JWT

אם נרצה שהAPI שלנו ישמש הרבה סוגים שונים של לקוחות (אנרואיד, IOS, דפדפן, תכונות שונות), זה יהיה טיפה בעייתי, כי דפדפן משתמש בעוגיות אבל IOS לא וכו'.

פה JWT בא לידי ביטוי

Json Web Token – JWT

יתרונות:

- מהיר
- Stateless – לא צריך דאטהבייס
- חוצה פלטפורמות

חסרונות:

- פוגע במפתח הפרטי
- אין לוגים על התחברות
- הטוקן יכול להיגנב

בוא נבין איך JWT עובד

- הלקוח שולח את האישורים(credentials) שלו לשרת
- השרת מאמת את האישורים ויוצר את הטוקן אם הם בסדר
- השרת שולח את הטוקן ללקוח
- הלקוח יישלח את הטוקן בכל בקשה שהוא יישלח
- השרת יוודא את הטוקן – אם הוא עדיין בתוקף ו האם הוא תקין

הטוקן שלנו מורכב מ 3

- הheader
- הpayload
- VERIFY SIGNATURE – הוא מוודא את החתימה של הכל