FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ISWZ3206-3470_3471-DESARROLLO DE SOFTWARE SEGURO

Introducción

Tarea

JWT

Adrián Bedón, Pablo Chasipanta, Dennis Ocaña, Xavier Ramos

Quito, 6 de junio de 2024

I DESARROLLO

I.1 Concepto

Los JSON Web Tokens (JWT) son un esquema de tokens ampliamente utilizado para autenticación y autorización en aplicaciones web y APIs. Son un formato de token seguros y compactos para transmisión de información.

- Los JWT son tokens que se utilizan para verificar de forma segura a los usuarios en aplicaciones y APIs.
- Contienen información compartida en forma de objetos JSON.
- Se emiten entre clientes y servidores para autenticar y autorizar solicitudes.

Los JWT funcionan cuando un cliente (por ejemplo, un navegador) solicita acceso a un recurso protegido y se ejecuta de la siguiente manera:

- El servidor genera un JWT y lo envía al cliente.
- El cliente incluye el JWT en las solicitudes posteriores (generalmente en el encabezado “Authorization”).
- El servidor verifica la firma y la validez del token antes de permitir el acceso al recurso.

Los JWT tienen ciertas ventajas como el ser compactos y facil de transmitir, además de no requerir almacenamiento en el servidor ya que la información está en token y también tienen la capacidad de incluir roles de usuario.

I.2 Estructura

Un JWT consta de tres partes:

- **Cabecera (Header):** Contiene información sobre el algoritmo de cifrado y el tipo de token (por ejemplo, “HS256” para HMAC-SHA256).
- **Carga (Payload):** Contiene la información que se quiere transmitir, como datos de usuario o permisos.
- **Firma (Signature):** Verifica la integridad del token y garantiza que no haya sido

alterado.

Estas partes están codificadas en Base64 y se combinan con puntos para formar el token completo.

I.3 Vulnerabilidades

- **Robo de token:** Si un atacante obtiene acceso al token, puede suplantar al usuario.
- **Firma débil:** Si la clave secreta utilizada para firmar el token es débil, el token podría ser falsificado.
- **Expiración:** Los JWT deben tener una fecha de expiración para limitar su validez.

Robo de cuentas, derivación de privilegios y filtraciones de datos son riesgos potenciales al usar JWT. Algunas amenazas se deben a implementaciones incorrectas o claves secretas débiles.