|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **bcrypt** | |  | | --- | | **JWT (JSON Web Token)** |  |  | | --- | |  | | **Cookie** |
|  | מפתח למחסן | מחסן |
| |  | | --- | | משמש **להצפנה** של סיסמאות בעת שמירתן במסד הנתונים. ככה גם אם יפרצו, לא יראו סיסמאות אמיתיות. |  |  | | --- | |  | | |  | | --- | | **מפתח**/טוקן שמונפק למשתמש **כשמתחבר** בהצלחה – כמו "כרטיס כניסה". |  |  | | --- | |  | | המקום שבו **נשמור** את ה־JWT אצל המשתמש (בצד לקוח). אפשר לעשות אותו HttpOnly כך שרק השרת יקרא אותו – דבר שמונע XSS. |

**סדר פעולות:**

**Bcrypt->מסד נתונים->שליחת סיסמא מהדפדפן->השוואה אם הסיסמא מהדפדפן שווה לסיסמא במסד נתונים-> נוצר JWTעם הפרטים של המשתמש-> JWT נשמר בעוגייה בשרת ונשלח לדפדפן-> בצד לקוח מנסה לעבור לנתיב מוגן->בדיקה אם התוקן שבתוך העוגייה בדפדפן תואמת לעוגייה בצד שרת בתוך מידלוור->מעבר לנתיב המוגן**

1. אני שולחת דרך הקובץ createOneUser.js שם משתמש וסיסמה.
2. הסיסמה מוצפנת עם bcrypt ונשמרת במסד נתונים.
3. המשתמש שולח שם משתמש וסיסמה באמצעות /login
4. השרת בודק האם הסיסמה נכונה באמצעות bcrypt.compare.
5. אם כן, נוצר JWT עם מזהה המשתמש.
6. הטוקן/מפתח/ JWTנשמר בעוגייה (Cookie) ונשלח ללקוח
7. כשאני מנסה לגשת לנתיב מוגן, העוגייה אוטומטית ע"י הדפדפן או Postman
8. במידלוור בודקים אם קיימת עוגייה עם טוקן תקין → אם כן, מאפשרים גישה.