

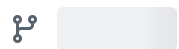
Commit c462977



ParisNeo committed on Jan 1

feat(friends): add authorization checks for responding to friend requests

- Verify the current user is part of the friendship before allowing a response.
- Ensure the responder is not the user who originally sent the request.
- Return appropriate HTTP 403 and 400 errors for unauthorized or invalid actions.



1 parent [76a54f0](#) commit c462977

1 file changed

+9

Filter files...

backend/routers

friends.py

Search within code

```

backend/routers/friends.py
@@ -124,6 +124,15 @@ async def respond_request(friendship_id: int, data:
FriendshipAction, current_db
124 124     fs = db.query(Friendship).filter(Friendship.id == friendship_id).first()
125 125     if not fs: raise HTTPException(404, "Request not found")
126 126
127 +     # Authorization Check 1: Is user involved in this friendship?
128 +     if current_db_user.id not in (fs.user1_id, fs.user2_id):
129 +         raise HTTPException(403, "You are not authorized to respond to this
request")
130 +

```

```
131 + # Authorization Check 2: Is user the recipient (not the requester)?
132 + # action_user_id is the user who initiated the request. The responder must
    be the other party.
133 +     if fs.action_user_id == current_db_user.id:
134 +         raise HTTPException(400, "You cannot respond to your own request")
135 +
127 136         if data.action == 'accept':
128 137             fs.status = FriendshipStatus.ACCEPTED
129 138             fs.action_user_id = current_db_user.id
```



Comments 0