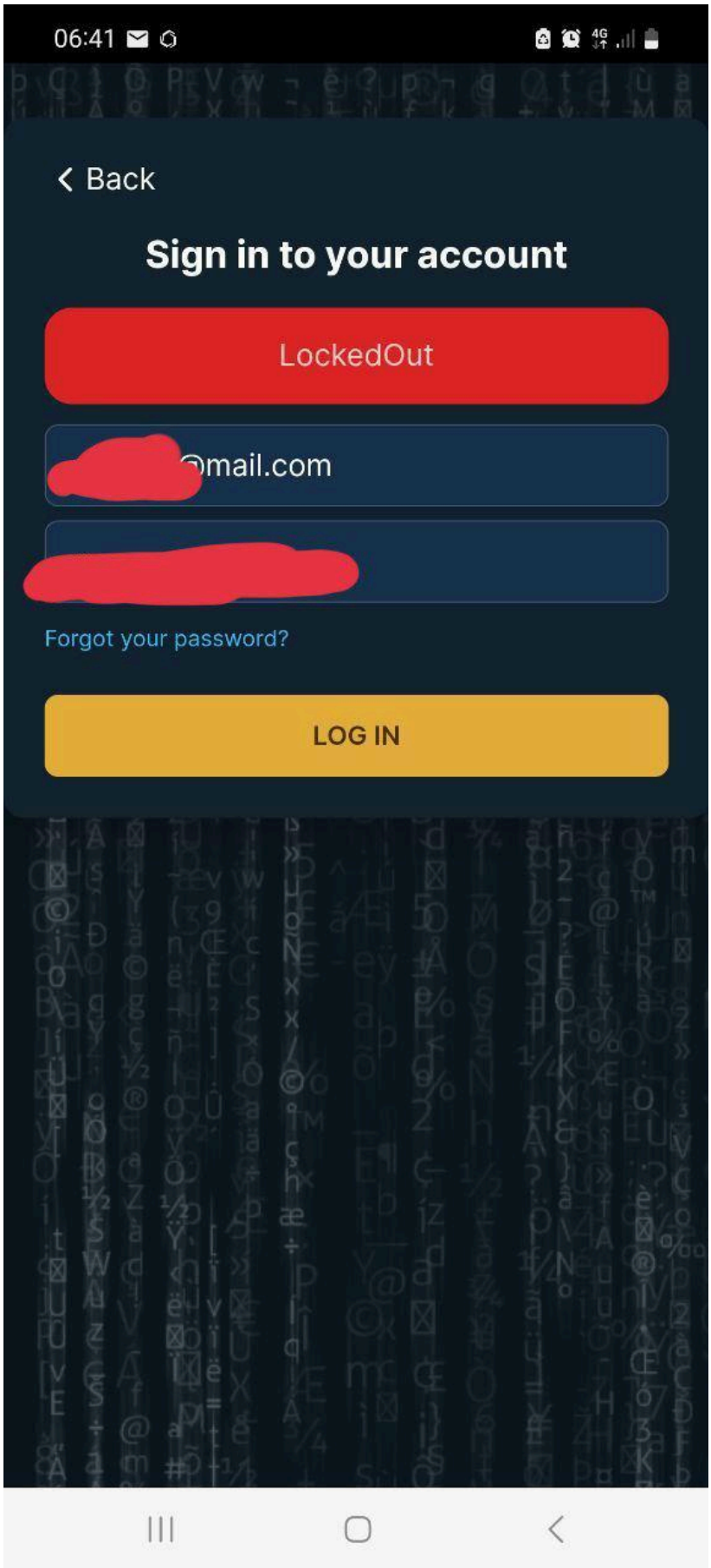
06:41
Back
Sign in to your account
LockedOut
[redacted]@mail.com
[redacted]
Forgot your password?
LOG IN

ISSUE CAUSED BY WALKING AWAY FROM INTERNET CONNECTION WHILE STILL ONLINE WITHIN THE APP
APP THEN LOGS USER OUT CAUSE A LACK OF TOKENS PERHAPS TO LOG BACK IN

THE MOBILE APP IS REFUSING TO ACCEPT PASSWORDS TO STUDENTS AND MODERATORS AND EVEN CAPTAINS
ABOVE IS THE END RESULT
- GO TO SIGN IN ON APP
REPEATEDLY DENIES ACCESS UNTILL LOCKED OUT
CHANGING PASSWORD ON APP DOES NOT HELP
CHANGING PASSWORD ON BROWSER CAN HELP RECONNECT THE APP TO ALLOW THE USER TO SIGN IN HOWEVER THIS IS STILL AN ISSUE AND NEEDS TO BE LOOKED

NOT EVERYONE CAN BRING LAPTOPS OR COMPUTERS WITH THEM

THE EFFICIENCY OF THIS APP RELIES ON THE FACT PEOPLE CAN USE IT FROM A MOBILE NOT JUST A COMPUTER IF THEY CANNOT SIGN IN WHEN THEY NEED TO THIS CAN BE DISCOURAGING.

BELOW I HAVE LISTED POTENTIAL PROBLEMS THAT IT CAN BE HOWEVER
THEY ARE BASIC and PROBABLY ALREADY KNOWN TO THE DEVS

HOW EVER I HOPE THIS HELPS

MOBILE APP PASSWORD LOCKOUT - HIGH PRIORITY ISSUE

Server issues: If there is a problem with the app's server, users may be unable to sign in or access their accounts.
To address this, the app's developers may need to investigate the server and determine what is causing the problem. They may need to fix any bugs or glitches in the server code or upgrade the server hardware to handle increased traffic.

Code issues: If there is an issue with the app's code, it may be preventing users from properly signing in or accessing their accounts.
To fix this, the developers may need to review the app's code and identify any errors or bugs. Once they have identified the problem, they can work on fixing it and deploying an updated version of the app.

Security settings issues: If there is a problem with the app's security settings, users may be prevented from accessing their accounts even if they have entered the correct login information.
To resolve this, the developers may need to review the app's security settings and ensure

that they are properly configured. They may also need to update the app's security protocols to prevent future issues.

Server Issues: When it comes to server issues, there are a variety of problems that could arise, which may prevent users from being able to sign into the app. These issues could include:

Overloaded servers: If there is a sudden spike in traffic to the app, it could cause the servers to become overloaded and unable to properly respond to user requests. This could result in long load times, connection timeouts, or error messages.

Downtime or maintenance: If the app's servers are undergoing maintenance or are experiencing downtime, users may not be able to access the app or sign in. During maintenance, the servers may be offline or in a read-only state, which could prevent users from being able to write data to their accounts.

Security breaches: If the app's servers have been hacked or compromised, it could lead to security breaches that prevent users from being able to sign in or access their accounts. In some cases, users' personal information or login credentials may be stolen or exposed, which could result in identity theft or other forms of fraud.

To address server issues, the app's developers may need to monitor the servers for unusual traffic patterns, regularly update the server hardware and software, and implement security protocols to protect against breaches. They may also need to perform regular maintenance to keep the servers running smoothly and prevent downtime.
Code Issues: When it comes to code issues, there are many potential problems that could prevent users from being able to sign into the app. These issues could include:

Bugs or glitches: If there are bugs or glitches in the app's code, it could cause errors that prevent users from being able to sign in or access their accounts. These issues could range from minor display errors to major system crashes, depending on the severity of the problem.

Compatibility issues: If the app's code is not compatible with certain devices or operating systems, it could prevent users from being able to sign in or access their accounts. This could lead to frustration for users who are unable to use the app on their preferred devices.

Outdated software: If the app's code is outdated, it may not be able to properly handle newer software updates or security protocols. This could lead to errors or other issues that prevent users from being able to sign in or access their accounts.

To address code issues, the app's developers may need to review the code to identify

any errors or bugs. They may need to update the code to ensure that it is compatible with newer devices and software, and they may need to perform regular updates to ensure that the app remains up-to-date with the latest security protocols.

Security Settings Issues: When it comes to security settings issues, there are a variety of problems that could arise, which could prevent users from being able to sign into the app.
These issues could include:

Incorrect authentication protocols: If the app's authentication protocols are not properly configured, it could prevent users from being able to sign in or access their accounts. This could lead to frustration and confusion for users who are unable to authenticate their credentials.

Improper password storage: If the app is not storing passwords securely, it could lead to security breaches or unauthorized access to users' accounts. This could result in data theft or other forms of fraud.

Outdated security protocols: If the app's security protocols are outdated, it may not be able to properly protect against newer forms of cyberattacks or data breaches. This could result in security vulnerabilities that could be exploited by hackers or other malicious actors.

To address security settings issues, the app's developers may need to review the app's security protocols and ensure that they are properly configuredThey may also need to update the app's password storage methods to ensure that they are secure and properly encrypted. Additionally, they may need to regularly update the app's security protocols to keep up with the latest threats and vulnerabilities. Overall, addressing these potential issues will require a thorough analysis of the app's code, servers, and security protocols to identify any areas that need improvement and implement effective solutions.

POTENTIAL ISSUES>>>

1. **Server connectivity issues**
2. **Security settings issues**
3. **API authentication issues**
4. **User account management issues**
5. **Encryption issues**
6. **User interface issues**
7. **Password reset token issues**
8. **Cross-site request forgery issues**

9. Session management issues
10. Network connectivity issues.