|  |
| --- |
| Assignment |
| ***Peer Assessment Form*** |

|  |  |
| --- | --- |
| ***Self Review*** | |
| Student Name: Abhishek Mittal | Role: |
| Student Number: s5256995 | Grade *[Out of 10]*: 10 |
| Comments:  [Insert comments reflecting on your performance and justifying grade awarded. If unsuitable justification is provided a grade of zero will be entered. Comments should be less than 100 words.]  The building of images user docker-compose files was a necessity to run the web application provided to us as a project, i.e., a pizza application. My part as a team member, was to attack the website using ZAP as a tool for exploring vulnerabilities in the project. On manually attacking the URL, we find errors might medium, low and informational level threats. On introspecting the vulnerabilities in the source code, deep analysis upon what the risk means and how it puts us at risk was conducted. Furthermore, the impacts of the found threat were looked at and a suitable remediation has been suggested for each issue. | |

|  |  |
| --- | --- |
| ***Peer Review*** | |
| Student Name: Yip Hing Wa Tom | Role: |
| Student Number: s5252235 | Grade *[Out of 10]*: 10 |
| Comments:  [Insert comments justifying grade awarded. If unsuitable justification is provided a grade of zero will be entered. Comments should be less than 100 words.] Yip worked on building the docker-compose files and automating the testing using ZAP as a tool. Files to set the working directory, copying json packages to required directoryand access to the container using the expose command was used to set execution on running container. Execution of mongo-express, node, server.js and 27017 using the CMD command when a container starts. Building docker-images for front-end, mongo-express, mongo and proxy was done next. “sudo docker-compose up” was used to execute the code and run the application. The docker-compose.yml file set the container volumes, network port settings, services and container names along with the environment. It mentions the build and image name for each container. | |

|  |  |
| --- | --- |
| ***Peer Review*** | |
| Student Name: Arnaud TACHNAKIAN | Role: |
| Student Number: s5307225 | Grade *[Out of 10]*: 10 |
| Comments:  [Insert comments justifying grade awarded. If unsuitable justification is provided a grade of zero will be entered. Comments should be less than 100 words.]  Arnaud worked on attacking the website using the ZAP attack tool, both automatically and using manual exploration. He found alerts on automation testing and went into deeper analysis by manually attacking the website and obtaining potential vulnerabilities in the scripts and how that could put the application at risk. He assessed the impact of the issue along with a detailed description of the risk and the threat it poses. In the end, he suggested appropriate remediation to deal with the threats found and the CWE issue code for all the mentioned threats has been written for reference. | |