**Icon

Description automatically generated**

**withdrive   
  
OWASP report**

# OWASP top 10 report

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Likelihood | Impact | Risk | Actions | Planned |
| [A01:2021-Broken Access Control](https://owasp.org/Top10/A01_2021-Broken_Access_Control/) | Likely | Severe | High | Use of access control instead of CORS, due to the limitations in the technology. | N/A |
| [A02:2021-Cryptographic Failures](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/) | Low | Low | Low | Usage of proper key management. (UUIDs). Can be exploited with the ‘Sandwich attack’. | N/A |
| [A03:2021-Injection](https://owasp.org/Top10/A03_2021-Injection/) | Low | Moderate | Very Low | JPA does not allow for SQL injection as it sanitises queries. | N/A |
| [A04:2021-Insecure Design](https://owasp.org/Top10/A04_2021-Insecure_Design/) | Low | Moderate | Low | Write tests that will check for errors | Unit tests,  Integration tests |
| [A05:2021-Security Misconfiguration](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/) | Very likely | Severe | Low | Using Security headers to ensure crucial requests are made by users with correct permissions. | Use of Auth0 |
| [A06:2021-Vulnerable and Outdated Components](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/) | Very unlikely | Moderate | Low | Deletion of unused/redundant dependencies and imports. | N/A |
| [A07:2021-Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/) | Likely | Moderate | Moderate | 2+-factor authentication could be used to counteract this vulnerability. | N/A |
| [A08:2021-Software and Data Integrity Failures](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/) | Unlikely | Moderate | Moderate | Ensure that CI/CD has been set up, and has all the important stages tested, and ensure that pushed code passes all tests. | N/A |
| [A09:2021-Security Logging and Monitoring Failures](https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/) | Very likely | Severe | High | Ensure all login, access control, and server-side input validation failures can be logged | N/A |
| [A10:2021-Server-Side Request Forgery](https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/) | Very likely | Severe | High | In the application layer, all data given or provided by the users, should be sanitized, and validated (using regex ect.). Whitelisting of supported sites for user uploaded content. | N/A |