**OWASP**

S3-CB04

Web Shop – “**S. H. A. I. N.”**

Text

Description automatically generated

**Name :** Shanessa Kostaman (450080)

**Student Number :** 4082419

**Email :** [genoveva.shanessakostaman@student.fontys.nl](file:///C:\Users\shanessa\OneDrive%20-%20Office%20365%20Fontys\Semester%202%20-%20Software\PRJ\s-cb04-s2-g3-prj\genoveva.shanessakostaman@student.fontys.nl)

**Teachers :**

Jacco Snoeren – [j.snoeren@fontys.nl](mailto:j.snoeren@fontys.nl)

Frenk Reemer – [f.reemer@fontys.nl](mailto:f.reemer@fontys.nl)

**Fontys University of Applied Sciences**

**Eindhoven – Netherlands**

**2020-2021**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Code | Category | Likelihood | Impact | Risk | Actions Possible | Planned |
| A01 | Broken Access Control | HIGH | SEVERE | HIGH | Implement check to see if the user login before giving the access. | YES |
| A02 | Cryptographic Failures | LOW | LOW | LOW | Nothing, fixed | YES |
| A03 | Injection | LOW | LOW | LOW | Nothing, fixed | YES |
| A04 | Insecure Design | HIGH | MODERATE | MODERATE | * Implement maximum amount of product(s) in one purchasing user. * Implement method that user has to pay before complete the order. | No, Risk will be accepted |
| A05 | Security Misconfiguration | LOW | LOW | LOW | Nothing, fixed | YES |
| A06 | Vulnerable and Outdated Components | LOW | LOW | LOW | Nothing, fixed | YES |
| A07 | Identification and Authentication Failures | HIGH | SEVERE | HIGH | Implement restrictions for creating a password | No, Risk will be accepted |
| A08 | Software and Data Integrity Failures | MODERATE | MODERATE | MODERATE | Implement security tools to check the component don’t contain known vulnerabilities. | YES |
| A09 | Security Logging and Monitoring Failures | HIGH | SEVERE | HIGH | Implement logger solution | No, Risk will be accepted |
| A10 | Server-Side Request Forgery | LOW | SEVERE | MODERATE | Implement security check for the URL to sent to the backend. | No, Risk will be accepted |

**REASON**

***A01*** *Broken Access Control* – Currently I don’t secure my pages, but I do plan to implement check to see if the use has the correct right to access the page before displaying the page.

***A02*** *Cryptographic Failures* – I use bcrypt for storing my password to the database. Bcrypt is one of the strong adaptive and salted hashing functions with a work factor.

***A03*** *Injection* – I use hibernate ORM for my application. I make sure that hibernate is using a prepare statement to communicate with the database.

***A04*** *Insecure Design* – Currently, I don’t force the user to do the payment before ordering, and I also didn’t limit the amount of product that have been added to the card. I’m going to implement all of that when the application will be use for real web shopping.

***A05*** *Security Misconfiguration* – I will not have default user in my database when I’m done with my application.

***A06*** *Vulnerable and Outdated Components* – I don’t have unused dependency in my application.

***A07*** *Identification and Authentication Failures*- I don’t check if the password that the user makes is easy to guess by the hacker.

***A08*** *Software and Data Integrity Failures* – even though I’m using SonarQube to check the quality of the code and to check the vulnerabilities of my code, but I don’t have tools like OWASP Dependency Check to check the security of my components.

***A09*** *Security Logging and Monitoring Failures –* Right now, I don’t have logger for my application, so of there’s a huge possibility for the hacker to keep doing it because we don’t even know that we’ve been hacked.

***A10*** *Server-Side Request Forgery –* Likelihood will be low because only admin who has control to send the URL to the backend, but the risk will be moderate if someone manage to hack the admin account, because they can submit any URL they want.

**CONCLUTION**

For now and for the scope of my application I believe I have implemented enough security checks. Most of the top 6 security problems that OWASP points out, I have planned for or I’m planning to implement the security for.