Alice and Bob

Attack Description

Blue Team #1: Blockchain Forever

1. **Implementation Attack:** No similarity results for the server side (alice.py)

   File comparison results are only displayed on the client side (for Bob). This means the project's goals weren't achieved since at the completion of the implementation, Alice has no information about which files she shares with Bob, if any.

2. **Implementation Attack:** Connection left open on server side (alice.py)

   After Alice sends the code segments from her end and Bob receives and computes similarity results, the connection is only closed from Bob's end but the program does not terminate on Alice's end until a keyboard interrupt occurs. This makes the communication channel vulnerable to attacks.

3. **Implementation Attack:** Only Alice is sending hashed digests to Bob, Bob is not sending anything to Alice

   In the implementation, only the hashed digests of Alice's code segments are signed and sent to Bob, who is then shown how many files they have in common. However, Bob doesn't share the digests of his files with Alice. This goes against the project expectation of Bob and Alice being hostile subcontractors who don't trust each other as only Alice is sharing information about her files with Bob while Bob does not do so.

4. **Theory Attack:** Does not specify which files are the same even on the client side (bob.py)

   The project achieves insufficient goals when displaying similarity results. Not only does it not provide the client (Alice) with the results about files she shares with Bob, but also the results displayed for Bob only indicate how many files are common to both of them. Bob does not learn which of his code segments are common to both Alice and him, rendering the protocol implementation incomplete and inadequate.

Blue Team #2: Blum Blum

1. **Implementation Attack:** Python code does not run successfully (main.py)

   After running main.py on two terminals, the client side is unable to run successfully, yielding multiple execution errors:

   - UnboundLocalError due to variables being used without declaration.
   - ValueError due to a substring not being found even though the correct files are inputted.

   After making minor changes in the code, the communication protocol executes and terminates.

2. **Theory Attack:** Code specification does not have well-defined security goals.

   The protocol specification does not clearly define what code segments Bob and Alice have access to. As a result, if all the code segments of the company they are hired by can be brute forced and hashed, the participant on the server side, who receives the hashed contents of the client's files, can possibly learn details about the original file of the client, resulting in a breach of the security goal of the project, which was to establish a communication protocol for Alice and Bob where neither learns anything about the other's code segments.