1. *We can use any user name and password to login to the server.*

* Choudhury-Sean-sean\_ch-n02RQ0O2K6FQbtsXvDcs5XzpqPENrsdeYfgFFR-rjYU=-Submission

1. *In the Client-Client Session Key Establishment process, the two components used to generate session key are sent in clear. Attackers can record the traffic and derive the session key, then decrypt the encrypted messages.*

* Oberstein-Jesse-joberste-UrfR0TIsQYY\_gr1YIpo5j\_7\_iVHrH6nizv4loI0Nuls=-joberstein\_networks\_final

1. *The authentication protocol between client and server is vulnerable to a Man-In-The-Middle attack, since the Diffie-Hellman key exchange conversation is not encrypted.*

* Atluri-Vamsi-vamsi-bGSP18833b0JukrIuT11GfIPTNmoH6t9Pnj63ekIOOs=-Vamsi\_Aashish

1. *Sending some mal-form message can cause the server crash.*

* Singh-Mahima-mahima-2steOVRLU-ktOd5qkSvyUyixQFBL037\_YYkvi-bv8So=-FinalProject
* Boni-Sharad-sharadboni-aXKO0zoLJHgU5EYbCNqkUB4mMOOH1yluTLIqCaTubcI=-netsec-project-final
* Nguyen-Tri-nntri-3Rotw8Z1Rc-kJFT73XtxGTpZoJGcJg\_ixvsBoZL1i6s=-Final code
* Mathur-Archit-architmathur-cZAYuvmoi-Cmf-k\_byFNQx3VLqxz4uRWFAcG9TA2VOM=-Final Project
* Mahajan-Janhavi-janhavim-oV8Fe4r0gyQWvnw\_hReIEYGk14Lpa-yG3dAhcPvapfo=-project\_submission (Did not use multi-thread to deal with the client requests. If I send some invalid messages like the following, the main thread will be stuck and cannot handle the following requests.)
* Lachyankar-Aniket-alachyankar-LjBLHVlUSgSJKsEUEz\_GvyG5ekHLUCa3eTtcDVs6mNU=-final\_code\_submission\_aniket\_lachyankar

**import** socket  
  
**for** i **in** range(10):  
 sock = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)  
 sock.sendto('fsfdsfsdfsf', ('127.0.0.1', 9090))  
  
**for** i **in** range(10):  
 sock = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)  
 sock.connect(('127.0.0.1', 9090))  
 sock.sendall('fdsfdsfdsfsdfsf')

1. *Attackers can make replay attack. Since no nonce is included in the messages, the attacker can record the sessions and replay the messages without causing the server to deny.*

*Specifically, the attacker can record the authentication session between A and B, and replay the messages to successfully build a connection with B. But since the attacker cannot know the value of a, he/she cannot calculate KAB, thus cannot decrypt the following conversations between A and B.*

* Driskill-Ceridwen-cdris-GJwQbyEQHoZ2xTvQ5zX4giYlUfZiJgv9IOZIDp2zNvY=-Driskill-Coghlan-Chat\_Program

1. *Does not have proof for the result of Diffie-Hellman key exchange process. If an attacker intercepts the DH component message and replaces with another recorded message, neither client nor server can know the DH key exchange fails.*

* Koduru-Ashok-ashok-AE2FDVPWtmz3jE6u8kSagJRYe03wtw\_3jCiEhaKw\_i4=-secure-chat-app\_AshokKoduru\_ParulSingh
* Sawarkar-Abhishek-abhisheksawarkar-4YaX9nl4RrCIifA-9Jl7iteObYALK7AEVNSdzRA2bJk=-Project\_Abhishek\_Pratik\_Updated

1. *Intruders can perform Denial-of-Service attack toward the server.*

* Choudhury-Sean-sean\_ch-n02RQ0O2K6FQbtsXvDcs5XzpqPENrsdeYfgFFR-rjYU=-Submission
* Dubey-Sumeet-sumeetdubey-REdFHyn1vQ6ijb1HxdhThlC2xKEz-bbGxhdEr0RwhOA=-Final\_Project\_NS\_Sumeet\_Shaurya
* Yang-Yang-kyang-Q2A9z9v1WDXsbA5DjD-gaMnMcgE42AXJj28DE9wDeew=-final\_project
* Sengupta-Ayanti-Ayanti-SnpRjiHuEWX3vgKAFkqyPJH8pxin5F4sHC5ZL-L1YuM=-Network Security Final Code

1. *Does not provide PFS. If the intruder records the encrypted session, and breaks into the system and steals the long-term secrets, he/she can decrypt the relevant conversations.*

* Yang-Yang-kyang-Q2A9z9v1WDXsbA5DjD-gaMnMcgE42AXJj28DE9wDeew=-final\_project
* kommajosyula-shalini-kommajosyulas-ZbkC0fn1Th2OnJbzfjBkzqBqO5oiJyGiuNI2dI-fX5E=-project
* Mathur-Archit-architmathur-cZAYuvmoi-Cmf-k\_byFNQx3VLqxz4uRWFAcG9TA2VOM=-Final Project
* Nagaraj-Nithesh-ninagaraj-jArAte2s87HY1aSzV97JDbvvj0eDQBYGtce7vVC-5e4=-Nithesh\_Naveen\_Final\_Code
* Rao-Vishal-vishalrao2911-E\_6pSjKPs3R\_DS4RzCUUvP1bQ-tsvgPCx\_MCq9wifuw=-SimpleChat

1. *Cannot run or login to the server following the instructions in README.*

* Shah-Samkeet-samkeet-bZq\_dVVBQYFlKvhdfyDXj5B-QHUqFks8blYoVg-\_u6U=-samkeet\_bhavik\_secureim
* McCarthy-Abraham-ramimac-zg-m3RtojMOOU4C26hoYw8LCiitzHWZimcCu21bwesw=-SecureIM\_Elci\_McCarthy
* Sengupta-Ayanti-Ayanti-SnpRjiHuEWX3vgKAFkqyPJH8pxin5F4sHC5ZL-L1YuM=-Network Security Final Code
* Sawarkar-Abhishek-abhisheksawarkar-4YaX9nl4RrCIifA-9Jl7iteObYALK7AEVNSdzRA2bJk=-Project\_Abhishek\_Pratik\_Updated