

# פרויקט סיום – סייבר

## הקדמה

במסגרת הפרויקט תשלבו את הידע שלמדתם במסגרת קורס הסייבר, ביחד עם עקרונות של שפת פיתוח בפי שלמדתם כדי לפתח מערכת מידע מבוססת ווב ומסד נתונים רלציוני.

## דרישות המערכת

יש לפתח מערכת ווב עבור חברת תקשורת דמיונית בשם LTD\_Communication, חברת זו משוקת חברות גלישה באינטרנט ובמגרם המידע שלה ניתן למצוא בין היתר מידע על לקוחות החברה, חברות הגלישה השונות והסקטורים אליהם היא משוקת את מוצריה.

## דרישות

1. מסד נתונים רלציוני. לדוגמה מסוג Sql express או MySql
2. הקמת אתר ווב . שפת פיתוח לבחירתכם . לדוגמה (פיתון Django או ג'אווה או C# )

## חלק א ( פיתוח עקרונות של פיתוח מאובטח )

- .1 מסך Register של משתמשים חדשים
- a. הגדרת יוזרים חדשים
- b. הגדרת סיסמא מורכבת ( הגדרות ודרישות סיסמא מורכבת ינויל באמצעות קובץ קונפיגורציה )
- c. סיסמא תשמר במסד הנתונים באמצעות שימוש בפונקציית HMAC + Salt

פ. הגדרת מיל למשתמש

2. מסך לשינוי סיסמה עבור משתמש

א. הזנת סיסמה קיימת

ב. הכנסת סיסמא חדשה אשר תעמוד בדרישות כפי ש谟גדר בקובץ הקונפיגורציה

3. מסך **Login** " למערכת מידע LTD\_Communication "

א. הזנת יוזר

ב. הזנת סיסמא

כ. בדיקה אם המשתמש קיים או לא והחזרת הודעה מתאימה.

4. מסך מערכת

א. הכנסת لكוח חדש עם פרטיים חדשים.

ב. הצגה למסך את שם החדש שהוזן.

5. מסך "שכח סיסמא"

א. המשתמש מפעיל אופציה זאת

ב. המערכת מייצרת ערך אקראי ושולחת אותו למיל של המשתמש

כ. הערך האקראי חייב להיות מוגדר באמצעות SHA-1

ד. המשתמש מזין ערך זה על מנת שיוכל להגיע לחלון שינו סיסמא של המשתמש.

## חלק ב (שימוש בטכניקות XSS + Sql)

- .1 הצגת דוגמא לשימוש בהתקפה מסוג XSS Stored בסעיף 4 מחלק א
- .2 הצגת דוגמא לשימוש בהתקפה מסוג Sqli בסעיף 1 + סעיף 3 + סעיף 4 מחלק א של הפרויקט.
- .3 הצגת פתרון נגד הפרצות בסעיף 1 על ידי שימוש בקידוד של תווים מיוחדים.
- .4 הצגת פתרון נגד הפרצות בסעיף 4 + סעיף 1 + סעיף 3 מחלק א על ידי שימוש ב Parameters או שימוש ב Stored procedures

שים לב – יש להגish 2 גרסאות של העבודה. גרסה אחת עם קוד פגיע לסעיפים בחלק ב, וגרסה אחרת עם קוד לא פגיע לסעיפים בחלק ב

### קובץ קונפיגורציה לניהול סיסמא ( ערכים ניתנים לשינוי על מנהל המערכת )

- .1 אורך סיסמא : [10]
- .2 סיסמא מורכבת : [אותיות גדולות , קטנות, ספרות, תוים מיוחדים]
- .3 היסטוריה : [ 3 פעמים ]
- .4 מניעת שימוש במילון [...] ]
- .5 מספר ניסיונות בשלב ה [3]>Login

**בהצלחה**