

HTTPS/TLS 1.2+

כל תקשורת בין הדפדפן לשרת חייבת להיות מוצפנת דרך HTTPS עם פרוטוקול TLS 1.2 או גובה יותר, וה SSL Certificate צריך להיות בתוקף ובודק כל 3 חודשים.

Database encryption (AES-256)

כל המידע בסיס הנתונים (שמות, אימיילים, חשבון בנק, עסקאות) חייב להיות מוצפן עם AES-256 כדי שגם אם מישחו גונב את הקובץ, הוא לא יוכל לקרוא את הנתונים.

Backup encryption (AES-256)

כל גיבוי של בסיס הנתונים (יומי, שבועי, חודשי) צריך להיות מוצפן עם AES-256 כדי שהנתונים יהיו בטוחים גם בעת אחסון בענן.

Secret Manager (credentials)

כל הסודות (API keys, database passwords, OAuth secrets) צריכים להיות מאוחסנים בתוך Secret Manager (AWS/Google Cloud) ולא בקובץ או בזיכרון.

(TOTP / Biometric) 2FA

כל משתמש חייב להפעיל Two-Factor Authentication דרך Biometric או Google Authenticator כדי שגם אם סיסמה נגנבה, עדין לא יוכל להיכנס.

Audit logs (24+ חודשים, בלתי ניתנים לשינוי)

כל פעולה (login, view, edit, delete) צריכה להיות מתועדת בנפרד עם תאריך, שעה, מי עשה, מה עשה, ו - IP בלוי יכולת למחוק או לשנות תחת db אחר.

Session timeout

משתמש שלא עשה שום דבר במשך זמן מוגדר (5 דקות אדמיין, 15 דקות משתמש) צריך להיות מנותק אוטומטית, כדי שאם אחד שכח את המחשב בפתחו, מישחו אחר לא יוכל להשתמש בו.

Restore Test (monthly)

כל חודש צריך לבחור גיבוי אקרים, לשחרר אותו לסייע בדיקה (לא לפירודקשן) ולבדק שכל הנתונים שם והאתר עובד - כדי לוודא שבחרום אפשר בעצם להחזיר הכל.

CORS configuration

הגדיר שטומיין מסוים בלבד (yourapp.com) יכול לגשת לAPI, CORS אסור לחלוtin כדי אתרים זדוניים לא יכולים לשולח בקשות בשם המשתמש. (לא יודע מה זה CORS אchkור את זה)

Rate limiting

אם משתמש משדר הרבה הדרישה בזמנים קצר (כמו ניסיון brute force) השרת צריך לחסום אותו זמןית - כדי להגן מפני התקפות של סיסמאות או 2FA tokens, קרייסות וכדומה.

SQL Injection prevention

אף פעם לא לשלב נתונים של משתמש ישירות בשאלילת SQL תמיד להשתמש ב-parameterized SQL - כלומר כדי שימושו לא יוכל להחריק קוד SQL מזיק דרך input field queries

XSS prevention

כל הקלט של המשתמשים צריך להיות escaped לפני הצגה בעמוד (או להשתמש (template engineJavaScript זמני שיגנוב מידע של משתמשים אחרים).

הסביר של איך עושים זאת:

במקום להכניס לדף שירות טקסט כמו:

```
<script>alert('xss')</script>
```

לתוכה שבו מוסיפים מידע, עושים לו escaping כולם ממירים את התווים המיעדים לייצוג בטוח, למשל:

```
&lt;script&gt;alert(&#39;xss&#39;)&lt;/script&gt;;
```

בדף זה יוצג כתקסט רגיל על המסך, ולא יירץ קוד JavaScript בפועל זה אומר:

- ↗ הופך ל-<
- ↘ הופך ל->
- ↗" הופך ל-
- ↘'" הופך ל->
- ↗' הופך ל->
- ↗&#39; הופך ל->

ככה ה-սենյու של המשתמש נשאר תוקן ולא הופך לקוד שרצ בתוך הדף.

CSRF protection

כל form בעמוד צריך להיות עם גסתר token (CSRF token) ששונה לכל משתמש - כדי שאתך זדוני לא יוכל לשדר משתמש שלנו לעשות פעולה בלי שהוא יודע.