מסמך פרויקט PT - תשע"ח

צוות: יונתן גבאי ומני קייזר

כיתה: אשדוד 6

מדריך: יעקב ויינרובסקי

מנטור:

הסבר כללי על המסמך

מסמך שילווה אתכם לשבועות הקרובים וגם בהמשך השנה.

אין ליצור עותקים של המסמך, ויש להשאירו בפורמט של גוגל-דוק! כל דרך אחרת עלולה ליצור בעיות למדריך או למנטור שלכם אשר עוקב אחר ההתקדמות בעבודה במסמך ובכלל. בזכות העבודה דרך גוגל-דוקס, יש גיבוי אוטומטי, סנכרון תוכן המסמך בין כל המשתתפים בו, ומעקב גרסאות.

בכל פעם שמשתנה או מתווסף תוכן מסוים למסמך, יש לציין זאת בתמציתיות בטבלת המעקב.

# **טבלת מעקב/עדכון גרסאות**

|  |  |  |  |
| --- | --- | --- | --- |
| תאריך | מבצע/ת העדכון | תוכן/מהות העדכון | הסעיפים שעודכנו |
| תאריך של היום | איך קוראים לך? | התחלת עבודה על מסמך ייזום | תיאור כללי, מטרת הפרוייקט... |
|  |  |  |  |
|  |  |  |  |

פרק 1: ייזום

# **מסמך שמטרתו סקירה כללי של הפרוייקט.**

יש למלא את המסמך עד למפגש הכיתתי הראשון. במפגש זה כל צוות יציג בקצרה את הפרוייקט שלו.

# **תיאור כללי**

כלי מבוסס web שמטרתו לעזור לבעלי אתרים לגלות חולשות אבטחת באתר ומציע פתרונות חסימת החורים.

# **מטרת הפרויקט**

נועד למענה נוח ונגיש לבעלי אתרים לפתירת בעיות אבטחה באתר..

# **סוגי משתמשים / קהל היעד של היישום**

בעלי אתרים.

# **פיצ'רים ותהליכים עיקריים**

* סריקה של חולשות אבטחה באותו אתר.
* הצעת פתרונות לבעיות האבטחה שנמצאו.

# 

# **טכנולוגיות עיקריות ושיקולים עיקריים**

לימודי ספריות של פייתון, ממשק על המחשב (לא וובי), אתר לגישה נוחה.

# **ידע, סיכונים ושאלות**

שיהיה קשה מידי, צריך לחקור המון בנושאים שאנחנו לא שולטים בהם, פיתוח מורכב

# **פתרונות קיימים**

Nessus

מסמך אפיון

# פיצ'רים ותהליכים עיקריים - הרחבה

* סריקה של חולשות אבטחה באתר - סריקה של כמה בעיות אבטחה (נקווה שנספיק כמה שיותר…) דוגמאות:
  + הזרקת SQL (באנגלית: SQL Injection) היא שיטה לניצול פרצת אבטחה בתוכנית מחשב בעזרת פניה אל מסד הנתונים. השם נובע מכך שהמשתמש מכניס קוד SQL לשדה קלט אליו אמורים היו להיכנס נתונים תמימים. באופן זה יכול משתמש זדוני לחרוג לחלוטין מן התבנית המקורית של השאילתה, ולגרום לה לבצע פעולה שונה מזו שיועדה לה במקור.
  + סריקת פורטים (port scan) - תהליך שבו מחשב מנסה ליזום חיבור עם כל פורט ופורט שבמחשב כלשהו, ולפי התגובה (או חוסר התגובה) מכל פורט, מסיק אילו פורטים פעילים כרגע ואילו לא.
  + מתקפת DoS - מתקפה שבה התוקף "מציף" (שולח כמות אדירה של פקטות) את השרת, עד שהשרת לא יוכל לעמוד בעומס שמשרה עליו התוקף, ויקרוס.
  + מתקפת DDoS - מתקפה שבה כמות אדירה של כתובות IP "מציפות" (שולחות כמות אדירה של פקטות) את השרת, כך שהשרת לא יוכל לעמוד בעומס שמשרים עליו התוקפים, ויקרוס.
  + פריצות XSS (אופציונאלי אם ישר זמן) - ניצול של פריצות אלו מאפשר הזרקת קוד זדוני אל אתר אינטרנט על ידי משתמש. כאשר משתמש תמים נכנס לאתר האינטרנט הפרוץ, מחשבו של המשתמש התמים מתייחס לקוד הזדוני כאל קוד לגיטימי של האתר הפרוץ, ומריץ את הקוד הזה. מכיוון שהקוד הזדוני נחשב לקוד לגיטימי של האתר הפרוץ, הוא יכול לקבל כל מידע הרלוונטי לאתר זה, כגון הרשאות כניסה של המשתמש לאתר. במקרים קיצוניים, למשל כאשר האתר נמצא ברשימת האתרים שהמשתמש התמים סומך עליהם, ניתן גם לנצל את הפרצה להרצת קוד זדוני בהרשאות של המשתמש עצמו.
* הצעת פתרונות לבעיות האבטחה שנמצאו - בהתחלה נפנה את הלקוח לקריאה על בעיית האבטחה, ובשלב מתקדם יותר ניתן מענה יותר יעיל ללקוח

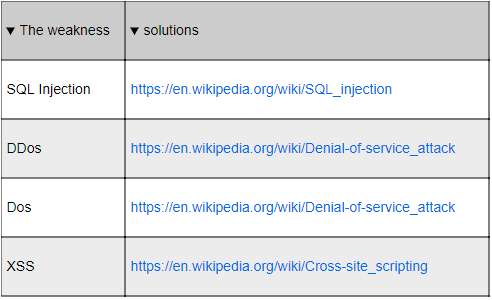
# 

# 

# מסכים והמחשה ויזואלית

הממשק הוא אתר web שמקבל מהמשתמש את המידע הרלוונטי - כתובת אתר - ושולח אותו לשרת שעורך בדיקות על אותו אתר.

כך נראה ויזואלית המסך הראשי באתר.



# דרישות שאינן פונקציונליות

תקשורת מאובטחת (כי אפשר)

חיבור אינטרנט (יציב)