



כללים לביצוע בדיקות חוסן PENETRATION TESTS

גרסה 1.8

מסמך זה כולל מידע השייך למערך הדיגיטל הלאומי, רשות התקשוב הממשלתי. כל חשיפה, שימוש או העתקה של מסמך זה או חלקים ממנו – ללא קבלת אישור בכתב ממנהל מערך ההגנה בסייבר במערך הדיגיטל הלאומי – אסורה בהחלט. מסמך זה מיועד לעובדי מערך הדיגיטל הלאומי ולקוחותיו



מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
1.0	29.11.2015	אופיר יהב	גרסא ראשונה לאחר הסבה לתבנית מערך הדיגיטל הלאומי. כוללת את כל התיקונים, השינויים והתוספות אשר נכנסו עד לגרסה 0.3 כולל.
1.1	14.7.2016	אופיר יהב	הבהרה לגבי פירוט הרכיבים הנבדקים. סעיף 5.2.6 (בגרסה הקודמת היה בסעיף 5.2.4). + הערות נוספות שביקש להכניס מנהל תחום בדיקות אפליקציה ר' הודעת דוא"ל מה- 14.7.2016
1.2	14.11.2017	אופיר יהב	הוספת מענה לדרישת תקן PCI – תהליך סיווג חומרת ממצאים.
1.3	4.3.2019	אופיר יהב	איסור שימוש בטכנולוגיית Flash
1.4	12.4.2019	אופיר יהב	הדגשה כי לאחר ביצוע כל שינוי במערכת (הוספת או הסרת אובייקט) יש לבצע בדיקות חוסן על מנת לבדוק את השפעת השינוי ולוודא כי לא נפגעה הקשחת המערכת.
1.5	14.05.2020	אופיר יהב	תיקוף המסמך ועדכון שמות מאשרי המסמך ותפקידיהם.
1.6	10.10.2020	אופיר יהב	תיקוף המסמך. עדכון הלוגו עם המעבר למשרד הדיגיטל הלאומי.
1.7	7.10.2021	אופיר יהב	תיקוף המסמך. עדכון הלוגו עם הקמת מערך הדיגיטל הלאומי.
1.8	7.10.2022	אופיר יהב	תיקוף ועדכון המסמך. עדכון הלוגו לאחר השינוי הארגוני.

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	ראש תחום אבטחת אפליקציות	אברהם ברדה	7.11.2022	(חתימה)
אושרה ע"י	מנהל מערך ההגנה בסייבר	חגי פרלמוטר	7.11.2022	(חתימה)

תוכן עניינים

1.	כללי.....	5
2.	הגדרות.....	6
3.	תרחישי איום.....	6
4.	מטרת בדיקת החוסן.....	6
5.	הנחיות לביצוע הבדיקה.....	7
6.	שלבי הבדיקה.....	8
7.	תאימות לתקן PCI.....	13
8.	דיווח.....	13

1. כללי

- 1.1 יחידת מערך הדיגיטל הלאומי, השייכת לרשות התקשוב הממשלתי שבמשרד הכלכלה, עוסקת בייזום, פיתוח ותפעול תשתיות ופתרונות טכנולוגים מאובטחים עבור גופי הממשלה, בין היתר במטרה להנגיש את שירותי הממשלה לאזרחים ועסקים ולשם חיבור גופי הממשל השונים לשירותים מקוונים ולשירותי מובייל מותאמים.
- 1.2 בהנגשת שירותים אלו – ללקוחות מערך הדיגיטל הלאומי (גופי הממשלה) ולתושבי ישראל – קיימת חובת השמירה על כל מרכיבי אבטחת המידע: חסיון המידע, שלמות המידע וזמינות המידע (רציפות השירות).
- 1.3 במטרה להבטיח את קיום כל מרכיבי אבטחת המידע על המערכות המהוות את תשתית השירותים לעבור מבדקי חדירות ובדיקות חוסן.
- 1.4 מסמך זה מהווה קובץ הנחיות כללי לביצוע בדיקות חדירה למערכות המתארחות במערך הדיגיטל הלאומי.
- 1.5 מערך הדיגיטל הלאומי או כל לקוח מטעמו אינו מנחה את מבצע הבדיקה.
- 1.6 באחריות הבודק להכיר את הפגיעויות, המגמות, והחידושים האחרונים בתחום אבטחת המידע.
- 1.7 בנוסף על כל המפורט לעיל, יש צורך לבצע, בין היתר, גם את הבדיקות המופיעות במסמך זה (לפי רלוונטיות הנושאים).
- 1.8 מסמך זה יעודכן ויופץ על ידי מנהל תחום מתודולוגיות הגנה בסייבר במערך הדיגיטל הלאומי.

2. הגדרות

- 2.1 **מבצע הבדיקה** - בודק או צוות בודקים המיומנים בביצוע בדיקת יישומים אשר נתבקשו לבדוק את חוסן היישום המאוכסן במערך הדיגיטל הלאומי.
- 2.2 **איום (THREAT)** - מקור למצבים בעלי פוטנציאל לגרימת הפסד/נזק למערכות תשתיות, כלכליות, חברתיות, צבאיות או ממשלתיות.
- 2.3 **פגיעות (VULNERABILITY)** - מידת הנזק הצפויה לרכיבים שונים של המערכת המאוימת במקרה שיתממש תרחיש איום.

3. תרחישי איום

- 3.1 תוקף באינטרנט ללא הרשאות ניהול מצליח לפרסם תוכן המכיל קוד עוין באתר הנבדק
- 3.2 תוקף גונב פרטים של משתמשי המערכת
- 3.3 תוקף משתמש בתשתיות המערכת לצורך פעילות זדונית או פלילית
- 3.4 תוקף באינטרנט משנה את מראה האתר
- 3.5 תוקף באינטרנט מפרסם מידע שגוי באתר
- 3.6 תוקף פוגע בזמינות המערכת
- 3.7 תוקף מנצל את המערכת לצורך תקיפת מערכת אחרת
- 3.8 תוקף לומד פרטים על תשתיות המערכת או תשתיות מערך הדיגיטל הלאומי

4. מטרת בדיקת החוסן

- קבלת תמונת מצב עדכנית ואמיתית המשקפת את מצב אבטחת המידע בהיבט החוסן האפליקטיבי במערכת הנבדקת באופן שתאפשר למערך הדיגיטל הלאומי:
- 4.1 לזהות כשלים הנובעים מתכנון ו/או יישום לקוי של מדיניות אבטחת המידע במערכת.
- 4.2 לאפשר למערך הדיגיטל הלאומי לבצע הערכת הסיכונים ולהגדיר את רמת חומרתם.
- 4.3 ליישם המלצות באופן שיאפשר את צמצום הסיכוי למימוש החשיפה לפגיעה במערכות הארגון.
- 4.4 לבצע הערכה של הדרישות ליישום ההמלצות.

- 4.5. **הערה חשובה:** לאחר ביצוע בדיקות החוסן וסקרי הקוד – יתקיים תהליך במהלכו יקבל כל ממצא וליקוי (ככל שיימצא במערכת) ציון אשר יסווג את חומרת הממצא/ליקוי. ממצאים וליקויים עם רמת סיווג/חומרה גבוהה או קריטית יקבלו התייחסות הולמת תוך הסתמכות על סטנדרטים מקובלים ומתודולוגיות מוכרות בתעשיית ההיי-טק בכלל ועולם הסייבר בפרט – ובהתאמה לכל תקני האיכות, אבטחת המידע וההגנה בסייבר.
- 4.6. **מועדי התיקון:** במקרה של מערכות בייצור, טיפול ותיקון ממצאים וליקויים קריטיים יתבצעו בתוך חודש ממועד ביצוע בדיקת החדירות, ואילו ממצאים וליקויים בסיווג חומרה גבוה ובינוני יטופלו בתוך שלושה חודשים ממועד ביצוע הבדיקה.

5. הנחיות לביצוע הבדיקה

5.1 תיחום והיקף הבדיקה

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

- 5.1.1. לאחר ביצוע כל שינוי במערכת (כגון הוספת או הסרת אובייקט) יש לבצע בדיקות חוסן על מנת לבדוק את השפעת השינוי ולוודא כי לא נפגעה הקשחת המערכת.
- 5.1.2. על הבדיקה להתבצע בסביבת ייצור או סביבת Staging הזוהר לה לאחר הקפאת תצורה.
- 5.1.3. מאמצי הבדיקה יתרכזו בניסיון לממש את התרחישים שיוגדרו בתחילת הבדיקה
- 5.1.4. הבדיקה חייבת להיות בלתי תלויה, כלומר בדיקת Black Box
- 5.1.5. אין להסתמך רק על כלים אוטומטיים אלא יש לבצע גם בדיקות ידניות.
- 5.1.6. באחריות הספק לבצע בדיקה מקצועית ומקיפה על פי מתודולוגיה שתוצג לפני הבדיקה על ידי הלקוח ותאושר על ידי מערך הדיגיטל הלאומי.
- 5.1.7. **הבדיקה תתבצע ממשרדי מערך הדיגיטל הלאומי ותתואם מול אנשי מערך הדיגיטל הלאומי**

5.2 מידע מקדים ומהלך הבדיקה

- 5.2.1. הבדיקה תתבצע על ידי בודקים מיומנים ועל ידי שימוש בכלל הכלים והאמצעים העומדים לרשות המבצע.

עמוד 8 מתוך 13

5.2.2. הבדיקה תתבצע מכתובת IP קבועה בבעלות מבצע הבדיקה. הכתובת תהיה מוקצית לבודקים בלבד ולא תשמש למשימות אחרות.

5.2.3. כאשר קיים חשש כי פעולה מסוימת עלולה ליצור נזק כלשהו ליישום, באחריותו לתאם זאת עם אחראי המערכת וצוות אבטחת המידע באמצעות מנהל הפרויקט האחראי.

5.2.4. באחריות צוות אירוח מערך הדיגיטל הלאומי להקשיח את המערכות הנבדקות טרם ביצוע הבדיקות.

5.2.5. על הלקוח לבדוק את הקשחות השרת במסגרת גבולות הגישה שניתנה לו אל השרת ומשאביו. הלקוח לא יקבל גישה פיזית לשרת למעט במקרים חריגים המחייבים קבלת אישור מנהל מערך הגנה בסייבר.

5.2.6. יש לבדוק ולציין בדוח בין היתר את הנושאים הבאים:

5.2.6.1. מידע שנאסף אודות המערכת כפי שהתברר במהלך הבדיקה:

- א. שם המערכת
- ב. סוג המערכת (WEB, Client/Server וכו')
- ג. תיאור המערכת
- ד. צורת ההזדהות למערכת

5.2.6.2. פירוט כל רכיבי המערכת שנבחנו בפועל במהלך הבדיקה, לדוגמא:

- א. שרת WEB
- ב. שירות WCF
- ג. ממשקים למערכות אחרות

5.2.6.3. רשימת הממצאים, מקורם והמלצות לתיקון.

6. שלבי הבדיקה

6.1 מצב פסיבי

בשלב זה הבודק ינסה להבין את הלוגיקה האפליקטיבית על ידי שיטוט כמשתמש רגיל. ניתן להשתמש בשלב זה בכלי בדיקה כגון Web Application Proxy לסקירת בקשות / תשובות HTTP.

בדיקות לביצוע:

עמוד 9 מתוך 13

- 6.1.1. שימוש ב- Robots, Spiders, Crawlers
- 6.1.2. גילוי מידע רגיש על ידי שימוש במנועי חיפוש כמו גוגל (במידה והמערכת פתוחה לעולם)
- 6.1.3. גילוי משאבי המערכת כגון סוגי שרתי WEB
- 6.1.4. גילוי של גרסאות קודמות / קבצים ישנים אשר הועתקו מסביבות פיתוח/ בדיקות
- 6.1.5. ביצוע אנליזה להודעות שגיאה

בסיום שלב זה יש להבין את כלל דרכי הגישה למערכת (Parameters, HTTP headers, cookies, וכו'). המטרה כאן הינה מיפוי של דרכי הגישה והצגת התוצר בסוף הבדיקה.

6.2 מצב אקטיבי

בשלב זה יש לבצע את בדיקות החדירה עצמן על פי מתודולוגיה הנבחרת (למשל Osstmm) בדגש על הנושאים הבאים

- 6.2.1. **בדיקות קונפיגורציה** (בהתאם ליכולת הגישה לנתונים).
 - הגדרות SSL (גרסה, אלגוריתם, אורך מפתח, תוקף).
 - בדיקות של DB Listener
 - הגדרות קונפיגורציה תשתית
 - הגדרות קונפיגורציה אפליקטיבית
 - טיפול בסיומות קבצים, לדוגמא קבצים עם סיומת של asa, inc לא אמורים להיות מוצגים למשתמשים כיוון שעלולים להכיל מידע רגיש. בנוסף קבצים עם סיומות כמו old, bak, rtf, ppt, xls, doc, pdf, txt, java, tgz, gz, tar, zip מוצגים או יורדים לתחנות המשתמשים, יש לוודא כי הנ"ל לא מתקיים ואם כן שלא מכיל מידע רגיש.
 - בדיקת המצאות קבצים ישנים / גיבויים / קבצים לא מקושרים
 - בדיקת מתודות HTTP מעבר ל GET ו POST – כגון: Trace, connect, options, delete, put – יש לוודא כי לא ניתן להפעיל מתודות אלה.
 - **הערה:** בתשתיות מערך הדיגיטל הלאומי לא ניתן להטמיע לומדות או לארח אתרים שנכתבו בשפת Flash. בטכנולוגיה זו ישנם ליקויי אבטחה רבים ברמות חומרה שונות ויתרה מזאת חברת Adobe הצהירה כי החל משנת 2020 תחדל

עמוד 10 מתוך 13

מתמיכה במוצר, ולכן אינה מאושרת להטמעה בתשתיות מערך הדיגיטל הלאומי.

6.2.2. בדיקות לוגיקה עסקית

- מעקף לוגיקה עסקית
- Reflected XSS
- Stored XSS
- DOM XSS
- Cross site flashing
- SQL Injection
- בדיקות התקפות אפליקטיביות נפוצות אחרות

6.2.3. בדיקות הזדהות

- בדיקת זרימת מידע רגיש בתווך לא מוצפן
- Brute Force בדיקת
- בדיקת מעקף מנגנון ההזדהות
- בדיקת ניהול Browser Cache
- בדיקת חוזק מזהה שלישי (במקרה של הזדהות חזקה)
- בדיקות של Race Conditions למשל על ידי הגדרת משתמשים מרובים עם אותו "שם משתמש" וביצוע התקפות Brute Force

6.2.4. בדיקות הרשאות

- Path Traversal
- מעקף מנגנון ההרשאות
- זיהוי וניצול הרשאות משתמש לקויות
- זיהוי/ניצול הרשאות לקויות במקורות המידע: בסיס הנתונים והקבצים.
- Privilege escalation

6.2.5. בדיקות ניהול תקין של Session

- בדיקות של חוזק Session token
- בדיקות הגדרות אבטחה של Cookies (Secure, HttpOnly)
- Session Fixation
- CSRF

6.2.6. בדיקות אימות קלטים

- LDAP Injection



עמוד 11 מתוך 13

- XML Injection
- SSI Injection
- XPath Injection
- IMAP/SMTP Injection
- Code Injection
- OS Command Injection
- HTTP Splitting/Smuggling

6.2.7. בדיקות DOS אפליקטיביות

- SQL Wildcard attack
- נעילת משתמשים
- שמירת מידע מיותר בקבצי הלוג
- שמירת מידע מיותר באובייקט Session

6.2.8. בדיקות שימוש ב- Web Services

- Information Gathering – למשל חשיפת WSDL
- בדיקת מבנה XML
- SOAP Attachments
- Replay Attacks
- בדיקת חשיפה של פרוטוקולים מעבר ל SOAP

6.2.9. בדיקות AJAX

- ביצוע בדיקות כלליות – SQL Injection , XSS , Ajax Bridging , CSRF וכו'.

6.2.10. בדיקות נוספות

- שמירת מידע רגיש בתחנת הקצה
- זיהוי ממשקים להעלאת קבצים למערכת
- זיהוי ממשקי עריכה, עדכון תוכן או כל שינוי תצוגת דפים באתר
- זיהוי כל סוג של ממשק אדמיניסטרטיבי
- בחינת אופן השימוש במנגנון Captcha
- בחינת מדיניות סיסמאות
- בדיקת יכולת הרצת קוד מרחוק
- בדיקת מניעת שירות למערכת
- זיהוי הפלטפורמות שעליהן מבוססת המערכת וניסיון לזהות הגדרות לקויות של אותה טכנולוגיה.



עמוד 12 מתוך 13

- 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 תהליך הזרימה המתוכננת.
 - באזורים מזוהים באפליקציה: יש לוודא ניהול מאובטח של ה- Session (הצפנה אפליקטיבית, חתימת נתונים, וכו')
 - חשיפת מידע: גרסאות תוכנה/חומרה, טכנולוגיות, קבלת הודעות מערכת ו/או הודעות שגיהא מפורטות.
 - זיהוי ויכולת ניצול שירותים מיותרים, תוכנות מיותרות/מסוכנות
 - הפעלה או חשיפה של קבצים, תוכן של מחיצות לא מורשים
 - יכולת ביצוע Denial of service
 - חשיפה לפורטים/שירותים אסורים
 - פרוטוקולים שאינם 80 או 443
 - התקפות ברמת ה- IP
- רשימה זו הינה קובץ הנחיות כללי ואינה תבנית מוגדרת לביצוע הבדיקה.

7. תאימות לתקן PCI

סעיף זה רלוונטי למערכות המחויבות לעמוד בדרישות תקן אבטחת המידע בתעשיית כרטיסי האשראי PCI-DSS – Payment Cards Industry Data Security Standard.

כמענה לדרישות תקן PCI – אליו מחויב מערך הדיגיטל הלאומי כגוף סולק המספק את שירות התשלומים – בכל בדיקת החדירות המתבצעת לאחד מרכיבי שירות התשלומים (המשמשים לעבוד, איחסון או מעבר נתוני אשראי), על מתודולוגיית הבדיקה לענות על הדרישות הבאות:

- 7.1. הבדיקות תהיינה מבוססות על גישות מקובלות בתעשייה לביצוע בדיקות חדירות (לדוגמא, (NIST SP800-115).
- 7.2. על בדיקות החדירות לכסות את כל סביבת נתוני מחזיקי כרטיסי אשראי ונתוני אשראי (כולל רכיבי החומרה המקושרים למערכת, כדוגמת 'קורא שפתיים').
- 7.3. במסגרת בדיקות החדירות תתבצענה בדיקות מתוך ומחוץ לרשת.
- 7.4. יבוצע בדיקות לאימות כל סגמנטציה ובקורות על היקף הבדיקות.
- 7.5. יבוצעו בדיקות חדירות לשכבת האפליקציה ולכל הפחות פגיעויות המפורטות בתקן PCI.
- 7.6. יוגדרו בדיקות חדירות לשכבת הרשת במטרה לכלול מרכיבים אשר תומכים ביכולות רשת ובמערכות הפעלה.
- 7.7. יתבצעו סקירה ובדיקה של איומים ופגיעויות אשר נתגלו בשנה האחרונה.
- 7.8. יתועדו תוצאות בדיקות החדירות ותוצאות פעולות התיקון אם היו כאלו.

8. דיווח

דוח הבדיקה יוגש למנהל תחום בדיקות חדירות במערך הגנה בסייבר במערך הדיגיטל הלאומי לאישורו הסופי, שיכלול את הדרך המלאה והמפורטת למימוש הממצאים, אם נמצאו כאלה, סיכום והתרשמות אישית וכמו כן את שיטת מימוש התרחישים וההמלצות לתיקונם.