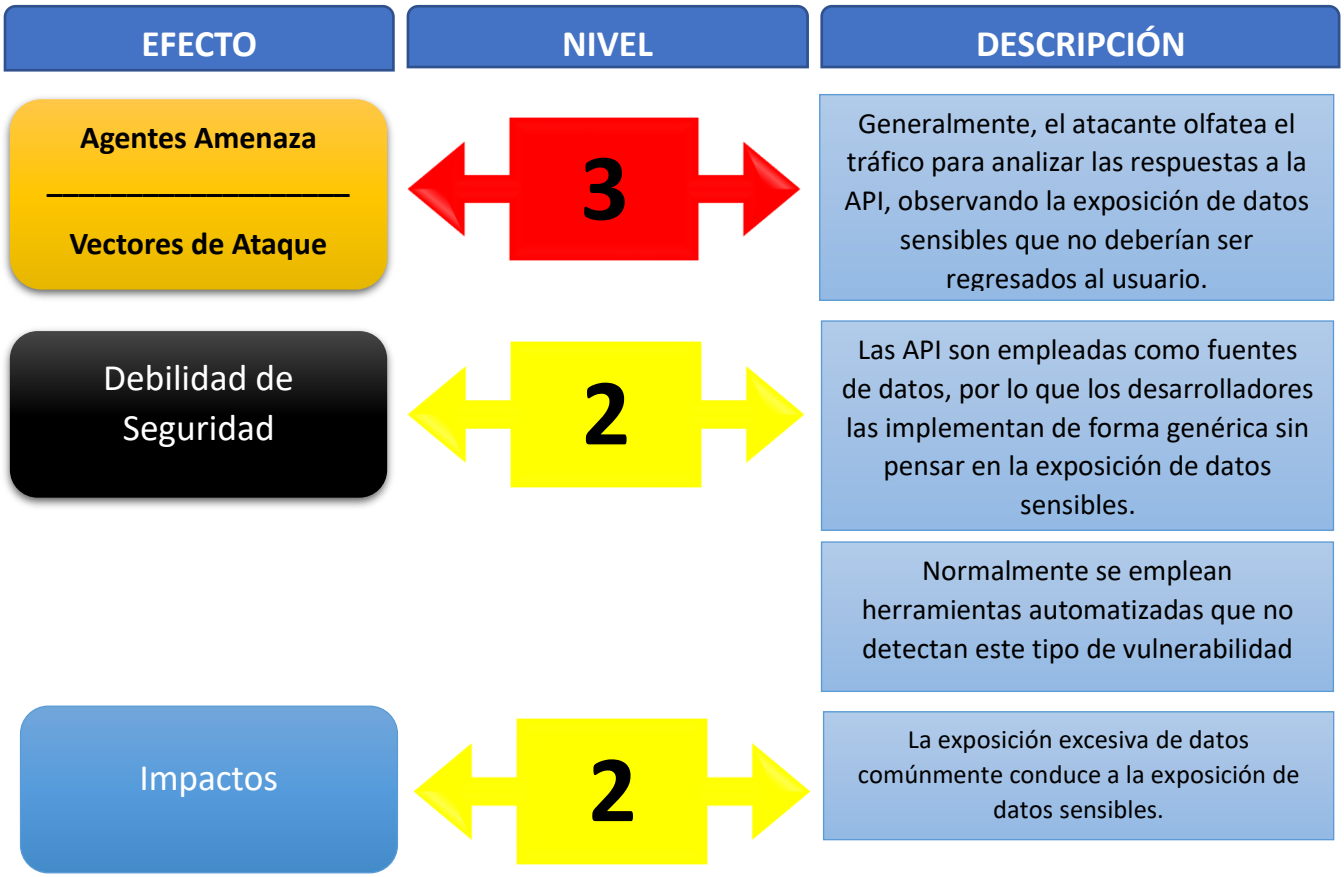
EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza _____ **Vectores de Ataque**	3	Tener un concepto erróneo de ingeniería acerca de cuáles son los límites de autenticación y cómo implementarlos correctamente.
Debilidad de Seguridad	2	Falta de mecanismos de protección, o su mala implementación.
Impactos	3	El atacante obtiene el control de las cuentas de otros usuarios en el sistema, lee datos personales y realiza acciones sensibles desde su ubicación.

API3:2019 – Exposición Excesiva de Datos

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por una razón principal:

1. La API regresa datos sensibles al cliente por diseño. Estos datos son normalmente filtrados en el "lado del cliente" (el cual es el ámbito donde el cliente ejecuta sus operaciones en una relación cliente-servidor) antes de ser presentada al usuario. Fácilmente, un atacante puede olfatear el tráfico y ver los datos sensibles.



API4:2019 – Falta de Recursos y Velocidad Limitada

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por una razón principal:

1. Se requiere la no autenticación, ya que se pueden realizar múltiples solicitudes simultáneas desde una sola computadora local o empleando recursos de cómputo en la nube.

EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza _____ **Vectores de Ataque**	2	Tener un concepto erróneo de ingeniería acerca de cuáles son los límites de autenticación y cómo implementarlos correctamente.
Debilidad de Seguridad	3	Las API´s que no implementan límites de velocidad o donde los límites no son configurados apropiadamente.
Impactos	2	La explotación puede conducir a una DoS, provocando que la API no responda o incluso quede no disponible.

API5:2019 – Autorización a Nivel Función Interrumpida

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

En esta vulnerabilidad, nos deberíamos preguntar al realizar un análisis profundo del mecanismo de autorización:

1. ¿Un usuario regular puede acceder a endpoints administrativos?

2. ¿Un usuario puede realizar acciones sensibles, como por ejemplo crear, modificar o eliminar, a las cuales no debería tener acceso, simplemente cambiando el método HTTP, como puede ser de GET a DELETE?

3. ¿Desde un grupo X, un usuario puede acceder a una función que debería ser expuesta únicamente para los miembros del grupo Y, simplemente adivinando la URL y los parámetros del endpoint, como por ejemplo /api/v1/users/export_all?.

EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza / **Vectores de Ataque**	3	Se encuentra expuesta la API a usuarios anónimos o por lo regular a usuarios no privilegiados. Es más fácil de descubrir la estructura en las API´s, y la forma de acceder a ciertas funciones es más predecible.
Debilidad de Seguridad	2	Una implementación de verificaciones adecuadas puede ser una tarea confusa, ya que aplicaciones modernas pueden contener muchos tipos de roles o grupos, por ejemplo, sub-usuarios o usuarios con más de un rol.
Impactos	2	Los atacantes acceden a funcionalidades no autorizadas, por lo que funciones administrativas son los objetivos clave para este tipo de ataque.

API6:2019 – Asignación Masiva

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por 2 razones:

1. Los Objetos en aplicaciones modernas podrían contener muchas propiedades, las cuales deberían ser actualizadas directamente por el cliente, como por ejemplo *user.first_name* o *users.address*, y algunas otras no deberían ser actualizadas, como por ejemplo *user.is_vip flag*.

2. El endpoint de la API es vulnerable si automáticamente convierte los parámetros del cliente dentro de las propiedades internas del Objeto, sin considerar la sensibilidad y el nivel de exposición de esas propiedades. Estas propiedades pueden encontrarse como:

   - Propiedades con permiso relacionado, donde el objeto *user.is_admin* debería ser configurado únicamente por los administradores.
   - Propiedades con proceso dependiente, donde el objeto *user.cash* debería ser configurado internamente sólo desde la verificación de pago.
   - Propiedades internas, donde el objeto *article.created_time* debería se configurado internamente por la aplicación.

EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza ——— **Vectores de Ataque**	2	Requiere entender la lógica del negocio, los objetos relacionados y la estructura de la API. Expone la implementación subyacente de la aplicación junto con los nombres de las propiedades.
Debilidad de Seguridad	2	Emplea frameworks modernos que enlazan automáticamente la entrada del cliente dentro de variables de código y objetos internos, permitiendo la sobreescritura de propiedades de objetos sensibles indebidamente.
Impactos	2	La explotación puede conducir a un escalamiento de privilegios, manipulación de los datos, mecanismos para bypass de seguridad, entre otros.

API7:2019 – Configuración Errónea de Seguridad

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por 7 razones:

1. Por la falta de un esfuerzo adecuado de seguridad en cualquier parte del stack de aplicación, o si lo tiene, los permisos se encuentran configurados inapropiadamente en los servicios en la nube.
2. Falta de los últimos parches de seguridad, o los sistemas se encuentran obsoletos.
3. Cuenta con funciones innecesarias en modo habilitado.
4. Falta del protocolo TLS (Transport Layer Security)
5. Las directivas de seguridad no son enviadas a los clientes, como pueden ser las cabeceras de seguridad.
6. Falta una política CORS (Cross-Origin Resource Sharing) o se encuentra configurada inapropiadamente.
7. Los mensajes de error incluyen seguimiento del stack de la aplicación u otra información expuesta.

EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza / **Vectores de Ataque**	3	A menudo, los atacantes intentan encontrar fallas en parcheo, endpoints comunes o archivos y directorios desprotegidos para obtener acceso no autorizado o reconocimiento del sistema.
Debilidad de Seguridad	3	Existen herramientas automatizadas que son capaces de detectar y explotar errores de configuración, así como servicios innecesarios u opciones legendarias.
Impactos	2	Los errores de configuraciones de seguridad pueden exponer no sólo los datos sensibles del usuario, sino también detalles del sistema que puede comprometes completamente el servidor.

API8:2019 – Inyección

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por 3 razones:

1. Los datos suministrados por el cliente no son validados, filtrados o analizados por la API.

2. Los datos suministrados por el cliente son usados directamente o concatenados para solicitudes SQL/NoSQL/LDAP, comandos OS, analizadores XML y Object Relational Mapping (ORM)/Object Document Mapper (ODM).

3. Los datos que vienen de sistemas externos, como pueden ser de sistemas integrados, no son validados, filtrados o analizados por la API.

EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza _____ **Vectores de Ataque**	3	Se encuentran disponibles los ataques con datos maliciosos a API´s a través de cualquier vector de inyección, como puede ser entrada directa, parámetros, servicios integrados, entre otros, esperando ser enviados a un interprete
Debilidad de Seguridad	3	Las fallas de inyección son muy comunes y a menudo se encuentran en solicitudes SQL/NoSQL/LDAP, comandos OS, analizadores XML y ORM.
Impactos	3	La inyección puede conducir a divulgación de información y pérdida de datos, lo que puede también conducir a una DoS o la toma del control completo del host.

API9:2019 – Gestión Inadecuada de Activos

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por 6 razones:

1. El propósito del host de una API es confuso.
2. No hay documentación, o la que existe no está actualizada.
3. No hay un plan de expiración para cada versión de API.
4. Falta un inventario de hosts o se encuentra obsoleto.
5. Falta un inventario de servicios integrados, o al menos una primera o tercera parte, o se encuentra obsoleto.
6. Las versiones antiguas o anteriores de la API se están ejecutando sin parches de seguridad.

EFECTO	NIVEL	DESCRIPCIÓN
Agentes Amenaza _____ **Vectores de Ataque**	3	Las versiones antiguas de las API´s normalmente no cuentan con parches de seguridad y son una forma fácil de comprometer el sistema.
Debilidad de Seguridad	2	La documentación obsoleta compleja encontrar y corregir vulnerabilidades. La falta de inventario de activos y retirar estrategias conducen a que se ejecuten sistemas sin parcheo.
Impactos	2	Obtención del acceso a datos sensibles, o incluso la toma del control del servidor a través de versiones antiguas de API´s sin parcheo conectadas al mismo.

API10:2019 – Monitoreo e Registros Insuficientes

¿¿¿POR QUÉ ES TAN IMPORTANTE ESTA VULNERABILIDAD???

Por 3 razones:

1. No genera ningún registro, el nivel de registro no está configurado correctamente o los mensajes de los registros no incluyen detalles suficientes.

2. La integridad de los registros no está garantizada, como por ejemplo la inyección de logs.

3. La infraestructura de la API no es monitoreada constantemente.

REFERENCIAS

- ✓ https://owasp.org/www-project-api-security/
- ✓ https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf