

תרגיל 3

עליכם לבנות DevSecOps pipeline בעזרת Gitlab (כפי שראינו בכיתה), אשר יכיל את האלמנטים הבאים, כאשר בכל אחד אתם משתמשים בכלי open source (למשל, OWASP ZAP בתור DAST, וב GITLAB עבור SAST וכו'):

- Secret detection
- SCA
- SAST
- IaC
- Container scanning
- DAST

עליכם לוודא שאתם מבינים (לוגית) מה התפקיד של כל אחד מהאלמנטים הנ"ל. למשל, מה ה scope של SAST - איזה סוג של בעיות הוא אמור לתפוס ואיזה לא, איך נגיד כלי שכזה ימומש וכו'. עליכם לחבר את ה pipeline ל instance של DefectDojo שתתקין, כך שתוצאות הרצת ה pipeline יופיעו ב DefectDojo.

עליכם להריץ את ה pipeline הזה עבור פרוייקט ה OWASP WebGoat.

עליכם להגיש דו"ח עם צילומי מסך והסברים (בקצרה) של תהליך התקנת ה pipeline, הגדרתו ועד שלב ההדגמה.

עליכם לייצר דו"ח בעזרת DefectDojo של הממצאים השונים שנמצאו לפרויקט. אם אחד מהאלמנטים הללו לא מוצא חולשות מתאימות (כי אין כאלו), הוסיפו בכוונה חולשות כאלו כדי שיתפסו על ידי ה pipeline.

עליכם לבחור שני ממצאים מכל אחד מהאלמנטים הנ"ל ולהסביר את הממצא, מהי הבעיה, לתקן אותה ולהראות שה pipeline אכן מאשר שהבעיה תוקנה.

הגשה בזוגות.

בהצלחה