פיתוח מאובטח	

נוהל עקרונות פיתוח מאובטח

1. כללי

אפליקציות ובהן אתרי אינטרנט חשופות למתקפות המתבססות על ניצול חולשות אפליקטיביות שונות כגון זליגת מידע , פגיעה באמינות ובזמינות המידע ,חשיפת מידע רגיש ועד להשתלטות על תשתיות הארגון .מתן דגש על שלבי הפיתוח המאובטח בתהליכי מחזור חיי המערכת , יצמצם בצורה משמעותית מתקפות אלו.

2. מטרת ההנחיה

2.1. להנחות את קהל היעד לרבות מיקור חוץ וספקי משנה ,בדבר אופן הביצוע וליווי תהליך הפיתוח בכל שלבי מחזור חיי המערכת ,בדגש על היבטי ניהול והערכת סיכונים בתחום אבטחת המידע.

3. הגדרות ומושגים

3.1. הזרקת קוד זדוני - (Injection) הזרקת קוד זדוני ע״י שאילתות SQL, PHP ,LDAP וכו׳.

3.2. Black Box - מבחן חוסן למערכת המבוסס על העובדה כי לתוקף אין ידע פנימי מקדים אודות המערכת. בדיקה זו מתבצעת בעיקר ע״י כלים אוטומטיים.

3.3. Gray Box - מבחן חוסן למערכת המשלבת בין ה white box ל black box לתוקף מידע חלקי על המבנה הפנימי של היישום ומטרתו היא למצוא בהם חולשה.

3.4. White Box - מבחן חוסן למערכת המבוסס על בדיקת קוד המקור וארכיטקטורת הרשת .מטרת הבדיקה היא לספק הערכה מקיפה של נקודות התורפה של המערכת.

3.5. Input Validation בדיקה לעיבוד קלט שמטרתה לקבלה או דחיית נתונים ע״פ כללים.

3.6. Parameter Tampering - וידוא כי הקלט המגיע מהמשתמש לשרת לא שובש ולא שונו בו פרמטרים.

3.7. התקפת מניעת שירות (DDOS – Distributed Denial Of Service) - מתקפה המנצלת את משאבי המערכת כגון מעבד ,רוחב פס או זיכרון ובכך גורמת לבעיות בזמינות השירות.

3.8. Agile Software Development – גישה בהנדסת תוכנה שגובשה כחלופה לגישת המפל. שיטה זו מחייבת פיתוח בצוותים רב תחומיים (כגון צד המפתח ,צד הלקוח , צד תשתיות ונציג אבטחת מידע) אשר משתפים פעולה בחבילת פיתוח ספציפית מתוך מטרה לתת מענה לדרישות העולות במהלך תהליך הפיתוח ועל ידי כך לייעל ולהאיץ את התהליך.

3.9. יירוט התעבורה (Man In The Middle) מתקפה בה התוקף מאזין לתעבורה וביכולתו לגנוב זהות או מידע העובר בין המשתמש לשרת.

3.10. נעילת מוות - (Dead Lock) מצב של נעילה מעגלית בה מספר טרנזקציות ממתינות זו לזו כדי לעדכן מקור נתונים המוחזק ע"י טרנזקציה שונה.

3.11. (Web API) Web service - דרך התחברות לתוכנה המאפשר צריכת שירותים על ידי שימוש בתקנים כגון SOAP ו-REST.

3.12. קוד פתוח – קוד מקור הניתן למפתחים אחרים לשימוש ,להפצה ולהעתקה . מפתחים המבצעים שינויים בקוד יכולים לבחור אם לשומרם או לפרסמם חזרה לקהילת המפתחים בהתאם לסוג רישיון קוד המקור הקובע את כללי השימוש בו מבחינה משפטית.

3.13. התממה (Anonymization) - תהליך הנועד להפחתת חשיפת נתונים באמצעות השמטת שדות או ערכים מקובץ המקור.

3.14. ערבול נתונים (Data Masking) - שינוי סדר הופעת הנתונים בצורה המאפשרת שמירה על לוגיקת הנתונים כגון ספרת ביקורת של תעודת זהות.

3.15. ערפול (Obfuscation) - שיטה להסתרת קוד המקור ,כך שהקוד הופך ללא קריא.

4. איומים

4.1. ארגון OWASP מוציא מדי תקופה את רשימת עשרת הפגיעויות הנפוצות ביותר שהתגלו בתקופה האחרונה . מחזור החיים של הפיתוח המאובטח נדרש להתעדכן מדי עת מול אותן פגיעויות ולבצע התאמות פיתוחיות בהתאם, לשם צמצומן.
להלן וקטורים מרכזיים:

4.1.1. הזרקת קוד זדוני - (Injection) מבוצע על ידי שאילתות SQL, PHP,LDAP תוך מניפולציה של נתונים אלו .על ידי כך יוכל התוקף לבצע מגוון פעולות , לדוגמה ,ביצוע שאילתות לא חוקיות בבסיס הנתונים ובכך לשלוף נתונים מתוך המערכת.

4.1.2. הזדהות שבורה – (Broken Authentication) הטמעת פונקציונאליות הקשורה להזדהות וניהול ההזדהות אל מול שרת המערכת אשר נעשית בצורה שגויה . ליקויים הנובעים מכך עלולים לאפשר לתוקף לנצלם להשגת גישה שאינה מורשית לחשבונות משתמשים ,סיסמאותיהם ,מזהה החיבור שלהם אל מול האתר (Session Tokens), מידע אודותיהם ועוד.

פיתוח מאובטח	

4.1.3. חשיפת מידע רגיש - (Sensitive Data Exposure) כאשר אפליקציות או מנגנוני API אינם מגנים כראוי על המידע הרגיש אותו הם מכילים(כגון מידע פיננסי , רפואי וכדומה) תוקפים עלולים להיחשף ,להדליף ואף לערוך את אותו מידע ולנצלו לרעה.

4.1.4. ישויות XML חיצוניות - (XML External Entities- XXE) פגיעות הנגרמת מליקוי הגדרה ב- (XML Parsersמנגנוני עיבוד) XML המאפשר לתוקף להכריז על ישות XML חיצונית (External Entity) שתעובד ע״י המנגנון הפגיע .מצב זה מאפשר לתוקף לנצל את המנגנון לחשיפת קבצים מקומיים במערכת ההפעלה לגשת לשירותים הקיימים על השרת ולהרצת קוד מרוחק.

4.1.5. בקרת גישה שבורה - (Broken Access Control) מצב בו תוקף ניגש לפונקציונאליות שאינה מורשית ולבצע פעולות כגון עריכת הרשאות ,פעולות אדמיניסטרטיביות ,גישה למידע רגיש אודות משתמשים אחרים במערכת וגישה לקבצים.

4.1.6. ליקויי הגדרות אבטחה (Security Misconfiguration) - חולשה נפוצה הנגרמת כתוצאה משימוש בהגדרות קונפיגורציה חלשות ,ברירת מחדל או הגדרות חלקיות .החולשה יכולה לבוא לידי ביטוי בהגדרות מערכת ההפעלה של שרת האפליקציה ,על שימוש בספריות קוד באופן לא מאובטח .יש לוודא כי אין סיסמאות חלשות ,סיסמאות ברירת מחדל, הסרת סקריפטים המוגדרים כברירת מחדל בשרתים ,ספריות ברירת מחדל והודעות שגיאה המוגדרות כברירת מחדל.

4.1.7. Cross-Site-Scripting (XSS) - פגיעות המתרחשת כאשר אפליקציה מאפשרת הזרקת קלט לא מהימן, בלי ביצוע תהליך אימות על אותו קלט . כתוצאה מכך ,תוקף אשר שולט בערכו של אותו קלט יוכל להזריק קוד זדוני לאתר ולבצע פעולות כגון הזרקת קוד אשר קורא את ערך ה Session ID -של משתמש אחר ושליחתו לתוקף ,השחתת פני האתר ,ביצוע , Phishing הורדת קובץ הרצה זדוני .קיימים חמישה סוגים של חולשת XSS כאשר שלושת העיקריים הינם Stored , Reflected ו DOM-based , שתי תצורות נוספות הינן Self XSS אשר דורש שילוב עם חולשה נוספת בכדי לנצלו(לדוגמה) CSRF ו . Blind XSS

4.1.8. Insecure Deserialization - סריאליזציה היא תהליך של תרגום אובייקט המכיל נתונים לפורמט הניתן לאחסון ולהעברה כגון , XML כאשר די-סריאליזציה הינה הפעולה ההפוכה לכך .כאשר האפליקציה מבצעת די-סריאליזציה של קלט משתמש לא מהימן ומייצרת ממנו אובייקט גנרי ,תוקף

פיתוח מאובטח	

אשר מורשה לערוך את אותו ערך עלול לגרום להיווצרות אובייקט המכיל פונקציונליות זדונית ,לרבות הרצת קוד זדוני בשרת המערכת.

4.1.9. שימוש ברכיבים עם פגיעויות ידועות Using Components with known vulnerabilities - רכיבים כגון ספריות קוד ,מודולים ותוכנות צד שלישי מורצים לרוב באותן ההרשאות של המערכת .במידה ורכיב מסוים פגיע ,תוקף עלול לנצלו לביצוע פעולות זדוניות ואף להשתלטות על השרת .לכן ,יש לעדכן את הרכיבים במערכת באופן קבוע.

4.1.10. תיעוד וניטור בלתי מספקים (Insufficient logging and monitoring) למרות נקיטת אמצעי בטיחות, עדיין עלול להתרחש אירוע אבטחת מידע .גילוי מוקדם ומהיר ימזער נזקים ולכן יש לדאוג לתיעוד, פיקוח וניטור המערכת ולהתריע על כל פעילות חשודה.

5. פירוט ההנחיה

5.1. עקרונות הפיתוח המאובטח:

5.1.1. עקרון החוליה החלשה -הרכיב החלש ביותר מבחינה אבטחתית הוא הקובע את חוזק מערכת ההגנה כולה . נקודת החולשה נקבעת גם על ידי מידת החשיפה לאיום ,ולא דווקא מהאיום עצמו.

5.1.2. הרשאה מינימלית -כל פעולה במערכת חייבת להתבצע בהרשאה מינימאלית הניתנת לפרק הזמן הקצר ביותר. הענקת הרשאות גבוהות מהנחוץ הופכת את המערכת המאובטחת לחשופה ופגיעה יותר. הבסיס למתן הרשאות גישה צריך להתבסס על תפקיד העובד (עפ"י העיקרון הצורך לדעת Need-to-Know) ומינימום הרשאות שנדרשות לצורך ביצוע עבודתו(Least Privilege).

5.1.3. פשטות - עקרון זה הופך את המערכת לצפויה (דטרמיניסטית)יותר וקלה יותר לבדיקה .מערכת מורכבת, קשה יותר לבדיקת חוסן .פשטות עוזרת להבנת אופן השימוש, איתור בעיות פוטנציאליות, קלות בתחזוקה והפחתת מקומות פוטנציאליים לטעות.

5.1.4. מצב ברירת מחדל בטוח -עקרון זה מנחה אילו פעולות ניתן לבצע על המערכת ולשלול כל פעולה אשר אינה צפויה או אינה עונה על תנאי מוגדר.

5.1.5. נקודות גישה מוגבלות ושמורות -יש להגביל את מספר נקודות הגישה למערכת ולהגן על נקודות אלו.

5.1.6. הגנת עומק על המערכת להתוות מספר קווי הגנה ,על מנת למנוע תלות בנקודה קריטית ,אפקט הדומינו והתפשטות הנזק .על כל תהליך להיות בנוי משלבים

פיתוח מאובטח	

אשר בכל אחד מהם מוטמע מנגנון אבטחה (אימות, מניעת זליגה ,רישום לקובץ לוג וכו').

5.1.7. שימוש ברכיבים קיימים - עקרון הסתמכות על מנגנוני אבטחה ידועים הופכת את המערכת לבטוחה ואמינה יותר.

5.1.8. השארת תיעוד - על המערכת להשאיר תיעוד של הפעילות בכדי לזהות מתקפה בצורה שתאפשר לשקם את הנזק ולאתר את מקור הפגיעה הנחוץ למניעה עתידית.

5.1.9. הצפנה - יש לשמור הן על סודיות אלגוריתם ההצפנה והן על סודיות המפתח. יש להקפיד על תכנון אופן שמירת המפתחות והגנת הגישה אליהם.

5.1.10. פרטיות וחשאיות - יש למנוע דליפת מידע אודות אמצעי האבטחה המיושמים במערכת.

5.1.11. הפרדת מערכות - מערכת הבקרה ומערכות אבטחת המידע צריכות להיות מחוץ להישג ידו של הגורם המבוקר .עקרון זה תקף לגבי קבצי חיווי ואמצעי גילוי ומניעה שונים.

5.2. תהליך הפיתוח

5.2.1. על הספק לדאוג להכשרת הצוותים בפיתוח מאובטח ולהגברת המודעות בנושא.

5.2.2. לתהליך פיתוח שתי שיטות עיקריות – המסורתית (Water fall) והאג'ילית (Agile) המסורתית מבוססת על שיטת עבודה טורית ,בה מתבצע אפיון מלא של המערכת כפי שתהיה בתצורתה הסופית .בסיום הפיתוח מתקבל תוצר סופי מוגמר ,דבר הגורם לסרבול בדיקות חוסן המערכת בעקבות ריבוי הפונקציונאליות .אבטחת המידע מתבצעת בשלב האפיון והעליה לאוויר ולא מתעדכנת לאורך כל תהליך הפיתוח כיום .להלן טבלה ובה עקרונות תפעוליים בשימוש בשיטת Agile.

- Agile - מתמקד במתודולוגיה .גישה זו מנהלת את הפרויקט בהתאם לדרישות ושינויי הלקוח לכל אורך תהליך הפיתוח.
- Continuous Integration and Continuous Delivery (CI/CD) - מתמקד ב lifecycle מחזור החיים של המוצר, עקרון זה מתמקדת באוטומציה ,תוך ביצוע בדיקות תכופות לקוד.
- DevOps - גישה המאגדת בתהליך שיתוף של צוות הפיתוח ,תפעול ואבטחת מידע .מיקוד השיטה הוא ביצוע הערכת סיכוני סייבר.

5.2.3. יתרונות השימוש בעקרונות אלו:

5.2.3.1. אפיון גמיש של הפרויקט.

5.2.3.2. תוצר ראשוני מהיר.

5.2.3.3. ביצוע סבבים קצרים של העלאות גרסה.

5.2.3.4. צוותי אבטחת המידע מהווים חלק בתהליך בכל שלביו.

5.2.3.5. צוותי אבטחת המידע בודקים רכיבים באופן נקודתי בכל העלאת גרסה.

5.2.3.6. צוותי אבטחת המידע בודקים את הרכיבים בתדירות גבוהה ,דבר המאפשר להתמקד באיומים בצורה עדכנית.

- מבחינות רבות ובכללן היבטי אבטחת מידע ,שיטת הפיתוח המועדפת היא עבודה ב Agile אשר מאפשרת לצוותים שיתוף פעולה והבנה של התהליך הקיים וביצוע תיקונים בכל שלב שהוגדר לביצוע .שיטה זו תמנע מצב בו המוצר מגיע לשלביו האחרונים מבלי שטופלו סוגיות אבטחת מידע.

5.3. שלב בדיקות אבטחת המידע בתהליך הפיתוח

תהליך ה) Secure Software Development Lifecycle) -SSDLC הינו תבנית לשלבי הפיתוח המאובטח הבנויה מחמישה שלבים:

5.3.1. דרישות :לאסוף את הדרישות המגדירות את אופן הפעולה של היישום.

5.3.2. עיצוב :תכנון הרכיבים בתוכנה ,הקשרים בניהם ושימוש ברכיבי צד שלישי.

5.3.3. קידוד :השתמש בדרישות כדי לקודד את הפונקציונליות של היישום.

5.3.4. בדיקה :לבדוק את היישום עבור כל הבאגים.

5.3.5. פריסה :לדחוף את היישום של פיתוח או בימוי לשרת הייצור.

5.3.6. בכל שלב במודל ה SSDLC- Secure Software Development Lifecycle מנהלי אבטחת המידע נדרשים להשתמש בתהליך Application Threat Modeling במקרים הבאים:

5.3.6.1. בכל פעם שמתבצע שינוי בארכיטקטורה.

5.3.6.2. לאחר כל שינוי או פגיעות שנמצאה.

5.3.6.3. בשלב הראשוני לאחר סיום בניית הארכיטקטורה.

5.3.6.4. תהליך ה Application Threat Modeling - מחולק לחמישה שלבים:

5.3.6.4.1. זיהוי משאבים – זיהוי משאבים רגישים עליהם יש להגן ,החל ממידע רגיש ועד זמינות אתר ה- WEB .

5.3.6.4.2. חלוקה לרכיבים עיקריים – פירוק האפליקציה לרכיבים עיקריים ,בחינת הקשרים ביניהם ומעברי המידע ביניהם .הצגה בעזרת תרשימי (Data Flow Diagram) DFD

5.3.6.4.3. זיהוי האיומים – שימוש במודל ,Spoofing) STRIDE Tampering, Repudiation, Information Disclosure, Denial of

פיתוח מאובטח	

Service, Elevation of privilege) על מנת לבחון האם האפליקציה פגיעה לסוגי התקפות שונות.

5.3.6.4.4. שערוך פוטנציאל נזק – שימוש במודל (DREAD Damage Exploitability, Affected users, potential, Reproducibility, Discoverability) על מנת לשערך את פוטנציאל הנזק והסיכוי לפגיעה של כל איום .סדר הטיפול באיומים יהיה מהכבד אל הקל.

5.3.6.4.5. תיעוד האיומים - לאחר ביצוע השלבים הנ"ל ,מפיקים מסמך אשר יכיל את כל המידע אשר נאסף בשלבים הקודמים.

5.4. תחזוקת סביבת הפיתוח

5.4.1. יש לנהל גרסאות פיתוח בשרת מרכזי (Source Control לדוגמה TFS או SVN.

5.4.2. יש לדאוג להפרדה מוחלטת בין סביבת הייצור לסביבת הפיתוח וסביבות הניסוי.

5.4.3. אין לאפשר לתכניתנים גישה לבסיסי נתונים בסביבת הייצור.

5.4.4. מומלץ לחתום את הקוד באמצעות אלגוריתמים קריפטוגרפים.

5.4.5. בכל עלייה של מערכת יש לוודא את החתימה על הקוד.

5.4.6. יש לחסום את הגישה לממשקי הניהול של האפליקציה מפני גורמים לא מורשים.

5.4.7. יש לתעד כל כניסה לממשקי הניהול של האפליקציה וכל שינוי שהתרחש באפליקציה.

5.4.8. יש לצמצם למינימום הנדרש את הרשאות הגישה לממשקי הניהול ולתשתיות המערכת.

5.4.9. אין להעביר בסיסי נתונים מסביבת הייצור לסביבת הפיתוח ללא התממה או ערפול.

5.5. בדיקות אבטחת מידע למערכת

5.5.1. בשלב זה הספק החיצוני או מנהל הפרויקט(בפיתוח פנימי)יבצע בדיקות , (Testing)בהתאם למפורט במסמך האפיון ,על מכלול תהליכים ,שיטות , פעילויות וכלים המלווים את פיתוח המערכות והמוצרים לאורך מחזור החיים , מתוך כוונה לבצע אימות והוכחת תקפות להתאמת התוצרים לדרישות , למפרטים הטכניים , לתקנים ולנהלים מחייבים.

5.5.2. ניתן לבצע את בדיקות אבטחת המידע במספר אופנים:

5.5.2.1. White Box - מעבר על קוד המקור של המערכת בהיבטי אבטחת מידע , בדיקת תצורת המערכת, תצורת התשתית ותצורת הרשת .בדיקה זו יסודית

ביותר ועלולה לקחת זמן רב(יחסית)במערכות גדולות .היתרון הנוסף של צורת בדיקה זאת היא בכך שלאחר שמתבצע שינוי במערכת ,ניתן לבדוק את ה Delta של השינוי בלבד ואין צורך לבדוק את כל המערכת מחדש .

5.5.2.2. Black Box - בדיקה זאת מהווה אינדיקציה על מצב המערכת מנקודת מבטו של הפורץ ,היא פחות יסודית מקריאת קוד המקור ,אך בדרך כלל אורכת פחות זמן בצורה משמעותית.

5.5.2.3. Gray Box – שילוב של שתי השיטות הנ״ל ,בו נבדקים רק חלקי קוד אשר הוגדרו כרגישים במיוחד ושאר המערכת נבדקת כמשתמש .היתרון של צורת בדיקה זו היא בחיסכון בזמן וכמו כן במיקוד לתוצאות המבוקשות.

5.5.2.4. סריקת הקוד - בכל הטמעה של קוד או קטע קוד לסביבת הייצור יש לבצע סריקה דינאמית וסטטית של הקוד Dynamic Application Security Testingו Static Application Security Testing . - יש להשתמש בתוכנות ייעודיות המשמשות לשם כך.

5.5.2.5. Code Review - בכל הטמעה של קוד או קטע קוד לסביבת הייצור יש לבצע, Code review בדיקה חצי אוטומטית אשר מתבצעת ע״י סוקר קוד , מאתרת ובודקת בצורה ידנית את נקודות התורפה בקוד.

5.5.3. דגשים בביצוע הבדיקות:

5.5.3.1. בכל אחת מהבדיקות יש לקבל דו״ח המתאר את ממצאי אבטחת המידע והמלצות לתיקונם.

5.5.3.2. יש לקיים ישיבה טכנית עם נציג מצוות הפיתוח ,לאחר שקרא את הדו״ח ועם נציג אבטחת המידע שבדק את המערכת .בישיבה זאת יוסברו הממצאים ויוחלט על הנדרש לתיקונם.

5.5.3.3. לאחר תיקון הממצאים יש לערוך בדיקת אבטחת מידע חוזרת.

5.5.3.4. במידה והתגלו פערים מהותיים ,בהתאם להגדרת מנהל אבטחת מידע והגנת הסייבר ,לא יינתן אישור להעביר את המערכת לייצור טרם תיקון הליקויים .במידה והתגלו פערים שאינם מהותיים ,מנהל אבטחת מידע והגנת הסייבר בשיתוף הגורם העסקי ימצאו פתרונות מול הספק/צוות הפיתוח באשר לתיקון הליקויים.

5.5.3.5. הגורם העסקי יגדיר תהליך של בדיקות מסירה המאמת שהן הפונקציונליות של המערכת פועלת באופן תקין והן הסיכונים העסקיים מנוהלים נכונה.

5.5.3.6. בין סבב בדיקות אחד למשנהו צוות הפרויקט יטפל בליקויי אבטחת המידע שנתגלו ויבצע בדיקה חוזרת בסביבת הבדיקות .בסיום כל סבב

פיתוח מאובטח	

יתבצע תיעוד של תוצאות הבדיקה והטיפול בליקויים .כמו כן ,גרסת התוכנה תעודכן בהתאם.

5.5.3.7. מנהל התשתיות יוודא הגדרת סביבת בדיקות למערכת במידת הנדרש . בכל מקרה לא תתבצענה בדיקות בסביבת ייצור של מערכת קיימת.

5.5.3.8. מנהל אבטחת מידע והגנת הסייבר יוודא כי סביבות פיתוח ובדיקות לא יכילו נתוני אמת מלאים (ישנה עדיפות לערבול שדות מזהים)אלא אם אמצעי אבטחת המידע המיושמים בסביבות אלו זהים לאלה המיושמים בסביבת הייצור.

5.6. דגשים בפיתוח כפתרון לאיומים

5.6.1. אימות קלט:

5.6.1.1. הגדרת סוגי תווים נתמכים בצורה מבוקרת ,לדוגמא UTF-8 ,לכל קלט המגיע מהמשתמשים.

5.6.1.2. ביצוע אימות לכל קלט המגיע מצד הקליינט ,לרבות ערכים של פקדים ופרמטרים המגיעים מה URL .

5.6.1.3. וידוא שערכי כותרי ה HTTP Headers -בבקשות ותשובות השרת מכילים אך ורק תווי ASCII .

5.6.1.4. וידוא כי הקלט המתקבל תואם לסוג הקלט המצופה לאותו מנגנון או שירות.

5.6.1.5. וידוא כי אורך הקלט המתקבל תואם לאורך המצופה לאותו מנגנון או שירות.

5.6.1.6. יש להציג פלט למשתמש (בין אם מקורו מתוך המערכת או בקלט משתמש) רק לאחר שעבר קידוד בהתאם להקשר בו הוא נמצא בשימוש.

5.6.2. הצפנה:

5.6.2.1. בביצוע הצפנת מידע רגיש ,יש לממש אלגוריתמי הצפנה מוכרים ע"פ הכללים הבאים:

- AESעבור הצפנה סימטרית
- RSAעבור הצפנה א-סימטרית
- SHA256עבור HASH חד כיווני

5.6.2.2. יש להצפין את תווך הגישה לאפליקציה באמצעות פרוטוקול1.2 ומעלה TLS.

5.6.2.3. התעודה הדיגיטלית תונפק ע"י CA מוכר ומהימן.

5.6.2.4. מפתחות ההצפנה לא יהיו Hardcoded בקוד המקור וישמרו במקום שאינו נגיש למשתמשים.

פיתוח מאובטח	

5.6.2.5. יש להימנע באופן מוחלט מהטמעה של המקרים הבאים:

- Anonymous Diffie-Hellman (לא מספק הזדהות).
- אין לבצע שימוש באלגוריתמים שפותחו בצורה עצמאית.
- NULL (ללא הצפנה בכלל).
- החצנה של אלגוריתמי הצפנה אשר אינם בטוחים בתהליך ה - Negotiation אך גם מורשים לשימוש ע"י שרת המעדיף אלגוריתמים חזקים (מתקפת FREAK).
- אלגוריתם RC4
- הצפנה באמצעות מנגנון 3DES

5.6.2.6. יש להשתמש באלגוריתמים הבאים כדרישת מינימום:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

פיתוח מאובטח	

5.6.2.7. יש לעמוד בסטנדרטים של מסמכי היישום הבאים:

- SSLLabs
- OWASP

5.6.2.8. במידה והמערכת נגישה לאינטרנט, ניתן להשתמש בשירותים חינמיים לבדיקת רמת האבטחה של האלגוריתמים להצפנה הנתמכים ע"י השרת, כגון SSLLabs.

5.6.2.9. במידה והמערכת פנים-ארגונית, ניתן להשתמש בכלים קיימים לביצוע בדיקות אלו מקומית כגון SSLSCAN .

5.7. מניעת מתקפות לניצול יכולות מובנות במערכת:

5.7.1. יש להגביל את המשתמש והאפליקציה בשימוש במשאבים כגון נפח דיסק, זיכרון, מעבד.

5.7.2. חתימה על קבצי ריצה (Executables) כמו DLL ו EXE על ידי חתימה דיגיטלית חתימה כזו תאפשר לוודא את אמינותם של קבצי הריצה המותקנים.

5.7.3. יש לאכוף דרישת הזדהות בכל העמודים והמשאבים של האפליקציה, מלבד אלו אשר נועדו להיחשף.

5.7.4. יש לשקול את השימוש ב Two-Factor Authentication (2FA) לצורך אימות המשתמש.

5.7.5. הליך שינוי סיסמה חייב להכיל: סיסמה ישנה, סיסמה חדשה ואימות סיסמה חדשה בהתאם.

5.7.6. בכל תהליך הכולל מילוי טפסים ושליחתם לשרת, יש להוסיף מנגנון למניעת מילוי טפסים בצורה אוטומטית, דהיינו מנגנון למניעת אוטומציה, כאשר מנגנון מומלץ הינו שימוש בשירות/פיתוח מנגנון Captcha. במידה ונדרש לפתח את המנגנון הנ"ל, יש לוודא כי ה Captcha -בה נעשה שימוש אינה קלה לניחוש (לדוגמה שימוש בתבנית חוזרת, שימוש במספרים ללא אותיות וכדומה) וכי מתבצעת בחינה, בדיקה ואישור בצד השרת של תוכן ערך ה Captcha -שהוזן ע"י המשתמש.

5.7.7. באתרים בהם המשתמש נדרש לבצע התחברות למערכת ע"י הזנת שם משתמש וסיסמה או הזנת פרטים רגישים, יש לבטל את האפשרות למילוי אוטומטי.

< INPUT TYPE="password" AUTOCOMPLETE="off">

פיתוח מאובטח	

5.7.8. תהליכים ופעולות המוגדרות כ״רגישות ,״לדוגמה ממשק ניהול המכיל עמוד המאפשר מחיקת משתמשים ע״י לחיצה על כפתור״ מחק / הסר ,״יכלול חלונית התראה למשתמשים כאשר יידרש אישור נוסף לביצוע הפעולה הנדרשת.

5.7.9. יש להשתמש אך ורק בפרטים המאוחסנים בשרת ולא בפרטים אשר התקבלו מהמשתמש.

5.7.10. יש להטמיע מנגנון נעילת משתמשים לאחר מספר ניסיונות כושלים לשינוי.

5.8. ניהול Session

5.8.1. יש להגביל את זמני פעילות ה Session. משתמש אשר יחרוג מזמן הפעילות שיוגדר ינותק. פעולה זו תביא גם לצמצום השימוש במשאבי המערכת.

5.8.2. יש לוודא כי קיים מנגנון במערכת המאפשר למשתמש להתנתק ולסגור את ה - Sessionהנוכחי.

5.8.3. על הערך המשויך ל Session של משתמש להיות מורכב לפחות מ 32 תווים מורכבים.

5.8.4. יש להימנע מניהול ה Session ID -דרך ה URL -ולוודא כי לא ניתן להעבירם בדרך אחרת מלבד Cookies וזאת בכדי להגן מפני מתקפות. Session Fixation

5.8.5. יש להימנע מלאפשר פתיחת יותר מ Session -אחד בו זמנית.

5.8.6. מומלץ להציג למשתמש את התאריך והשעה בהם בוצעה התחברות למערכת לאחרונה.

5.8.7. יש לוודא כי החלפת ה Session ID -מוגנת מהאזנה ע״י הצפנת התעבורה (HTTPS) לאורך כל פעילות ה Session. בנוסף ,יש להגדיר את ״דגלון האבטחה ״ ב cookie המכונה Secure בערך True , על מנת למנוע העברה של ערך ה - Session IDבתווך שאינו מוצפן .בנוסף ,יש להגדיר ״דגלון אבטחה ״ב cookie המכונה HttpOnly בערך , True על מנת למנוע העברה של ערך ה SessionID באמצעות סקריפט זדוני העלול לחדור למערכת באמצעות XSS.

5.8.8. יש להתייחס ל Session ID כמו לכל קלט משתמש לא מהימן ולבצע ולידציה לתוכנו.

5.8.9. יש לחדש את ה Session ID -לאחר כל שינוי ברמת ההרשאות של המשתמש על מנת לצמצם את השימוש במשאבי המערכת.

5.9. וידוא קונפיגורציה בטוחה

5.9.1. יש לוודא כי לא נותרו הגדרות ברירת מחדל אותם ניתן לנצל לביצוע פעולות לא מורשות במערכת. היות ומשתמשים יינטו לביטול מאפייני אבטחה אשר מקשים על נוחותם ,יש להגדיר הגדרות אבטחה מינימאליות אותן לא ניתן יהיה להסיר.

פיתוח מאובטח	

5.9.2. יש לוודא כי הגדרות האבטחה הבסיסיות (בהתאם ל Framework בשימוש) מוגדרות לרמה הגבוהה ביותר שניתן, לדוגמא(ASP.Net) :

- יש למנוע הצגה של Trace ע"י הוספת הערך הבא לאלמנט : system.web

<trace xdt: Transform="Remove" />

- יש למנוע Debugging ע"י הגדרת דגלון ה Debug -בקובץ ה web.config - ל- False -

5.9.3. הצפנה של Connection string ב-web.config.

5.9.4. יש לוודא שהקוד מקומפל ב Release וכן שלא להעלות לשרת הייצור קבצי PDB.

5.10. הטמעת די-סריאליזציה בטוחה

5.10.1. יש לבצע די-סריאליזציה לאובייקטים מהימנים מוגדרים מראש בלבד, לדוגמא :

result = JsonConvert.DeserializeObject< TrustedObject > (reader.ReadToEnd()); , כאשר TrustedObject מייצג אובייקט מהימן מוגדר מראש אשר מבצע אימות של הקלט בשביל הליך הדה-סריאליזציה.

5.10.2. במידה והמערכת יכולה לדעת אילו הודעות יש לעבד לפני הדי-סריאליזציה, ניתן לחתום אותן דיגיטלית כחלק מהתהליך, ולבחור לא לבצע די-סריאליזציה להודעות אשר אינן מכילות את החתימה.

5.11. דלתות אחוריות(Back Doors)

5.11.1. יש לוודא כי הקוד נבדק במטרה לזהות את קיומן של" דלתות אחוריות "או Debug.

5.11.2. יש לוודא כי לא קיימות מתודות במערכת אשר נועדו לעקוף מנגנוני אבטחה (לרבות בשביל ביצוע ניסיונות, שימוש פנימי ועוד).

5.11.3. יש להימנע משימוש בשמות משתמשים או סיסמאות ברירות מחדל .שמות משתמשים צריכים להיווצר בצורה ייחודית וסיסמאות צריכות להיווצר בצורה רנדומאלית.

5.12. אחסון מידע רגיש על השרת

5.12.1. יש לשמור קבצי מערכת בתיקיות ייעודיות בלבד, בכונן נפרד מכונן השרת עצמו.

5.12.2. במידה ונדרש, יש לבצע אינטראקציה עם קבצי מערכת דרך ערך מזהה (ID) אשר מאומת ע"י טבלה המכילה את אותו ערך ואת שם הקובץ.

5.12.3. יש להצפין את כל המידע האישי או הרגיש של משתמשי המערכת ע"י מנגנון אבטחה עם מפתח הצפנה.

5.12.4. יש להימנע מאחסון מפתחות הצפנה בקוד (Hardcoded) על המפתחות להיות מאוחסנים במיקום חיצוני.

5.13. אחסון מידע רגיש בצד הלקוח

5.13.1. אין לאחסן מידע רגיש ב Cookie במידה ונדרש ,יש לשמור Token ב Cookie אשר ע"פ השרת ידע לקשר משתמש למידע מסוים המאוחסן בשרת.

5.13.2. יש לבצע הפרדה ברורה בין מידע הנועד לשימוש ע"י ה Client למידע שנועד לשימוש ע"י השרת.

5.14. מניפולציה על שדות Hidden

בהתקפה זו מנסה התוקף לשנות ערכים שונים המגיעים לדפדפן ומוסתרים על ידי שימוש בשדה Hidden. ההנחה כי הסתרת ערכים אילו בהכרח מוגנים בפני שינוי של משתמש הינה שגויה ותוקף יכול לבצע שינויים ולבצע בהם מניפולציות על השרת.

5.15. דגשים עיקריים בהגנה עלWeb services

5.15.1. הגבלת מתודות HTTP

5.15.2. אימות Content-Types

5.15.3. CORS (Cross-Origin Resource Sharing)

5.15.4. JWT (JSON Web Tokens)

5.15.5. ממשקי ניהול

5.15.6. טיפול בשגיאות

5.15.7. XXE (XML External Entity Processing)

5.15.8. העברת מידע רגיש בבקשות HTTP

5.15.9. העלאת קבצים

5.15.10. ניצול משאבי זיכרון ותהליך חילוץ קבצי ארכיון ע"י יצירת לולאה אינסופית של חילוץ הקבצים ובכך אף להגיע לקריסת השירות.

5.16. דגשים בהגנה על בסיסי נתונים:

5.16.1. יש להשתמש בהצפנה לכל מידע המקושר לזהות משתמשים וכל מידע רגיש אחר.

5.16.2. שמירת סיסמאות באופן מאובטח בבסיס הנתונים תעשה באופן הבא:

- הסיסמאות יישמרו בבסיס הנתונים לאחר ביצוע הצפנה חד כיוונית HASH
- יש להשתמש באלגוריתם SHA256 וערך SALT עבור כל משתמש:

פיתוח מאובטח	

- (סיסמא + ערךSALT) SHA256

- בעת יצירת סיסמא ייבחר ערך רנדומאלי SALT אשר ישורשר לסיסמא ויישמר בבסיס הנתונים יחד עם פרטי המשתמש.
- בדיקת נכונות הסיסמא תיעשה על ידי שרשור ה SALT -מבסיס הנתונים לסיסמא שהתקבלה ,ביצוע HASH והשוואה מול ה HASH השמור בבסיס הנתונים.

5.16.3. יש לוודא כי מידע רגיש הנמצא בגיבויים מוצפן באותו אופן.

5.16.4. עקרון מינימום הרשאות בבסיס הנתונים(Least Privilege Principle)

5.16.4.1. יש לתת למשתמש בסיס הנתונים הרשאות כתיבה/קריאה בהתאם לנדרש לכל פעולה תוך הפעלת Stored Procedure.

5.16.4.2. אין לאפשר הרשאות גבוהות למשתמש מסד הנתונים במתן דגש על משתמשי dbowner ו sysadmin

5.16.4.3. במידה וישנו צורך נקודתי ניתן לאפשר שימוש במשתמש בעל הרשאות גבוהות בדומה הרשאות ddl_admin

5.16.4.4. בביצוע שאילתות במסד הנתונים אין לשרשר פרמטרים לשאילתה בצורה דינאמית .יש להשתמש ב- Stored Procedureהמקבלים פרמטרים או ב Prepared Statements -עם Parameterized Queries - למידע נוסף.

5.16.4.5. יש לוודא ש xp_cmdshell ו sp_send_dbmail אינן פעילות .במידת הצורך יש להעדיף שימוש ב SQLCLR כחלופה.

5.16.4.6. יש לוודא כי נעשה שימוש בעקרון 3 Tier Architecture בביצוע תקשורת מאפליקציית המשתמש אל מול מסד הנתונים .דהיינו ,שימוש בשרת מערכת/שרת מתווך לביצוע הפעולות הנדרשות אל מול מסד הנתונים . יש לוודא כי לא מתבצעת תקשורת מאפליקציית המשתמש ישירות אל מול מסד נתונים של המערכת.

6. מסמכים ישימים

6.1. Top 10 New Open Source Security Vulnerabilities

6.2. אתר CVE

6.3. Vulnerability Type Change By Year

6.4. NVD Dashboard

6.5. National Checklist Program (NCP)

6.6. Portswigger top 10 web hacking techniques

6.7. cxsecurity

6.8. Rapid7