Module 5- Computer Systems (2021-22)
Project

UNIVERSITY OF TWENTE.

Final Product-Security by Design Checklist

Team ID: Team 30	**Team Members:** Jan van Zwol, Vo Nhat Minh, Tran Duc Duc, Marjolein Bolten, Ho Hoang Phuoc, Daan Velthuis
Project Name: Ball on the wall	**Mentor(s):** Puru Vaish & Venelina Pocheva

<table>
<tr><th>Security Review for the system</th><th>Put ✔ if you have completed all the points as mentioned in column 1.</th></tr>
<tr><td>
i) Need to ensure if the previous security control work for the system
<table>
<tr><th>Security requirements</th><th>Passed/failed</th><th>How did we solve/check it?</th></tr>
<tr><td>SQL injections</td><td>Passed</td><td>We make use of parameterized query of psycorg2 to not execute input as code but as string.
To check it we try to input the SQL injection code through the user's username input (only possible via username because password will be hashed) and print out the result after</td></tr>
</table>
</td><td>✓</td></tr>
</table>

		executing to make sure that the code is not executed.
		Example of user’s input SQL injection
		`"'' OR '0' = '0'; SELECT *`
		`FROM mod5_project.score”`

Password strength check	Passed	We make a function to make sure that to register an account a user's password needs to have at least a length of 8 with 1 uppercase, 1 lowercase, 1 digit and 1 special character. To check it, we make automated test cases missing 1 requirement and it show that the password is not accepted
Slowing down passwords	Passed	We did this by using the Bcrypt hashing function with a high number of rounds, which takes 3 seconds. Therefore, it will take about 3 seconds delay after the user presses the login button to log in. To check it, we make a automated test case to see that the login time takes at least 2s
Hashing + salt password	Passed	We use the Bcrypt hashing function with random salt to make sure that every hashed password is different. We check with registering 2 same passwords, we see the passwords are hashed to different values, so they are hashed with 2 different random salts.

Non-admin user rights	Passed	In the game there is only one type of user, the normal user. So in the game everyone has the same rights. To access the database there is an admin account and only this account has access to the online database and can perform actions in the database.
Privacy of users	Passed	We checked the database and found no images or videos in the database. We also did a code review to check whether the video recording was used in any other way then intended, which was not the case.

ii) If not, address the reason and discuss the mitigation plan among your team members	Not necessary
iii) Identify if any significant changes are required for the system at the end. If yes, then ensure to update the impacted control decisions in the document as finalized in the previous phases.	No significant changes for our system.
iv) Review and approve it with your TA	

Team members' reviewed:

Jan van Zwol	Yes
Daan Velthuis	Yes
Marjolein Bolten	Yes
Vo Nhat Minh	Yes
Tran Duc Duc	Yes
Ho Hoang Phuoc	Yes

Mentor(s) reviewed and verified:

Puru Vaish	-
Venelina Pocheva	-

Prepared by:

Dipti K. Sarmah