API Security Project

Es un elemento fundamental de innovación en el mundo actual impulsado por las aplicaciones es la API. Es utilizado comúnmente en bancos, comercios minoristas y transporte hasta IoT, así como en vehículos autónomos y ciudades inteligentes, las API son una parte fundamental de las aplicaciones móviles.

Por naturaleza, las API exponen la lógica de la aplicación y datos de confidencialidad como la información de identificación personal (PII) y, debido a esto, se han convertido cada vez en un objetivo para los atacantes. Sin API seguras la innovación rápida sería imposible.

API Security se centra en estrategias y soluciones para comprender y mitigar las vulnerabilidades y riesgos se seguridad únicos de las interfaces de programación de aplicaciones (API).

- **API Broken Object Level Authorization:** es un mecanismo de control de acceso que usualmente esta implementado a nivel código, encargado de validar que un usuario acceda solamente a los objetos que tiene permitido acceder y no a toda la información.

Proyecto donde ha sido utilizado:

Un ejemplo simple de su uso es un proyecto de Java Spring, El punto final de la API (ejemplo de código) elimina los pedidos por ID, pero no verifica si este pedido ha sido realizado por el usuario que ha iniciado la sesión. Esto supone una oportunidad muy fácil para que un atacante aproveche esta laguna y elimine los pedidos de otros usuarios.

Ejemplo de código con vulnerabilidad:

```
public boolean deleteOrder(Long id) {
    Order order = orderRepository.getOne(id);
    if (order == null) {
      log.info("No found order");
      return false;
    }
    User user = order.getUser();
    orderRepository.delete(order);
    log.info("Delete order for user {}", user.getId());
    return true;
```

Ejemplo de código aplicando restricciones:

```
public boolean deleteOrder(Long id) {
    User user = userService.getUserByContext();
    boolean orderExist = getUserOrders().stream()
        .anyMatch(order -> (order.getId() == id));
    if (orderExist) {
      orderRepository.deleteById(id);
      log.info("Delete order for user {}", user.getId());
      return true;
    } else {
      log.info("No found order");
      return false;
```

Importancia:

Yo considero que el uso de estas herramientas de seguridad ha sido y siguen siendo muy importantes, ya que buscan identificar cuales son las vulnerabilidades que puede tener un proyecto y ofrecer medidas necesarias para prevenir o combatirlas, además de que muestra la importancia de una buena seguridad web y las consecuencias que puede haber en caso de que no prestemos atención a las advertencias. También considero que es muy importante tomar en cuenta los conocimientos y estrategias que OWASP nos ofrece y aunque es para ayudara las grandes empresas también nos puede ayudar a nosotros cuando desarrollemos un nuevo proyecto.

Fuente:

Security, B. (s. f.). Guía de OWASP para APIs 2023. *www.linkedin.com*. https://www.linkedin.com/pulse/gu%C3%ADa-de-owasp-para-apis-2023-base4-security/?originalSubdomain=es