שאלה 2 – ניתוח פרוטוקול
מתן כשר

המערכת שממומשת ע"י המערכת הינה פלטפורמה לשמירת קבצים אצל השרת .
הפלטפורמה מבצעת זאת ע"י הצפנה סימטרית וא-סמטרית ע"מ לשמור על אבטחת הקבצים בעת שליחתם בסוקט.
ההצפנה מתבצעת ע"י שיתוף מפתחות ושיתופם בין הצדדים.

להלן כמה חולשות הנמצאות בפרוטוקול
בהמשך אציג מסמך מחקר כמבוקש

- הזרקת SQL :
  התוקף מתיימר לשתול מידע במאגר הנתונים ע"י הזרקתו בקוד הSQL .
  במערכת הנ"ל – בעת התקשורת בין השרת ללקוח , התוקף ישתיל בכוונה בחבילת ה headerאו payload מידע להכנסה למאגר הנתונים , לדוגמא – שם לקוח שהוא בכלל תנאי שתמיד מתקיים , ובכך לקבל מהמאגר מפתח ציבורי שכבר קיים מלקוח אחר ולהשתמש בו באופן זדוני.

- חוסר בהזדהות :
  הפרוטוקול חשוף לכל, מה שמאפשר גישה למקורות לא מהימנים שיודעים את מספר הפורט בלבד , השרת מתנהג כרגיל כל עוד הוא מקבל חבילה במבנה של header , payload .
  בנוסף , בעת חיבור מחדש נדרש מהמשתמש רק את שמו , כמובן מה שיכול לגרום להתחזות אליך.

- Man in the middle attack –
  התוקף מתחזה לאדם בתווך המקשר בין השרת ללקוח .
  הדבר אפשרי משום שהפרוטוקול חשוף , וכך כל אחד מהצדדים חושב שהוא מדבר עם הצד השני , רק שהכל עובר דרך התוקף והתוקף יכול להעביר איזה מידע שהוא רוצה לשני הצדדים.

אשתמש בחולשת Man in the middle attack להצגה במסמך התחקור

Risk Analysis

Threat : Leakage of information to a third party

Affecte component: encryption keys, files to save

Module details: Man in the middle attack

Vulnerability class: communication channel

Description:
The attacker impersonates a person in the middle connecting the server and the client.

This is possible because the protocol is exposed, and thus each of the parties thinks that he is talking to the other party, only that everything goes through the attacker and the attacker can transmit any information he wants to both parties.

In a situation where the attacker is successful, he is able to receive all communication transmissions and transmit false information that will be seen as reliable towards the server and the client side

Business impact: When the attacker manages to impersonate and act as a third party in the communication ,He can do almost everything, from receiving the encryption keys and user information, to delivering false messages to the server and the client, thus harming the privacy of users and their files

Proposed remediation:
A stricter identification means must be added to the client

The server side will add an additional means of identification to clients

The client side will check that it is indeed a verified and reliable server

Risk Damage potential: 10
Reproducibility: 8
Exploitability: 5
Affected users: 7
Discoverability: 9

Overall: 8