**שאלה 2: מסמך מחקר**

|  |  |
| --- | --- |
| מסמך מחקר – חולשה בפרוטוקול | |
| איום | עקיפת מנגנוני ההזדהות בפרוטוקול והתחזות ללקוח |
| רכיבים מושפעים | פעולות 1101,1103-1106 בפרוטוקול – החלפת מפתחות, העלאת קובץ, פעולות אימות checksum של קובץ. |
| סוג החולשה | Man in the middle |
| הסבר | במידה וצד שלישי נמצא בתווך התקשורת בין השרת לבין הלקוח, הוא יכול לגנוב בקלות מידע רב שנשלח כ-plaintext – כדוגמת הclient id, אשר נשלח כחלק מה-header של הפרוטוקול בכל בקשה (מלבד Register), ובתגובה של Register. באמצעות מידע זה ניתן להשיג מידע אודות הפעולות שמבצע הלקוח אל מול השרת, ואף להשתמש במידע זה באופן זדוני – לביצוע פעולות שונות מול השרת בשם הלקוח. |
| תוצאה | צד שלישי יכול להזדהות בתור הלקוח בכל אחת מהפעולות לעיל שכוללות הזדהות, ובתוך כך: להעלות קבצים בשם הלקוח (וכך לדרוס קבצים קיימים), לאמת אותם או למחוק אותם בשמו, ולהחליף את מפתחות ההצפנה בצורה שתמנע מהלקוח שימוש בשירות.  מעבר לכך, במידה והצד השלישי מצליח להתחזות לשרת, הוא יוכל לתעל את התעבורה דרכו, לדלות ולהחליף מפתחות הצפנה, שיסייעו לו לפענח את המידע המוצפן בפרוטוקול. |
| דרישות | אפשרות להאזין לתווך התקשורת בין השרת לבין הלקוח (להאזין להודעות בפרוטוקול). |
| השפעה | התחזות ללקוחות שונים, שיבוש פרוטוקול התקשורת בעת ביצוע רצף פעולות. באופן פוטנציאלי – אף עקיפה מוחלטת של תהליך ההצפנה בפרוטוקול והשגת גישה לקובץ מוצפן בהעברתו. |
| פתרון מוצע | הצפנה מוחלטת של כל התעבורה כולה בין הלקוח לבין השרת, כולל כל שדות הפרוטוקול – כדוגמת TLS/SSL. הצפנה זו תמנע השגה של כל פרט פגיע פוטנציאלי אודות הלקוח, ובכך תמנע כל התחזות אליו או השגה של פרטים בנוגע לפעולות שהוא מבצע או הקבצים שהוא מעביר.  מעבר לכך, שימוש בפרוטוקול TLS עם ביסוס Chain of Trust יצמצם את פוטנציאל ההתחזות לשרת על ידי צד שלישי וזדוני, ללא קשר. |