פרוייקט Glitter – שלב ב'

השנה היא עדיין 2025, כ-3 חודשים אחרי ההשקה החגיגית של אפליקציית גליטר. בזכות המאמצים של חוליית הפנטסטריות של גליטר (אלה אתן!), האפליקציה הושקה בתאריך המתוכנן, ועשרות אלפי תלמידים כבר נרשמו לרשת החברתית החדשה של משרד החינוך. התגובות מארגוני ההורים והתקשורת שיבחו את העבודה היסודית שנעשתה על האפליקציה, וגליטר אפילו השיקה אתר אינטרנט בנוסף לאפליקציה. הכל היה מושלם.

זאת אומרת, הכל **היה** מושלם עד חודש אוקטובר 2025, בו פרסם האקר אלמוני המכונה StudentZER0 כי הוא מצא חולשה קריטית באפליקציית גליטר המאפשרת לו לפרוץ לחשבונות של משתמשים אחרים. העיתונים ומהדורות החדשות לא חיכו הרבה והכותרות זעקו – "ציון 0 באבטחה לגליטר", "שרת החינוך קיבלה נכשל בסייבר", "חולשה קריטית מסכנת את ילדי ישראל" ועוד ועוד.

עוד באותו הלילה קראה שרת החינוך לעוזרה האישי לפגישה דחופה. "**אני לא מבינה, הרי נעזרנו בצוות Pen Testers והן הגישו דו"ח שמפרט את כל החולשות, אז איך הגענו למצב הזה?"** -"תראי, השרה, אי אפשר להיות בטוח במא... **"פתרנו את כל החולשות או לא?!"** -"הבעיה היא שאין כזה דבר *כל* החולשות..." - **"אני לא רוצה לשמוע את זה! תראה, זה מאוד פשוט. אם אתה לא תפתור את זה, אני אמצא עוזר אישי חדש שיכול לפתור את זה. יש לך שבוע בדיוק".**

חלק א' - קצת רקע

אז למה העוזר אמר שאין דבר כזה 'כל החולשות'?

אחת הבעיות של עולם האבטחה ושל מוצר כמו גליטר, הוא שצוות של Pen Testers, מוכשר ככל שיהיה, לא יכול לאתר את **כל החולשות שקיימות**. מחקר חולשות הוא תהליך מורכב, שדורש יצירתיות ומחשבה מחוץ לקופסא. חברת אבטחה יכולה לעשות עבודה מצוינת, אך עדיין אדם מוכשר מאוד אי שם בעולם עשוי למצוא חולשה שאף אחד אחר לא חשב עליה.

אז איך מתמודדים עם מה שלא יודעים?

עבור חברות כמו גליטר, פרסום חולשה או גניבת מידע יכולות להוות נזק של עשרות מיליוני דולרים ואף לגרום לירידת המניה ולפגיעה אנושה בחברה. לכן חברות חייבות לחשוב כיצד הן מגדילות את הסיכוי שלהן למצוא את החולשות הנסתרות **לפני** שהאקרים / עבריינים / חברות מתחרות / גורמי בטחון מוצאים אותן.

כדי להתמודד עם האיום הזה, התפתחה גישה חדשה בעולם אבטחת המידע בשנים האחרונות, הנקראת **Bug Bounty.**

במסגרת תכניות **Bug Bounty** (פרס = Bounty) מציעה חברה פרסים כספיים לכל מי שיוכיח שמצא חולשה בשירותים שלה. התכניות גורמות לכך שבמקום שמחקר האבטחה של התוכנה ייערך על ידי צוות מצומצם, הוא בפועל נערך על ידי אלפי אנשים בכל העולם, ורובם עושים זאת ללא קבלת תשלום!

בנוסף, תכניות Bug Bounty יוצרת להאקרים נתיב תעסוקה חדש - חוקי, מוסרי ומתגמל, שמהווה אלטרנטיבה אל מול פנייה לכיוונים לא חוקיים.

מה מרוויחים אנשים שמוצאים ומדווחים על חולשות?

תכניות Bug Bounty נותנות תמריצים רבים להאקרים לפעול בדרך חוקית ומוסרית.

בעבר, האקר שהיה מוצא חולשה לא היה יכול לדווח עליה (זה היה חושף אותו לתביעה), ולכן היו לו יותר תמריצים לפנות לכיוונים לא חוקיים – לנצל את החולשה בעצמו או למכור אותה לגורמים עבריינים.

כיום, בעזרת תכניות Bug Bounty, האקרים וחוקרי אבטחת מידע יכולים להנות מכל העולמות – הם פועלים בצורה חוקית, ולעיתים גם מקבלים תגמול כספי על החולשה שמצאו. בנוסף, הם יכולים לפרסם את ההישגים שלהם ולזכות בכבוד והערכה, ואפילו להעשיר את "תיק העבודות" שלהם שיעזור להם להשיג עבודות בתחום הסייבר בעתיד.

ומה מרוויחה האנושות מתכניות אלה?

תכניות ה-Bug Bounty מייצרות את מה שנהוג לכנות **"המערכת החיסונית של האינטרנט"**, מושג אותו טבעה חוקרת הסייבר הישראלית קרן אלעזרי. לפי אלעזרי, תכניות באג באונטי הן קצת כמו חיידקים טובים בגוף אשר עוזרים לנו להילחם במחלות. ככל שיש יותר חיידקים טובים כאלה, האינטרנט הוא מקום בטוח יותר מפני גורמים רעים ועבריינים. "תוכניות הבאונטי מאפשרות להאקרים לצאת מהמחשכים. הן משתמשות בשכלם של עשרות אלפי האקרים שרוצים להיות חלק מהמערכת החיסונית, חלק מהפתרון", סיכמה אלעזרי בראיון לעיתון דה מארקר.

כמה סייגים חשובים לגבי עולם ה-Bug Bounty

- לא כל החברות מציעות תכנית כזאת. אם חברה לא מציעה תכנית Bug Bounty, ביצוע מחקר חולשות מולה הוא **אינו חוקי.**
- לכל תכנית יש תנאים משלה. התנאים שחוזרים לרוב:
  - המחקר חייב להתבצע על משתמשים שנוצרו לצורך המחקר ולא מול משתמשים אמיתיים.
  - אין להתמקד בהצפה או מניעה של השירות (DoS).

חשוב מאוד לקרוא את כל התנאים לפני שמשתתפים, אחרת תהיו חשופים להליך פלילי.

חלק ב' – תכנית ה-Bounty של גליטר!

בעקבות המחקר שביצע עוזרה האישי של השרה, הוחלט במשרד החינוך לפרסם תכנית Bug Bounty הפתוחה לקהל הרחב. גליטר פירסמה 5 אתגרים, והיא מציעה לכל מי שיוכיח שמצא חולשה הקשורה לאחד האתגרים את התגמול הבא –

- פרסום מאמר תודה והכרה בקהילת הסייבר.
- העסקה כעובד קבוע בצוות האבטחה של גליטר.
- פגישה אישית ותעודת הוקרה משרת החינוך.

חמשת האתגרים שפרסמה גליטר:

- **אתגר הלוגאין –** חולשות הקשורות למנגנון הלוגאין של האפליקציה.
- **אתגר הסמא –** חולשות המאפשרות השגת סמא של משתמשים (שימו לב, זה אתגר שאינו קשור לאתגר הלוגאין).
- **אתגר העוגיה –** חולשות הקשורות להשגת עוגייה של משתמש אחר.
- **אתגר הפרטיות –** חולשות הקשורות להשגת מידע על **פעולות** פרטיות שביצעו משתמשים אחרים (כאלה שלא אמורות להיות חשופות).
- **אתגר XSRF –** חולשות הקשורות להשמשת XSRF (בעזרת XSS, בדומה לפעילות פיצה סייבר שעברתן ואפשר להיעזר בחומריה).

את כל האתגרים אפשר לנסות ולפתור באפליקציית גליטר, ובנוסף גם באתר החדש של גליטר בכתובת http://cyber.glitter.org.il.

Glitter

מה ההבדל בין המחקר בשלב א' למחקר בשלב ב'?

בשלב א' למדנו למצוא חולשות אשר חקרנו לפי הבקשה (נק' כניסה). כל החולשות של שלב א' בנויות על מחקר ספציפי של בקשה ואינן דורשות שילוב של מספר תהליכים או מחקר ארוך מאוד. ברגע שניסינו תרחיש והוא הצליח – מצאנו את החולשה.

בשלב ב' אנו עובדים על 5 האתגרים אשר החברה פתחה לציבור הרחב במסגרת תכנית ה-Bug Bounty. אתגרים אלו מורכבים יותר ודורשים מאיתנו מחקר של תהליכים באתר (או במילים אחרות, לא נמצא אותן על ידי שינוי של פרמטר וזהו). המחקר סביב כל חולשה יקח זמן ארוך יותר.

* בשלב ב' יש לעבוד גם מול האפליקציה וגם מול האתר של גליטר (חשוב מאוד לחקור את שניהם).

המשימה שלנו

בשלב ב' של הפרוייקט, עליכן להשתתף באתגר ה-Bounty הפתוח לקהל הרחב. עליכן לפתור **לפחות שלושה מהאתגרים**. בסיום התהליך, יש לכתוב ולהגיש את **כלי האולר -** סקריפט פייתון אשר מציג מגוון חולשות שמצאתן במערכת גליטר.

חלק ג' – הוראות לכלי האולר

מטרתו של כלי האולר היא להדגים את היכולות שנרכשו במהלך מחקר האבטחה כולו. על האולר להציג הוכחת פעולה של החולשות שמצאתן. החולשות שיש להדגים באולר:

- כל החולשות שמצאתן הקשורות לאתגרי ה-Bug Bounty בשלב ב'.
- בנוסף, לפחות 2 מהחולשות שמצאתן בשלב א'.

כעת נפרט על הדרישות הכלליות מכלי האולר.

חווית משתמש

האולר צריך להיות נוח לשימוש לאדם שאינו מתמצא בקוד, כך שיוכל להוות הדגמה חיה לעובדי גליטר. בעת הכניסה לתוכנה, יתבקש המשתמש לבצע לוגאין עם שם וסמא (יתקבלו בקלט ולא בקבועים).

לאחר מכן יוצג למשתמש תפריט של מגוון החולשות האפשריות. במידת הצורך, בכל חולשה יתבצע קלט נוסף, אך נסו שהקלט יהיה כמה שיותר ידידותי ולא ידרוש ידע נוסף. למשל, אם החולשה שלכם קשורה לפוסט מסוים, הדרך הפשוטה תהיה לבקש את ה-ID שלו מהמשתמש. אבל מכיוון שמשתמש ממוצע לא מכיר ID, ניתן להציג לו את רשימת הגליטים הקיימים עם המזהים שלהם, מה שיקל עליו את הבחירה. או, כדוגמא נוספת, אם החולשה קשורה למשתמש אחר, נסו לבקש את השם המוצג שלו ולא את ה-ID שלו.

ככל שהאולר יהיה יותר ידידותי למשתמש תרוויחו נק' נוספות.

Glitter

מבנה כללי

על הפרוייקט לכלול קובץ main בשם swissknife.py וספרייה (מודול) בשם glitter. הספריה תרכז את כל הפונקציונליות שקשורה ל-glitter (מעין API, ממשק גישה לפרוטוקול של גליטר), ולא תתעסק בתקשורת עם המשתמש או בתצוגה למסך. הקובץ הראשי שלכם ייבא את הספריה, וישתמש בפונקציות שלה כדי לבצע את כל הפעולות הנדרשות.

שימו לב שרצוי לשמור על חיבור קבוע עם השרת (במידת האפשר) ולא לבצע התחברות בכל פעם מחדש. כדי לשתף משתנים או סוקטים בין פונקציות בספריה, תוכלו להשתמש במשתנים גלובלים (global).

דגשים

- ההפרדה בין הקובץ swissknife לספרייה glitter היא חשובה. אם לא ברור לכן לגמרי מה צריך להיות בכל קובץ, התייעצו איתנו!
- נסו כמה שיותר להשתמש בפונקציות עזר, שישמשו אתכם בכמה מקומות בקוד.
- הימנעו ~~**ככל האפשר**~~ **לחלוטין** משכפול קוד!
- זכרו לתעד הכל כפי שלמדנו.
- בדקו שהאולר עובד אל מול גליטר – כל מימוש חולשה צריך להופיע באפליקציה או באתר.
- ככל שנכניס הדגמה של יותר חולשות לאולר – זה טוב יותר!

דוגמא לפלט אולר (החולשות לא בהכרח אמיתיות.. ☺) :

(הפלט לא מחייב מילה במילה אבל שמרו על המבנה הזה בגדול)

```
D:\>python swissknife.py

Welcome to Glitter Swissknife!
Please enter username:  new_user
Please enter password:  12345678

Logging in...
Logged in!

MAIN MENU:
1. Make many likes to a glit
2. Get user's password
3. Add glit in the name of someone
Please choose:  1


Glits from new_user:
1. "Hey everyone!!!!" (12/12/2019)
2. "Glitter is cool man!"  (10/12/2019)
Please choose: 1

3 Likes added to glit.

MAIN MENU:

.......
```

חלק ד' – יאללה מתחילות!

פרטים טכניים

כתובת אתר גליטר:

http://cyber.glitter.org.il

בהצלחה!