פרוייקט Glitter – שלב א'

השנה היא 2025 והוריאנט השמיני של נגיף הקורונה – ה-Delta Lite SE – מתפשט ברחבי מדינת ישראל. תלמידי מערכת החינוך הישראלית, בילו כ-50% מימי הלימוד שלהם בשנתיים האחרונות מול מסכי הזום. במקביל הולכות וגוברות תופעות מטרידות ברשת החברתית החדשה – Bitpunk. סרטוני הסתה, חרמות ושיימינג הולכים וצוברים תאוצה יותר ויותר.

בתאריך 20.06 כינסה שרת החינוך מסיבת עיתונאים מיוחדת ובה הודיעה על המהלך החדש של משרד החינוך – הקמת רשת חברתית חדשה, המיועדת לבני נוער. הרשת החדשה תהיה נעימה, בטוחה לשימוש ותאפשר לתלמידים להתחבר עם חבריהם לכיתה ולשכבה בסביבה בטוחה ונקייה מבריונות ושיימינג. "אנחנו ניקח אחריות מלאה על הרשת החדשה", אמרה שרת החינוך, "ולהורים שצופים בבית, אני רוצה להגיד – אתם יכולים לסמוך עלינו. נשמור על הילדים שלכם בטוחים ונשמור עליהם מחוברים אחד לשני!". וכך נולדה הרשת החברתית החדשה – Glitter.

שרת החינוך הבטיחה שגליטר תושק בדיוק שבועיים מהיום. "תוכלי לפרט על איך תשמרו על הרשת הזאת בטוחה מעברייני רשת והאקרים?" שאל אותה כתב כלכליסט. "הצוות שלנו עובד מסביב לשעון כדי להבטיח את רמת ההגנה המקסימלית", ענתה השרה וירדה מהבימה.

מאחורי הקלעים, לחשה השרה לעוזר האישי שלה: **"אנחנו באמת מוגנים ברמת ההגנה המקסימלית, נכון?".** "אממ, תראי, השרה, נכון לעכשיו, זה קצת מורכ.." -**"הבנתי. יש לך שבוע לטפל בזה. נתתי את המילה שלי מול כל המדינה. אל תאכזב אותי."**

העוזר האישי החליט לגייס בצורה דחופה צוות Pen Testers אשר יחקור את גליטר, ויפתור את כל בעיות האבטחה ברשת בתוך שבוע בלבד. וכך הגענו אליכן.

חלק א' - קצת רקע

אז מה זה בכלל Pen Testing?

Pen Testing הוא קיצור של המושג Penetration Testing או בעברית "בדיקת חדירות".

זהו תהליך במהלכו מקבלות אנשי ונשות אבטחה אישור לנסות ולתקוף מערכת במטרה למצוא בה חולשות, ולהעריך את מידת האבטחה שלה. כחלק מהתהליך אוספת ה-Pen Testerית את שלל הסיכונים הקיימים על המערכת, מדרגת אותם על פי חשיבותם והנזק שעשוי להיגרם מהם, ומייצרת תמונה כללית של מצב המערכת.

אז רגע, Pen Testing זה כמו האקינג?

האקר פועל כדי למצוא ולנצל חולשות בצורה לא חוקית. גם אם לדעת עצמו הוא פועל במוסריות וגם אם אין לו מטרות זדון, זו עדיין עבירה על החוק, מכיוון שאין לו אישור לבצע את הפעולות הללו.

פנטסטר מבצע את אותן פעולות אך בצורה חוקית ומאושרת, כחלק מתהליך הפיתוח של מוצר.

ניתן להתייחס לפנטסטר גם כ-White hat hacker.

למה Pen Testing הוא תהליך כל כך חשוב בפיתוח מוצר?

בתהליך פיתוח של תוכנה, מעורבות בעלות תפקידים רבות – מפתחות, בודקי תוכנה (QA), מעצבות, מתכננות, מנהלות מוצר, ועוד ועוד. כל בעלות התפקידים הללו עובדות מול משהו שנקרא **תרחישי משתמש (User Stories).**

למשל, אם אנחנו כותבות אפליקציה להזמנת פיצה, יכולים להיות מספר **תרחישים** של משתמש:

- בחירת מוצרים לסל קניות.
- יצירת חשבון חדש.
- תשלום והזמנת משלוח.
- שינוי פרטים וכו'..

כל בעלות התפקידים צריכות לדאוג שהדברים יעבדו כמו שצריך לפי תרחישי המשתמש. כלומר, הן דואגות למשתמשים הרגילים של התוכנה. אבל, בעולם האינטרנט, אנחנו יודעים שלא כל המשתמשים של התוכנה הם לגיטימיים ותמימים.

הצוות היחיד שלא מתעניין רק בתרחישי משתמש הוא צוות ה-Pen Testing. הוא יעבוד דווקא עם **תרחישים של תוקף (Attacker Stories).** הם ינסו להיכנס לראש של מישהו שאינו משתמש לגיטימי אלא תוקף פוטנציאלי שמנסה לשבור את המערכת.

איזה מין עבודה זו?

Pen Testing היא עבודה מחקרית, הדורשת יצירתיות והרבה סבלנות. מחקר הוא תהליך שתוצאותיו לא ברורות בתחילת התהליך. זה יכול להיות תהליך מתסכל לעיתים, אבל זה גם מה שהופך אותו למעניין יותר.

אפשר לדמות את ההבדלים בין פיתוח רגיל לתהליך מחקרי, להבדל בין בנייה של בית לבין חיפוש מאגר נפט. **קבלן** הבונה בית עובד לפי לוח זמנים מסודר, והוא רואה את ההתקדמות שלו בכל יום. **מחפש הנפט** יכול לסרוק את הים במשך חודשים ושנים ללא תוצאות, אבל כאשר הוא מגלה משהו – זה חתיכת הישג!

זכרו תמיד – בתהליך מחקרי, העובדה **שעוד לא** הגענו לתוצאות לא אומרת שלא **התקדמנו**...

חלק ב' – עקרונות העבודה שלנו

עבודה לפי נק' כניסה

כדי לוודא שאנחנו ממפים את כל הסיכונים על המערכת, נסרוק את המערכת לפי מיפוי של נק' הכניסה השונות למערכת.

או במילים אחרות, נתעניין בכל מקום שבו המשתמש יכול להכניס קלט כלשהו למערכת.

כמו במשפט הידוע, מערכת היא תמיד מאובטחת כמו החוליה חלשה ביותר שלה.

תיעוד!

כמו מחפש הנפט, לא נרצה לסרוק פעמיים את אותו אזור באוקיאנוס. לכך חלק חשוב מאוד בעבודה שלנו הוא תיעוד של כל פעולה שאנחנו עושים. כך נדע שאנחנו כל הזמן מתקדמות ולא חוזרות על אותן פעולות.

חלק ג' – צורת העבודה שלנו

עבור כל נק' כניסה, נעבוד תמיד **בתהליך מעגלי** אשר נראה כך:

1. **תיעוד פרטי הבקשה** – נלמד איך הבקשה עובדת ונתעד את הפרטים במסמך שלנו.
2. **כתיבת תרחישים לא רגילים ובדיקתם –** נחשוב על כמה שיותר תרחישי תוקף ונכתוב אותם.
3. **בדיקת התרחישים בפועל –** נבדוק אילו מן התרחישים שכתבנו עובדים ואילו לא. זה השלב בו אנחנו ממש מנסים למצוא חולשות.
4. **תיעוד חולשה שנמצאה -** אם מצאנו חולשה, נתעד אותה היטב במסמך.

כשנסיים תהליך אחד, נעבור לנק' הכניסה הבאה וכך שוב ושוב.

חלק ד' - דוגמא חיה

דוגמא לצורת העבודה שלנו – בסרטון הבא.

חלק ה' – יאללה מתחילות!

המשימה שלנו

משימתנו היא להוות צוות ה-Pen Testers של אפליקציית גליטר, ולמצוא כמה שיותר חולשות. בשלב א' עלינו למצוא **לפחות 5 חולשות** מנק' כניסה שונות.

בסיום התהליך, יש להגיש את מסמך האבטחה הכולל תיעוד מלא של כל הפעולות שביצענו והחולשות שמצאנו.

אילו חולשות יש לחפש?

ניתן לחפש אילו חולשות שרוצות, בכל מקום במערכת!

שימו לב שאתן מוצאות חולשות ב-5 מהמנגונים הבאים לפחות:

- הוספת גליט לקיר שלי
- הוספת גליט לקיר של משתמש אחר
- הוספת תגובה לגליט
- הוספת וביטול לייק
- שינוי פרטי משתמש
- בקשת ואישור חברות
- חיפוש
- קבלת רשימת הבקשות לחברות שנשלחו אלי

שימו לב שהחיפוש לא מוגבל למנגנונים האלה ואפשר לחקור כל נק' כניסה שתמצאו!

מצאתי משהו מוזר, איך אני יודעת אם זו חולשה ממש?

דברים שיכולים להיחשב כחולשה:

- **התנהגות שאי אפשר להגיע אליה** כאשר משתמשים בתוכנת הלקוח
- **פרצת פרטיות** (גילוי מידע שמשתמש רגיל לא אמור לגלות)
- ביצוע פעולה **שלא אמורות להיות הרשאות** עבורה
- **ביצוע זיוף או התחזות** למישהו אחר
- מצב בו השרת **מחזיר מידע** שהוא לא אמור לתת

גבולות גזרה (או: מה אסור לעשות במסגרת הפרוייקט)

- **DoS מחוץ לתרגיל!** אנחנו לא מתעניינות בהפלת השרת או בבדיקות עומסים.
- **אין להריץ לולאות על השרת!** אין להשתמש בלולאות של מנייה כדי להוציא מידע מהשרת או לבצע פעולה מספר גדול של פעמים (זכרו, הפנטסטרית לא מתעניינת במידע או בניצול, אלא רק בלהוכיח את קיומה של החולשה).
- **כל אחת עובדת בעולם משלה -** ביכולתכן ליצור כמה משתמשים שתרצו. את כל הבדיקות שלכן תבצעו אך ורק על **המשתמשים שלכן**. אין לגעת במשתמשים של חניכות אחרות!

* כמשנה זהירות, בעת ההרשמה אין לבחור סיסמא אמיתית שאתן משתמשות בה בשגרה.

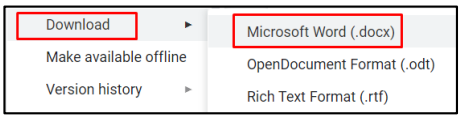
פרטים טכניים!

הורדת אפליקצייה גליטר

(יש ללחוץ על כפתור ההורדה ולאחר מכן לבצע Extract לכל הקבצים בזיפ, בעזרת תוכנה כמו 7zip או Winrar).

הורדת מסמך האבטחה שיש למלא

(מומלץ להוריד את הקובץ בפורמט docx ולעבוד בתוכנת Word. בעזרת File->Download)



בהצלחה!!!