**OWASP TOP 10**

**WEBSHOPPING APPLICATION**

# Hristo Hristov

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Likelihood | Impact | Risk | Actions possible | Planned |
| A01:2021 Broken Access Control | LOW | MODERATE | LOW | N/A fixed | Yes |
| A02:2021 Cryptographic failures | LOW | LOW | LOW | N/A fixed | Yes |
| A03:2021 Injection | LOW | LOW | LOW | N/A fixed | Yes |
| A04:2021 Insecure Design | MODERATE | HIGH | MODERATE | Improve checkout process | No, risk accepted |
| A05:2021 Security Misconfiguration | LOW | LOW | LOW | N/A fixed | Yes |
| A06:2021 Vulnerable and outdated components | MODERATE | MODERATE | MODERATE | Implement tools that monitor if all of the libraries / frameworks are up to date and don’t have vulnerabilities | No, risk accepted |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A07:2021 Identification and Authentication Failures | HIGH | MODERATE | MODERATE | Implement checks to see if the password of a created user is weak | No, risk accepted |
| A08:2021 Software and Data Integrity Failures | LOW | LOW | LOW | N/A fixed | Yes |
| A09:2021 Security Logging and Monitoring Failures | HIGH | SEVERE | HIGH | Implement logging to my application | No, risk accepted |
| A10:2021 Server-Side Request Forgery | LOW | LOW | LOW | N/A fixed | Yes |

# Explanations

A01:2021 Broken Access Control – I have secured all of my website by ensuring that if a user is not logged in as the correct user with the correct rights, he cannot access protected pages (he will be redirected to the homepage)

A02:2021 Cryptographic failures – I have secured my users passwords by using the hashing algorithm Bcrypt so even if a hacker steals the password he will have a very hard time to crack them

A03:2021 Injection – I am using the hibernate in addition to spring boot to secure my application against SQL Injection. I make sure that all of the queries to the database use prepared statements.

A04:2021 Insecure Design – Currently when making an order the user is not required to put in any credit card information so they can put 20 pieces of a very expensive item and make an order that they do not plan on paying.

A05:2021 Security Misconfiguration – I make sure that I only send messages back to the user from the backend that say if the action they wanted to take has been successful or not.

A06:2021 Vulnerable and outdated components – I currently do not have an automatic system to monitor the versions of all of my frameworks and libraries

A07:2021 Identification and Authentication Failures – I do not check if the user has entered a weak password before creating his account

A08:2021 Software and Data Integrity Failures – My application does not use any auto-update functionality

A09:2021 Security Logging and Monitoring Failures – My application does not have logging implemented

A10:2021 Server-Side Request Forgery – My application does not allow users to send URLs to the backend