# Vulnerabilities Faced by a Chatbot

## Introduction

As technology advances and makes life easier a medical chatbot is the perfect software to ease pressure on the healthcare sector. Medical chatbot's are increasingly more popular, especially in well-developed countries. Medical chatbots provide more convenient, efficient and faster services to customers/patients.

However, the usage of the chatbot brings potential security and technical vulnerabilities to the user and the company that owns the software. In this document, there will be evidence of examples and an explanation of the potential vulnerabilities faced by a chatbot.

## Ways AI chatbots can be vulnerable to bot repurposing

There are several ways that AI chatbots can be vulnerable to bot repurposing:

Insecure API: If the chatbot's API is not properly secured, it can be accessed and modified by unauthorized users.

Weak authentication: If the authentication mechanism used to access the chatbot's API is weak, it can be easily bypassed by attackers.

Poorly designed intent recognition: If the chatbot's intent recognition mechanism is not robust, attackers can use cleverly crafted messages to trick the chatbot into performing unintended actions.

Lack of input validation: If the chatbot does not properly validate user inputs, it can be vulnerable to attacks that exploit input validation vulnerabilities.

Insufficient testing: If the chatbot is not tested thoroughly, it may have vulnerabilities that can be exploited by attackers.

## Different Types of Attacks

### Man in the Middle

A medical chatbot is vulnerable to a man-in-the-middle attack. This occurs when an external party (third party) intercepts communication between a user and the chatbot (Yasar, 2022). The external party will have access to sensitive information that is shared between the user and the chatbot. Information such as name and health history.

To prevent this attack from taking place we have designed a chatbot that does require the user for their personal information or their old health history.

### Injection Attacks

The chatbot is vulnerable to injection attacks if the user using the chatbot is a well-trained hacker. An injection attack occurs when a hacker inserts malicious code into the chatbot's input field (Muscat, 2019). This will lead to the chatbot performing unusual requests and can potentially lead to sensitive information of another user being leaked.

To prevent this type of attack, the chatbot should have good security input validation filters.

### Social Engineering

Social engineering attacks can take place when a hacker mimics the chatbot and sends phishing emails to a different but identical chatbot. The hacker will trick the chatbot user into revealing their sensitive personal and health information (Social Engineering - Information Security Office - Computing Services - Carnegie Mellon University, n.d.).

Social engineering attacks are difficult to prevent, however, if the user is well-educated and trained on such attacks this can be prevented.

### Brute Force Attacks

Brute force attacks are very common for websites and applications, this will require us developers to develop good authentication protocols and two-factor authentication to prevent this attack. A brute force attack is when a hacker repeatedly tries different usernames and passwords to gain access to the chatbot's system (Buckbee, 2021).

The medical chatbot that the team has created will not require a user to log in, these measures were taken to prevent an attack like this from taking place.

### Denial of Service

A medical chatbot is created to ease pressure on a healthcare service. However, more pressure is created when a hacker decides to hack the chatbot and deny users of the service. A denial service attack occurs when a hacker floods the chatbot service with traffic, causing the chatbot to crash.

### Data Privacy Vulnerabilities

Medical chatbots may contain sensitive information about patients, such as their medical history and personal details. If this data is not encrypted or protected appropriately, it can be easily accessed by hackers. It could also be stored on a database or a server and if that was hacked then it would affect the users data as it would have been in a data breach.

The chatbot may also share patient data with third-party providers, and other companies (insurers or pharmaceutical companies especially) that want to harvest user data for advertising purposes. This will further affect user privacy.

## Conclusion

In conclusion, medical chatbots provide a convenient way for patients to get medical advice and support. However, the use of the chatbot has a risk to patient data confidentiality due to the potential security vulnerabilities. To ensure the security of the user, chatbot developers must implement the appropriate security protocols and software measures. In addition, patients should be educated and aware of the risks taken when using the software.

# Bibliography

Yasar, K. (2022, April 28). *man-in-the-middle attack (MitM)*. Retrieved from TechTarget: https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

Muscat, I. (2019, April 18). *What are injection Attacks*? Retrieved from Acunetix: https://www.acunetix.com/blog/articles/injection-attacks/

*Social Engineering - Information Security Office - Computing Services - Carnegie Mellon University*. (n.d.). Retrieved from Social Engineering - Information Security Office - Computing Services - Carnegie Mellon University: https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

Buckbee, M. (2021, July 20). *What is a Brute Force Attack?* Retrieved from Varonis: https://www.varonis.com/blog/brute-force-attack