|  |  |  |  |
| --- | --- | --- | --- |
| ASPECT | RISK LEVEL | VULNERABILITY | RECOMMEDATION |
| Network Security | High | Weak Encryption | Implement robust encryption protocols |
| Application | Medium | Cross Site Scripting | Conduct regular code reviews |
| Security | High | Insecure APIs | Secure APIs through authentication |
| Physical Security | Low | Limited Surveillance | Enhance Physical monitoring systems |

SUMMARY:

1. Network security poses a high risk due to weak encryption and unauthorized access.
2. Application security vulnerabilities include cross site scripting and insecure APIs, requiring regular code reviews and enhanced authentication measures.
3. Physical security risks are low but could be mitigated by improving surveillance systems.
4. Security poses high risk if there is insecure APIs, to improve this there is need to secure the APIs through authentication.

RECOMMENDATION:

1. Enhance physical surveillance systems to minimize potential risks.
2. Conduct regular code reviews to address application security vulnerabilities.
3. Strengthen encryption protocols and access controls for network security.
4. Implement secure authentication measures for APIs.