

Centre for Cyber Security Research & Innovation

ASD Essential Eight Mitigation Maturity Model Toolkit

Project Handover Document

Trimester 3/2020

Project Client

Please specify your Product Owner or Tribe Leader

Academic Mentor/Supervisor

Please specify your academic mentor/supervisor

Project Team [Tribe and Squad Name]

|  |  |  |
| --- | --- | --- |
| Student Id | Student Name | Role |
| Student#1 id | Name | Role |
| Student#2 id | Name | Role |
| Student#3 id | Name | Role |
| Student#4 id | Name | Role |
| Student#5 id | Name | Role |
| Student#6 id | Name | Role |
| Student#7 id | Name | Role |
| Student#8 id | Name | Role |
| Student#9 id | Name | Role |
| 218506112 | Ben Landers | Testing / App Security |

# Project Overview

# Please provide a description of what the project is about and list the overall aims and deliverables of the project.

# Document Purpose

This document records the transfer of all the information and artefacts produced during the duration of this Trimester (Trimester 1, 2020). The handover document and delivery package includes the following:

1. Please specify what is included in your delivery and documented here. This may include initial proposal, plans, status reports, demos, iteration reports, squad reflections, source code – if any, executables – if any, key open issues, assumptions, vision for future work on the project, or other relevant documents. Please make sure to refer to document name or folder name as needed.
2. ..
3. …

# Completed Deliverables

Please provide a list of product features and/or deliverables, including a brief description thereof, that have been completed so far, either by your Squad this Trimester, or by a previous Squad before this Trimester. Please only include features and/or deliverables that are fully complete – incomplete work is to be listed below. Please explicitly highlight which features and/or deliverables where completed this Trimester and which Squad member(s) were primarily responsible for their completion. Please also clearly indicate where each of the completed deliverables can be found (e.g, MS Teams, Bitbucket repository).

Please refer to project’s Trello board here (if applicable).

**Iteration 0**

|  |  |  |  |
| --- | --- | --- | --- |
| **DELIVERABLE** | **ITEM LOCATION** | **BRIEF DESCRIPTIONS** | **PRIMARILY INVOLVED**  **MEMBER(S)** |
| **Feasibility Study**  **(ASD-8 and ASD-11)** | [*Deployment and Testing*](https://teams.microsoft.com/l/file/74956706-27E8-44BD-A2D4-A568CAEEC655?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=pptx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2F_T3%202020%20Files%2FDeployment%20and%20Testing%2FIteration%200%2Ffeasibility_report.pptx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9) | Conducted a feasibility study to identify the best tool for automating testing | Ben |
| **Security Report**  **(ASD-12)** | [*Application Security*](https://teams.microsoft.com/l/file/7EA04909-39E0-4370-8EDA-DE633E2BAF8E?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2F_T3%202020%20Files%2FApplication%20Security%2FIteration%200%2Fsecurity_risk_assessment_zap_nikto.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9) | Wrote a security report based on the results of Nikto and OWASP Zap scans. Identified potential XSRF vulnerability | Ben |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Iteration 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **DELIVERABLE** | **ITEM LOCATION** | **BRIEF DESCRIPTIONS** | **PRIMARILY INVOLVED**  **MEMBER(S)** |
| **Penetration Test**  **(ASD-20)** | [*Application Security*](https://teams.microsoft.com/l/file/4DEBB57E-7AC3-42DC-80C4-8E6671820618?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2F_T3%202020%20Files%2FApplication%20Security%2FIteration%201%2Fsecurity_report_iteration_1.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9) | Conducted penetration test and demonstrated application is vulnerable to XSRF and exposed routes | Ben |
| **Test Scripts**  **(ASD-19)** | [*Deployment and Testing*](https://teams.microsoft.com/_#/school/files/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit?threadId=19%3A1986bd18a5f14a37b6a77545d2b9e0db%40thread.tacv2&ctx=channel&context=scripts&rootfolder=%252Fsites%252FDeakinCloudVentures-PG%252FShared%2520Documents%252FASD%2520Essential%2520Eight%2520Cyber%2520Mitigation%2520Toolkit%252F_T3%25202020%2520Files%252FDeployment%2520and%2520Testing%252FIteration%25201%252Fscripts) | Used Sikuli to generate scripts to test 4 out of the 8 mitigation strategies | Ben |
| **Testing Framework**  **(ASD-21)** | [*Deployment and Testing*](https://teams.microsoft.com/l/file/2543F785-11EE-4269-915B-79185DFA996E?tenantId=d02378ec-1688-46d5-8540-1c28b5f470f6&fileType=docx&objectUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG%2FShared%20Documents%2FASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit%2F_T3%202020%20Files%2FDeployment%20and%20Testing%2FIteration%201%2Ftesting_framework_iteration_two.docx&baseUrl=https%3A%2F%2Fdeakin365.sharepoint.com%2Fsites%2FDeakinCloudVentures-PG&serviceName=teams&threadId=19:1986bd18a5f14a37b6a77545d2b9e0db@thread.tacv2&groupId=2e345470-9c36-407f-8dc7-6a73d1fee8f9) | Wrote Markdown document outlining framework for automating testing across | Ben |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Iteration 2**

|  |  |  |  |
| --- | --- | --- | --- |
| **DELIVERABLE** | **ITEM LOCATION** | **BRIEF DESCRIPTIONS** | **PRIMARILY INVOLVED**  **MEMBER(S)** |
| **Test Case Results**  **(ASD-67)** | [*Deployment and Testing*](https://teams.microsoft.com/_#/school/files/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit?threadId=19%3A1986bd18a5f14a37b6a77545d2b9e0db%40thread.tacv2&ctx=channel&context=manual_calc_results&rootfolder=%252Fsites%252FDeakinCloudVentures-PG%252FShared%2520Documents%252FASD%2520Essential%2520Eight%2520Cyber%2520Mitigation%2520Toolkit%252F_T3%25202020%2520Files%252FDeployment%2520and%2520Testing%252FIteration%25202%252Fmanual_calc_results) | Used Sikuli to dynamically generate each test case, saved each test case in a series of Excel spreadsheets and manually calculated the expected results using the revised maturity logic | Ben and Sunny |
| **README file**  **(ASD-65)** | [*Deployment and Testing*](https://deakin365.sharepoint.com/sites/DeakinCloudVentures-PG/Shared%20Documents/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit/_T3%202020%20Files/Deployment%20and%20Testing/Iteration%202/scripts/README.md) | Created README file to explain how to use automated test scripts | Ben |
| **Test Scripts**  **(ASD-64 and ASD-66)** | [*Deployment and Testing*](https://teams.microsoft.com/_#/school/files/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit?threadId=19%3A1986bd18a5f14a37b6a77545d2b9e0db%40thread.tacv2&ctx=channel&context=scripts&rootfolder=%252Fsites%252FDeakinCloudVentures-PG%252FShared%2520Documents%252FASD%2520Essential%2520Eight%2520Cyber%2520Mitigation%2520Toolkit%252F_T3%25202020%2520Files%252FDeployment%2520and%2520Testing%252FIteration%25202%252Fscripts) | Re-calibrated existing test scripts and created new test scripts in line with revised maturity logic for the 8 mitigation strategies | Ben and Sunny |
| **Baseline Testing Data**  **(ASD-68)** | [*Deployment and Testing*](https://teams.microsoft.com/_#/school/files/ASD%20Essential%20Eight%20Cyber%20Mitigation%20Toolkit?threadId=19%3A1986bd18a5f14a37b6a77545d2b9e0db%40thread.tacv2&ctx=channel&context=testing_data&rootfolder=%252Fsites%252FDeakinCloudVentures-PG%252FShared%2520Documents%252FASD%2520Essential%2520Eight%2520Cyber%2520Mitigation%2520Toolkit%252F_T3%25202020%2520Files%252FDeployment%2520and%2520Testing%252FIteration%25202%252Ftesting_data) | Produced baseline testing data for the 8 mitigation strategies | Ben |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Iteration 3**

|  |  |  |  |
| --- | --- | --- | --- |
| **DELIVERABLE** | **ITEM LOCATION** | **BRIEF DESCRIPTIONS** | **PRIMARILY INVOLVED**  **MEMBER(S)** |
|  |  |  |  |
|  |  |  |  |

# Planned work

Please provide a list of features and/or deliverables that are planned to be completed in the next phase of the project (e.g., next Trimester) as well as features and/or deliverables that your Squad has started this Trimester, but not yet fully completed. The state of each incomplete work item should be briefly described.

Please refer to project Trello board here too (if applicable).

# Open issues

Please provide a list of open issues/challenges in the project, and any investigation that you have conducted so far to resolve them.

# Lessons Learned

Please provide a list of key lessons learned from the project work this Trimester, especially in relation to processes and/or technology you would recommend to be changed in future Trimesters. Please provide a rationale why you think they need to be changed.

# High-level architecture of the product

Depending on the state of the project: please provide a high-level architecture of your project highlighting the key components of the project and how they integrate/talk to each other. Please provide any necessary deployment details.  
  
Note that this may not be applicable to all projects.

# Source code

Please add all necessary details for your project’s source code – links, key components, classes, database components, URLs of online hosted repositories, etc. Please make sure to include your project’s source code in the delivery package if it is hosted on a server outside Deakin.

# User manual

Please provide detailed instructions on how end user can use your system (where applicable).

# Other relevant documents

Please provide any relevant information not covered in the above sections.

# Appendices

Please include appendices for all artefacts delivered during the course of the project

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ARTEFACT | TIME PRODUCED  (ITERATION) | PRIMARILY INVOLVED MEMBER(S) | COMPLEXITIES/ISSUES (IF RELEVANT) | FURTHER DEVELOPMENT |
| Security risk assessment | 0 | Ben Landers | OWASP Zap and Nikto are efficient methods for detecting potential vulnerabilities. However, further manual tests must be undertaken to verify any alerts. | Automated tests provided baseline data about potential vulnerabilities based on the state of the application at the start of Iteration 0. Further automated scans should be undertaken as the web application evolves. |
| security report | 1 | Ben Landers | The penetration test only focused on authorisation and authentication. The report documented exposed routes and a XSRF vulnerability. | Penetration tests should be repeated and expanded in Trimester 1 2021 to ensure vulnerabilities have been patched. |
| workflow for Encrypting and decrypting | 2 | Andrew Cunningham and Ben Landers | A workflow document was developed for sharing authentication tokens between groups members securely. GPG was selected as the encryption standard. The workflow document includes the commands for the CLI tool but not GUI tools. | Users unfamiliar with using the GPG CLI tool may need further instructions on using the available GUI tools to complete the steps to decrypt authentication tokens. This can be undertaken in a live mentoring session if required. |
| scripts for automating testing | 1 and 2 | Ben Landers and Sunny Pannu | The scripts are written in Python and use the image recognition software, Sikuli to run. The scripts need to be modified when used across different devices. This is because, unlike a machine learning model, the software has limited generalization capabilities | Although Sikuli was able to be used to generate testing data for the 8 mitigation strategies, it could be integrated with Selenium to make the scripts more robust. |
| basline testing data | 2 |  | The maturity logic was revised across Iteration 1 but not implemented until the end of Iteration 2. This means that the revised maturity logic was measured against a version of the web application that had not been updated. | Re-calibrate all test scripts to match the updated back and front-end. |
| manually calculated test results | 2 |  | Although all testing is automated with Sikuli, the expected result for each test case had to be manually calculated using the revised maturity logic. This was used to compare the actual result with the expected result. | If a test case fails, the manually calculated result should be checked against the details in the revised maturity logic document. |