**Security Risk Analysis**

**Assests:**

1. Java code: Stored on computers and in Github. Users with access are Deji, Minh, Gahyun.
2. React code: Stored on computers and in Github. Users with access are Deji, Minh, Gahyun.
3. Team files: Stored on Google Drive. Users with access are Deji, Minh, Gahyun.

**Security Risk Matrix:**

|  |  |
| --- | --- |
| **Threats** | **Effects on project** |
| Passwords | Can be stolen |
| SQL Injection | Data can be created, deleted modified |
| Server | Insecure web server |
| Phishing | Unauthorized access to team files |
| Man-in-the-middle | Data entered can be captured |

**Threat Mitigation:**

Passwords: make sure site is secure using https:// in the address bar.

SQL injection: ensure data fields are validated and filtered when submitted. Use appropriate priviledge.

Server: use a secure webserver, make sure patches are up-to-date, enable security features.

Phishing: beware of suspicious emails, do not trust email links and enter passwords carefully.

Man-in-the-middle: make sure wireless connection is secure, use a VPN when login into system.

**Threat Rating:**

Password: not likely to occur, medium impact

SQL injection: highly likely to occur, medium impact

Server: likely to occur, high impact

Phishing: not likely to occur, medium impact

Man-in-the-middle: not likely to occur, low impact