# **CTF Topic: SQL injection**



# **1. Introduction**



In-band SQL injection is a common and potent form of SQL injection where the attacker uses the same communication channel to launch the attack and retrieve the results. This method is often easier for attackers to exploit and detect since the responses are direct and immediate. Two primary techniques under in-band SQL injection are error-based and union-based SQL injection.

# **2. Scenario**



You are required to bypass the login page of altoro.testfire.net using in-band sql injection. After the sql injection has been performed you are required to transfer money from bank account 10000000 to bank account 200000000.

# **3. Begin**

Step 1: Go to the website altoro mutual:<http://altoro.testfire.net/login.jsp>

Step 2: On user name perform Sql injection with the payload ' OR '1'='1'--

Step 3: Type any random password you want to.

Step 4: Go on inside altoro mutual drop down bottom.

# **4. Let’s begin the Challenge**

# **Question**

**Flag1:** Enter the payload you used to bypass the login page.

**Answer:** 'OR '1'='1'--'

**Flag 2 :** How many are managed assets on altoro mutual?

Answer : $20 billion

Flag Captured.

# **Hint**



