דוח סיכום פרויקט

|  |  |
| --- | --- |
| אם הגעת לכאן, כנראה שסיימת פרויקט - **כל הכבוד לך!**  סיום של פרויקט הוא רגע כיף שבדרך כלל מלווה בתחושת הצלחה אדירה. זוהי נקודת ציון חשובה בהתקדמות שלך השנה, אבל מה שעוד יותר חשוב הוא התהליך שעברת עד שהגעת כאן.  זוכרת? התחלת פרויקט, ניסית לחשוב על פתרונות - חלק עבדו, חלק פחות, חקרת ולמדת עוד נושאים ועוד ועוד...עד שהצלחת.  עכשיו, הגיע הזמן להתבונן לאחור ולסכם את התהליך שעברת, להעלות תובנות ולהפיק לקחים.  לפניך שני חלקים של הדו"ח: הראשון מסכם את החלק הטכנולוגי של הפרויקט והפתרון של המחקר והשני הוא על התהליך והחוויה האישית שלך במהלך ובסיום הפרויקט. עני על שני החלקים ובסיום הגישי את הקובץ ב-Moodle. | |
| שם החוקרת | נעמה ביטון |
| שם הפרויקט | glitter |



# חלק א' - סיכום טכנולוגי

בחלק זה עליך לפרט את השלבים השונים מתחילת הפרויקט ועד סופו אשר הובילו אותך לפתרון. בכל שלב יש להציג:

* על איזו שאלה רצית לענות (למשל: איזה סוג של קובץ קיבלתי?)
* מה התשובה לשאלה
* מה עשית מבחינה טכנולוגית שהובילה אותך לתשובה (אין צורך לציין ניסיונות שלא הובילו לתשובה הסופית אלא רק כאלה שכן עזרו). בחלק זה אפשר לשים צילומי מסך מכלים שהשתמש בהם, להוסיף סקריפטים שכתבת, לספר מה היית צריכה ללמוד או כל דבר אחר שיסביר מה עשית.

טיפ: אחד הדברים שיעזרו לך למלא סעיף זה הוא העמודה של 'ממצאים, גילויי ומסקנות' מתוך ה-subtask.

|  |
| --- |
| חלק א':  המשימה הייתה למצוא לפחות חמש חולשות.  בחלק א' של הפרויקט ניסיתי למצוא חולשות שהן ממש ויזואליות בתוך האפליקציה ז"א שכבר מההסנפה או אפילו כבר מתוך האפליקציה/אתר ראו אותן.  אז מצאתי את החולשות הבאות:   * הוספת יותר מלייק אחד לגליט * רואים את ה ID של המשתמש בהסנפה * בחיפוש אפשר לראות פרטים אישיים של משתמשים אחרים כמו ID או כתובות מייל * אפשר לראות שיחות של משתמש אחד עם אחר כאשר נכנסים לו לעמוד(השיחות לא פרטיות) * אפשר להתחזות למשתמש (ליצור משתמש שזהה אחד לאחד)   חלק ב'+ג':  בחלק ב' המטרה הייתה למצוא חולשות עמוקות יותר- שאפשר להתעמק בהם יותר לפי האתגרים שניתנו בחלק ב'.  בחלק ג' המטרה הייתה לממש את החולשות האלה ולבנות אולר.  אני בחרתי באתגר הcookie, באתגר ה login ובאתר xsrf  אתגר Login באתגר הזה הייתי צריכה להתחבר למשתמש מבלי שתהיה לי את הסיסמה שלו.  דבר ראשון שעשיתי זה הסנפתי את תהליך ההתחברות של שחקן, ומשם ראיתי שיש ascii checksum בהודעת ההתחברות, אז ניסיתי להבין ממה מורכב ה checksum הזה ובסוף הגעתי לכך שהוא מורכב מחיבור של השם משתמש והסיסמה בהמרת האותיות לקודי ascii.  ואז בעצם אם יש לי את השם משתמש של שחקן, אני יכולה לשלוח לגליטר הודעה התחברות שגויה, לקבל את הchecksum הדרוש על מנת להשלים את פעולת ההתחברות וממנו להחסיר את שם המשתמש, כך לקבל את הסכום של קודי האסקי של תווי הסיסמה ומהם ליצור קומבינציה שתעלה על הדרישות – וזה בעצם גם האלגוריתם שמיממשתי על מנת לקבל את סיסמת המשתמש, ואת הסיסמה והשם משתמש שלחתי בסוקט וכך התחברתי למשתמש מבלי שתהיה לי הסיסמה שלו.  אתגר xsrf:  באתגר הזה הייתי צריכה לבצע שליחה של משהו מאחורי הקלעים כך שבפועל למשתמש הוא ייראה רגיל – אני שלחתי לינק שהשם שלו על פניו נראה רגיל והלינק זדוני כביכול.  אז דבר ראשון שעשיתי זה נכנסתי לאתגר של הפיצה שעשינו בשנה שעברה משום שהפנו אותנו לשם בקובץ של הסעיף ומשם הבנתי שההודעה שצריכה להישלח כפורמט של קישור html  אז בניתי מבנה של הודעה של html ושלחתי אותו כבקשה להעלאת גליט אצל המשתמש.  אתגר cookie:  באתגר הזה ביצעתי פעולות דרך האתר בלבד, וניסיתי להשיג עוגייה של משתמש אחר.  הסנפתי כמה דברים עד שהגעתי לכך ששליחת בקשת חברות לשחקן בהסנפה תראה לי את העוגייה של אותו שחקן ששלחתי לו בקשת חברות ומשם חילצתי את העוגייה של המשתמש. |

# חלק ב' - סיכום אישי

בחלק זה בחרי 2-3 שאלות, ועני עליהן בעמודה השמאלית.

|  |  |
| --- | --- |
| אילו מיומנויות חדשות רכשת בתהליך המחקר? (לדוגמה: חיזוק הלמידה העצמית או בפן המקצועי שימוש בתוכנה שלא הכרת) | הרחבתי את הידע שלי על cookies |
|  |  |
| ספרי על קושי שבו נתקלת במהלך הפרויקט.  מה הדרך שבה נקטת כדי להתמודד עם הקושי? | לא היה לי כל כך ידע בעוגיות ולכן היה לי קושי באתגר הזה הכי הרבה, אז קראתי בגוגל |
|  |  |
| שתפי ברגע של הצלחה במהלך פרויקט! | כל אתגר שהצלחתי לממש דרך פייתון הרגיש כמו הצלחה |
|  |  |
| מה למדת על עצמך במהלך הפרויקט? מה היית רוצה לשפר? מה היית רוצה לשמר? |  |
|  |  |
| שתפי ברעיון מקורי/יצירתי/מגניב שהיה לך במהלך הפרויקט (גם אם הוא לא צלח בסוף…) |  |