Security Threats in the code

# Unchecked Ownership in transfer\_points

In the provided code, there’s no check to verify whether the signer is authorized to transfer points from the sender account. This means anyone who knows the seed for the sender's account can invoke the program and transfer points without the sender's permission.

**Fix:** We need to add a check that verifies whether the signer is the owner of the sender account.

*sender.owner != \*ctx.accounts.signer.key*

# Integer Overflow/Underflow Risk in transfer\_points

There is no protection against integer overflow/underflow during point transfers. This can lead to an unanticipated point balance, potentially allowing users to transfer more points than they should or cause unexpected behavior.

**Fix:** Use safe arithmetic methods like ***checked\_sub*** and ***checked\_add*** to prevent overflow and underflow.

*sender.points = sender.points.****checked\_sub****(amount).ok\_or(MyError::AmountUnderRange)?;*

*receiver.points = receiver.points.****checked\_add****(amount).ok\_or(MyError::Overflow)?;*

# String Size Limitation for name

The name field is a String, and there’s no explicit limit on the length of the string. This can potentially result in exceeding the allocated space.

**Fix:** Limit the length of name string to prevent users from storing arbitrarily long names.

*if name.len() > 10 { return err!(MyError::InvalidName); }*

# Hardcoded Point Initialization

In the ***initialize*** function, every user is created with a fixed 1000 points. This could lead to abuse or unintended behavior if different initial balances are required.

**Fix:** It would be better to make the initial Point as a parameter or set rules for assigning points e.g., based on when the account was created, user type etc.

# Unchecked remove\_user Permissions

The ***remove\_user*** function does not verify whether the signer has the right to remove a user. Anyone can invoke this function and potentially close another user’s account.

**Fix:** Only the account owner should be able to remove their account.