דוח דוגמה בדיוני

דוח בדיקת חדירות לדוגמה

נתונים להמחשה בלבד. אלה אינם ממצאים של לקוחות.

מחבר הדוח · BTNXIO SECURITY · btnxio@gmail.com ·
btnxiosecurity.com

בקרת מסמך

מהדורת המחשה ציבורית · גרסה 2.0 · הוכן על ידי BTNXIO SECURITY. מזהי היעדים שמורים לדוגמאות והתרחישים סינתטיים.

מחבר הדוח · BTNXIO SECURITY · btnxio@gmail.com · btnxiosecurity.com

תוכן עניינים

בקרת מסמך	2
סקירת הנהלה	3
היקף	4
משטח תקיפה	5
DEMO-01 · חשיפה של רשומות בין חשבונות	6
DEMO-02 · בדיקת הרשאת ייצוא חסרה	7
DEMO-03 · תגובות לא אחידות בשחזור חשבון	8
DEMO-04 · הפרדת תוכן ותצוגה בפרופיל	9
DEMO-05 · ביטול חלקי של סשנים	10
DEMO-06 · הגבלת בקשות לא מספקת	11
DEMO-07 · מדיניות אבטחת דפדפן חסרה	12
DEMO-08 · חשיפת פרטים מיותרים בשגיאות	13
DEMO-09 · מדיניות מטמון מתירנית מדי	14
DEMO-10 · חסר תיעוד בעלות על שירות	15
השפעה עסקית	16
תיקון	17
מעקב תיקונים ואימות	18
בדיקה חוזרת	19

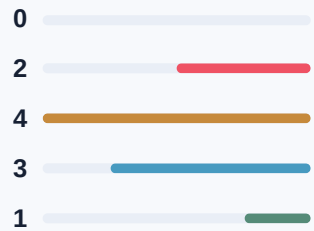
סקירת הנהלה

הדוגמה מדמה סקירה בהיקף מוגדר של פורטל לקוחות בדיוני ושירותים תומכים. בידוד בין חשבונות והרשאות ייצוא נמצאים בראש סדר העדיפויות לתיקון. לוח הבקרה משקף רק את ממצאי ההמחשה המופיעים בדוח.

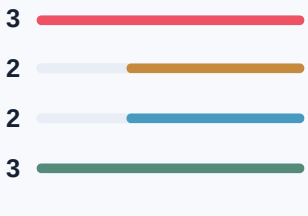
החומרה מוצגת באופן איכותני. לא הוקצה ציון CVSS מספרי.

10
סך הממצאים

התפלגות חומרה



סטטוס תיקונים



יעדי ההערכה

להעריך בידוד בין חשבונות, אכיפת הרשאות לפי תפקיד, טיפול ברשומות פרטיות ובקרות הגנה בתהליכים מייצגים בפורטל ובממשק.

היקף ומגבלות

ההיקף הבדיוני כולל את הפורטל, הממשק שלו ובקרות נבחרות לזהות ולתשתית תחת example.test. מערכות ייצור, גורמי צד שלישי, פעולות הרסניות ובדיקות מניעת שירות אינם כלולים.

מתודולוגיית הבדיקה

הגדרת גבולות מורשים, מיפוי נכסים מייצגים, הערכת בקרות, אימות תצפיות, דירוג סיכון איכותני ותיעוד תיקונים. הדוגמה מדמה תהליך זה בעזרת רשומות סינתטיות.

מלאי נכסים שאותרו

הספירות מתייחסות לנכסים במודל. עמודת הכיסוי מציגה את החלקים שנבחרו לסקירת הדוגמה.

נקודות קצה	24
תת־דומיינים	2
ממשקי API	2
רכיבי תשתית	3
דומיין	1
שירותי וב	3
רכיבי הזדהות	2

תהליכי חשבון, רשומות וייצוא שנבחרו לבדיקה.

נקודות הכניסה לפורטל ולממשק.

רשומות וייצוא.

שער גישה, מטמון ומדיניות ניתוב.

דומיין שמור להמחשה בלבד.

פורטל, שער גישה ושירות ייצוא.

בקרות התחברות ושחזור.

DEMO-01 · חשיפה של רשומות בין חשבונות

גבוה

רכיב מושפע
פורטל לקוחות

תיאור
רשומה ששויכה לחשבון בדיקה הופיעה בחשבון אחר במודל המדומה.

השפעה עסקית
רשומות פרטיות עלולות להיחשף ללקוח אחר.

תיקון
בדקו בעלות ותפקיד בצד השרת לפני החזרת רשומה.

תנאי קבלה
בקשות בין חשבונות נחסמות ומשתמשים מורשים רואים את הרשומות שלהם.

סטטוס ראיה
תצפית סינתטית בלבד

סיווג
CWE-639 · OWASP A01:2021

השפעה טכנית
בקרת בעלות לא עקבית עלולה לחשוף רשומות.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
החילו מדיניות הרשאה אחת על תצוגת הרשימה והפרטים, עם חסימה כברירת מחדל.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
פתוח

ראיה סינתטית EX-01

תצפית בדיונית
רשומה ששויכה לחשבון בדיקה הופיעה בחשבון אחר במודל המדומה.

התנהגות שנצפתה בסימולציה
המודל מציג רשומה בחשבון נוסף.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
רשומות נשארות בחשבון שהוקצה להן.

פרשנות
בקרת בעלות לא עקבית עלולה לחשוף רשומות.

ממצא קשור
DEMO-01

DEMO-02 · בדיקת הרשאת ייצוא חסרה

גבוה

רכיב מושפע
ממשק ייצוא

תיאור
חשבון שהוגדר לצפייה קיבל ייצוא המיועד למפעילים מורשים.

השפעה עסקית
ייצוא בודד עלול לכלול מספר רשומות של לקוחות.

תיקון
בדקו הרשאת ייצוא בפתיחת הפעולה ובקבלת התוצר.

תנאי קבלה
תפקידים לא מורשים אינם יכולים להתחיל ייצוא או לקבל את התוצר.

סטטוס ראיה
תצפית סינתטית בלבד

סיווג
CWE-862 · OWASP A01:2021

השפעה טכנית
בדיקת הרשאה חסרה עלולה לחשוף נתונים בכמות גדולה.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
החילו מדיניות זהה על משימות בתור ועל תוצרי ייצוא שמורים.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
בטיפול

ראיה סינתטית EX-02

תצפית בדיונית
חשבון שהוגדר לצפייה קיבל ייצוא המיועד למפעילים מורשים.

התנהגות שנצפתה בסימולציה
חשבון הצפייה קיבל פרטי ייצוא להמחשה.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
רק מי שמורשה לייצא יכול לקבל ייצוא.

פרשנות
בדיקת הרשאה חסרה עלולה לחשוף נתונים בכמות גדולה.

ממצא קשור
DEMO-02

DEMO-03 · תגובות לא אחידות בשחזור חשבון

בינוני

רכיב מושפע
שחזור חשבון

תיאור
משוב השחזור המדומה השתנה בין שני מצבי חשבון בדיוניים.

השפעה עסקית
גורם חיצוני עלול לזהות חברות בשירות.

תיקון
אחדו את נוסח התגובה ואת ההתנהגות הנצפית.

תנאי קבלה
שני מצבי הדוגמה מקבלים משוב ציבורי זהה.

סטטוס ראיה
תצפית סינתטית בלבד

סיווג
CWE-204 · OWASP A07:2021

השפעה טכנית
הבדלים נצפים עלולים לחשוף אם חשבון קיים.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
השאירו פרטי תוצאה מפורטים במערכות הפנימיות.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
בטיפול

ראיה סינתטית EX-03

תצפית בדיונית
משוב השחזור המדומה השתנה בין שני מצבי חשבון בדיוניים.

התנהגות שנצפתה בסימולציה
המודל הציג סוגי תגובה שונים.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
תהליך השחזור מחזיר משוב אחיד בשני המצבים.

פרשנות
הבדלים נצפים עלולים לחשוף אם חשבון קיים.

ממצא קשור
DEMO-03

DEMO-04 · הפרדת תוכן ותצוגה בפרופיל

בינוני

רכיב מושפע
תצוגת פרופיל

תיאור
בסקירה הבדיונית זוהה שדה טקסט שהועבר לרכיב תצוגה עשיר.

השפעה עסקית
אמון המשתמשים בשלמות הפורטל עלול להיפגע.

תיקון
הציגו את תוכן שדה הפרופיל כטקסט.

תנאי קבלה
הערך נשאר טקסט בכל תצוגות הפרופיל הנתמכות.

סטטוס ראיה
תצפית סינתטית בלבד

סיווג
CWE-79 · OWASP A03:2021

השפעה טכנית
הדפדפן עלול לפרש נתונים שאינם מהימנים.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
השתמשו בקידוד המתאים להקשר והגבילו תוכן עשיר לרכיבים מאושרים.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
פתוח

ראיה סינתטית EX-04

תצפית בדיונית
בסקירה הבדיונית זוהה שדה טקסט שהועבר לרכיב תצוגה עשיר.

התנהגות שנצפתה בסימולציה
המודל מעביר את הערך לרכיב המציג תוכן עשיר.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
ערכים שמגיעים מהמשתמש מוצגים כטקסט.

פרשנות
הדפדפן עלול לפרש נתונים שאינם מהימנים.

ממצא קשור
DEMO-04

DEMO-05 · ביטול חלקי של סשנים

בינוני

רכיב מושפע
שירות סשנים

תיאור
סשן במודל נשאר פעיל לאחר אירוע אבטחה בחשבון.

השפעה עסקית
תהליך שחזור חשבון עלול שלא לבלום גישה בלתי מורשית.

תיקון
בטלו סשנים לאחר השלמת אירוע האבטחה בחשבון.

תנאי קבלה
סשנים שבוטלו נדחים, וסשנים חדשים תקינים ממשיכים לפעול.

סטטוס ראיה
תצפית סינתטית בלבד

סיווג
CWE-613 · OWASP A07:2021

השפעה טכנית
סשן שיצא משימוש עלול להמשיך לספק גישה.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
בדקו את סטטוס הביטול באופן עקבי בכל השירותים.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
מוכן לבדיקה חוזרת

ראיה סינתטית EX-05

תצפית בדיונית
סשן במודל נשאר פעיל לאחר אירוע אבטחה בחשבון.

התנהגות שנצפתה בסימולציה
המודל השאיר סשן במצב פעיל.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
אירוע רגיש בחשבון מבטל את הסשנים הקשורים.

פרשנות
סשן שיצא משימוש עלול להמשיך לספק גישה.

ממצא קשור
DEMO-05

DEMO-06 · הגבלת בקשות לא מספקת

בינוני

רכיב מושפע
ממשק רשומות

סיווג
CWE-770 · OWASP A04:2021

תיאור
מדיניות הדוגמה אינה מגבילה את נפח הבקשות בתהליך עתיר משאבים.

השפעה טכנית
שימוש מופרז עלול למצות משאבים משותפים.

השפעה עסקית
משתמשים לגיטימיים עלולים לחוות עיכוב או שיבוש.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

תיקון
החילו מגבלות על הפעולה עתירת המשאבים.

הנחיה למפתחים
הגדירו מכסות לפי זהות ומשוב עקבי כאשר המגבלה מופעלת.

תנאי קבלה
בקשות עודפות מוגבלות ושימוש רגיל נשאר זמין.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס ראיה
תצפית סינתטית בלבד

סטטוס תיקון
פתוח

ראיה סינתטית EX-06

תצפית בדיונית
מדיניות הדוגמה אינה מגבילה את נפח הבקשות בתהליך עתיר משאבים.

התנהגות צפויה
פעולות עתירות משאבים כפופות למגבלות שימוש.

התנהגות שנצפתה בסימולציה
בתהליך המדומה לא הוגדרה מגבלת שימוש.

פרשנות
שימוש מופרז עלול למצות משאבים משותפים.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

ממצא קשור
DEMO-06

DEMO-07 · מדיניות אבטחת דפדפן חסרה

נמוך

רכיב מושפע
שער גישה

סיווג
CWE-693 · OWASP A05:2021

תיאור
בתצורה המדומה לא הוגדרה מדיניות דפדפן מאושרת בנתיב מסמך.

השפעה טכנית
ההגנה בשכבות נחלשת בתצוגות המושפעות.

השפעה עסקית
קשה יותר לצמצם את ההשפעה של חולשת דפדפן נפרדת.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

תיקון
פרסמו מדיניות מאושרת בשער הגישה.

הנחיה למפתחים
נהלו את הכותרת במרכז ובדקו התנהגות בנתיבים רלוונטיים.

תנאי קבלה
המדיניות מופיעה בנתיבים הרלוונטיים ופעולת האתר הרגילה נשמרת.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס ראיה
תצפית סינתטית בלבד

סטטוס תיקון
סגור

ראיה סינתטית EX-07

תצפית בדיונית
בתצורה המדומה לא הוגדרה מדיניות דפדפן מאושרת בנתיב מסמך.

התנהגות צפויה
תגובות מסמכים רלוונטיות כוללות את המדיניות שנבדקה.

התנהגות שנצפתה בסימולציה
המדיניות לא הופיעה בסיכום התגובה המדומה.

פרשנות
ההגנה בשכבות נחלשת בתצוגות המושפעות.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

ממצא קשור
DEMO-07

DEMO-08 · חשיפת פרטים מיותרים בשגיאות

נמוך

רכיב מושפע
טיפול בשגיאות

תיאור
עמוד שגיאה מדומה חשף פרטי שירות מיותרים.

השפעה עסקית
חשיפת מידע עודף עלולה להגדיל את מאמצי החקירה.

תיקון
החזירו הודעת שגיאה כללית למשתמש.

תנאי קבלה
השגיאות הציבוריות נשארות כלליות ומפעילים יכולים לאתר פרטים באופן פנימי.

סטטוס ראיה
תצפית סינתטית בלבד

סיווג
CWE-209 · OWASP A05:2021

השפעה טכנית
מידע על מבנה המערכת עלול להיחשף.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
שמרו פרטי אבחון ביומנים עם בקרת גישה.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
מוכן לבדיקה חוזרת

ראיה סינתטית EX-08

תצפית בדיונית
עמוד שגיאה מדומה חשף פרטי שירות מיותרים.

התנהגות שנצפתה בסימולציה
תצוגת הדוגמה הציגה פרטי שירות פנימיים.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
שגיאות ציבוריות כוללות הודעה קצרה ומזהה פנייה.

פרשנות
מידע על מבנה המערכת עלול להיחשף.

ממצא קשור
DEMO-08

DEMO-09 · מדיניות מטמון מתירנית מדי

נמוך

רכיב מושפע
מטמון הפורטל

תיאור
בתצורה הבדיונית ניתן היה לשמור דף פרטי במטמון רחב מדי.

השפעה עסקית
במכשירים משותפים תוכן פרטי עלול להישאר גלוי.

תיקון
התאימו מדיניות מטמון לרגישות המידע.

תנאי קבלה
תגובות מסמכים פרטיים משתמשות בהנחיית המטמון המגבילה שאושרה.

סטטוס ראיה
תצפית סינתטית בלבד

סיווג
CWE-525 · OWASP A05:2021

השפעה טכנית
תוכן פרטי עלול להישמר מעבר להקשר שבו נועד להופיע.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
הפרידו כללים לנתיבים ציבוריים ולנתיבים המחייבים הזדהות.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
סגור

ראיה סינתטית EX-09

תצפית בדיונית
בתצורה הבדיונית ניתן היה לשמור דף פרטי במטמון רחב מדי.

התנהגות שנצפתה בסימולציה
המודל זיהה כלל מטמון רחב מדי.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
תגובות של מסמכים פרטיים כפופות למדיניות מטמון מגבילה.

פרשנות
תוכן פרטי עלול להישמר מעבר להקשר שבו נועד להופיע.

ממצא קשור
DEMO-09

DEMO-10 · חסר תיעוד בעלות על שירות

לידיעה

רכיב מושפע
קטלוג נכסים

השפעה טכנית
בעלות לא ברורה עלולה לעכב החלטות תחזוקה.

מגבלות ההערכה
הדוגמה מוגבלת לרכיב המייצג ולתנאים שתוארו במודל.

הנחיה למפתחים
כללו שדות בעלות בהוספת נכסים ובסקירה תקופתית.

דרישות לבדיקה חוזרת
אמתו את תנאי הקבלה ואת ההתנהגות הרצויה מול אותו תרחיש המחשה מאושר.

סטטוס תיקון
סגור

תיאור
קטלוג הדוגמה אינו מציין בעלים לשירות תמיכה.

השפעה עסקית
ניתוב אירוע לגורם אחראי עלול להימשך זמן רב יותר.

תיקון
תעדו צוות אחראי ותדירות סקירה.

תנאי קבלה
לנכס מוגדרים בעלים ולוח זמנים לסקירה.

סטטוס ראיה
תצפית סינתטית בלבד

ראיה סינתטית EX-10

תצפית בדיונית
קטלוג הדוגמה אינו מציין בעלים לשירות תמיכה.

התנהגות שנצפתה בסימולציה
השירות מופיע בקטלוג ללא איש קשר לתחזוקה.

מגבלות הראיה
תוצר של מודל בלבד. הדוגמה אינה מציגה תעבורת רשת, חשבון לקוח או ראיה שאומתה באופן עצמאי.

התנהגות צפויה
לכל שירות מוגדר גורם אחראי.

פרשנות
בעלות לא ברורה עלולה לעכב החלטות תחזוקה.

ממצא קשור
DEMO-10

השפעה עסקית

פערים בבידוד חשבונות ובבקרת ייצוא מציגים את ההשפעה האפשרית הגדולה ביותר על סודיות הנתונים במודל. מומלץ לטפל בהם תחילה, ואז להפחית את הסיכון לשיבושים ולעיכובים תפעוליים.

- DEMO-01 · רשומות פרטיות עלולות להיחשף ללקוח אחר.
- DEMO-02 · ייצוא בודד עלול לכלול מספר רשומות של לקוחות.

מסקנות

המודל ממחיש תיקון בשלבים. סגירת ממצא תתבצע לאחר שהבדיקות המוסכמות ידגימו את יעילות הבקרה ואת תקינות תהליכי המשתמש.

מפת דרכים לתיקון

סדר העדיפויות הוא המלצה לתרחיש ההמחשה. לוחות הזמנים תלויים בהשפעה, בתלויות ובהסכם ההתקשרות.

קריטי

טיפול מיידי

גבוה

תיקון בעדיפות גבוהה

בינוני

תיקון מתוכנן

נמוך

הקשחה מתוזמנת

לידיעה

סקירה שגרתית

המלצות אבטחה

רכזו את מדיניות ההרשאות, כסו גבולות אבטחה בבדיקות רגרסיה ומנו צוותים לתחזוקת הניטור והתיעוד.

מעקב תיקונים ואימות

מזהה	ממצא	חומרה	צוות אחראי	עדיפות	סטטוס תיקון	סטטוס בדיקה חוזרת
DEMO-01	חשיפה של רשומות בין חשבונות	גבוה	צוות יישומים	תיקון בעדיפות גבוהה	פתוח	ממתין לתיקון
DEMO-02	בדיקת הרשאת ייצוא חסרה	גבוה	צוות ממשקים	תיקון בעדיפות גבוהה	בטיפול	ממתין לתיקון
DEMO-03	תגובות לא אחידות בשחזור חשבון	בינוני	צוות זהויות	תיקון מתוכנן	בטיפול	ממתין לתיקון
DEMO-04	הפרדת תוכן ותצוגה בפרופיל	בינוני	צוות יישומים	תיקון מתוכנן	פתוח	ממתין לתיקון
DEMO-05	ביטול חלקי של סשנים	בינוני	צוות זהויות	תיקון מתוכנן	מוכן לבדיקה חוזרת	בתור לבדיקה
DEMO-06	הגבלת בקשות לא מספקת	בינוני	צוות ממשקים	תיקון מתוכנן	פתוח	ממתין לתיקון
DEMO-07	מדיניות אבטחת דפדפן חסרה	נמוך	צוות תשתיות	הקשחה מתוזמנת	סגור	עבר בסימולציה
DEMO-08	חשיפת פרטים מיותרים בשגיאות	נמוך	צוות תשתיות	הקשחה מתוזמנת	מוכן לבדיקה חוזרת	בתור לבדיקה
DEMO-09	מדיניות מטמון מתירנית מדי	נמוך	צוות תשתיות	הקשחה מתוזמנת	סגור	עבר בסימולציה
DEMO-10	חסר תיעוד בעלות על שירות	לידיעה	צוות יישומים	סקירה שגרתית	סגור	עבר בסימולציה

תוכנית בדיקה חוזרת

תעדו את גרסת התיקון ואת הסביבה, חזרו על הבדיקות שאושרו עם חשבונות סינתטיים, אמתו את תנאי הקבלה ואת הפעילות הרגילה ותעדו מגבלות שנותרו.

מסקנות

המודל ממחיש תיקון בשלבים. סגירת ממצא תתבצע לאחר שהבדיקות המוסכמות ידגימו את יעילות הבקרה ואת תקינות תהליכי המשתמש.

נספח טכני

מזהים המתחילים ב־DEMO וב־EX מקשרים ממצאים וראיות בדיוניים. הפניות CWE מתארות סוגי חולשות. הפניות OWASP מתייחסות למהדורת 2021. הדירוג האיכותני מביא בחשבון השפעה וסבירות בהיקף המדומה.

מחבר הדוח · BTNXIO SECURITY · btnxio@gmail.com · btnxiosecurity.com