

פרוייקט סיום – סייבר

הקדמה

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

דרישות מהמערכת

יש לפתח מערכת ווב עבור חברת תקשורת דמיונית בשם Communication_LTD, חברה זו משווקת חבילות גלישה באינטרנט ובמאגר המידע שלה ניתן למצוא בין היתר מידע על לקוחות החברה, חבילות הגלישה השונות והסקטורים אליהם היא משווקת את מוצריה.

דרישות

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

חלק א (פתוח עקרונות של פיתוח מאובטח)

1. מסך Register של משתמשים חדשים

a. הגדרת יוזרים חדשים

b. הגדרת סיסמא מורכבת (הגדרות ודרישות סיסמא מורכבת ינוהל באמצעות קובץ קונפיגורציה)

c. סיסמא תשמר במסד הנתונים באמצעות שימוש בפונקציית HMAC + Salt

- d. הגדרת מייל למשתמש
2. מסך לשינוי סיסמא עבור משתמש
 - a. הזנת סיסמא קיימת
 - b. הכנסת סיסמא חדשה אשר תעמוד בדרישות כפי שמוגדר בקובץ הקונפיגורציה
3. מסך Login " למערכת מידע LTD_Communication "
 - a. הזנת יוזר
 - b. הזנת סיסמא
 - c. בדיקה אם המשתמש קיים או לא והחזרת הודעה מתאימה.
4. מסך מערכת
 - a. הכנסת לקוח חדש עם פרטים חדשים.
 - b. הצגה למסך את שם לקוח החדש שהוזן.
5. מסך "שכח סיסמא"
 - a. המשתמש מפעיל אופציה זאת
 - b. המערכת מייצרת ערך אקראי ושולחת אותו למייל של המשתמש
 - c. הערך האקראי חייב להיות מוגדר באמצעות SHA-1
 - d. המשתמש מזין ערך זה על מנת שיוכל להגיע לחלון שינוי סיסמא של משתמש.

חלק ב (שימוש בטכניקות Sqli + XSS)

1. הצגת דוגמא לשימוש בהתקפה מסוג Stored XSS בסעיף 4 מחלק א
 2. הצגת דוגמא לשימוש בהתקפה מסוג Sqli על סעיף 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.
- שימו לב – יש להגיש 2 גרסאות של העבודה. גרסה אחת עם קוד פגיע לסעיפים בחלק ב , וגרסה אחת 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, תווים מיוחדים]
3. היסטוריה : [3 פעמים]
4. מניעת שימוש במילון [.....]
5. מספר ניסיונות בשלב ה Login [3]

בהצלחה