**שאלה 2:**

|  |  |
| --- | --- |
| איום | התחזות לאחד מין הצדדים, הלקוח או השרת. |
| רכיב מושפע | פונקציית החלפת המפתחות ופונקציית שליחת הקבצים. |
| סוג הפרצה | אדם בתווך – Man in the middle. |
| תיאור | ניתן לגנוב מידע שמועבר בצורה לא מוצפנת בheader של הבקשות ובכך לשלוח ולהשיג מידע מהשרת. למשל ניתן להשיג מידע על בקשות שנשלחות לשרת ולשנות בהן נתון לא מוצפן ולקבל מידע אחר (כמו למשל שינוי של client id על מנת להתחזות ולקבל מידע על לקוחות אחרים). |
| תוצאה | משתמש זדוני יכול לגשת למידע של לקוחות אחרים, לבצע פעולות בשמם או לחבל להם בקבצים ובפרטי המשתמש. |
| תנאים מקדימים | גישה למידע לא מוצפן ולסוגי בקשות ותשובות מהשרת. |
| השפעה | התחזות ללקוחות אחרים, חבלה בקבצים של לקוחות ובמשתמשים עצמם. התוצאה שרת גיבוי קבצים לא מאובטח, משתמש זדוני יכול למחוק או לשנות קבצים שמשתמש אחר גיבה ובכך לפגוע לו בגיבוי. |
| תיקון מוצע | הצפנה של כלל התעבורה. לדוגמה TLS או SSL. הצפנת כל המידע המועבר בין הלקוח לשרת ולהפך תמנע ממשתמשים זדוניים אפשרות להשיג פרטים על לקוחות אחרים ובכך תמנע את האפשרות שם לחבל להם בקבצים או במשתמש. |

איום נוסף:

|  |  |
| --- | --- |
| איום | ניצול יתר של זיכרון השרת |
| רכיב מושפע | שמירת הקובץ בשרת |
| סוג הפרצה | התקפת מניעת שירות – Dos |
| תיאור | ניתן להעלות לשרת קבצים עד 4 ג'יגה בכל פעם וללא הגבלה בכמות הפעמים או בכמות הזיכרון הכוללת. משתמש זדוני יכול לבצע אינסוף העלאות כאלו ובכך למלא את זיכרון השרת עד אשר אין מקום נוסף לקבצים ובכך לנטרל את פעולת השרת |
| תוצאה | זיכרון השרת יהיה מלא ומשתמשים אחרים לא יוכלו להעלות אליו קבצים לגיבוי. כלומר מניעת שירות, לא יהיה אפשר להעלות קבצים לשרת. |
| תנאים מקדימים | אין מגבלה של כמות העלאות או של זיכרון עבור כל משתמש. |
| השפעה | האטה בפעולות השרת או מניעה של שימוש בו ע"י ניצול כלל הזיכרון. |
| תיקון מוצע | פתרון אפשרי הוא הגבלת כמות העלאות או כמות הזיכרון שכל משתמש רשאי להעלות לשרת, בנוסף הגבלת כמות העלאות והזיכרון בכלל השרת על מנת למנוע ניצול יתר של כמה משתמשים במקביל. |