*פיתוח אתר אינטרנט מאובטחת*

מטרות ודגשים:

1. פיתוח האתר יתבצע באחת משפות הפיתוח הבאות:JAVA, .Net או PHP.
2. הפיתוח יתבצע באמצעות Design Pattern של MVC.
3. Keep it simple stupid. על השירות להיות פשוט, נוח, ומעוצב.
4. מומלץ להשתמש ב Bootstrap על מנת להקל על של העיצוב של המערכת.
5. על המערכת להיות מאובטחת לפי הדגשים והעקרונות שנלמדו במהלך הקורס.
6. מומלץ לעבוד עם מסד נתונים מסוג SQLite מסיבות של נוחות.
7. יש לכתוב קוד נקי, תקין, מסודר וברור לפי עקרונות פיתוח שנלמדו בתואר.
8. יש לתת שמות לגיטימיים למשתנים לפונקציות. למשל, מקרה הבא לא יתקבל: "inttmp = 0;".
9. ההגשה הינה עד התאריך3.1.17 בשעה 23:59.

ממשק משתמש:

1. ~~עמוד Login– העמוד יכלול שם משתמש, סיסמה וכפתור login. לאחר ביצוע הזדהות המערכת תעביר את המשתמש לעמוד Home. כמו כן בעמוד Login, יהיה לינק שיעביר את המשתמש לעמוד Registration.~~

~~יש לנעול את המשתמש לאחר X פעמים של ניסיון התחברות.~~

~~יש להשתמש בSha256בשביל הסיסמא~~

~~יש לשמור בcookie את הsessionID ולפתוח Session חדש למשתמש~~

~~לשמור בsession האם משתמש רגיל או אדמין~~

~~יש להשתמש בAntiXSS~~

1. ~~עמוד Registration– באמצעות עמוד זה לקוח חדש יוכל לייצר משתמש במערכת. משתמש כולל את הפרטים הבאים:~~
   * ~~שם משתמש~~
   * ~~סיסמה~~
   * ~~שם~~
   * ~~שם משפחה~~
   * ~~כתובת מייל~~
   * ~~מספר טלפון~~
   * ~~תמונה~~

~~יש להשתמש בSha256בשביל הסיסמא~~

~~יש לשמור בcookie את הsessionID ולפתוח Session חדש למשתמש~~

~~יש לשמור בsession שהמשתמש הוא משתמש רגיל~~

~~יש להשתמש בAntiXSS~~

1. ~~עמוד Home– עמוד הבית של המערכת, מורכב מהחלקים הבאים:~~
   * ~~חלק עליון של העמוד – תפריט של המערכת דרכו ניתן לנווט לפונקציונליות השונה במערכת.~~

~~פרופיל, התנתקות, חנות, עגלת קניות, דף הבית, עמוד אדמין, פורום.~~

* + ~~מרכז העמוד – מנוע חיפוש המאפשר לחפש מידע אודות ה Business Logic של המערכת.~~

~~יש להשתמש ב AntiXSSבדף החיפוש~~

~~יש להשתמש ב~~[~~Prepared Statement~~](https://www.google.co.il/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjS96vNisfVAhWLWRoKHc76BNAQFggwMAA&url=http%3A%2F%2Fsoftware-security.sans.org%2Fdeveloper-how-to%2Ffix-sql-injection-in-java-using-prepared-callable-statement&usg=AFQjCNEwfitsYf_8ZxqcmLiRuupDQDLrog)~~למניעת Sql Injections~~

~~חיפוש של ערך (תקליט, אומן, ז'אנר...) והצגת תוצאות בעמוד תוצאות חיפוש (Store). גם ב Store אפשר לחפש ערכים ולמיין לפי רשימת קטגוריות.  
כמו כן מרכז העמוד יכלול מידע וחדשות הרלוונטים ל Business Logic של המערכת (יש לציין כי חלק זה יכול להיות סטטי לצורך הפשטות).~~

~~הצגת תקליטים חדשים שנוספו לחנות.~~

* + ~~חלק תחתון של העמוד – יש לייצר Footer, כך שיכלול קישורים ל:~~

    - ~~Help~~
    - ~~Jobs~~
    - ~~Terms~~
    - ~~Privacy~~
    - ~~Contact Us~~

**~~דגש: אין צורך לממש את העמודים של הקישורים ב Footer.~~**

~~יש לבדוק שהמשתמש מחובר~~

1. תפריט של המערכת והפונקציונאליות של המערכת:
   * עמוד Forum– בפונקציונאליות זו משתמש יוכל לפרסם שאלות ולקבל עליהן תשובות שרלוונטיות ל Business Logic של המערכת.

יצירת נושא (על אומן, תקליט, שיר.....), כניסה לנושא ופרסום תגובות.

יש להשתמש בAntiXSSכשכותבים שאלה ותשובה

יש להשתמש ב[Prepared Statement](https://www.google.co.il/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjS96vNisfVAhWLWRoKHc76BNAQFggwMAA&url=http%3A%2F%2Fsoftware-security.sans.org%2Fdeveloper-how-to%2Ffix-sql-injection-in-java-using-prepared-callable-statement&usg=AFQjCNEwfitsYf_8ZxqcmLiRuupDQDLrog)למניעת Sql Injections

יש לבדוק שהמשתמש מחובר

* + ~~שני עמודי Business Logic– יש לממש שני עמודי פונקציונאליות רלוונטים למערכת. למשל, אם מדובר במערכת בנקאית אפשר לממש עמוד באמצעותו ניתן לקחת הלוואה מהבנק. דוגמה נוספת, עמוד באמצעותו המשתמש יכול להעביר כספים מהחשבון שלו לחשבון של משתמש אחר.~~

1. ~~צפייה בפרטי תקליט, בחירת כמות, צבע, הקדשה, בחירת רצועות מוזיקה מתוך התקליט והוספה לעגלת קניות.~~
2. ~~סיכום הזמנה והזנת פרטי Shipping.~~

~~יש להשתמש בAntiXSSכשמכניסים קלט~~

~~יש להשתמש ב~~[~~Prepared Statement~~](https://www.google.co.il/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjS96vNisfVAhWLWRoKHc76BNAQFggwMAA&url=http%3A%2F%2Fsoftware-security.sans.org%2Fdeveloper-how-to%2Ffix-sql-injection-in-java-using-prepared-callable-statement&usg=AFQjCNEwfitsYf_8ZxqcmLiRuupDQDLrog)~~למניעת Sql Injections~~

~~יש לבדוק שהמשתמש מחובר~~

* + ~~עמוד Information– עמוד בו המשתמש יכול לראות נתונים אודות החשבון שלו לפי ה Business Logic של האתר. למשל, במערכת בורסה, יהיה עמוד בו המשתמש יכול לראות את כל המניות שהוא קנה.~~

~~יש לבדוק שהמשתמש מחובר~~

~~המשתמש צופה בהיסטוריית הקניות שלו.~~

* + ~~עמוד Profile– עמוד בו משתמש יכול לערוך את הפרופיל שלו.~~

~~יש לבדוק שהמשתמש מחובר (לקחת את הנתונים מהsession שלו)~~

~~יש להשתמש ב AntiXSS~~

* + ~~עמוד Logout–עמוד שמאפשר להתנתק מהמערכת. לאחר ההתנתקות המשתמש יעבור לעמוד login.~~

~~יש למחוק את הcookie של המשתמש וגם למחוק את הsession~~

* + **עמוד Admin– ממשק ניהול של המערכת, רק משתמש ברמת הרשאה של ADMIN יוכל לראות ולהשתמש בפונקציונליות זו. באמצעות ממשק Admin, מנהל המערכת יכול לערוך את רמת ההרשאות של משתמשי המערכת ממשתמש רגיל למשתמש Admin.**

יש לבדוק שהמשתמש מחובר ומסוג אדמין (עבור כל קריאה לשרת)

הוספה\עריכה של תקליטים חדשים, ניהול קטגוריות, ניהול רמת הרשאה של משתמשים.......

אובייקטים שצריך:

User (UserID, FirstName, LastName, UserName, Password, Email, Phone, PictureUrl,IsAdmin)

Category (CategoryID, CategoryName)

Disc (DiscID, Name, Artist, CategoryID, **CategoryName**,PictureUrl, Price,Duration,SongsAmount)

Order (OrderID, UserId,OrderTime,DiscID , Amount, Address, City , Country, IsBought)