**<ADP – ATTACK DEFENCE PROGRAM>**

מסמך אפיון

<תומר פרץ>

<V1>

<11.12.17>

**היסטוריית גרסאות המסמך**

|  |  |  |
| --- | --- | --- |
| **תאריך** | גרסה | **תקציר השינויים** |
| 11.12.17 | V1 | גרסא ראשונית |
|  |  |  |
|  |  |  |
|  |  |  |



**1. הקדמה**

1.1 מטרה

*מה המטרה של המסמך ומי קהל היעד שלו*

1.2 המוצר

* *שם המוצר: ATTACK DEFENCE PROGRAM*
* *המוצר לוקח אתר וסורק אותו למציאת פרצות אבטחה מסוגים שונים ברמה שונה בכל התקפה והתקפה.*
* *המטרה של המוצר היא לאפשר למשתמש לסרוק אתר כלשהו(שיש אישור לסרוק אותו), ולמצוא פרצות אבטחה שונות. לתכנה יהיה לפחות 5 סוגים שונים של פרצות אבטחה ולפחות תהיה מסוגלת למצוא פרצה ברמה הבסיסית. היתרונות של המוצר יהיו שהוא קל לשימוש והבנה שיהיה לו הסבר קצר על כל התקפה ושהוא יוכל למצוא כל פרצת אבטחה ברמה הבסיסית.*

1.3 הגדרות

*בחלק זה יש לציין את כל ההגדרות, המושגים וראשי התיבות בהם תשתמשו בהמשך המסמך.*

**1.4** תקציר

*הסבר מה מופיע בהמשך המסמך ופירוט כיצד זה מסודר לאורך המסמך*

1. תיאור כללי

2.1 פונקציונליות

התכנה תאפשר למשתמש להכניס כל סוג קישור כלשהו של אתר(עם WWW או HTTP בהתחלה ובלי כמובן).

* התכנה תראה למשתמש כל שלב בסריקה של האתר ואת הפרצה שהיא סורקת כעת.
* כאשר תהיה שגיאה בתכנית היא תפלוט את גורמי השגיאה לתוך קובץ ומתי זה קרה ובנוסף לזה היא תציג למשתמש הודעה שקרתה שגיאה ואת סוג השגיאה(לכל שגיאה תהיה מספר).
* לתכנה תהיה לפחות חמישה סוגים שונים של התקפות(הכי נפוצות), ותמצא את כל הפרצות הכי בסיסיות שיש.
* המשתמש יוכל לבחור אם לרשום את הפלט של הסריקה של האתר לתוך קובץ וורד(בהתחלה של הסריקה תהיה לו אפשרות אם אוטומטית לשים את הפלט של הסריקה בקובץ וורד).
* הממשק משתמש יהיה פשוט מאוד ויאפשר שימוש קל וברור של התכנה.

2.2 קהל היעד

* **קהל היעד של התכנית הוא בעלי אתרים שרוצים לסרוק את האתר שלהם ולבדוק פרצות אבטחה שיכולות לסכן באופן חמור את לקוחות האתר.**

2.3 אילוצים עיקריים

* התכנה תצטרך חיבור רציף לאינטרנט ותרוץ על כל סוג של מערכת הפעלה(Liunux/windows).

2.4 הנחות ותלויות

* בכל מערכת הפעלה קיימות חיבור לאינטרנט ושימוש בכל מיני סוגים של פרוטוקולים.
* *בכל מערכת הפעלה עשוי ממשק המשתמש להיראות שונה ש כיוון שאנו משתמשים במקרים רבים באפשרויות ברירת המחדל של המערכת.*

**2.5** סיקור מצב השוק כיום (אופציונלי)

* בשוק קיימות ספר אופציות אבל כולם דורשות תשלום רב על כל סריקה של אתר ומגבילה את המשתמש לכמות האתרים שהוא יכול לסרוק.

1. דרישות מפורטות

3.1 דרישות פונקציונליות

* התכנה תאפשר לסרוק אתר למציאת הפרצות הבאות לפחות.
  + Sql Injection
  + Xss
  + Blind SQL Injection
  + Man-in-the-middle attack
  + Brute force attack
* *תהיה אפשרות לסרוק כמה אתרים במקביל.*
* *התכנית תמצא כל פרצה ברמה בסיסית של כל התקפה.*
* *התכנית תוכל לשלוח אימייל עם פרטי הסריקה.*
* *התכנית תוכל להציג הגנה חלקית על ההתקפה.*
* *התכנית תוכל להראות הסבר קטן על כל התקפה ועל רמת הסיכון שלה.*
* *תהיה בדיקה תקינה של קלט.*
* *התכנית תאפשר ללקוח לפלוט לתוך קובץ את כל פרטי הסריקה.*
* *לכל שגיאה יהיה מספר ייחודי כדי שיהיה אפשר לתת מענה על כל סוג שגיאה.*
* *התכנית תציג הודעה כאשר יש שגיאה.*

3.2 דרישות של ממשקים חיצוניים

* *הממשק משתמש יהיה פשוט וברור לשימוש.*
* *הממשק משתמש יציג את כל תהליך הסריקה.*

3.3 דרישות לא פונקציונליות

* *התכנית תעמוד בקצב גבוה של סריקה וכמה סריקות במקביל.*
* *כאשר בתכנית תיווצר שגיאה היא לא תקרוס והיא תוכל לטפל בה באופן שהיא לא תקרוס ותאבד נתונים.*
* *התכנה תהיה זמינה כל הזמן.*
* *התכנה לא תגלה לעולם החיצון את פרטי הסריקה לצורך שמירה על פרטיות.*
* *לתכנה תהיה מערכת של עדכון אוטומטי של התכנה.*
* *יהיה אפשר להעביר את התכנית ממחשב למחשב בלי תלות בסוג המחשב.*

3.4 דרישות בסיס נתונים

* *התכנית תשמור בקובץ טקסט או וורד(לבחירת המשתמש), את פרטי הסריקה.*