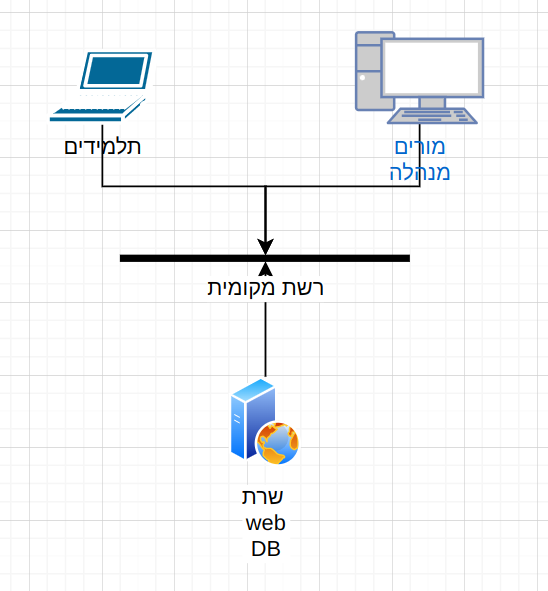
**תרגילי כיתה פיתוח מאובטח**

**ניתוח סיכונים**

1. בחברת התוכנה קימסו מפתחים אפליקציית ווב לניהול בית ספר.

הגרסה הנוכחית של המוצר קיימת 15 שנה, עם ארכיטקטורה מונוליטית ותוכנה שמותקנת on premise. המערכת לא מחוברת לאינטרנט.



ה next-gen של המוצר מתוכנן להיות micro services ב ענן.

עליכם לזהות לפחות 4 חולשות תשתיתיות ברמת סיכון גבוהה שקיימים במערכת החדשה אבל לא קיימים בישנה. השתמשו במודלים שלמדנו CIA ו STRIDE.

2. במהלך בדיקת חדירות תשתיתית במערכת הקיימת, דווחו הממצאים הבאים:

* תוקף בלתי מאומת מבצע סריקת פורטים מהרשת המקומית ומגלה שפורט 80 פתוח
* תוקף מאומת כתלמיד מתחבר מהרשת המקומית ומצליח להעלות הרשאות לאדמין ע"י exploit ידוע שתוקן בגרסה חדשה (המערכת לא מעודכנת).
* תוקף לא מאומת מתחבר לוקאלית (גישה פיזית לשרת) ומצליח לקרוא נתונים של כל התלמידים.

דרגו את חומרת הממצאים לפי CVSS https://www.first.org/cvss/calculator/3.0

איזה הגנות מתאימות לחולשות הנ"ל?

**Secure Design**

התגובה של מנהל ה IT לדו"ח הממצאים הנ"ל היא שהמערכת מנותקת מהאינטרנט ולכן היא מאובטחת.

האם זאת גישה של defense in depth?

תכננו הגנות לפי עקרונות Secure Design בשקף 97.

**הצפנה**

ספק הענן הבטיח למנהל ה IT שכל בעיות האבטחה בענן נפתרות ע"י הצפנה.

תכננו בקרות קריפטוגרפיות עבור האיומים שזיהיתם בתרגילים הקודמים. האם אכן כל האיומים טופלו?

האיומים:

1. חשאיות: ה DATA נמצא בענן משותף עם עוד לקוחות

2. חשאיות, שלמות: לספק הענן יש גישה למידע

3. שלמות: אפשר לשנות את המידע ישירות ב DB בלי לעבור דרך ה WEB

4. חשאיות: ה API חשוף כ REST API לאינטרנט

5. זמינות: המערכת חשופה לאנטרנט