משרד האוצר
החשב הכללי

ממשל זמין

כללים לביצוע בדיקת חוסן (**Penetration Test**)

מסמך זה מהווה קובץ הנחיות כללי לביצוע בדיקת חדירה עבור פרויקט תהילה.
פרויקט תהילה או כל לקוח מטעמו אינו מנחה את מבצע הבדיקה. באחריות הבודק להכיר את הבעיות, המגמות, והחידושים האחרונים בתחום האבטחה.

ע"מ שתתבצע בדיקה מוצלחת חשוב להקפיד על הכללים הבאים:

- **אין** להסתמך על מי שפיתח את האפליקציה.
  הבדיקה חייבת להיות בלתי תלויה (לגורם חיצוני אין "סנטימנטים" וברוב הפעמים ייתקל בדברים שנסתרו מעיני מי שנמצא כבר בתוך מעגל הפיתוח).

- אין להסתמך בלעדית על כלים אוטומאטיים

- רצינות והיקף הבדיקה:
  כאמור איננו מנחים את מי שמבצע את הבדיקה. באחריותו לספק בדיקה מקצועית ומקיפה. בסיום התהליך יש לייצר דוח מסודר ולסכם:
  - מידע כללי על מבנה המערכת כפי שהוא התברר במהלך הבדיקה
  - מהם רכיבי המערכת שנבחנו
  - מה נבדק: איזה סוג בעיות, פגיעויות נבחנו
  - מה נמצא תקין ומה לא
  - עבור מה שלא נמצא תקין יש לפרט לכל אחד מה מקור הפגם וכיצד לתקן אותו

- לצורך ביצוע הבדיקה, על השרת להיות מוכן, פעיל, ומותקן ברשת תהילה.

- אישור הבדיקה ע"י צוות ממשל זמין יהיה על סמך הדוח הסופי. קיים סיכון שהיקף הבדיקה ואו הדוח לא ייספקו ועל כן הכנסת האתר לא תאושר.

- להלן מספר נקודות החייבות להמצא בתכולת הבדיקה. התחומים קשורים ותלויים אחד בשני ולכן אנו לא מפרידים בדיקה לתחום ספציפי:

1. אפליקטיבי

- זיהוי ממשקים להעלאת קבצים למערכת
- זיהוי ממשקי עריכה, עדכון תוכן או כל שינוי תצוגת דפים באתר
- זיהוי כל סוג של ממשק אדמיניסטרטיבי או כניסת admin
- זיהוי יכולת הזרקת קוד לצד שרת (ב-URL, דרך פרמטרים, עוגיות, וכו'..)
- זיהוי יכולת הזרקת קוד בצד לקוח דוגמת XSS. (ב-URL, דרך פרמטרים, עוגיות, וכו'..)
- קלט משתמש: מוגדר היטב ומוגבל עד כמה שניתן. עדיפות לתפריטים על פני טקסט חפשי. שימוש במנגנוני מניעת הצפה, Captcha. בזיהוי משתמשים: נוסף גם שימוש ב -SSL, מנגנוני אנטי Brute Force, הגבלת כמות ה- Login.
  אם ניתן, לוודא מדיניות סיסמאות נאותה, תצורת שיחזור סיסמא.
- זיהוי לוגיקה בצד הלקוח (אימות סופי של הקלט רק בצד השרת). קשירת נתוני משתמש לנתוני ה-Session, יישום הגבלות על קלט, פרמטרים, וכו'
- בדיקת המערכת על שלל מקרי קצה, קלטים לא תקינים וכו'..
  ווידוא תוך כך שאין יכולת לערער את מצב המערכת, לבצע הרצת קוד מרחוק או ליישם מניעת שירות והשבתה.
- יש לנסות לזהות את הפלטפורמות שעליהן מבוססת המערכת. או כאשר ידוע כי נעשה שימוש בטכנולוגיה מסוימת, יש לנסות לנצל פגיעויות ידועות ולזהות הגדרות לקויות של אותה טכנולוגיה:
  דוגמאות: סוג בסיס הנתונים, אפליקצית האירוח (WebSphere, CMS, MOSS), מוצרים נלווים (GIS, Reporting server,…), וכו'...
- זיהוי /ניצול הרשאות לקויות במקורות המידע: בסיס הנתונים והקבצים. חשיפה או יכולת הרצה של פרוצדורות, פונקציות, חשיפת WS אסורים, גישה (כולל קריאה) לטבלאות חסויות וטבלאות מערכת.
- בתהליכים המחייבים פעולה לפי סדר מתוכנן: יש לוודא שאין יכולת להגיע למקומות באפליקציה שלא דרך הזרימה (flow) המתוכננת.
- באזורים מזוהים באפליקציה :יש לוודא ניהול מאובטח של ה- Session (SSL, הצפנה אפליקטיבית, חתימת נתונים, וכו'..)
- חשיפת מידע: גרסאות תוכנה/חומרה, טכנולוגיות, קבלת הודעות מערכת ואו הודעות שגיאה מפורטות, לא מקוסטמות. "לכלוך" ושאריות משלב הפיתוח.
- שימוש ב- directory traversal: ../../..
- ועוד ועוד

משרד האוצר
החשב הכללי

www.gov.il

ממשל זמין

2. <u>מערכת ההפעלה</u>

- חשיפת מידע על המערכת – גרסאות, תוכנות, חומרה, מבנה, תקשורת, משתמשים
- התקנת עדכוני אבטחה, זיהוי פגיעויות/פרצות ידועות
- זיהוי ויכולת ניצול שירותים מיותרים, או תוכנות מיותרות/מסוכנות
- זיהוי וניצול הרשאות משתמש לקויות
- הפעלה או חשיפה של קבצים, תוכן של מחיצות לא מורשים
- יכולת ל DOS
- באופן כללי כל גילוי של הקשחות או הגדרות לקויות

3. <u>הרשת</u>

- חשיפה לפורטים/שירותים אסורים
- פרוטוקולים שאינם 80 או 443
- התקפות ברמת ה- IP

❖ על נקודות אלה יש לפרט בדוח המסכם מה בוצע ומה התגלה.

❖ ההיצמדות לנהלים הינה קפדנית ובלתי מתפשרת.

❖ רשימה זו הינה קובץ הנחיות כללי ואינה תבנית מוגדרת לביצוע הבדיקה.

בברכה,
מאיר קראוסהר
מנהל צוות Web Hosting
ממשל זמין