Coworking App -Backend-JWT Token

Ivan <<<mark>ossan</mark>>> Pesenti Software Developer



TOKEN... TOKEN... TOKEN OVUNQUE!



Prima dei Token...

- Prima che fosse introdotta l'autenticazione tramite i token, il meccanismo più usato era quello basato sulle password
- Quest'ultima metodologia implicava i seguenti aspetti:
 - ☐ L'utente doveva generare molte password
 - ☐ L'utente doveva ricordarsi tutte le varie password
 - L'utente, ogni volta che doveva accedere, doveva immettere le password



Svantaggi delle Password

- Le persone tendono a scriverle su file o carta. Questo facilita i furti di credenziali
- □ Le persone tendono a ripetere la stessa password per più account. In caso di compromissione di un account, a cascata, ne vengono compromessi molti altri
- Le persone, quando richiesto loro di modificare la password, tendono a cambiare solamente un carattere. Questo indebolisce la sicurezza e facilita l'hacker
- Aumenta il consumo di **memoria** sul server in quanto ogni volta che un utente si logga viene creato un record per la sua transazione



AUTENTICAZIONE BASATA SUI TOKEN

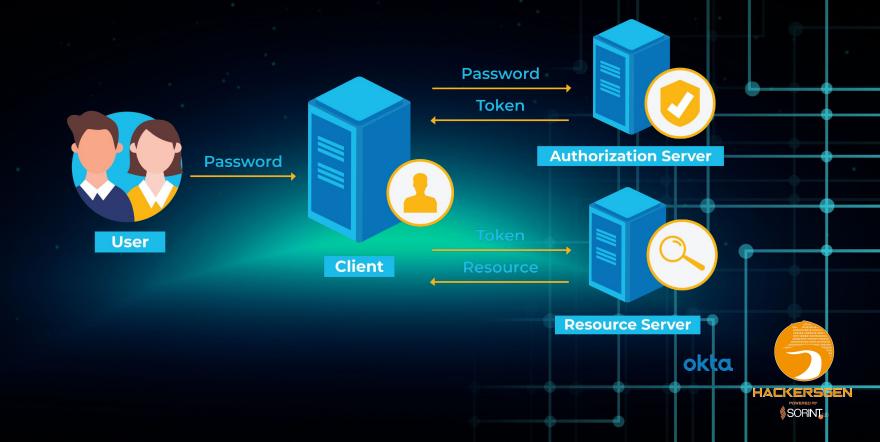


Autenticazione a Token

- ☐ Funzionano come i **biglietti** per i mezzi pubblici
- ☐ Trascorso il periodo di validità (può dipendere dal numero di accessi e/o dal periodo di tempo), il token deve essere rigenerato
- ☐ Deve essere incluso in ogni richiesta che il client invia al server
- □ Solitamente, viene passato in un header della richiesta HTTP
- È una semplice stringa di testo che contiene delle informazioni sull'utente
- ☐ È il meccanismo più usato per l'autenticazione e/o autorizzazione



Il Flusso



TOKENJWT

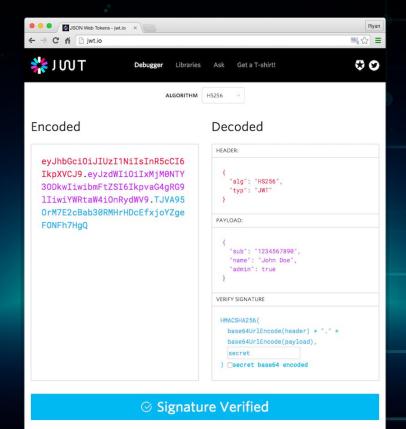


Cosa Sono?

- □ JSON Web Token (o JWT) è uno standard libero
- ☐ È una stringa compatta che viene passata da un sistema all'altro durante la comunicazione
- ☐ Contiene informazioni riguardanti l'utente e i suoi permessi. Le informazioni scritte sul token vengono chiamate claims
- - ☐ Header: definisce il tipo di token e l'algoritmo per la sua firma digitale
 - Payload: contiene l'emittente del token, la data di scadenza e altre informazioni
 - □ Signature: verifica che il messaggio non è stato cambiato durante il transito da un punto all'altro



jwt.io



HACKERSEN SORINT

TOKEN IN GO



THANKS!

@ossan



HACKERSGEN

