

# שימוש בתקן אימות אבטחת היישומים

ישנן שתי מטרות עיקריות:

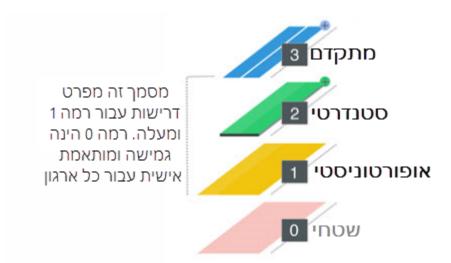
- לסייע לארגונים לפתח ולתחזק יישומים מאובטחים.
- לאפשר שירותי אבטחה, ספקי כלי אבטחה, וצרכנים ליישר דרישותיהם הצעותיהם.

### רמות אבטחה

ישנן שלוש רמות במדורגות לפי עומק ורמת האבטחה בהתאמה:

- רמה 1 נועדה לכל תוכנה.
- רמה 2 נועדה עבור יישומים המכילים מידע רגיש המחייב הגנה.
- רמה 3 נועדה עבור היישומים הקריטיים ביותר יישומים המבצעים עסקאות בעלי ערך גבוה, מכילים מידע רפואי רגיש, או כל יישום הדורש את הרמה הגבוהה ביותר של אמון.

כל רמה מפרטת רשימת דרישות אבטחה. כל אחת מהדרישות ניתנת למיפוי ליכולות ותכונות אבטחתיות ואלו נדרשות ליישום ופיתוח בתוכנה ע"י הגורם המפתח.



1 – OWASP, תקן אימות אבטחת היישומים 3.0 לפי רמות

# כיצד להשתמש בתקן זה

אחת הדרכים הטובות ביותר להשתמש בתקן זה היא בתור תכנית או קו מנחה ובכך לגבש רשימת ביצוע לפיתוח מאובטח ספציפי ליישום, פלטפורמה או הארגון. התאמת התקן ליישום האישי תשפר את המיקוד על דרישות האבטחה החשובות ביותר לפרויקטים ולסביבת השפעתם.

### רמה 1: אופורטוניסטי



אפליקציה מדורגת ברמה 1 כאשר אם היא מגנה במידה הולמת מפני פגיעויות אבטחת יישומים נפוצות או הקלות לזיהוי ובנוסף מספקת מענה לרשימת ה-10 המדורגים ביותר של OWASP או רשימות דומות.

רמה 1 היא בדרך כלל מתאימה עבור: יישומים בהם רמת האמון האבטחתי של המשתמש בזמן שימוש היישום היא נדרשת, מענה אבטחתי מהיר עבור מספר יישומים או כחלק מסיוע לפיתוח היישום בצורה אבטחתית כחלק מהמאמץ הכולל. שליטה ברמה 1 ניתנת לבדיקה ע"י כלים אוטומטיים או דרך גישה ידנית ללא גישה לקוד המקור. הדרישה היא שרמה 1 היא הרמה המינימאלית ביותר עבור כל יישום.

המאיימים על האפליקציה יהיו קרוב לודאי תוקפים אשר משתמשים בשיטות פשוטות וללא מאמץ על מנת להשיג הישגים קלים – קל למצוא וקל לנצל. זאת בניגוד לתוקף נחוש אשר ישקיע מאמץ ומיקוד על היישום הספציפי. אם לנתונים העוברים ביישום יש ערך גבוה ורגיש, מומלץ להמשיד לשלבים הבאים.

### רמה 2: סטנדרטי

אפליקציה מדורגת ברמה 2 כאשר אם היא מגנה במידה הולמת מפני רוב הסיכונים הקשורים ליישום כיום.

רמה 2 מבטיחה כי בקרות האבטחה ממומשות ומשומשות כראוי ובצורה יעילה. רמה 2 היא לרוב מתאימה ליישומים המממשים תעבורת מידע בין עסקית (עסק לעסק), תהליכי העברת מידע רפואי, פעולות עסקיות קריטיות או תהליכים רגישים וחשובים.

המאיימים על האפליקציה יהיו קרוב לוודאי תוקפים מיומנים ובעלי מוטיבציה. תוקפים אלו ממוקדים על מטרה מסוימת. הם ישתמשו בכלים וטכניקות מתקדמות, חדשניות או לא מוכרות מה שישפיע על תהליך הזיהוי והניצול של פגיעויות אלו באפליקציה.

# רמה 3: מתקדם

רמה 3 היא הרמה הגבוהה ביותר המסווגת בתקן זה. רמה זו מסווגת ליישומים אפשר דורשים רמת אבטחה גבוהה, כגון אפליקציות בתחומים הצבאיים, בריאות וביטחון, תשתיות קריטיות (חברת חשמל, מים) וכו'. ארגונים עשויים לדרוש את רמה 3 עבור אפליקציות המשמשות לפעולות קריטיות אשר כשל מערכתי עלול להוביל לפגיעה בפעילות הארגון ואף בשרידתו.

אפליקציה מדורגת ברמה 3 כאשר אם היא מגנה במידה טובה מפני סיכוני אבטחה מתקדמים האבטחה בגזרתה (הגנה עמוקה),. נדרש לתעד את התהליך וסטטוס של כל שכבה. נדרשת אחריות כוללת עבור סודיות (לדוגמא הצפנה), אמינות המידע (אימות קלט, ביצוע פעולות), זמינות המידע, אימות (כולל בין מערכות), אי-התכחשות, הרשאות וביקורת (לוגים).

### הלכה למעשה

לאיומים שונים יש מוטיבציות שונות. חלק מהתעשיות יש מידע חיוני, נכסים טכנולוגים ותחום ספציפי לדרישות התקנות.

מטה מסופקת הדרכה תבניתית לגבי רמות התקן המומלצות. למרות כמה הבדלים ומעט שוני באיומים עבור כל תעשייה, וקטור נפוץ ומשותף בין כל החברות הינו ההזדמנות והאפשרות שתוקפים יחפשו וינצלו אפליקציות בעלות חולשה פשוטה לניצול במערכות החברה, וזו הסיבה שרמה 1 הינה מומלצת עבור כל האפליקציות ללא קשר לתעשייה. זו היא הצעה לנקודת פתיחה על מנת לנהל את הסיכונים הקלים ביותר לחשיפה. מומלץ לארגונים לרדת לשורש מאפייני הסיכונים הייחודים בארגון לאור התהליכים העסקיים. מצד שני של הספקטרום היא רמה 3, שנועדה למקרים בעלי אופי הרסני כלפי חיי אדם, ביטחון או פגיע חמורה באפליקציה שתוביל לפגיעה חמורה בארגון.

L3 המלצת	L2 המלצת	המלצת L1	פרופיל איום	תעשָׂיָה
יישומים המכילים כמויות גדולות של מידע רגיש או המאפשרות העברה מהירה של סכומים גדולים של כסף (העברות בנקאיות למשל) ו / או העברה של סכומי כסף גדולים בצורה של עסקות בודדות או כקבוצה של העברות קטנות.	אפליקציות המכילות מידע רגיש כגון מספרי כרטיסי אשראי, פרטים אישיים, שיכול להזיז כמויות מוגבלות של כסף בצורה (i) העברת כספים בין חשבונות באותו מוסד או (ii) צורה איטית של תזרים מזומנים (למשל ACH) עם	כל אפליקציות הרשת הנגישות.	למרות שמגזר זה חווה ניסיונות מפני תוקפים פוטנציאליים, זה מוצג לעתים קרובות כמטרת ערך גבוה על ידי תוקפים והתקפות מוטיבציה ולרוב הוא העניין הכספי. בדרך כלל, תוקפים מחפשים נתונים או חשבונות רגישים, שניתן להשתמש בם על מנת לבצע הונאות או לנצל באופן ישיר על ידי פונקציונליות המערכת להזרמת מזומנים בתוך יישומים. טכניקות כוללות לעתים קרובות גניבת הרשאות, התקפות ברמת האפליקציה, והנדסה חברתית.	פיננסי וביטוח



	(iii) העברות בנקאיות מוקשחות עם גבולות העברה ובתוך פרק זמן מסוים.			
יישומים המכילים קניין רוחני יקר, סודות מסחריים, או סודות ממשלתיים קריטיים להישרדות או ההצלחה של הארגון. אפליקציות שליטה פונקציונלית רגישות (למשל, ציוד ייצור, מערכות בקרה) או שיש את הסבירות לפגיעה בבטיחות חיי אדם.	אפליקציות המכילות מידע על עובדים העשויים להיות מעורבים בהנדסה חברתית. אפליקציות המכילות מידע לא חיוני, אבל חשוב, על מידע אישי וסודות מסחריים.	כל אפליקציות הרשת הנגישות.	לתעשיות נראה שאין הרבה מאוד במשותף, אבל האיומים אשר צפויים לתקוף ארגונים במגזר זה נוטים יותר לבצע תקיפות ממוקדות עם יותר זמן, מיומנות, ומשאבים. לעתים קרובות את המידע או מערכות הרגישים אינן קלות לאיתור ודורשות משפתי פעולה פנימיים וטכניקות הנדסה חברתית. התקפות עשויות להיות כרוכות משפתי פעולה פנימיים, אנשים מבחוץ, או להיות שילוב בין השתיים. מטרותיהם עשויות לכלול צבירת גישה לקניין אינטלקטואלי עבור יתרון אסטרטגי או טכנולוגי. אין להתעלם מהתוקפים המנצלים פונקציונליות אפליקציה לרעה על מנת להשפיע על ההתנהגות או לשבש מערכות רגישות. רוב התוקפים מחפשים מידע רגיש, שניתן להשתמש בו במישרין או בעקיפין למטרות רווח – מידע, נתונים משרלות הונה אישי. לעתים קרובות, הנתונים יכולים לשמש לגניבת זהות, תשלומי הונאה, או מגוון של	ייצור, מקצועיות, תחבורה, טכנולוגיה, שירותים, תשתיות, והגנה
אפליקציות המשמשות לשלוטה בציוד רפואי, מכשירים, או רשומות שעשויים לסכן חיי אדם. מערכות תשלום ומכירה (POS) המכילות כמויות גדולות של נתוני עסקה שניתן לנצלן על מנת לבצע הונאות. כולל את כל ממשקי הניהול עבור אפליקציות אלה	אפליקציות עם כמות קטנה או מתונה של מידע רפואי רגיש (מידע מוגן במשרד הבריאות), פרטי זיהוי אישיים, או נתונים התשלום.	כל אפליקציות הרשת הנגישות.	רוב התוקפים מחפשים מידע רגיש, שניתן להשתמש בו במישרין או בעקיפין למטרות רווח – מידע, נתונים תשלום וזיהוי אישי. לעתים קרובות, הנתונים יכולים לשמש לגניבת זהות, תשלומי הונאה, או מגוון של פעולות הונאה.	בריאות
תשלום ומערכות נקודות מכירה (POS) המכילות כמויות גדולות של מידע רגיש שיכול לשמש על מנת לבצע הניהול עבור אפליקציות אלה. אפליקציות עם כמויות גדולות של מידע רגיש כגון מספרי כרטיסי אשראי מלאים, מספרי ביטוח לאומי וכו'.	מתאים עבור אפליקציות עסקיות, אלו המכילות מידע על קטלוג מוצרים, מידע ארגוני פנימי, ואפליקציות עם מידע משתמש מסווג או פרטי (פרטי קשר למשל). אפליקציות עם כמויות קטנות או מתונות של נתונים והעברות תשלומים.	כל אפליקציות הרשת הנגישות.	רבים מן התוקפים במגזר זה מסגלים לעצמם טקטיקת ניצול "לרסק ולתפוס". עם זאת, יש גם איום קבוע של התקפות ספציפיות על אפליקציות הידועים כמכילות פרטי תשלום, עסקות פיננסיות, או איזסון מידע אישי. אמנם פחות סביר מאשר האיומים שהוזכרו לעיל, יש גם את האפשרות של איומים ותוקפים מתקדמים יותר שיתקפו מגזר תעשייה זה כדי לגנוב קניין רוחני, לקבל מודיעין תחרותי, או להשיג יתרון על ארגון היעד או שותף עסקי במשא ומתן.	קמעונאות, מזון, אירוח

# דרישות אימות מפורטות

V1. ארכיטקטורה, תכנון ומודל איומים

.V2 אימות

Session ניהול.V3

.V4 בקרת גישה

V5. טיפול קלט זדוניות

V7. קריפטוגרפיה



V8. טיפול ורישום שגיאות

V9. הגנת מידע

V10. תקשורת

אבטחה HTTP. תצורת אבטחה V11

V13. שליטה זדונית

V15. לוגיקה עסקית

V16. תיוק ומשאבים

V17. מובייל

V18. שירותי רשת

V19. תצורה

# V1: ארכיטקטורה, תכנון ומודל איומים

### מטרת על

ודא שהאפליקציה הרצויה עומדת ברמה הגבוהה ביותר בדרישות הבאות:

- ברמה 1, רכיבים של היישום מזוהים וקיומם באפליקציה מוצדק
- ברמה 2, הארכיטקטורה הוגדרה. הקוד שומר על הארכיטקטורה ואפיונה כפי שהוגדר.
  - ברמה 3, האדריכלות והעיצוב הוגדרו ומומשו כראוי, בשימוש כולל, וביעילות

#	תיאור	1	2	3
1.1	ודא שכל רכיבי האפליקציה מזוהים וידועים כנדרשים.	V	V	V
1.2	ודא שכל הרכיבים שאינם חלק מהאפליקציה אך מסתמכת עליהם לפעולות שונות, מזוהים ומוכרים על ידי המערכת, כגון ספריות, מודולים ומערכות חיצוניות,.		V	V
1.3	ודא שארכיטקטורת האפליקציה הוגדרה ברמה גבוהה.		V	V
1.4	ודא שכל רכיבי האפליקציה מוגדרים במונחים של פונקציות עסקיות ו / או פונקציות אבטחה שהם מספקים.			V



V		ודא שכל הרכיבים שאינם חלק מהאפליקציה אך האפליקציה מסתמכת עליהם לפעולות, מזוהים ע"י המערכת, כגון ספריות, מודולים ומערכות חיצוניות, ואלו מוגדרים במונחים של הפונקציות, ו / או פונקציות אבטחה, שהם מספקים.	1.5
V		ודא שמודל איומים עבור אפליקציית היעד הופק ומסקר את הסיכונים הקשורים בזיוף, שיבוש, התכחשות, גילוי מידע, מניעת שירות, והעלאת רמת הרשאות.	1.6
V	V	אמת שלכל בקרות האבטחה (כולל ספריות הקוראות שירותי אבטחה חיצוניים) יש מימוש מרכזי ומעמיק.	1.7
V	V	ודא כי רכיבי האפליקציה מופרדים זה מזה באמצעות הגדרת שליטה ביטחונית, כגון פילוח רשת (סגמנטים), חוקים בחומת האש, או ענן מבוסס קבוצות אבטחה.	1.8
V	V	בדוק כי לאפליקציה יש הפרדה ברורה בין שכבת הנתונים, שכבת השליטה ושכבת התצוגה (MVP\MVC), כך קבלת החלטות בנושאי אבטחה ניתן לאכוף על מערכות מהימנות.	1.9
V	V	ודא כי אין כל מידע אודות תהליכים עסקיים רגישים, מפתחות סודיים או מידע קנייני אחר בקוד צד הלקוח.	1.10
V	V	ודא שכל רכיבי התוכנה היישומית, ספריות, מודולים, מסגרות העבודה ומערכות הפעלה חסינים ממפגעים ידועים.	1.11

לקבלת מידע נוסף, ראה:

- מודל איומים (אנגלית) •
- https://www.owasp.org/index.php/Application\_Security\_Architecture\_Cheat\_Sheet
  - מודל איומים (עברית)
    - ניתוח שטח תקיפה

https://www.owasp.org/index.php/Attack\_Surface\_Analysis\_Cheat\_Sheet

### :V2 דרישות אימות

### מטרת על

אימות היא המעשה של ביסוס, או אישור, משהו (או מישהו) כמו אותנטי, כלומר, כי הבקשות שהועלו על ידי או על הדבר הם אמת. ודא שאפליקציה עומדת ברמה הגבוהה בדרישות האימות הבאות:



- מאמת את הזהות הדיגיטלית של השולח בתקשורת.
- לוודא כי רק המורשים מסוגלים לעבור את תהליך האימות ונתוניהם מועברים באופן מאובטח.

3	2	1	תיאור	#
V	V	V	וודא כי כל הדפים והמשאבים דורשים אימות כברירת מחדל, למעט אלו שנועדו להיות ציבוריים.	2.1
V	V	V	ודא כי צורות המכילות מידע רגיש או חסוי לא מולאו על ידי האפליקציה באופן אוטומטי (cache). טרום מילוי המידע ברגיש על ידי האפליקציה מרמז כי נתונים רגישים מאוחסנים בטקסט או בפורמט הפיך, אשר אסור במפורש.	2.2
V	V	V	ודא כי כל אמצעי הזיהוי נאכפים בצד השרת.	2.4
V	V	V	ודא כי כל בקרות האימות נכשלות באופן מאובטח על מנת להבטיח כי תוקף לא יצליח להתחבר.	2.6
V	V	V	לאפשר או לעודד הזנת שדות הסיסמה, בשימוש passphrases, ואינם מונעים סיסמאות מנהלים, passphrases ארוך או סיסמאות מורכבות ביותר.	2.7
V	V	V	אמת את כל פונקציות אימות זהות (כגון עדכון פרופיל, מנגנון שכחתי את הסיסמה, חסומים / Token אבוד, Help Desk או UVR) שעשוי להחזיר גישה לחשבון, עמידים לתקוף לפחות כמו מנגנון אימות ראשוני.	2.8
V	V	V	ודא פונקציונליות הסיסמה שינוי כוללות את הסיסמה הישנה, הסיסמה החדשה, ואישור הסיסמה.	2.9
V	V		ודא כי כל תהליכי האימות מתועדים, מבלי לאחסן Session, מידע רגיש או סיסמות. כולל בקשות עם metadata רלוונטי לו זקוקים בעת חקירות ביטחוניות.	2.12
V	V		ודא כי סיסמות החשבון הן ממולחות (Salt) לצד אחד, ויש חסם המספק סיכול התקפות Bruteforce ואחזור סיסמאות Hash.	2.13
V	V	V	ודא כי אישורים מועברים באמצעות קישור מוצפן. כל הדפים / הפונקציות שדורשות משתמשים להזין אישורים עושות זאת באמצעות קישור או תווך מוצפן.	2.16
V	V	V	ודא כי פונקציית הסיסמה שנשכחה ופונקציות התאוששות אחרות לא חושפות את הסיסמה הנוכחית, ובנוסף הסיסמה החדשה אינה נשלחת בטקסט גלוי בפני המשתמש.	2.17



V	V	V	ודא כי דליית מידע אינה אפשרית באמצעות תהליכי התחברות, איפוס סיסמא, או "שכחתי את שם החשבון".	2.18
V	V	V	ודא אין סיסמאות ברירת המחדל בשימוש במסגרת האפליקציה או כל רכיב בשימוש על ידי האפליקציה (כגון "password / admin").	2.19
V	V	V	ודא קיום אנטי-אוטומציה כדי למנוע שימוש זדוני בממשק ההתחברות, Brute forcing, והתקפות נעילת חשבונות.	2.20
V	V		ודא שכל נתוני האימות לגישה לשירותים חיצוניים לאפליקציה מוצפנים ומאוחסנים במקום מוגן.	2.21
V	V	V	ודא שפוטנציאליות "שכחתי סיסמא" ודרכי והתאוששות אחרות עושות שימוש ב-TOTP או טוקן אחר, או כל מנגנון התאוששות מנותק (Offline). שימוש בערך אקראי בהודעת דואר אלקטרונית או SMS צריך להיות מוצא אחרון, כי הינו ידוע כחלש.	2.22
V	٧		ודא כי נעילת החשבון מחולקת מצב נעילה רך וקשה, והם אינם סותרים. אם חשבון נעול זמנית במצב רך עקב התקפת Brute force, זה לא צריך לאפס את מצב הנעילה הקשה.	2.23
V	V	V	ודא כי אם נדרש שאלות אבטחה, השאלות לא יפרו את חוקי הפרטיות ויהיו חזקות מספיק כדי להגן על חשבונות מן התקפה זדונית.	2.24
V	V		ודא כי המערכת יכולה להיות מוגדרת כך שאסור להשתמש בסיסמאות קודמות.	2.25
V	V		להעברות נתונים ולעסקות בעלות ערך גבוה ודא כי מומש מנגנון אימות מחדש, אימות דו-שלבי או קוד דינמי (PIN code).	2.26
V	V	V	ודא כי ישנה פוליסת סיסמא חזקה כדי לחסום את השימוש בסיסמאות שכיחות או חלשות.	2.27
V			ודא שכל שלבי האימות, אם הצליח או נכשל, צריכים להגיב בזמן תגובה ממוצע.	2.28
V			ודא כי מידע רגיש, מפתחות API, וסיסמאות אינם כתובים בקוד המקור, או המאגרים של קוד המקור באינטרנט.	2.29
V	V		ודא כי אם אפליקציה מאפשרת למשתמשים לבצע אימות, הם יכולים לאמת את זהותם באמצעות אימות דו-שלבי או אימות חזק אחר, או כל תכנית דומה המספקת הגנה מפני גילוי שם משתמש וסיסמא.	2.31
V	V	V	ודא ממשקי הניהול אינם נגישים לגורמים לא אמינים.	2.32
V	V	V	השלמה אוטומטית ע"י הדפדפן, ואינטגרציה עם מנהלי סיסמות מותרות אלא אם נאסר על פי מדיניות מבוססת סיכונים.	2.33



לקבלת מידע נוסף, ראה:

- בדיקת OWASP מדריך 4.0: בדיקה OWASP אימות אימות אימות אימות for\_authentication אימות הבדיקה אימות אימות מדריך אומות מדריך אימות מדריך אימות מדריך אומות מד
- גיליון מידע על אחסון
  https://www.owasp.org/index.php/Password\_Storage\_Cheat\_Sheet סיסמה
- "שכחתי שכחתי גיליון מידע על מנגנון "שכחתי "אליון מידע על מנגנון "שכחתי https://www.owasp.org/index.php/Forgot\_Password\_Cheat\_Sheet
- בחירה ושימוש שאלות אבטחה
   https://www.owasp.org/index.php/Choosing and Using Security Questions Cheat Sh
   eet

# V3: דרישות אימות לניהול סשן

### מטרת על

אחד מרכיבי הליבה של כל אפליקציה מבוססת אינטרנט הוא המנגנון שבאמצעותו היא שולטת ושומרת על סטטוס האינטראקציה עבור משתמש מסוים. ניהול סשן (Session) מוגדר כסט של כל הפקדים השולטים באינטראקציה המפרטת סטטוס או מצב שבין משתמש לבין האפליקציה מבוססת האינטרנט.

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות ניהול הסשן הבאות:

- Sessions הם ייחודיים לכל אדם ולא ניתן לנחשם או לשתפם.
- או עקב חוסר פעילות. Session יפוג כאשר כבר לא נדרש, תם הזמן שהוקצב או עקב חוסר פעילות.

3 2	1	תיאור	#
v v	V	ודא כי אין מנהל סשן מותאם אישית, או שמנהל הסשן המותאם הינו עמיד בפני כל סוגי תקיפות ניהול סשן נפוצות.	3.1



3.2	ודא כי הסשן פג כאשר המשתמש מתנתק.	V	V	V
3.3	ודא כי הסשן פג לאחר פרק זמן מסוים של חוסר פעילות.	V	V	V
3.4	ודא כי הסשן פג לאחר תקופת זמן מקסימלית ללא קשר לחוסר פעילות הסשן.		V	V
3.5	ודא שלכל הדפים הדורשים אימות יש גישה נוחה וגלויה לפונקציונלית ההתנתקות	V	V	V
3.6	ודא כי זיהוי הסשן לא מועבר דרך כתובת ה-URL, הודעות שגיאה, או בלוגים. לוודא כי האפליקציה או שרת האפליקציה אינם תומכים בהעברת הסשן דרך כתובת ה-URL.	V	V	V
3.7	ודא שכל תהליכי האימות (שעברו בהצלחה) יוצרות סשן חדש בסוף התהליך.	٧	V	V
3.10	ודא כי רק הסשנים שנוצרו על ידי מסגרת האפליקציה מוכרים כפעילים ידי האפליקציה.		V	V
3.11	ודא כי הסשנים שנוצרים הם מספיק ארוכים, אקראיים וייחודיים.	V	V	V
3.12	ודא כי בעוגיות בהן מאוחסן הסשן מוגדרות עם מאפיין Path מגביל עבור האפליקציה. עבור סשנים שנועדו לאימות יש בנוסף להגדיר את מאפייני "HttpOnly" ו-"Secure".	V	V	V
3.16	ודא כי האפליקציה מגבילה את מספר הסשנים הפעילים עבור משתמש או לקוח מסוים.	V	V	V
3.17	ודא כי הסטוריית ורשימת הסשנים הפעילים מוצגות בפרופיל החשבון. המשתמש צריך להיות מסוגל לסיים את כל סשן פעיל.	V	V	V
3.18	לוודא כי האפליקציה מכריחה את הסשנים הפעילים של המשתמש להתנתק או לדרוש אימות מחדש לאחר הצלחה בתהליך שינוי סיסמה.	٧	V	V

לקבלת מידע נוסף, ראה:

- בדיקת OWASP מדריך 4.0: בדיקת OWASP מדריך 6.1: בדיקת owasp.org/index.php/Testing for Session Management סשן
  - Cheat sheet ניהול סשן

https://www.owasp.org/index.php/Session\_Management\_Cheat\_Sheet :OWASP



# :V4 דרישות בקרת גישה

### מטרת על

ניהול הרשאות הוא רעיון של היתר גישה למשאבים רק לגורם המוגדר כלגיטימי להשתמש בהם. ודא שאפליקציה עומדת ברמה הגבוהה בדרישות בקרות גישה הבאות:

- אנשי גישה למשאבים מחזיקים באישורים התקפים לעשות זאת.
- משתמשים מוגדרים על בסיס סט תפקידים והרשאות המוגדר ומאופיין היטב.
  - אות נתונים או חבלות. Metadata לגבי הרשאות והיתרים מוגן מפני אחזור נתונים או חבלות.

3	2	1	תיאור	#
V	V	V	ודא כי קיים רמת הרשאות פחותות - יש לוודא שמשתמשים ברמת הרשאות אלו יוכלו רק לגשת לפונקציות, קבצי נתונים, כתובות, בקרים, שירותים, ומשאבים אחרים, שברשותם אישור ספציפי לפעולות אלו. משמעות הדבר היא הגנה מפני זיוף והעלאת רמת הרשאות.	4.1
V	V	V	ודא כי הגישה למידע רגיש מוגנת, כך שהיחיד שרשאי לגשת לאובייקטים או לנתונים הוא משתמש הספציפי הלגיטימי. (למשל, להגן מפני שיבוש פרמטר מפני חשיפה, שינוי מידע או נתונים של חשבון של משתמש אחר).	4.4
V	V	V	ודא כי אינומרציית האתר חסומה אלא אם רצויה בכוונה תחילה. בנוסף, האפליקציה לא תאפשר גילוי או חשיפה של metadata של קבצים או ספריות, כגון ,DS_Store, git,Thumbs.db או תיקיות svn.	4.5
V	V	V	וודא כי ממשקי הגישה נכשלים באופן מאובטח.	4.8
V	V	V	ודא כי אותם הכללים בממשקי גישה בשכבת התצוגה בצד הלקוח (display) נאכפות ומיושמות גם כן בצד השרת.	4.9
V	V		ודא כי בעזרת משתמש קצה לא ניתן להשפיע או לשנות את פרטי המשתמשים, הנתונים הרגישים ופוליסות רגישות של האפליקציה, המותנים בבקרת גישה (התחברות), אלא אם כן הדבר הותר באופן מפורש.	4.10
V			ודא כי קיים מנגנון מרכזי להגנה על ממשקי גישה לכל סוג של מקור או משאב מוגן.	4.11
V	V		ודא שכל ניסיון התחברות בממשקי הגישה יכולים להיות מתועדים (לוגים) ובעיקר הניסיונות להתחברות שנכשלו.	4.12



V	V	V	ודא כי האפליקציה או מסגרת העבודה משתמשות באסימונים אנטי CSRF אקראיים וחזקים ולא יש לוודא כי קיים מנגנון הגנה עסקי חלופי.	4.13
V	V		בדוק כי המערכת יכולה להתגונן מפני גישה רציפה דרך פונקציות אבטחה, משאבים, או נתונים. לדוגמא, לשקול להגביל את השימוש של מקור נאמן (משתמש מאומת) ולחסום את מספר הפעמים בשעה בו המקור יכול לערוך נתונים ובכך למנוע השחתה של ממסד הנתונים כולו על ידי משתמש או מקור אחד בודד.	4.14
V	V		ודא כי לאפליקציה יש ממשק התחברות נוסף (אימות אדפטיבית) למערכות בעלות שווי נמוך יותר, ו / או פרדת תפקידים עבור אפליקציות בעלות ערך גבוה ולאכוף בקרות אנטי הונאה לפי סיכוני האפליקציה וההונאות בעבר.	4.15
V	V	V	ודא כי האפליקציה אוכפת כראוי אישורים תלויי-קשר כדי לא לאפשר מניפולציה ואישור בלתי מורשה באמצעות חיבול בפרמטר.	4.16

לקבלת מידע נוסף, ראה:

- יבדיקות אישורים OWASP מדריך 4.0:
- https://www.owasp.org/index.php/Testing\_for\_Authorization אישור
  - :Cheat sheet בקרת גישה

https://www.owasp.org/index.php/Access\_Control\_Cheat\_Sheet

# יות אימות טיפול קלט זדוניות:V5

### מטרת על

חולשת אבטחת האפליקציה אינטרנט הנפוצה ביותר היא אי אימות או חוסר באימות נכון של קלט המגיע מצד הלקוח או מהסביבה ממנה מגיע הקלט לפני השימוש. חולשה זו גורמת כמעט לכל נקודות התורפה הגדולות באפליקציות, כגון מהסביבה ממנה מגיע הקלט לפני השימוש. Interpreter injection ,SQL injection ,XSS, התקפת overflow.

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- כל קלט עובר תהליך אישור על מנת לוודא כי הינו תקין למטרה המיועדת.
- נתונים ממקור חיצוני או לקוח לעולם יוגדרו כלא מהימנים, יש לטפל בקלט זה בהתאם.



3	2	1	תיאור	#
V	V	V	ודא כי האפליקציה בזמן הריצה לא רגישה ל-Buffer overflow, או כי בקרות האבטחה מונעות Buffer overflow.	5.1
V	V	V	ודא כי כאשר הקלט בצד השרת נכשל האפליקציה מכריחה הכנסה מחדש של הקלט, ובנוסף יש לתעד את הכשל.	5.3
V	V	V	ודא כי אימות הקלט נעשה באופן שגרתי ונאכף בצד השרת.	5.5
V	ודא כי בקר אימות קלט בודד יופעל ע"י האפליקציה עבור כל סוג של נתונים שהאפליקציה מקבלת.		5.6	
V	V	V	ודא כי כל שאילתות SQL, HQL, OSQL, NoSQL ופרוצדורות האחסון או קוראות של פרוצדורות אחסון מוגנות מפני שימוש בשאילתות זדוניות מוכנות או אינומרציית הפרמטרים, וכך למנוע פגיעות ל-SQL injection.	5.10
V	V	V	ודא שהאפליקציה לא רגישה ל-LDAP injection, או כי בקרות אבטחה יודעות להתמודד ולמנוע LDAP injection.	5.11
V	V	V	ודא שהיישום לא רגיש הזרקת פקודות למערכת ההפעלה, או כי בקרות אבטחה יודעות להתמודד ולמנוע הזרקת פקודות למערכת ההפעלה.	5.12
V	V	V	ודא שהיישום לא רגיש הכללת קובץ מרחוק (RFI) או הכללת קובץ מקומי (LFI) כאשר התוכן משמש כנתיב לקובץ.	5.13
V	V	V	ודא שהיישום לא פגיע להתקפות XML נפוצות, כגון שיבוש שאילתא XPath, התקפה חיצונית, והזרקת XML.	5.14
V	V	V	ודא שכל המשתנים מסוג מחרוזת ב-HTML או בקוד הלקוח מקודדים באופן ידני ומותאם, או לנצל תבניות קידוד באופן אוטומטי כדי להבטיח שהאפליקציה אינה רגישה להתקפות XSS כגון Stored, Reflected, DOM.	5.15
V	V		אם מסגרת האפליקציה מאפשרת הקצאת אוטומטית מרובה פרמטרים מהבקשה לתוך מודל, ודא ששדות בטחוניים רגישים כגון " accountBalance ", " role " או "password " מוגנים מפני בניה אוטומטית זדונית.	5.16
V	V		ודא כי האפליקציה כוללת הגנות מפני זיהום פרמטר ב-HTTP, במיוחד אם מסגרת האפליקציה אינה מבחינה בין מקורות הפרמטרים בבקשה עצמה (GET, POST, עוגיות, Header, סביבה ועוד)	
V	V		ודא כי קיים אימות בצד הלקוח שישמש כקו הגנה משני, בנוסף לאימות בצד השרת.	5.18
V	V		ודא שכל נתוני הקלט תקינים, לא רק בשדות טפסי HTML אלא לכל מקורות קלט אפשריות כגון קריאות REST, פרמטרים של שאילתה, HTTP Headers,	5.19



		עוגיות, קבצי batch, הזנות RSS, וכו'; כל זאת נעשה באמצעות (בסדר חשיבות יורד) greylisting ,whitelisting (ביטול מחרוזות זדוניות ידועות), או blacklisting.	
V	V	ודא כי הנתונים המובנים מאופיינים ומאומתים נגד סכימה מוגדרת: תווים מותרים ואורך הקלט (מספרי כרטיסי אשראי או טלפון למשל, או על מנת לאשר כי בשני תחומים אלו הקלט הינו תקין והגיוני, כגון אימות בין כתובת למיקוד).	5.20
V	V	ודא כי נתונים לא מובנים אכופים באמצעי בטיחות כללי כגון תווים מותרים ואורכם, טיהור מתווים מזיקים (עלול להזיק כאשר בקלט הנתון יש תו לא שגרתי אך לגיטימי, למשל שמות טבעיים עם Unicode או גרשיים, כגון ね או O'Hara א	5.21
V	V	ע ולאחר מכן לטפל HTML Sanitizer א מהימנים עם HTML הולאחר מכן לטפל בהם כראוי על פי משימת אימות הקלט וקידוד הנתונים.	5.22
V	V	עבור טכנולוגיית "auto escaping" אוטומטית, אם הטכנולוגיה מושבתת בשכבת ה-UI, נדרש לוודא חיטוי ה-HTML במקום.	5.23
V	V	ודא כי נתונים המועברים DOM אחת לאחרת, משתמשים בשיטות JavaScript בטוחות, כגון שימוש innerText.	5.24
V	V	ודא בעת ניתוח JSON בדפדפנים, כי JSON.parse משמש כדי לנתח JSON בדפדפנים, כי על צד הלקוח. אין להשתמש בפונקציית ()eval כדי לנתח JSON על צד הלקוח.	5.25
V	V	ודא שנתונים רגישים (כגון נתוני אימות) נמחקים מאחסון הלקוח, כגון DOMהדפדפן, כאשר ולאחר שה-Session הסתיים.	5.26

לקבלת מידע נוסף, ראה:

- מדריך 4.0: בדיקות אימות קלט OWASP https://www.owasp.org/index.php/Testing\_for\_Input\_Validation
- אימות: OWASP Cheat sheet https://www.owasp.org/index.php/Input Validation Cheat Sheet קלט
- מדריך (4.0 מדריך OWASP מדריך (4.0 מדריך OWASP בדיקת זיהום פרמטר https://www.owasp.org/index.php/Testing for HTTP Parameter pollution %28 HTTP OTG-INPVAL-004%29
  - אניליון לרמות הזרקת OWASP https://www.owasp.org/index.php/LDAP Injection Prevention Cheat Sheet LDAP



סWASP מדריך 4.0: בדיקה בצד OWASP ●

https://www.owasp.org/index.php/Client\_Side\_Testing לקוח

Cheat OWASP Cross Site Scripting •

https://www.owasp.org/index.php/XSS\_%28Cross\_Site\_Scripting%29\_Prevention\_Sheet Cheat\_Sheet

סעדוד הפרויקט OWASP Java ●

https://www.owasp.org/index.php/OWASP Java Encoder Project

לקבלת מידע נוסף על-מילוט אוטומטי, עיין:

- עמצום XSS בדרך של XSS בדרך של Automatic Context-Aware Escaping מערכות אמצרם XSS מערכות מערכות מערכות מערכות מערכות automatic.html
  - AngularJS Strict Contextual Escaping https://docs.angularjs.org/api/ng/service/\$sce בריהת
  - https://cwe.mitre.org/data/definitions/915.html •

# יציאה / בריחה: V6

סעיף זה שולב ב-5V דרישת 5.16 כתובות קידוד פלט הקשרים כדי לסייע במניעת XSS.

### :V7 קריפטוגרפיה

### מטרת על

ודא שהאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- מודולים הצפנה כאשר ונכשלים עושים זאת באופן מאובטח, ובנוסף לכך יש לבדוק ניהול שגיאות ראוי.
  - שימוש במנגנון הגרלת מספר אקראי כאשר עולה הצורך.
    - הגישה למפתחות אבטחה מנוהלת בצורה מאובטחת.



3	2	1	תיאור	#
V	V	V	ודא כי כל המודולים הצפנה נכשלים באופן מאובטח, וניהול השגיאות נעשה בצורה שאינה מאפשרת oracle padding.	7.2
V	V		ודא שכל הפרמטרים האקראיים: מספרים, שמות קבצים, GUIDs ומחרוזות נוצרים באמצעות מודול ההצפנה אשר מחולל מספרים אקראי כאשר ערכים האקראיים אלה יהיו קשות לניחוש על ידי תוקף.	7.6
V	V	V	ודא כי אלגוריתמי הקריפטוגרפיה בהם יש שימוש באפליקציה אומתו מול תקן FIPS 140-2 או תקן מקביל.	7.7
V			ודא כי מודולי ההצפנה פועלים באופן מבוקר ובהתאם למדיניות האבטחה הציבורית.	7.8
V	V		ודא כי קיימת מדיניות מפורשת לאופן ניהול הצפנת המפתחות (למשל, יצירת מפתח, הפצה ותוקף). ודא כי ניהול מחזור החיים של מפתח נאכף ומבוקר כראוי.	7.9
V			ודא כי לכל הצרכני שירותי ההצפנה אין גישה ישירה לחומר המפתח. לבודד תהליכי הצפנה, כולל סודות מאסטר ולשקול את השימוש בכספת מפתח וירטואלית או פיזית (HSM).	7.11
V	V		מידע המאפשר זיהוי האישי צריך להיות מאוחסן ומוצפן, ולהבטיח כי התקשורת דרכה עובר מידע זה עוברת דרך ערוצים מוגנים.	7.12
V	V		ודא כי סיסמות רגישות או חומר המפתח שנשמרו בזיכרון מוחלפים באפסים ברגע שאלו כבר לא נדרשים, כדי למנוע התקפות זיכרון.	7.13
V	V		ודא שכל המפתחות והסיסמאות ניתנות להחלפה, ונוצרות או מתחלפות בעת ההתקנה.	7.14
V			ודא מספרים אקראיים נוצרים עם האנטרופיה הנכונה גם כאשר האפליקציה תחת עומס כבד, או שהאפליקציה מדרדרת בנסיבות דומות.	7.15

### הפניות

לקבלת מידע נוסף, ראה:

• בדיקת OWASP מדריך 4.0: בדיקת סWASP בדיקת סWASP החלשה https://www.owasp.org/index.php/Testing for weak Cryptography



### -OWASP Cheat sheet •

https://www.owasp.org/index.php/Cryptographic\_Storage\_Cheat\_Sheet אחסון

### V8: שגיאת טיפול ורישום דרישות אימות

### מטרת על

המטרה העיקרית של טיפול בשגיאות ורישום היא לספק תגובה שימושית על ידי המשתמש, מנהלים וצוות תגובה לאירוע. המטרה היא לא ליצור כמויות אדירות של יומנים, אך יומנים באיכות גבוהה, עם אות יותר רעש מבוטל.

תיעוד באיכות גבוהה בדרך יכיל מידע רגיש, ולכן יש להגן עליו לפי חוקי הפרטיות. ודא שהאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- אין צורך באיסוף ותיעוד מידע רגיש אלא אם כן נדרש באופן ספציפי.
- לוודא כי כל המידע המתועד מטופל באופן מאובטח ומוגן בהתאם לסיווגו.
- לוודא כי התיעוד אינו נשמר באופן תמידי, כלומר אורך החיים של תיעוד מוגדר לפרק זמן מסוים וקצר ככל האפשר.

אם התיעודים כוללים מידע פרטי או רגיש, אלו עשויים להחזיק בחלק מהמידע הרגיש ביותר שקיים באפליקציה ובכך מאוד אטרקטיביים עבור תוקף.

3	2	1	תיאור	#
V	V	V	ודא כי האפליקציה אינה פולטת הודעות שגיאה, פלט או עקבות מחסנית המכילים מידע רגיש שיכול לסייע לתוקף, כולל Session ID, תוכנה / גרסאות המסגרת ומידע אישי אודות האפליקציה.	8.1
V	V		ודא כי ניהול הטיפול בשגיאות בבקרות אבטחת לא מאפשר גישה כברירת מחדל.	8.2
V	V		ודאו כי בקרת התיעוד של תעבורת ממשקי ההתחברות מספקת את האפשרות לתעד את צליחת ההתחברות ובדגש על אירועי כשל המזוהות ככשל אבטחתי.	8.3
V	V		ודא כי כל תיעוד כולל את המידע הדרוש לחקירה מפורטת של הציר הזמן כאשר אירוע מתרחש.	8.4
V	V		ודא שכל התיעודים הכוללים נתונים לא מהימנים לא יפעלו כקוד בתוכנת הצפייה הייעודית (תוכנה לצפייה בתיעודים השונים).	8.5



V	V		ודא כי תיעודי האבטחה מוגנים מפני גישה לא מורשת ועריכה לא מורשת.	8.6
V	V		ודא כי האפליקציה אינה מתעדת מידע רגיש כהגדרתה תחת חוקי הפרטיות המקומיים או התקנות, נתונים רגישים המפרטים מידע ארגוני כפי שהוגדר על ידי הערכת הסיכונים, או נתוני אימות רגישים העלולים לסייע לפורץ, כולל Session של המשתמש, סיסמאות, הצפנות, או אסימוני API.	8.7
V			( , ) ודא שכל סימנים שאינם ניתנים להדפסה ומפרידי השדה ( , ) מקודדים כראוי בתהליך התיעוד, כדי למנוע Log injection.	8.8
V			ודא כי בתיעוד קיימים שדות ברורים המפרידים בין ממקורות מידע אמינים ולאלו שאינם מהימנים.	8.9
V	V	V	ודא כי בדיקת תיעוד או תהליך דומה מאפשר אי-התכחשות של עסקות מפתח.	8.10
V			ודא כי לתיעודי האבטחה יש פעולה כלשהי של בדיקת שלמות המידע (ע"י סימון, דגל וכדומה) כדי למנוע שינוי לא מורשה.	8.11
V			ודא כי התיעודים מאוחסנים במחיצה אחרת מהמיקום בו האפליקציה פועלת.	8.12
V	V	V	מקורות זמן צריכים להיות מתואמים כדי לוודא שהזמן בתיעוד הינו תקין ואמין.	8.13

לקבלת מידע נוסף, ראה:

סעמול בדיקות מדריך 4.0 תוכן: בדיקה עבור טיפול OWASP סעריך מדריך אונק: בדיקות מדריך סעריקות מדריך אונק://www.owasp.org/index.php/Testing\_for\_Error\_Handling בשגיאות

### ידע מידע:V9

# מטרת על

ישנם שלושה מרכיבים מרכזיים המרכיבים את רמת הגנת הנתונים: סודיות, אמינות וזמינות (CIA). תקן זה מבוסס על ההנחה כי הגנת נתונים נאכפת על מערכה מהימנה, כגון שרת, אשר כבר מוקשח ויש לו הגנות מספיקות.

האפליקציות מחויבות להניח כי כל מכשירי המשתמשים נמצאים בסיכון כלשהו. כאשר האפליקצגיה משדרת או מאחסנת מידע רגיש במכשירים שאינם מאובטחים, כגון מחשבים משותפים, טלפונים וטאבלטים, האפליקציה אחראית להבטיח כי הנתונים המאוחסנים במכשירים אלה מאוחסנים לאחר תהליך הצפנה ולא ניתן להשיג, לשנות או לגלות אותם בקלות.

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הגנת המידע הבאות:



- סודיות: נתונים צריכים להיות מוגנים מתצפית או גילוי מפני גורמים בלתי מורשים בזמן תעבורה ואחסון.
  - **אמינות** : נתונים צריך להיות מוגנים מפני יצירה, שינוי או מחיקה בזדון על ידי התוקפים לא מורשים.
    - זמין: נתונים צריכים להיות זמינים למשתמשים מורשים.

3	2	1	תיאור	#
V	V	V	ודא שכל הצורות המכילות מידע רגיש אינן שומרות את המידע הזה במטמון בצד הלקוח, כולל אפשרויות השלמה אוטומטיות.	9.1
V			ודא כי האפליקציה מכירה ומגינה על רשימת נתונים רגישים, וכי קיימת מדיניות מפורשת כיצד גישה, הצפנה ואכיפת נתונים אלה נעשית, תחת הנחיות להגנה על נתונים רלוונטיים.	9.2
V	V	V	ודא כי כל הנתונים הרגישים נשלחים לשרת בגוף הודעת HTTP או בכותרות (Headers) (כלומר, פרמטר כתובת האתר לא משמש כדי לשלוח נתונים רגישים).	9.3
V	V	V	ודא כי האפליקציה קובעת כותרות אנטי-מטמון מתאימות לפי הסיכון של האפליקציה, לדוגמא הכותרות הבאות: Expires: Tue, 03 Jul 2001 06:00:00 GMT  Last-Modified: {now} GMT  Cache-Control: no-store, no-cache, must-revalidate, maxage=0  Cache-Control: post-check=0, pre-check=0  Pragma: no-cache	9.4
V	V		ודא כי בשרת, כל העותקים או המידע הזמני והרגיש במטמון מאוחסנים ומוגנים מפני גישה לא מורשית או לאחר שהמשתמש מורשה ניגש נתונים רגישים שלא מורשים לו.	9.5
			ודא כי יש פונקציונליות המתחוללת בסוף של מדיניות ההחזקה כדי להסיר כל סוג של מידע רגיש.	9.6
V	V		בדוק כי האפליקציה ממזערת את מספר הפרמטרים בבקשה, כגון שדות מוסתרים, משתנה Ajax, עוגיות וכותרות.	9.7
			בדוק כי לאפליקציה יש את היכולת לזהות ולהזהיר על מספר חריג של בקשות קצירת מידע.	9.8



9.9	ודא כי הנתונים המאוחסנים בצד הלקוח (כגון אחסון מקומי HTML5, אחסון IndexedDB, session, עוגיות רגילות או עוגיות פלאש) אינו מכיל נתונים רגישים או פרטים אישיים מזהים.	
9.10	ודא כי הגישה לנתונים רגישים מתועדת, אילו הנתונים שנאספו לפי הנחיות להגנה על נתונים רלוונטיים או היכן שרישום של כניסות (ממשקי התחברות) נדרש.	
9.11	ודא כי מידע רגיש הנשמר בזיכרון מוחלף עם אפסים ברגע שהוא כבר לא נדרש, כדי למתן התקפות השלכת זיכרון.	

# לקבלת מידע נוסף, ראה:

הגנת פרטיות Cheat Sheet • https://www.owasp.org/index.php/User\_Privacy\_Protection\_Cheat\_Sheet המשתמש:

# יתקשורת:V10

# מטרת על

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- נעשה שימוש ב-TLS ובו מועבר מידע רגיש.
- נעשה שימוש באלגוריתמים וצופנים חזקים בכל העת.

3	2	1	תיאור	#
V	V	V	Transport Layer מהימן עבור כל CA מהיבנות מתוך (certificate) אישור שרת (server certificate (TLS) Security תקף.	10.1
V	V	V	ודא כי יש שימוש ב-TLS עבור כל החיבורים (כולל חיבורים חיצוניים ו-backend) המשמשים לאימות או כוללים נתונים או פונקציות רגישות, ואינו לנפול חזרה לפרוטוקולים לא מאובטחים או לא מוצפנים. ודא כי האלטרנטיבה החזקה ביותר היא האלגוריתם המועדף ויש להשתמש בו.	10.3
V			לוודא שחיבור backend TLS שנכשלו מתועדים.	10.4
V			לאמת כי לאישור יש נתיבים בנויים ומאומתים עבור כל אישורי הלקוח באמצעות trust anchors ו-revocation information.	10.5



V	V		ודא שכל החיבורים למערכות חיצוניות שכוללות מידע או פונקציות רגישות הם מאומתים.	10.6
V			ודא כי קיים מימוש תקן TLS יחיד המשמש את האפליקציה ומוגדר לפעול בעת תקשורת או פעולה שלא כשורה.	10.8
V	V		ודא כי הצמדת מפתח אישור TLS ציבורי (HPKP) מיושם עם מפתחות ייצור ציבוריים ומפתחות גיבוי. לקבלת מידע נוסף, עיין באזכור להלך.	10.10
V	V	V	ודא כותרות HTTP Strict Transport Security מוגדרות וחלות על כל הבקשות ועבור כל תחומי השרת (sub domains), כגון -Strict Transport-Security: max-age=15724800; includeSubdomains.	10.11
V			ודא כי כתובת אתר אינטרנט ייצור הוגשה לרשימה שנטענה מראש של תחומי Strict Transport Security ומתוחזק על ידי ספקי דפדפני האינטרנט. עיין האזכור להלן.	10.12
V	V	V	ודא כי נמצא שימוש בצופן ביטחון לפנים (forward secrecy) סודיות כדי להקטין תוקפים פסיביים מהקלטת תעבורת הנתונים.	10.13
V	V	V	Online ראוי, כגון פרוטוקול (certificate) ודא כי שלילת אישור (OCSP) (OCSP), מופעלת ומוגדרת.	10.14
V	V	V	ודא כי נעשה שימוש רק באלגוריתמים חזקים, צופנים, ופרוטוקולים, דרך כל היררכית התעודה, כולל root ואת אישורי ביניים של הרשות המאשרת (certifying authority) שבחרה.	10.15
V	V	V	ודא שהגדרות TLS עולות בקנה האחד עם הפרקטיקה המובילה הנוכחית, במיוחד כאשר הגדרות נפוצות, צופנים, ואלגוריתמים נפרצים ברבים.	10.16

לקבלת מידע נוסף, ראה:

Cheat sheet – OWASP •

https://www.owasp.org/index.php/Transport\_Layer\_Protection\_Cheat\_Sheet .TLS

. "Approved modes of TLS " הערות על

(https://wiki.mozilla.org/Security/Server\_Side\_TLS)

/ גנרטור./https://mozilla.github.io/server-side- TLS / SSL-config

• מצמיד תעודה . לפרטים נוספים נא לעיין . https://tools.ietf.org/html/rfc7469 . הרציונל מאחורי התעודה מצמידה את מפתחות ייצור וגיבוי ובן נשמר הוא המשכיות עסקית - https://noncombatant.org/2015/05/01/about-http-public-key-pinning/



Cheat Sheet תעודת הצמדה OWASP

https://www.owasp.org/index.php/Pinning\_Cheat\_Sheet

• סWASP תעודת המפתח ציבור הצמדתו

https://www.owasp.org/index.php/Certificate\_and\_Public\_Key\_Pinning

Time of first use (TOFU) Pinning •

https://developer.mozilla.org/en/docs/Web/Security/Public\_Key\_Pinning

Pre-loading HTTP Strict Transport Security

https://www.chromium.org/hsts

### ועורת אבטחה V11: תצורת אבטחה

### מטרת על

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- שרת האפליקציה עבר הקשחה כראוי מתצורת ברירת המחדל.
- תגובות ה- HTTP מגדירות בכותרת Content-Type את סוג ה- HTTP

3	2	1	תיאור	#
V	V	V	ודא כי האפליקציה מקבלת רק קבוצה מוגדרת של שיטות בקשת HTTP נדרשות, כגון GET ו- POST, ושיטות לא בשימוש (למשל TRACE, PUT, ו-DELETE) נחסמות במפורש.	11.1
V	V	V	ודא שכל תגובת HTTP מכילה Header המגדיר את סוג התוכן וטווח תווים בטוח (למשל, UTF-8, ISO 8859-1).	11.2
V	V		ודא כי ה-Headers שנוספו באמצעות שרת פרוקסי מהימן או מכשירי SSO, כגון אסימונים, יאומתו על ידי האפליקציה.	11.3
V	V		ודא כי מוגדר X-Frame-Options Header מתאים וכי נמצא בשימוש עבור אתרים או דפים שאינם מיועדים להצגה מגורם צד שלישי כלשהו.	11.4



11.5	ודא כי HTTP headers או כל חלק של תגובת HTTP אינם חושפים מידע אודות גרסת המערכת או פירוט של רכיבי המערכת.	V	V	V
oniff on"	X-Content-Type- מכילות API- מכילות העבובות ה-API מכילות Content- Content-Disposition: ו- Options: nosniff (או קובץ מתאים attachment; filename="api.json" אחר עבור סוג התוכן).	V	V	V
לעזו לעזו	ודא כי מדיניות אבטחת תוכן (CSPv2) ממומשת כראוי כדי לעזור לצמצם פגיעויות נפוצות של DOM, XSS, JSON, והזרקות JavaScript.	V	V	V
11.8	Header: X-XSS-Protection: 1; mode=block-ודא כי נכלל בכל תגובה, על מנת לאפשר סינון בסיסי ל- Reflected .XSS	V	V	V

### לקבלת מידע נוסף, ראה:

- HTTP אבדריך 4.0: בדיקות הבלות OWASP https://www.owasp.org/index.php/Testing\_for\_HTTP\_Verb\_Tampering\_%28OTG- הבלת INPVAL-003%29
  - הוספת Content-Disposition לתגובות API המסייעת במניעת תקיפות רבות המבוססות על אי-הבנת MIME בין הלקוח והשרת.

 $\frac{\text{https://www.blackhat.com/docs/eu-14/materials/eu-14-Hafif-Reflected-File-Download-A-New-Web-Attack-Vector.pdf}{\text{A-New-Web-Attack-Vector.pdf}}$ 

ימות אבטחה V12: דרישות אימות תצורת אבטחה

סעיף זה שולב ב-V11.

ישליטה זדונית:V13

מטרת על

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- פעילות זדונית מטופל באופן מאובטח כדי לא להשפיע על שאר רכיבי האפליקציה.
  - אין פעצות זמן או בתכפות מרותתות זמן אחרים מורוים אותם



- לא "התקשר הביתה" ליעדים זדוניים, לא מורשים או לא מוכרים.
- לאפליקציות אין דלתות אחוריות, התקפות סלמי, או פגמי היגיון שיכולים להוות מקור נשלט על ידי תוקף.

קוד זדוני הוא נדיר ביותר, והוא קשה לזהוי. סקירה ידנית על הקוד (שורה-שורה) יכולה לסייע למצוא Logic bombs, אבל אפילו סוקר הקוד המנוסה ביותר יתקשה למצוא קוד זדוני גם אם הם יודעים שזה קיים. סעיף זה אינו ניתן להשלים אבל אפילו סוקר הקוד המקור, כולל מספר רב של ספריות צד שלישי ככל האפשר.

### דרישות

#	תיאור	1	2	3
13.1	ודדא כי כל הפעילות הזדונית רצה בארגז חול מוגבל או מבודדת כדי לעכב ולהרתיע תוקפים מלתקוף אפליקציות נוספות.			V
13.2	ודא כי קוד המקור של האפליקציה, וכן כמה שיותר ספריות צד שלישי, אינו מכיל דלתות אחוריות, פגמי היגיון בתהליכי אימות, בקרת גישה, אימות קלט והלוגיקה העסקית של עסקאות בעלי ערך גבוה.			V

### הפניות

# לקבלת מידע נוסף, ראה:

http://www.dwheeler.com/essays/apple-goto-fail.html •

V14: דרישות אימות ביטחון הפנים

סעיף זה שולב ב- V13.

V15: לוגיקה עסקית

### מטרת על

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- הלוגיקה העסקית רציפה ולפי סדר הגיוני.
- הלוגיקה עסקית כוללת מגבלות שנועדו לזהות ולמנוע התקפות אוטומטיות, כגון העברות כספים קטנים ומתמשכות, או הוספה מיליון חברים בפעם אחת, וכן הלאה.
- תזרימי הלוגיקה עסקית בעלי ערך גבוה עלולים להיות מעורבים במקרי התעללות ושחקנים זדוניים, ומול אלו יש להציב הגנות מפני זיוף, שיבוש, התכחשות, גילוי מידע, והתקפות העלאת רמת הרשאות.



#	תיאור	1	2	3
15.1	בדוק כי האפליקציה תעבד תזרים לוגיקה עסקית רק כאשר הוא רציף, עם סדר הצעדים המוגדר לפי הלוגיקה, בזמן אדם מציאותי, ולא לעבד תהליך מקולקל, דילוג על שלבים מהלוגיקה, עיבוד תהליך ושלבי תהליך ממשתמש אחר, או עסקות שהוגשו במהירות לא אנושית.		V	V
15.2	בדוק כי לאפליקציה יש גבולות עסקיות והיא אוכפת אותן כראוי על כל משתמש בסיסי, עם התראות לפי הגדרה ותגובות אוטומטיות לתקיפה אוטומטית או יוצאת דופן.		V	V

### הפניות

# לקבלת מידע נוסף, ראה:

• בדיקת OWASP מדריך 4.0: בדיקה הלוגיקה העסקית OWASP עסקית עסקית שסקית https://www.owasp.org/index.php/Testing\_for\_business\_logic

Cheat OWASP

https://www.owasp.org/index.php/Business\_Logic\_Security\_Cheat\_Sheet :Sheet

# V16: תיוק ומשאבים

## מטרת על

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- קבצי נתונים לא מהימנים צריכים להיות מטופלים בהתאם ובאופן מאובטח
- שבצים המתקבלים ממקורות לא מהימנים מאוחסנים מחוץ לנתיב ה-Webroot ובהרשאות מוגבלות.

#	תיאור	1	2	3
16.1	ודא כי הפניות URL מתאפשרות רק ליעדים מורשים, או להציג אזהרה כאשר ישנו פוטנציאל להפניה לתוכן לא מהימן.	V	V	V
16.2	ודא כי קבצים לא מהימנים שנשלחו לאפליקציה אינם מוזרקים ישירות עם קובץ פקודות I / O , במיוחד כדי להגן מפני חציית נתיב, הכללת קובץ מקומי, סוגי קבצי MIME, ונקודות תורפה להזרקת פקודות למערכת ההפעלה.	V	V	V



V	V	V	וודא כי הקבצים המתקבלים ממקורות לא מהימנים מאומתים להיות מסוג מוכר (סוג התוכן, סוג הקובץ) ויש לסרוק את התוכן על ידי אנטי וירוס כדי למנוע העלאה של תוכן זדוני.	16.3
V	V	V	ודאו כי אין שימוש בנתונים לא מהימנים בתוך הכללת קבצים, טעינת Class, או יכולות השתקפות כדי למנוע פגיעויות הכללת קבצים מקומיות או מרוחקות.	16.4
V	V	V	ודא כי אין שימוש בנתונים לא מהימנים ממקורות שיתוף משאבים בין תחומיים (CORS) כדי להגן מפני תוכן זדוני מרוחק.	16.5
V	V		וודא שקבצים המתקבלים ממקורות לא מהימנים מאוחסנים מחוץ לנתיב ה-Webroot, עם הרשאות מוגבלות, ורצוי עם תהליך אימות.	16.6
V	V		כברירת מחדל ודא כי שרת האינטרנט או האפליקציה מוגדרים למנוע גישה למשאבים מרוחקים או למערכות מחוץ לשרת האינטרנט או האפליקציה.	16.7
V	V	V	וודא כי קוד האפליקציה אינו מריץ נתונים או קבצים שהועלו ממקורות לא מהימנים.	16.8
V	V	V	אל תשתמש בפלאש, Java ,Active-X, Silverlight, NACL בצד הלקוח או טכנולוגיות צד לקוח אחרים שאינם נתמכים באופן מקורי באמצעות סטנדרטי הדפדפן W3C.	16.9

# לקבלת מידע נוסף, ראה:

טיפול סיומות קובצים עבור מידע

https://www.owasp.org/index.php/Unrestricted\_File\_Upload :רגיש

# ייל: V17

## מטרת על

### דרישות לאפליקציות ניידות:

- רמת בקרות האבטחה בתוך הלקוח הנייד חייבת להיות זהה לזו שנמצאת על השרת, על ידי אכיפת בקרות אבטחה בסביבה מהימנה.
  - אחסון נכסי מידע רגיש במכשיר הנייד צריך להיעשות באופן מאובטח
  - Transport Layer Security כל המידע הרגיש מועבר מהמכשיר צריך להיעשות עם קונספט



#	תיאור	1	2	3
17.1	ודא כי ערכי מזהה המאוחסנים במכשיר וניתנים לאחזור על ידי אפליקציות אחרות, כגון UDID או מספר IMEI שאינם משמשים כאסימוני אימות.	V	V	V
17.2	ודא כי האפליקציה לנייד אינה מאחסנת נתונים רגישים על גבי מקורות משותפים ולא מוצפנים במכשיר (כרטיס SD למשל או תיקיות משותפות).	V	V	V
17.3	ודאו שנתונים רגישים אינם מאוחסנים ללא הגנה על המכשיר, אפילו באזורים המוגנים של מערכת כגון מחזיקי מפתחות.	V	V	V
17.4	ודא כי מפתחות סודיים, אסימונים API, או סיסמאות נוצרים באופן דינאמי באפליקציות על גבי המכשיר.	V	V	V
17.5	ודא כי האפליקציה לנייד מונעת דליפה של מידע רגיש (למשל, צילום מסך של האפליקציה ובה מופיע מידע רגיש).		V	V
17.6	ודא כי היישום מבקש הרשאות מינימאליות עבור פונקציונליות ומשאבים נדרשים.		V	V
17.7	ודא כי קוד האפליקציה הרגיש ערוך ומפוזר באופן בלתי צפוי בזיכרון (לדוגמא ASLR).	V	V	V
17.8	ודא כי ישנן טכניקות אנטי באגים נוכחית שיש בהן מספיק כדי להרתיע או לעכב תוקפים סבירים מהזרקת debuggers לאפליקצייה הניידת (לדוגמא GDB).			
17.9	ודא כי האפליקציה אינה מייצאת פעילויות רגישות, או ספקי תוכן עבור אפליקציות ניידות אחרות באותו המכשיר.	V	V	V
17.10	ודא כי מידע רגיש הנשמר בזיכרון מוחלף עם אפסים ברגע שהוא כבר לא נדרש, כדי למתן התקפות השלכת זיכרון.		V	V
17.11	ודא כי האפליקציה מאמתת קלט לפעילויות.	V	V	V

### הפניות

לקבלת מידע נוסף, ראה:

פרויקט האבטחה הניידת •

https://www.owasp.org/index.php/OWASP\_Mobile\_Security\_Project :OWASP

Developer Cheat גיליון

https://www.owasp.org/index.php/IOS\_Developer\_Cheat\_Sheet :iOS



# V18: שירותי רשת

### מטרת על

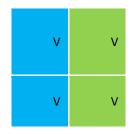
ודא שהאפליקציה המשתמשת בשירותי רשת המבוססים RESTful כוללת:

- אימות, ניהול Session והרשאות נאותים עבור כל שירותי הרשת באפליקציה
  - אימות קלט של כל הפרמטרים המועברים מרמת אמון נמוכה לגבוהה •
- יכולת פעולה הדדית בסיסית של שכבת שירותי הרשת SOAP כדי לקדם את השימוש ב- API

3	2	1	תיאור	#
V	V	V	ודא כי יש את אותו סגנון הקידוד בין הלקוח לבין השרת.	18.1
V	V	V	וודא כי הגישה כי לפונקציות ניהוליות וניהול בתוך שירותי הרשת של האפליקציה מוגבלות רק למנהלים.	18.2
V	V	V	אמת כי ישנו שימוש ב-XML או סכימת JSON ולהם מתבצע אימות לפני קבלת קלט.	18.3
V	V	V	ודא שכל קלט מוגבל במגבלת גודל מתאימה או הגיונית.	18.4
V	V	V	ודא כי שירותי הרשת מבוססי SOAP תואמים לשירותי הרשת ההדדיים (WS-I) פרופיל בסיסי לכל הפחות. זה למעשה מורה על הצפנת TLS.	18.5
V	V	V	בדוק את השימוש ב-Session מבוסס תהליך אימות והרשאות. עיין בסעיפים 2, 3 ו -4 לקבלת הדרכה נוספת. יש להימנע משימוש ב"מפתחות API" סטטיים וכדומה.	18.6
V	V	V	ודא ששירות REST מוגן מפני זיוף בקשה בין אתרים (CSRF) באמצעות השימוש בלפחות אחת או יותר מהפעולות הבאות: בדיקות ORIGIN, דפוס יצירת עוגיה (Cookie) כפולה,	18.7
V	V		בדוק כי שירות REST מוגדר לבדוק את REST מוגדר לבדוק את הנכנס וכי הוא צפוי, כגון xml / application או application / json.	18.8



ודא כי תוכן ההודעה חתום על מנת להבטיח תחבורה אמינה בין הלקוח ושירות, באמצעות חתימת JSON Web או -WS צבור בקשות SOAP.	18.9
ודא כי באפליקציה לא קיימות חלופות ושבילי גישה פחות מאובטחות.	18.10



### לקבלת מידע נוסף, ראה:

- OWASP מדריך 4.0: בדיקות קונפיגורציה ופריסת ניהול OWASP https://www.owasp.org/index.php/Testing\_for\_configuration\_management
  - Cross-Site Request Forgery cheat sheet OWASP
    <a href="https://www.owasp.org/index.php/Cross-Site\_Request\_Forgery">https://www.owasp.org/index.php/Cross-Site\_Request\_Forgery</a> (CSRF) Prevention\_Cheat\_Sheet
    - אסימונים (וחתימה) א JSON Web אסימונים (https://jwt.io

## V19. קונפיגורציה

### מטרת על

ודא שאפליקציה עומדת ברמה הגבוהה בדרישות הבאות:

- עדכן ספריות ופלטפורמות לעדכון האחרון ביותר.
  - תצורת ברירת מחדל מאובטחת.
- הקשחה מספקת על מנת למנוע או ליצור חולשות אבטחה על מערכות עליהן האפליקציה מסתמכת, כאשר המשתמש משנה את הקונפיגורציה לברירת המחדל.

#	תיאור	1	2	3
19.1	כל הרכיבים צריכים להיות מעודכנים עם קונפיגורציה וגרסה מאובטחת ומספקת. זה כולל הסרה של הגדרות קונפיגורציה ותיקיות מיותרות כגון אפליקציות לדוגמה, תיעוד , ומשתמשים ברירת מחדל או משתמשים לדוגמא.	V	V	V
19.2	תקשורת בין רכיבים, כגון בין שרת האפליקציה לבין שרת מסד הנתונים, צריכה להיות מוצפנת, במיוחד כאשר הרכיבים במערכות שונות.		V	V



V	V	תקשורת בין רכיבים, כגון בין שרת האפליקציה לבין שרת מסד הנתונים צריכה להיות מאומתת באמצעות חשבון עם ההרשאות המספקות הפחותות ביותר.
V	V	ודא לפריסות יישומים הם בארגז חול מוגבל כראוי, במכולות או מבודדים לעכב ולהרתיע התוקפים מלתקוף יישומים אחרים.
V	V	ודא כי האפליקציה פורסת ובונה תהליכים בצורה מאובטחת.
V		ודא שמנהלי המערכת המורשים יש את היכולת לוודא את תקינות עבור כל תצורות האבטחה-רלוונטיות, כדי להבטיח שהן לא הזדהמו.
V		ודא שכל רכיבי האפליקציה נחתמים.
V		ודא כי רכיבי צד שלישי מיובאים ממאגר מהימן.
V		ודא כי בבנית התהליכים של שפות ברמת המערכת יש את כל דגלי האבטחה מופעלים, כגון ASLR, DEP, ובדיקות אבטחה אחרות.
V		ודא שכל נכסי האפליקציה מאוחסנים בתוך האפליקציה, כגון ספריות JavaScript, סגנון ה-CSS וגופני אינטרנט ולא להסתמך על CDN או ספק חיצוני.

# לקבלת מידע נוסף, ראה:

סWASP סדריך 3.0: בדיקות קביעת קונפיגורציה ופריסה ניהול OWASP • https://www.owasp.org/index.php/Testing\_for\_configuration\_management