**תכנות מערכות דפנסיבי** פרויקט

דולב חגבי 316016757

**חלק א – מחקר חולשות**

|  |  |
| --- | --- |
| **איום** | **התקפת אדם באמצע** |
| **הרכיב המושפע** | העברת הקבצים |
| **פרטי מודול** | - |
| **מחלקת פגיעות** | MITM |
| **תיאור** | דליפה של RSA private keyבעקבות רשלנות הלקוח, יאפשר למאזין עוין לפענח את הAES key |
| **תוצאה** | התוקף יקבל גישה לתוכן כל הקבצים שיעברו בין הלקוח לשרת (בכל פעם יפענח את מפתח הAES , מכוון שהמפתח הפרטי לא משתנה) |
| **דרישות** | * האזנת אדם באמצע לשיחה * גישה למפתח הפרטי של הלקוח |
| **השפעה עסקית** | חומרת הנזק תהיה בהתאם לרגישות הקבצים המוצפנים |
| **הצעות לתיקון** | * יש להחליף את המפתח הפרטי אחת לתקופה * גורם אנושי – על השרת לחדד ללקוח את חשיבות השמירה על המפתח הפרטי. * על הלקוח לצמצם ככל הניתן את כתיבת המפתח הפרטי: כרגע הלקוח רושם את המפתח בשני קבצים – priv.key וme.info יש לשקול לכתוב את המפתח בקובץ אחד בלבד. * יש לשקול לשנות את שם הקובץ priv.key כדי שהקובץ לא יהיה מטרה לתוקף. * יש לשקול להצפין את הקובץ בו רשום המפתח על ידי סיסמה/ העלאה לענן מאובטח. |
| **סיכון** | פוטנציאל נזק, יכולת שחזור, ניצול, השפעה על משתמשים, ויכולת הגילוי  תלוי באופי החברה |

|  |  |
| --- | --- |
| **איום** | **התחזות** |
| **הרכיב המושפע** | התחברות חוזרת |
| **פרטי מודול** | קובץ request.py , פונקציה handle\_requests |
| **מחלקת פגיעות** | MITM |
| **תיאור** | קבלת הID של הלקוח (לדוג' באמצעות האזנה פשוטה של אדם באמצע), תאפשר התחברות של התוקף והתחזות ללקוח בעל אותו הID. |
| **תוצאה** | * המתחזה יוכל להעביר לשרת קבצים בשם הלקוח. * העברה לשרת קבצים זדוניים. |
| **דרישות** | * האזנת אדם באמצע לשיחה * גישה למפתח הפרטי של הלקוח |
| **השפעה עסקית** | חומרת הנזק תהיה בהתאם לרגישות הקבצים (דוגמה לנזק חמור: אם הקבצים הם הוראות בנקאים למערכת הבנק / פקודות קצינים בצבא) |
| **הצעות לתיקון** | * פרוטוקול ההתחברות מחדש בעייתי. יש לאמת את זהות המתחבר. * יש לשקול את סדר הפרוטוקול: ייתכן שכדאי שהלקוח ישלח את שמו ואת המפתח הציבורי שלו בהודעה הראשונה כדי שהשרת ישלח את הID מוצפן. * אם הוחלט שלא לבצע את הסעיף הקודם, ייתכן שכדאי להצפין את הID בשאר ההודעות, כדי שאם הודעה מאוחרת תודלף התוקף לא יוכל לפענח אותה. |
| **סיכון** | פוטנציאל נזק, יכולת שחזור, ניצול, השפעה על משתמשים, ויכולת הגילוי  תלוי באופי החברה |

|  |  |
| --- | --- |
| **איום** | **דריסה של קבצי השרת** |
| **הרכיב המושפע** | תפקוד השרת |
| **פרטי מודול** | קובץ request.py, פונקציה get\_file |
| **מחלקת פגיעות** | - |
| **תיאור** | העברת קבצים בשם קבצי המערכת של השרת יובילו לדריסת קבצי השרת |
| **תוצאה** | אובדן בסיס נתונים / קובץ מספר פורט יובילו לכך שהשרת לא יתפקד כשורה (לדוגמה: יאזין לפורט אחר, ולא תהיה גישה אליו).  כמו כן, ניתן לדרוס קבצי קוד ולהכניס במקומו קוד זדוני שירוץ במקום השרת. |
| **דרישות** | ניחוש שמות הקבצים ומיקומם |
| **השפעה עסקית** | * פגיעה בתפקודו התקין של השרת. * אובדן קוד השרת |
| **הצעות לתיקון** | * (בוצע) הורדת הקבצים לתוך תיקיה נפרדת מקבצי השרת * לפני שמירת קובץ יש לבדוק אם קיים קובץ כזה בתיקיה (ע"י הספריה os), ואם כן לשמור אותו בשם אחר. |
| **סיכון** | פוטנציאל נזק, יכולת שחזור, ניצול, השפעה על משתמשים, ויכולת הגילוי  תלוי באופי החברה |

|  |  |
| --- | --- |
| **איום** | **הזרקת SQL** |
| **הרכיב המושפע** | גישה לבסיס הנתונים |
| **פרטי מודול** | קובץ db.py |
| **מחלקת פגיעות** | SQL Injection |
| **תיאור** | הכנסת קוד SQL בתור ID של לקוח, יאפשר גישה לנתוני כלל הלקוחות |
| **תוצאה** | קבלת המפתחות של הלקוחות תאפשר פיענוח כל ההודעות המועברות ברשת כולל תוכן הקבצים. |
| **דרישות** | - |
| **השפעה עסקית** | * חומרת הנזק תהיה בהתאם לרגישות הקבצים המוצפנים * פגיעה בפרטיות הלקוחות |
| **הצעות לתיקון** | * (בוצע) הגישה לנתוני השרת מתבצעים על ידי מילון המהווה עותק של הנתונים (Clients\_table), ולכן הזרקת פקודות SQL לא רלוונטית. * (בוצע) פונקציות הגישה לנתונים יחזירו משתנה אחד מתוך הנתונים, ולא טבלה הכוללת מספר משתנים |
| **סיכון** | פוטנציאל נזק, יכולת שחזור, ניצול, השפעה על משתמשים, ויכולת הגילוי  תלוי באופי החברה |

|  |  |
| --- | --- |
| **איום** | **התקפת מניעת שירות על השרת** |
| **הרכיב המושפע** | זמינות השרת |
| **פרטי מודול** | קובץ main.py |
| **מחלקת פגיעות** | DDOS |
| **תיאור** | הצפת השרת בבקשות או העברת קבצי זבל גדולים כדי להעמיס על השרת כדי למנוע שירות ללקוחות אחרים. |
| **תוצאה** | המתחזה יוכל להעביר לשרת קבצים בשם הלקוח |
| **דרישות** | * האזנת אדם באמצע לשיחה * גישה למפתח הפרטי של הלקוח |
| **השפעה עסקית** | חומרת הנזק תהיה בהתאם לרגישות הקבצים (דוגמה לנזק חמור: אם הקבצים הם הוראות בנקאים למערכת הבנק / פקודות קצינים בצבא) |
| **הצעות לתיקון** | * פתרונות סטרנדטים עבור DDOS: הקצאת רוחב פס גדול, שימוש בחומות אש ומערכות למניעת חדירה, rate limiting * יש לשקול התחברות של לקוחות מוכרים בלבד (מתוך רשימה, שקיבלו אישור) |
| **סיכון** | פוטנציאל נזק, יכולת שחזור, ניצול, השפעה על משתמשים, ויכולת הגילוי  תלוי באופי החברה |

**חלק ב – דוגמאות הרצה**

1. **יצירת DB, הרשמה, התחברות, ושליחת קובץ תקין**

שרת:

**תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיתמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי**

לקוח:

**תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי**

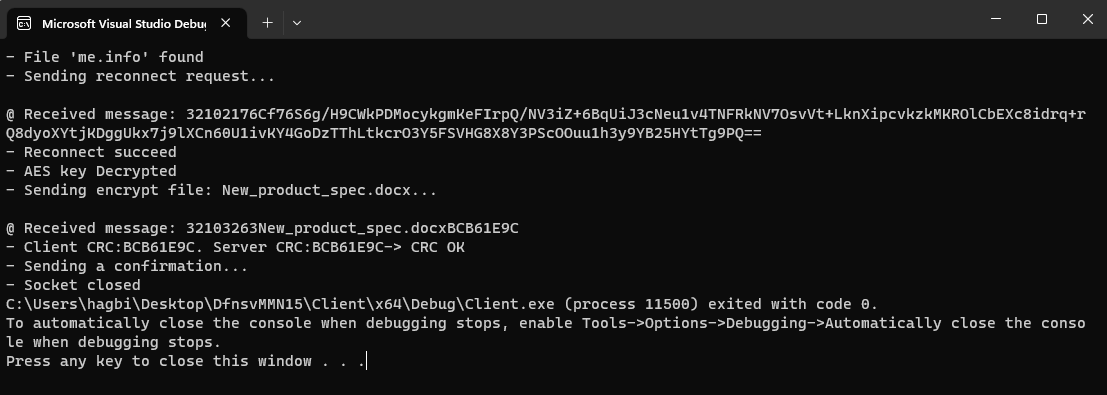
1. **התחברות חוזרת**

שרת:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

לקוח:



1. **חבלה בפונקציית חישוב CRC של השרת (מחזיר אפסים)**

שרת:

**תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי**

לקוח:

**תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי**