Network Security

The measures taken to improve our program against network security attacks

Overview

In today's world of the technology, securing your web services and programs against security attacks has become an essential task. The number of vulnerabilities which can be used to attack and shut down your systems are countless but implementing and using some basic techniques can easily defend your program against a wide range of attacks. Here are a summary of the attacks and actions that we've done to protect our system from them.

1. Improper Inputs

Many input types can be transmitted to your server resources. But processing these inputs without any validation or weak validation can vastly harm your system. This can happen by throwing an unwanted exception in the server side or even make your systems completely shut down.

The purpose of this attack is to establish technical problems in the server side or damage server availability by supplying improper inputs.

Preventive actions:

- Limiting the number of possible characters of inputs, dependent to usage a functionality.
- Checking if the user has entered the correct input type before sending any request to the server.

2. Broken Authentication

The main purpose of the attacker is to log in the system with other users' credential information (such as username and password in most cases) to access confidential and important data such as a bank account information.

This can be done by deceiving the implemented authentication system in the server side in many ways.

Preventive actions:

- **Checking password weakness:**

  Using weak passwords can dangerously increase the chance of the attacker to access to users' accounts. Each password should supply below qualifications:

  - It must contain at least 8 characters.
  - It must include at least one digit.
  - It shouldn't be default, easy to guess, or well-known (Our system checks whether the password is among a list of the thousand worst passwords or not).

- Authentication failure responses don't indicate which part of the authentication data was incorrect. For example, instead of "Invalid username" or "Invalid password", "Invalid username and/or password" is used for both.

3. Brute force

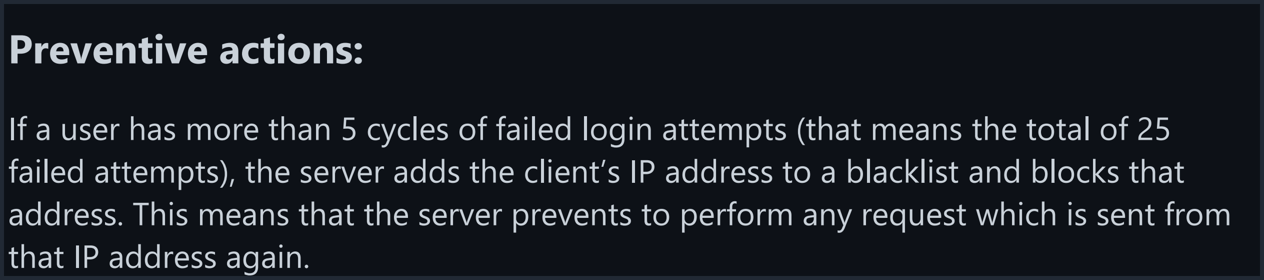
The attacker intends to access to the secured parts of the system by trying every possible combination of credential information (i.e. the username and password for most cases). This can put users' important data in a high risk of fraud or other dangerous measures.

Preventive actions:

- Our program doesn't allow the user to try many guesses in a short time. If the user has 5 failed login attempts in less than 10 seconds, the program disables the client-side login form temporarily. The disability duration increases if more failed attempts occur later.

4. Denial of Service (DoS)

Sending requests to the server in a very-high rate can slow down and even break down the whole service. The attacker tries to send too much requests to the server to shut down the machine or network, making it inaccessible to its users.



Preventive actions:

If a user has more than 5 cycles of failed login attempts (that means the total of 25 failed attempts), the server adds the client’s IP address to a blacklist and blocks that address. This means that the server prevents to perform any request which is sent from that IP address again.