Vulnerability Management Tool

Final Report

Student Name: Síne Doheny
Supervised by: Richard Butler
Student ID: C00226237

Table of Contents

Abstract

The purpose of this report is to document the process carried out in developing the final product of the "Vulnerability Management Tool" project. The document will provide a detailed over view of the web application, its features, users and the development process.

Introduction

Vulnerability Management is a web application service which provides a vulnerability management solution for organizations to strategically and dynamically manage their IT vulnerability environment and the security teams the organization has carrying out this process. The project simplifies the enterprise vulnerability security operations approach while providing a traceable and accountable vulnerability cycle which results in leveraging business cyber security exposure with ease, performing efficient tracking and reporting of the vulnerability process while it is carried out. The platform creates enterprise environment visibility through asset inventory and vulnerability posture improvements through tracking of the following vulnerability cycle components; vulnerability tests and assessments, identification of vulnerabilities, risk management with priority through the DREAD matrix framework, and the storage of vulnerability analysis, evaluation and remediation which also incorporates mitigation reporting based on the MITRE ATT&CK framework. Through tracking each of these vulnerability cycle processes and their data from start to finish, the project drives value in the traceable progress and resulting data, enabling visible insight into an IT environment, its identified vulnerabilities, analysis of how remediations took place and the whole process in general from start to finish. The project provides full in depth data tracking and storing of every vulnerability cycle step, from the moment a test for an asset is created. As well as the full vulnerability cycle being managed, a security team is also managed through the application. Each user in the vulnerability cycle process has a significant role and this project provides an interface where each users roles have been comprehensively calculated and consciously implemented as a result, separating tasks based on the user logged in and their role, a system for tracking every task the user undertakes and separating each user appropriately in accordance with their allowed privileges. The historical data reporting throughout the application flow holds the vulnerability cycle and the users involved in the process accountable providing business management of all levels reporting and intelligence of their systems, security team actions and vulnerabilities in all time senses, current and previous for continuous strategic comparison of past vulnerabilities and system weaknesses resulting in business growth through continuous improvement and evolvement. All of these elements combined will improve vulnerability management, risk management, vulnerability remediation, reduce the risk of cyber-attacks, save attack damage costs and breach costs, business loss prevention, operational time savings and regulation compliance.

Project Description

Vulnerability Management was built using the Microsoft Visual Studio Development environment. The Visual Studio inbuilt local server was used to run the application through Google Chrome.

The Project backend was developed using an array of development languages including C#, SQL, JavaScript, jQuery, Ajax and MVC Razor. Each of these languages except for SQL were all new or relatively new to me and throughout the creation process I had learned how to develop using them from scratch.

The base of the application is an SQL database used in the Visual Studio server. This database was configured and used to store the details of the user accounts, user roles, assets, asset tests, the tests log which stores the actions of the logged in penetration testers in accordance to the ID of the test item they have been assigned and performed an action with, the intelligence of vulnerabilities found from asset tests, vulnerability assignments assigned to security engineers, vulnerability assignments log which stores the actions of the logged in security engineers in accordance to the ID of the vulnerability item they have been assigned and performed an action with and vulnerability mitigation information.

The project was built using the ASP.Net MVC framework in order to impart the in depth data in appropriate separation manner. I chose to take the route of the framework due to the project data being so large and knew it would eventually get very complicated using other methods hence decided to separate the data based on its concerns. MVC is a model, view, controller framework approach which allowed me to separate the business data and logic in the Model and Controller and then further display the data seamlessly through the view. C# was used for coding the general development data where I was creating models for users, assets, tests, vulnerabilities etc., and then further in controlling what is happening with the code like creating methods which then use SQL to aggregate data to and from the database, it was further used in the controllers where a data access object and the information or methods used to gather or perform an action with the data, this code in the controller will act as a guide which informs the data where it is to be displayed. C# was also used in the views where razor code which is an adjoin of CSHTML code is used. C# was used to pull through the model data such as a vulnerability name through the controller and further into the view which was then displayed using HTML code. In specific scenarios I had used JavaScript, jQuery and Ajax in the CSHTML pages as this was the only way to send data from the view back to the controller to perform an action with that data and send it back to the view again. I used these languages on two occasions, one being where a user has to select a MITRE Tactic for the vulnerability mitigation information and then the techniques associated with this specific Tactic are populated in the second drop down list based on the chosen Tactic. The Technique is then chosen and the information is stored in the database. I had to use these languages to send the chosen item back to the controller to perform the population of the second drop down list with the techniques based on the chosen item, this data is then sent back to the view and performs the pull through of data and populates the second drop down list. The second occasion where I had used JavaScript, jQuery was to perform the DREAD matrix threat severity total of each

DREAD value gathering the total severity of the vulnerability when the adding the vulnerability to the system process.

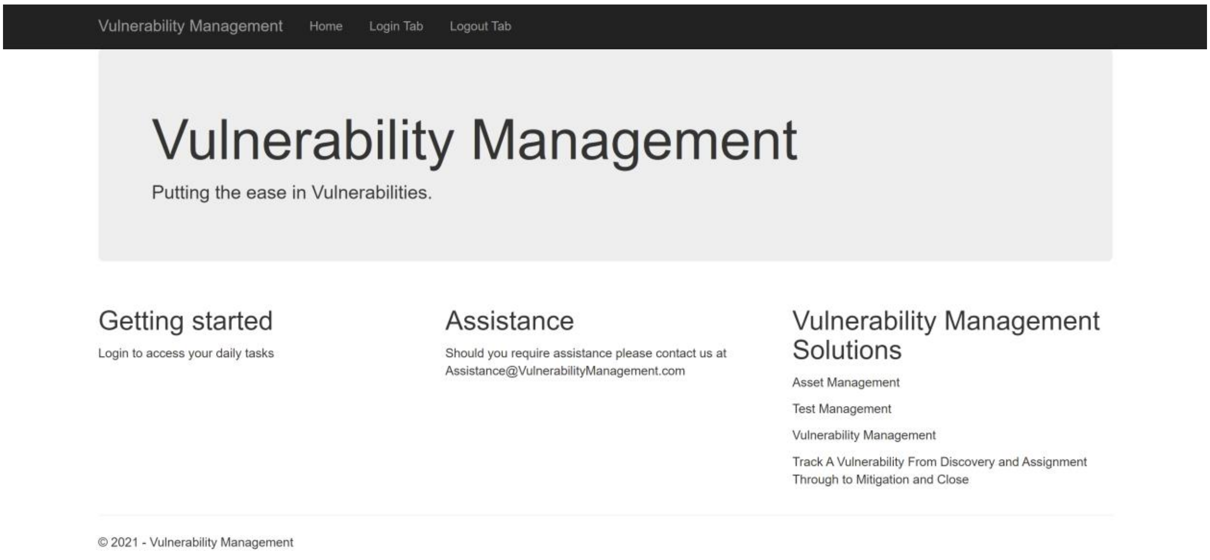
The front end languages used in the development of the web application were HTML, CSS, JavaScript and Bootstrap.

In summary the application requires an SQL database, MVC Framework, C#, JavaScript, jQuery, Ajax, Razor which is used in markup by the server, HTML and CSS.

Application Flow

The following is an outline of the Vulnerability Management application flow in accordance with its users, their functionality and privileges within the application. The application flow will convey how the application would be used in a realistic vulnerability management cycle scenario. The users of the application are the Administrator, Penetration Tester and Security Engineer. If the application was used in a company environment these users would also be the same category of users using the application. In the application there is no registration functionality for a new user as the idea of the project was to provide the interface for an organization who will add their users manually to the secure configured database this would allow no new users to register and join the application without secure approval prior. There is only one Administrator, however there can be many Penetration Testers and Security Engineers.

This is the home page of the application for an unauthorized user.



Vulnerability Management

Putting the ease in Vulnerabilities.

Getting started

Login to access your daily tasks

Assistance

Should you require assistance please contact us at Assistance@VulnerabilityManagement.com

Vulnerability Management Solutions

Asset Management

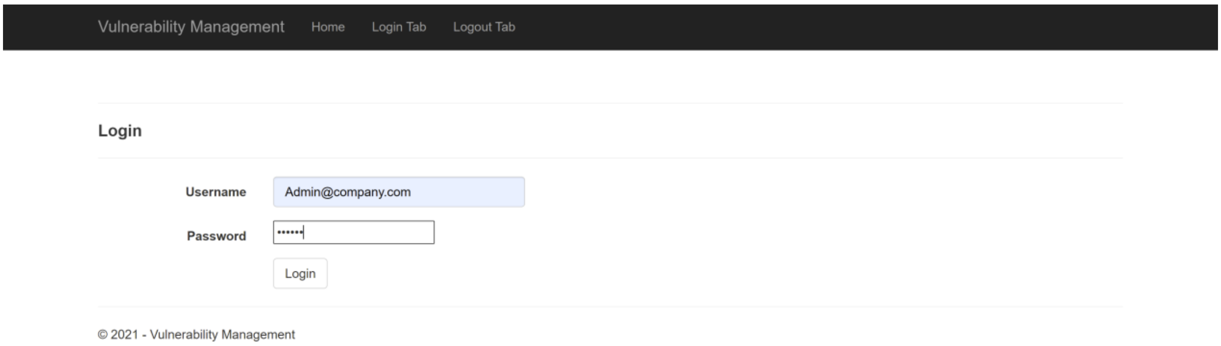
Test Management

Vulnerability Management

Track A Vulnerability From Discovery and Assignment Through to Mitigation and Close

© 2021 - Vulnerability Management

The role of the Administrator, is to add assets to the asset inventory, set up vulnerability tests for assets and further assign any unassigned tests to the on site Penetration Tester(s). The following is the Administrator logging in using the login interface.



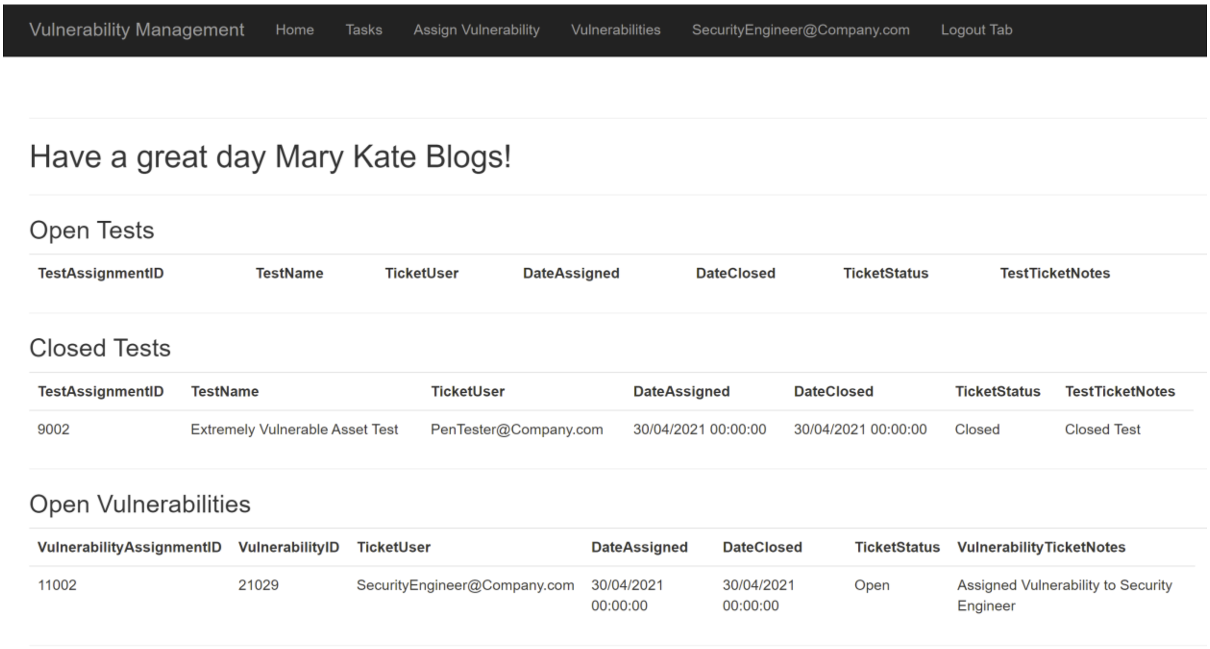
Login

Username: Admin@company.com

Password: ••••••

© 2021 - Vulnerability Management

The following is the dashboard for the authorized homepage which provides contextual information about the current vulnerabilities in the organization. This is not the full page as you have to scroll down to see the full page. The vulnerabilities shown by status of open and closed, and items for example all high severity vulnerabilities in the organization will give the user an idea when they log in of the organizations security posture and their speed in completing tests and mitigating vulnerabilities. These lists could be changed to suit an organization based on their needs as they provide in depth data regarding the whole vulnerability and test environment for the company.



Have a great day Mary Kate Blogs!

Open Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes

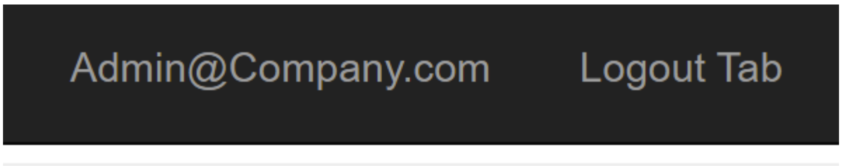
Closed Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes
9002	Extremely Vulnerable Asset Test	PenTester@Company.com	30/04/2021 00:00:00	30/04/2021 00:00:00	Closed	Closed Test

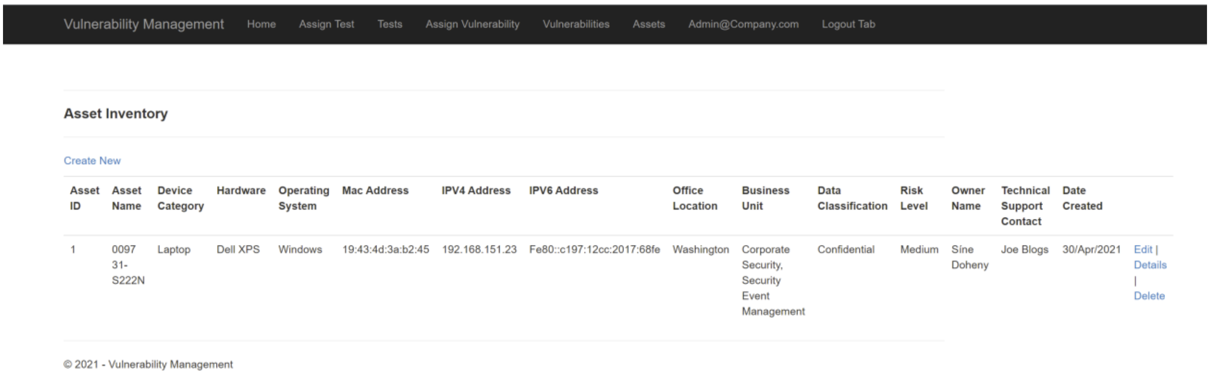
Open Vulnerabilities

VulnerabilityAssignmentID	VulnerabilityID	TicketUser	DateAssigned	DateClosed	TicketStatus	VulnerabilityTicketNotes
11002	21029	SecurityEngineer@Company.com	30/04/2021 00:00:00	30/04/2021 00:00:00	Open	Assigned Vulnerability to Security Engineer

Here we can see the user logged in is the Administrator:



The following is the asset added by the Administrator to the asset inventory.



Asset Inventory

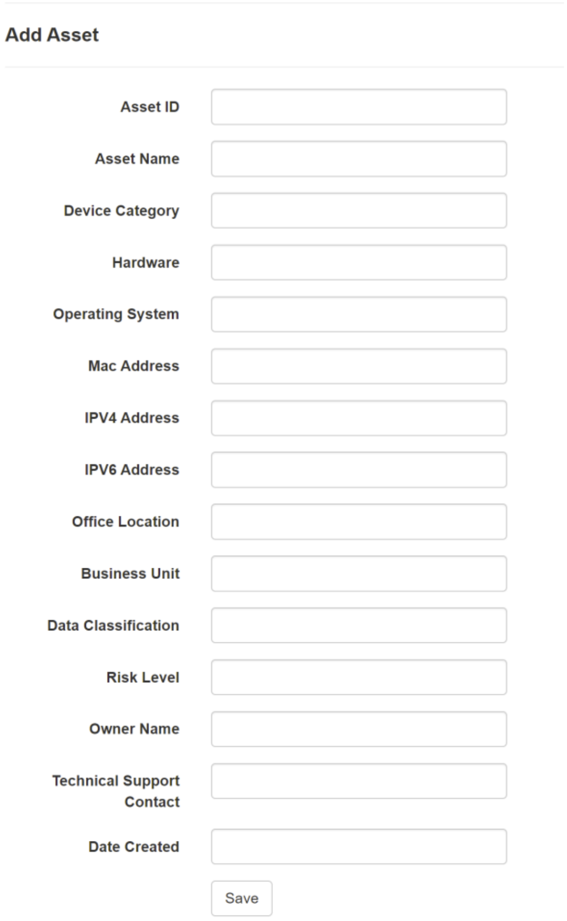
Create New

Asset ID	Asset Name	Device Category	Hardware	Operating System	Mac Address	IPV4 Address	IPV6 Address	Office Location	Business Unit	Data Classification	Risk Level	Owner Name	Technical Support Contact	Date Created	
1	009731-S222N	Laptop	Dell XPS	Windows	19:43:4d:3a:b2:45	192.168.151.23	Fe80::c197:12cc:2017:68fe	Washington	Corporate Security, Security Event Management	Confidential	Medium	Síne Doheny	Joe Blogs	30/Apr/2021	Edit | Details | Delete

© 2021 - Vulnerability Management

Important attributes of the asset are recorded when creating a test and are displayed as above.

The following are the required attributes for adding an asset which can be found in the Add Asset page.



Add Asset

Asset ID

Asset Name

Device Category

Hardware

Operating System

Mac Address

IPV4 Address

IPV6 Address

Office Location

Business Unit

Data Classification

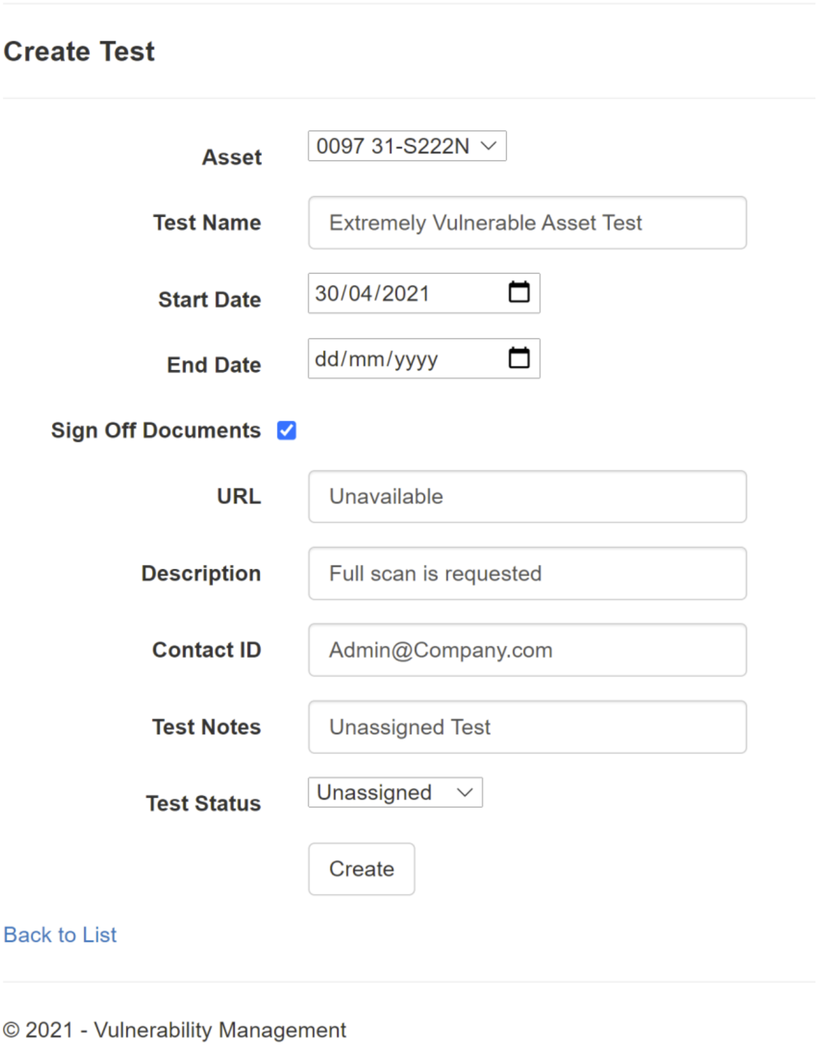
Risk Level

Owner Name

Technical Support Contact

Date Created

When the Asset is created a test can be created for the asset by the Administrator as follows:

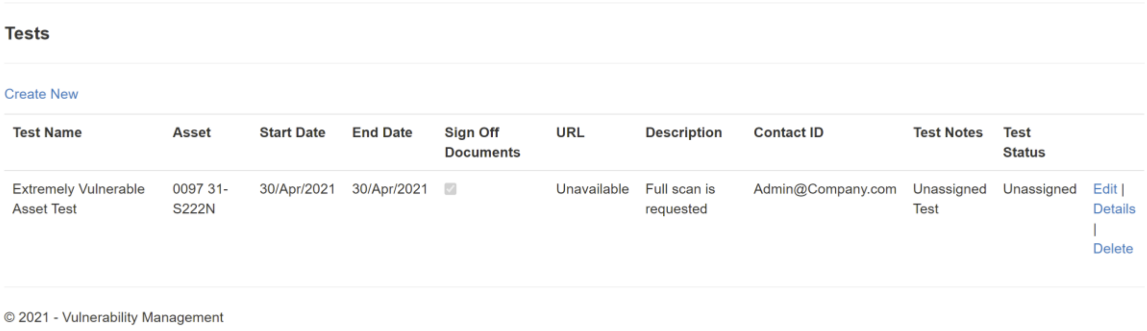


Create Test

Asset	0097 31-S222N
Test Name	Extremely Vulnerable Asset Test
Start Date	30/04/2021
End Date	dd/mm/yyyy
Sign Off Documents	☑
URL	Unavailable
Description	Full scan is requested
Contact ID	Admin@Company.com
Test Notes	Unassigned Test
Test Status	Unassigned

© 2021 - Vulnerability Management

The following is the test in the test inventory:

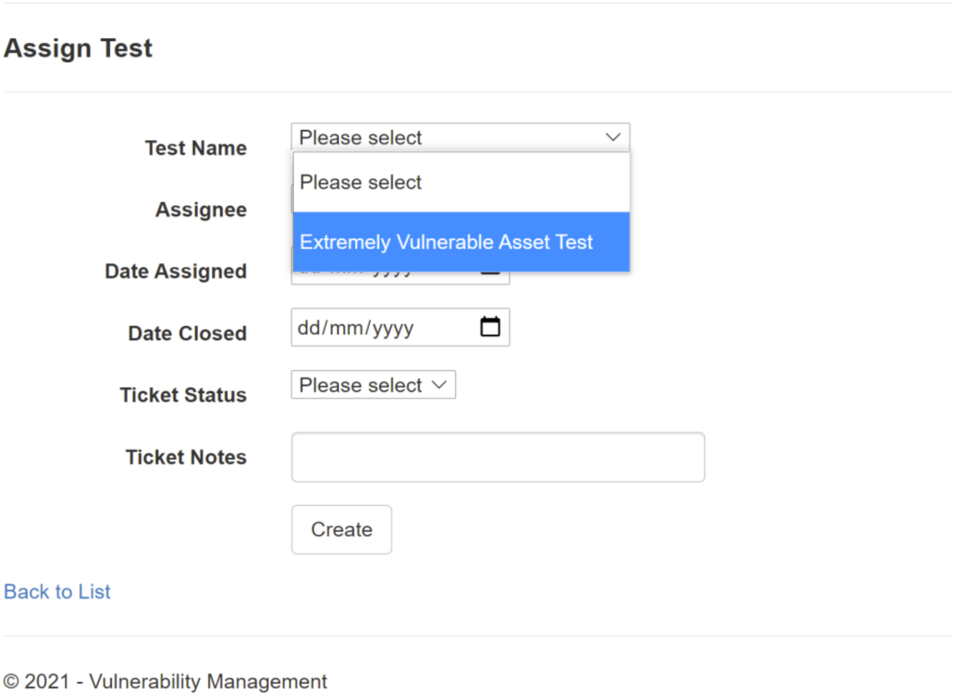


Tests

Test Name	Asset	Start Date	End Date	Sign Off Documents	URL	Description	Contact ID	Test Notes	Test Status	
Extremely Vulnerable Asset Test	0097 31-S222N	30/Apr/2021	30/Apr/2021	☑	Unavailable	Full scan is requested	Admin@Company.com	Unassigned Test	Unassigned	Edit | Details | Delete

© 2021 - Vulnerability Management

Next the Administrator assigns the test to a Penetration Tester to perform the vulnerability test. The following the creation of the test assignment. Here the tests ready to be assigned are populated in the dropdown list as follows:



Assign Test

Test Name: Please select
- Please select
- Extremely Vulnerable Asset Test

Assignee

Date Assigned

Date Closed: dd/mm/yyyy

Ticket Status: Please select

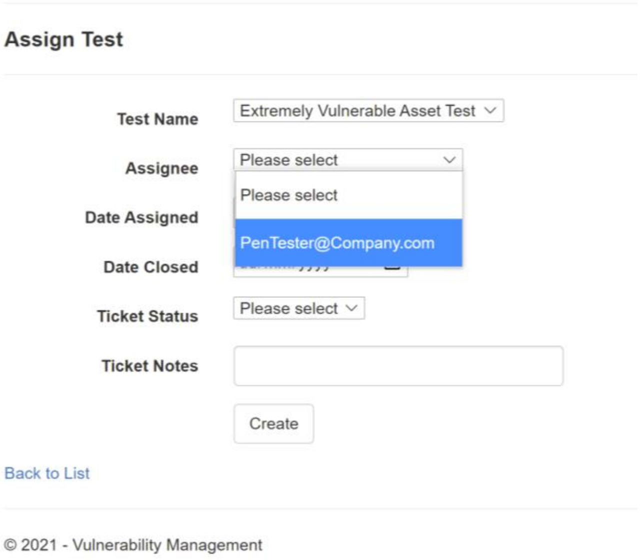
Ticket Notes

Create

Back to List

© 2021 - Vulnerability Management

The next drop down list is populated for users to assign the test to. This is a list of all Penetration Testers in the company:



Assign Test

Test Name: Extremely Vulnerable Asset Test

Assignee: Please select
- Please select
- PenTester@Company.com

Date Assigned

Date Closed

Ticket Status: Please select

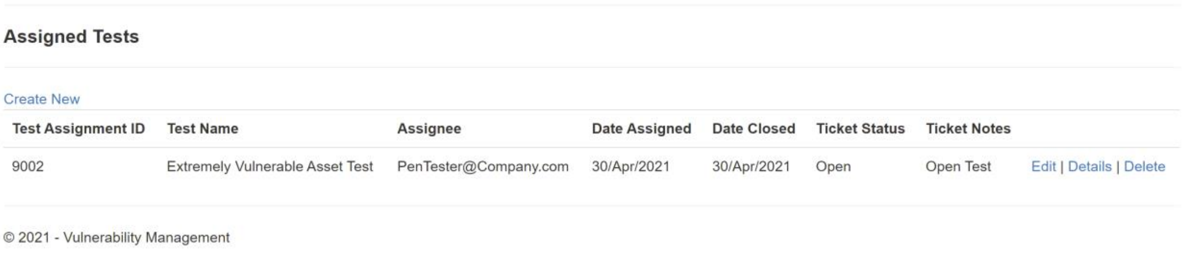
Ticket Notes

Create

Back to List

© 2021 - Vulnerability Management

The ticket status will be set to open and this will dynamically update the status of the test in the list of tests with that ID to open also. Below is the assigned test:

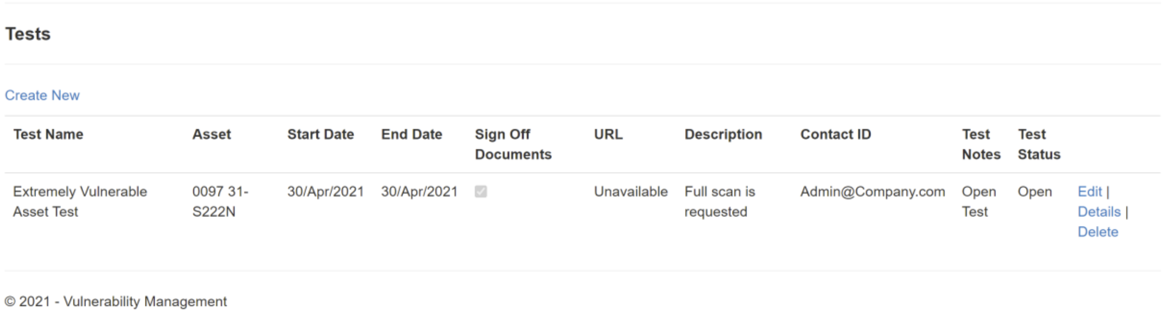


Assigned Tests

Test Assignment ID	Test Name	Assignee	Date Assigned	Date Closed	Ticket Status	Ticket Notes	
9002	Extremely Vulnerable Asset Test	PenTester@Company.com	30/Apr/2021	30/Apr/2021	Open	Open Test	Edit | Details | Delete

© 2021 - Vulnerability Management

The following is the test in the list of tests but with its status dynamically updated, previously it was Unassigned now it is Open:

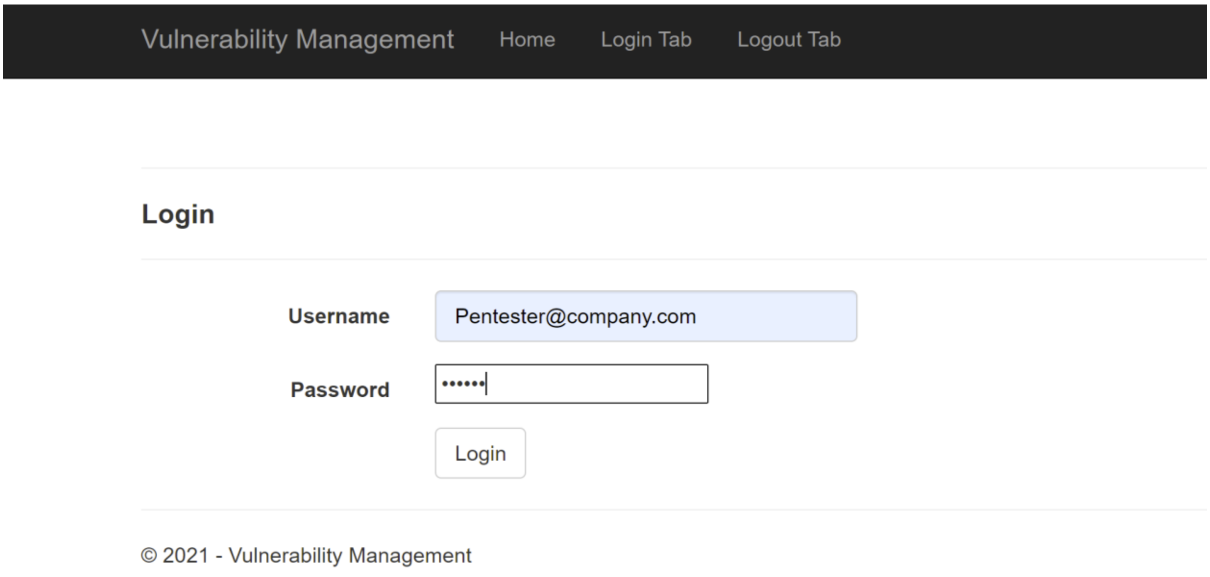


Tests

Test Name	Asset	Start Date	End Date	Sign Off Documents	URL	Description	Contact ID	Test Notes	Test Status	
Extremely Vulnerable Asset Test	0097 31-S222N	30/Apr/2021	30/Apr/2021	☑	Unavailable	Full scan is requested	Admin@Company.com	Open Test	Open	Edit | Details | Delete

© 2021 - Vulnerability Management

The role of the Penetration Tester is to then check their tasks box and they will see all tasks allocated to them personally. Each task in the task box is populated in accordance to the specific logged in user dynamically. The following is the above test which populated in the assigned Penetration Testers task box which was seen after logging in:



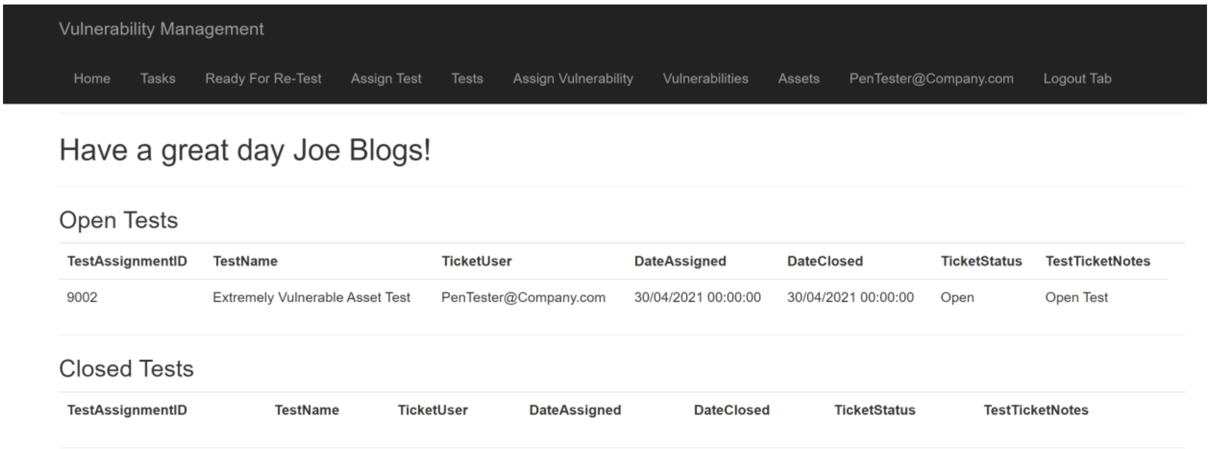
Login

Username: Pentester@company.com

Password: ••••••

© 2021 - Vulnerability Management

The test has appeared on the dashboard dynamically in the open tests section:



Have a great day Joe Blogs!

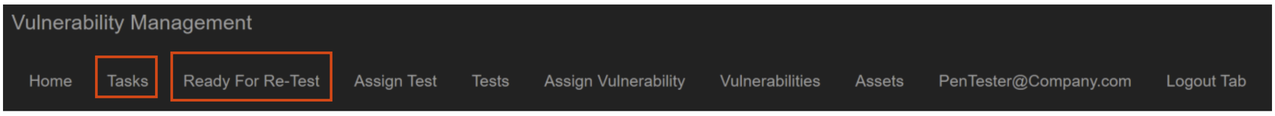
Open Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes
9002	Extremely Vulnerable Asset Test	PenTester@Company.com	30/04/2021 00:00:00	30/04/2021 00:00:00	Open	Open Test

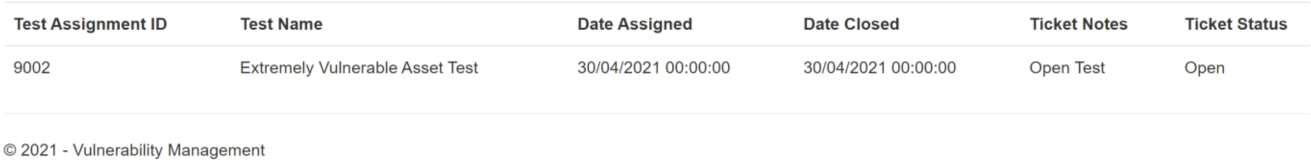
Closed Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes

Here we can see the different navigation bar links which only appear if the Penetration Tester logs in:



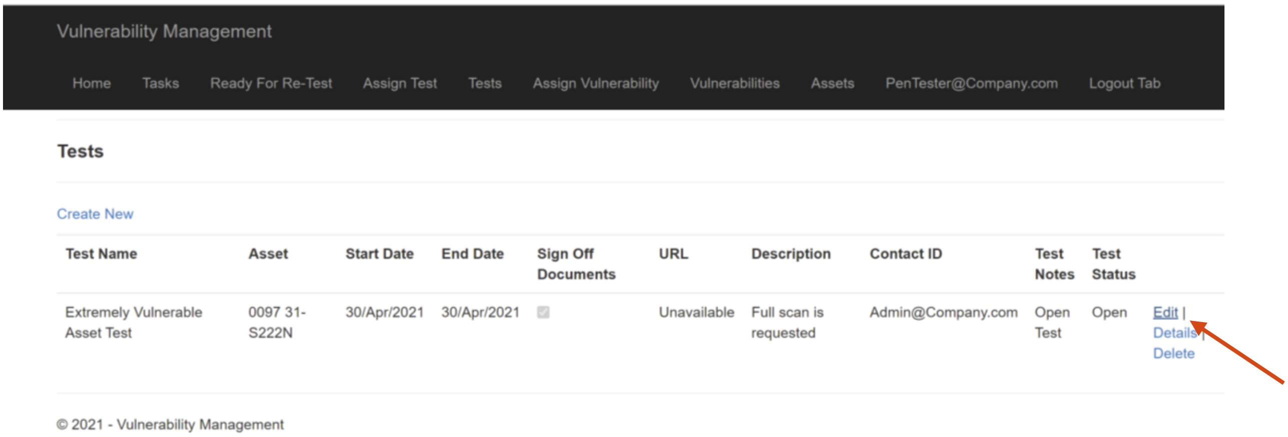
The following is the Test in the Tasks link, Test 9002 which was assigned to PenTester@Company.com:



Test Assignment ID	Test Name	Date Assigned	Date Closed	Ticket Notes	Ticket Status
9002	Extremely Vulnerable Asset Test	30/04/2021 00:00:00	30/04/2021 00:00:00	Open Test	Open

© 2021 - Vulnerability Management

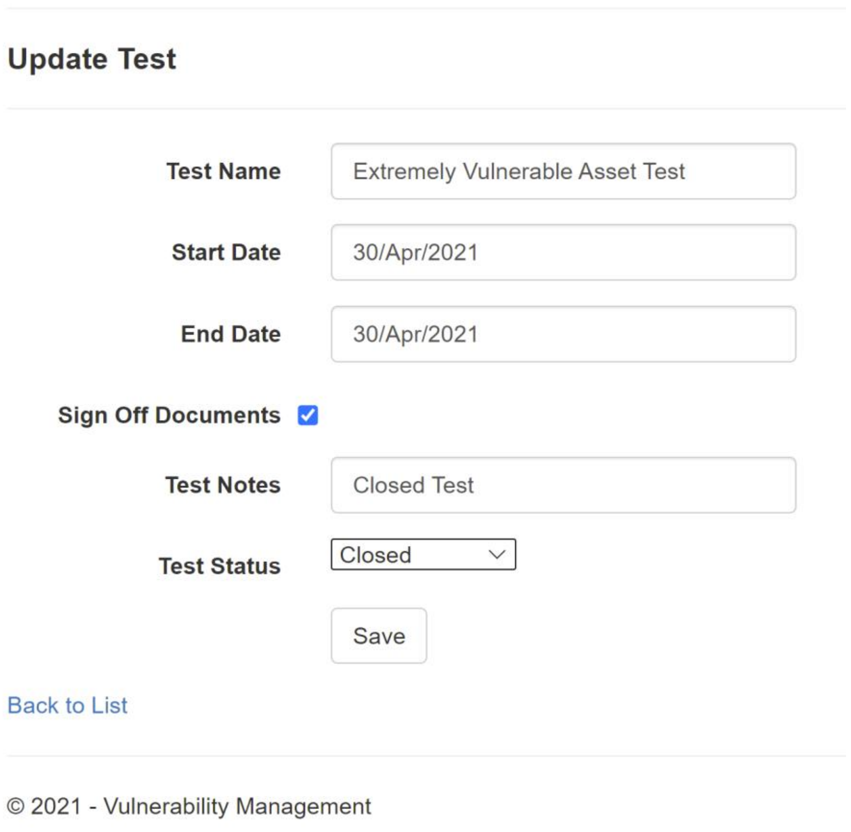
The Penetration Tester will then perform the vulnerability test and when complete will edit the assigned test as closed in the edit button for the test in the test page, they will include details of the test information and the action they completed.



Tests

Test Name	Asset	Start Date	End Date	Sign Off Documents	URL	Description	Contact ID	Test Notes	Test Status	
Extremely Vulnerable Asset Test	0097 31-S222N	30/Apr/2021	30/Apr/2021	☑	Unavailable	Full scan is requested	Admin@Company.com	Open Test	Open	Edit | Details | Delete

© 2021 - Vulnerability Management



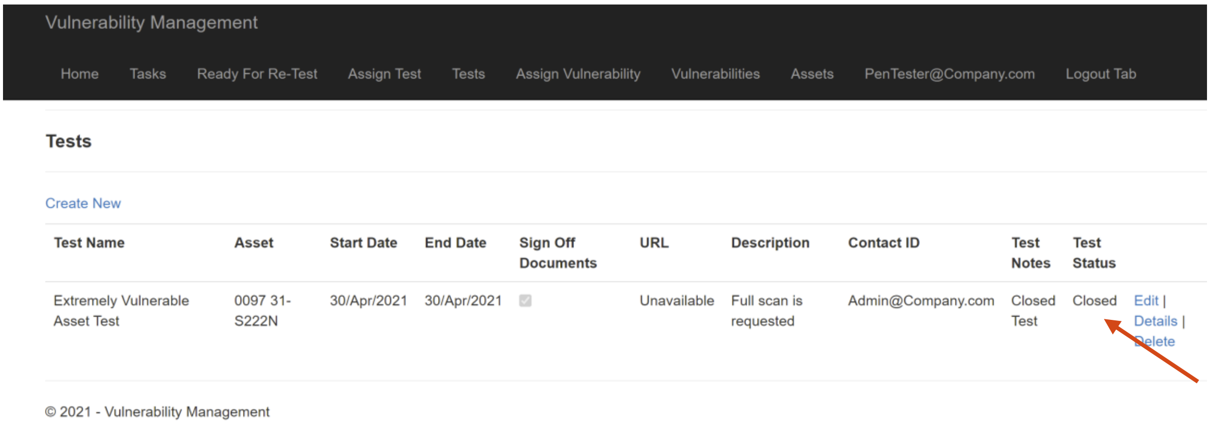
Update Test

Test Name	Extremely Vulnerable Asset Test
Start Date	30/Apr/2021
End Date	30/Apr/2021
Sign Off Documents	☑
Test Notes	Closed Test
Test Status	Closed

© 2021 - Vulnerability Management

This will then dynamically update the test in the current tests list to closed also and the task will disappear from the Penetration Testers task box as follows:

Tests List

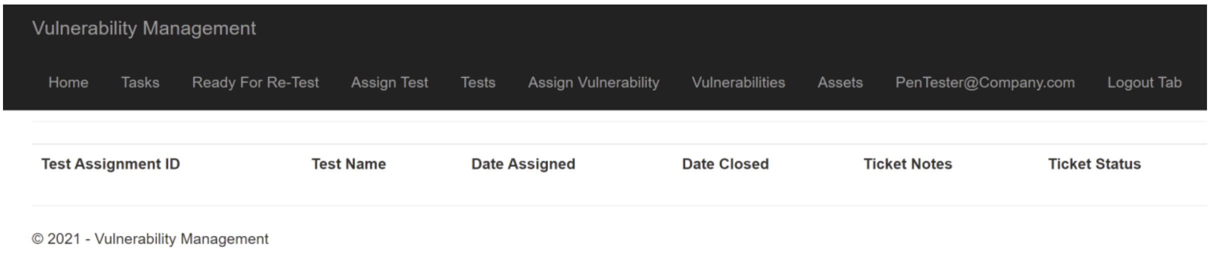


Tests

Test Name	Asset	Start Date	End Date	Sign Off Documents	URL	Description	Contact ID	Test Notes	Test Status	
Extremely Vulnerable Asset Test	0097 31-S222N	30/Apr/2021	30/Apr/2021	☑	Unavailable	Full scan is requested	Admin@Company.com	Closed Test	Closed	Edit | Details | Delete

© 2021 - Vulnerability Management

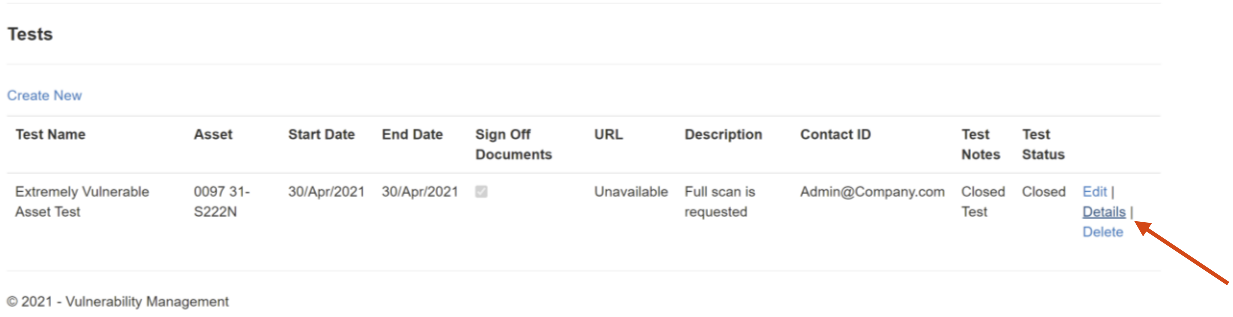
Tasks is empty:



Test Assignment ID	Test Name	Date Assigned	Date Closed	Ticket Notes	Ticket Status

© 2021 - Vulnerability Management

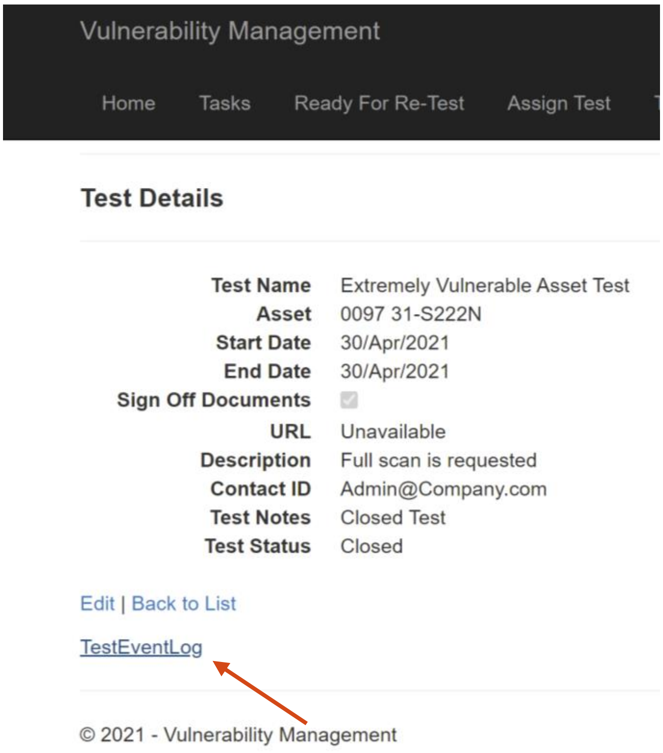
Only open assigned tests will display in the task box as per the individual they are assigned to. This will also log the event and the ticket information to the test event log and for each individual test there is functionality provided in the details of the individual test where there is a test event log button link which will display the full list of events in association with that particular test name. This can be found through the following links:



Tests

Test Name	Asset	Start Date	End Date	Sign Off Documents	URL	Description	Contact ID	Test Notes	Test Status	
Extremely Vulnerable Asset Test	0097 31-S222N	30/Apr/2021	30/Apr/2021	☑	Unavailable	Full scan is requested	Admin@Company.com	Closed Test	Closed	Edit | Details | Delete

© 2021 - Vulnerability Management

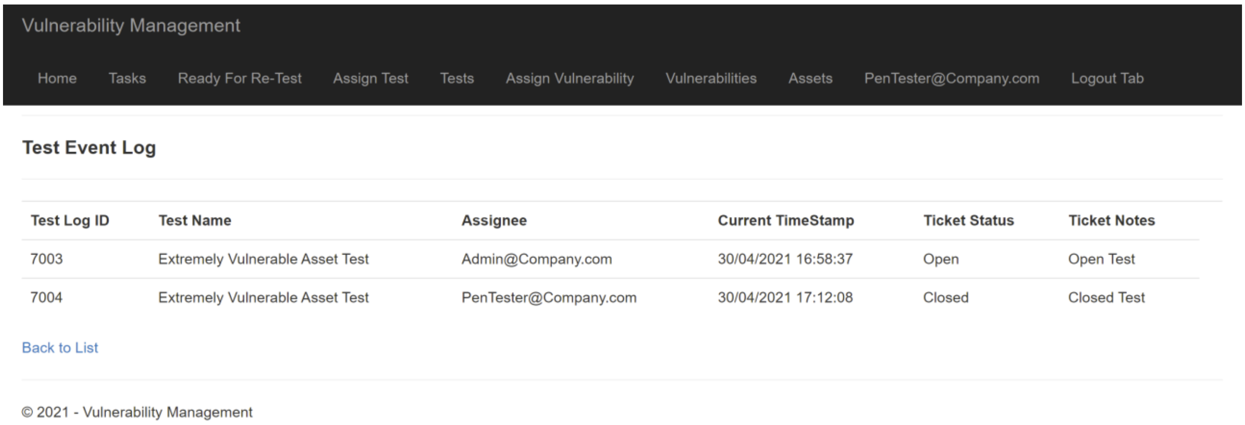


Test Details

Test Name	Extremely Vulnerable Asset Test
Asset	0097 31-S222N
Start Date	30/Apr/2021
End Date	30/Apr/2021
Sign Off Documents	☑
URL	Unavailable
Description	Full scan is requested
Contact ID	Admin@Company.com
Test Notes	Closed Test
Test Status	Closed

© 2021 - Vulnerability Management

The following is the full event log of the test from when it was assigned to the Penetration Tester to closed by the Penetration Tester:



Test Event Log

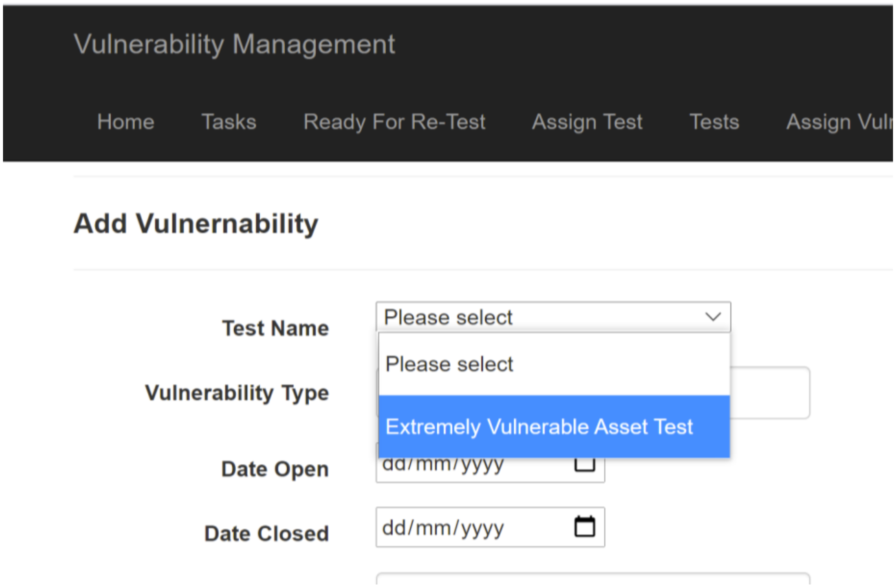
Test Log ID	Test Name	Assignee	Current TimeStamp	Ticket Status	Ticket Notes
7003	Extremely Vulnerable Asset Test	Admin@Company.com	30/04/2021 16:58:37	Open	Open Test
7004	Extremely Vulnerable Asset Test	PenTester@Company.com	30/04/2021 17:12:08	Closed	Closed Test

Back to List

© 2021 - Vulnerability Management

Here it can be seen for the test of 'Extremely Vulnerable Asset Test' when the action took place with the Time Stamp information, what action was performed with the Ticket Status and Ticket Notes and by whom with the Assignee information.

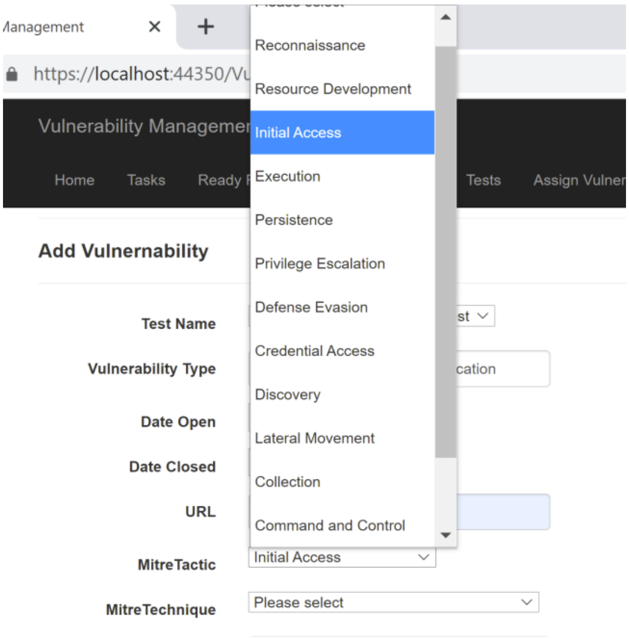
The Penetration Tester will then add if found a vulnerability or vulnerabilities to the application vulnerability system and each vulnerability added for that test will be linked to the test and asset it came from through ID's. Below shows in the add vulnerability interface the test names drop down list populates with all tests.



Add Vulnernability

Test Name: Please select
Please select
Extremely Vulnerable Asset Test
Vulnerability Type
Date Open: dd/mm/yyyy
Date Closed: dd/mm/yyyy

As mentioned earlier in the document I had used jQuery, Ajax and Javascript to perform the drop down of the Mitre Tactic and Technique information to provide mitigation advice. An example is below when Initial Access is chosen, the second drop down list of Techniques will populate with the Techniques relating to Initial Access:



Add Vulnerability

Test Name

Vulnerability Type

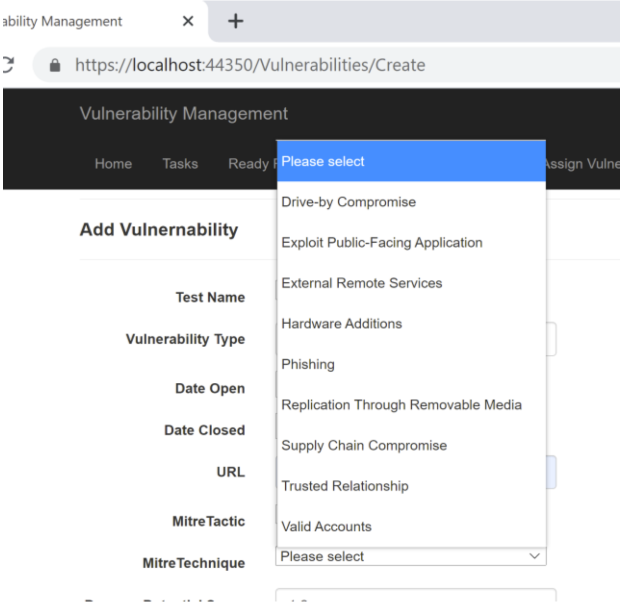
Date Open

Date Closed

URL

MitreTactic Initial Access

MitreTechnique Please select



Add Vulnerability

Test Name

Vulnerability Type

Date Open

Date Closed

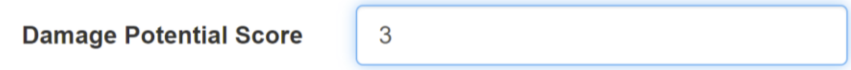
URL

MitreTactic

MitreTechnique Please select

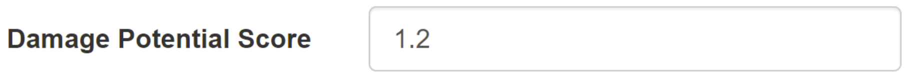
In the add vulnerability functionality, a DREAD matrix score must be added for each of the DREAD headings. Here I have created an automatic calculator which updates when the number is entered and calcutes the total when all headings are filled in. It works as follows:

A number is entered



Damage Potential Score 3

There are different calculations for each heading level. For Damage Potential Score the number entered is multiplied by 40% this is proven when the number automatically updates in the text box as follows:



Damage Potential Score	1.2

This calculation is performed for each of the remaining headings at the following rates:

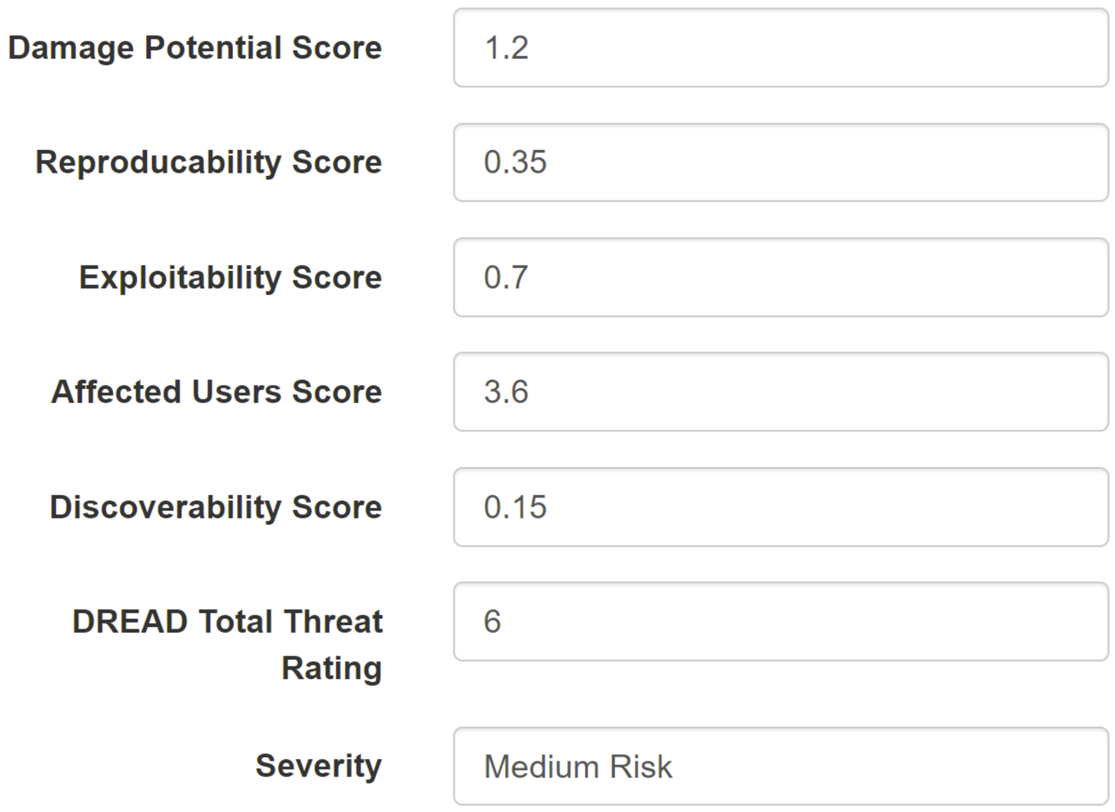
Reproducability * 5%

Exploitability * 10%

Affected Users * 40%

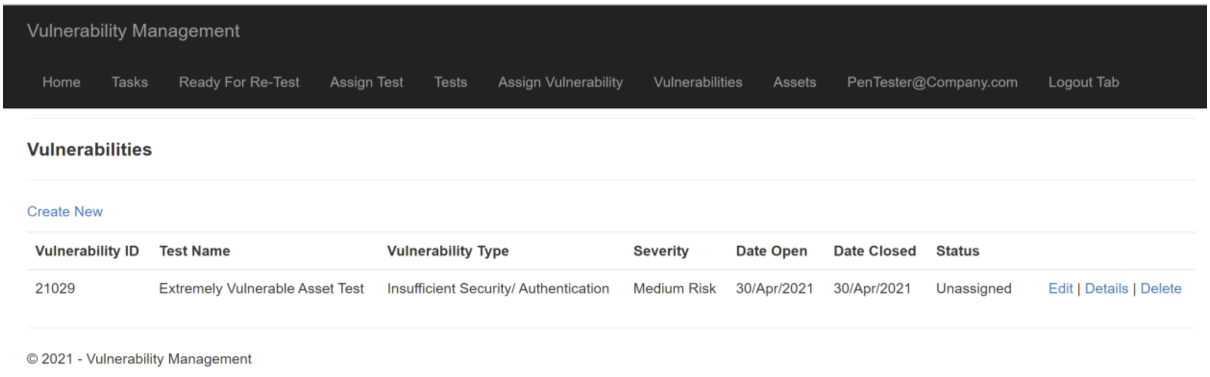
Discoverability * 5%

When I click the box for DREAD Total it automatically inserts the total and when I click Severity it automatically inserts the level of severity of the vulnerability in accordance to the score of the DREAD matrix:



Damage Potential Score	1.2
Reproducability Score	0.35
Exploitability Score	0.7
Affected Users Score	3.6
Discoverability Score	0.15
DREAD Total Threat Rating	6
Severity	Medium Risk

Vulnerability information from the ‘Extremely Vulnerable Asset Test’ added:



Vulnerabilities

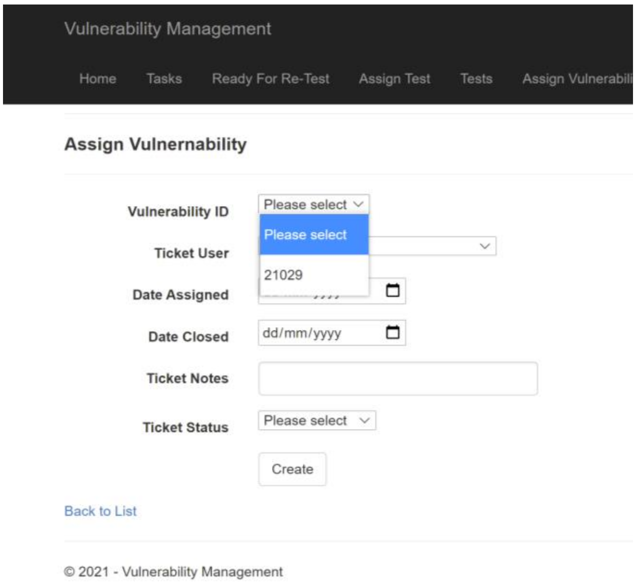
Create New

Vulnerability ID	Test Name	Vulnerability Type	Severity	Date Open	Date Closed	Status	
21029	Extremely Vulnerable Asset Test	Insufficient Security/ Authentication	Medium Risk	30/Apr/2021	30/Apr/2021	Unassigned	Edit | Details | Delete

© 2021 - Vulnerability Management

The Penetration Tester will then assign the found vulnerability to an on-site Security Engineer.

When Assigning the Vulnerability, the Vulnerability ID of the unassigned tests automatically populate in the drop down list:

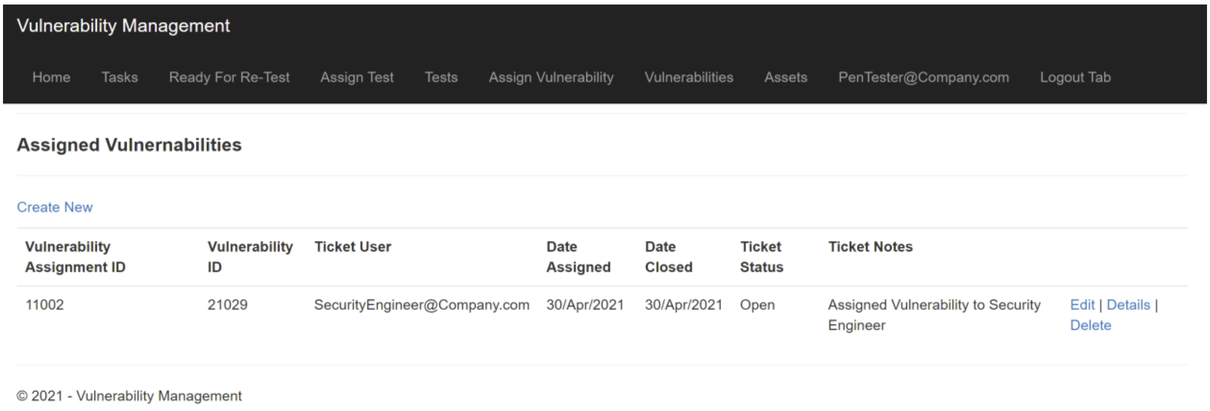


Assign Vulnernability

Vulnerability ID	Please select Please select 21029
Ticket User	
Date Assigned	
Date Closed	dd/mm/yyyy
Ticket Notes	
Ticket Status	Please select

© 2021 - Vulnerability Management

Assigned Vulnerability:



Assigned Vulnernabilities

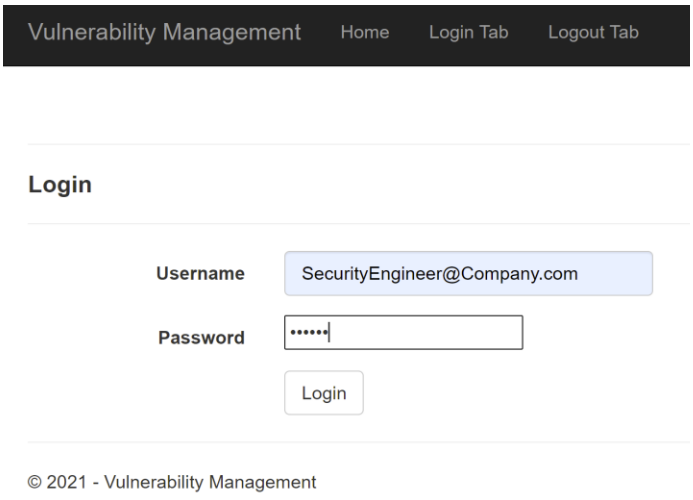
Create New

Vulnerability Assignment ID	Vulnerability ID	Ticket User	Date Assigned	Date Closed	Ticket Status	Ticket Notes	
11002	21029	SecurityEngineer@Company.com	30/Apr/2021	30/Apr/2021	Open	Assigned Vulnerability to Security Engineer	Edit | Details | Delete

© 2021 - Vulnerability Management

This vulnerability will then populate in the allocated Security Engineers task box and when they log in they will see they have been assigned the vulnerability.

Security Engineer logging in:



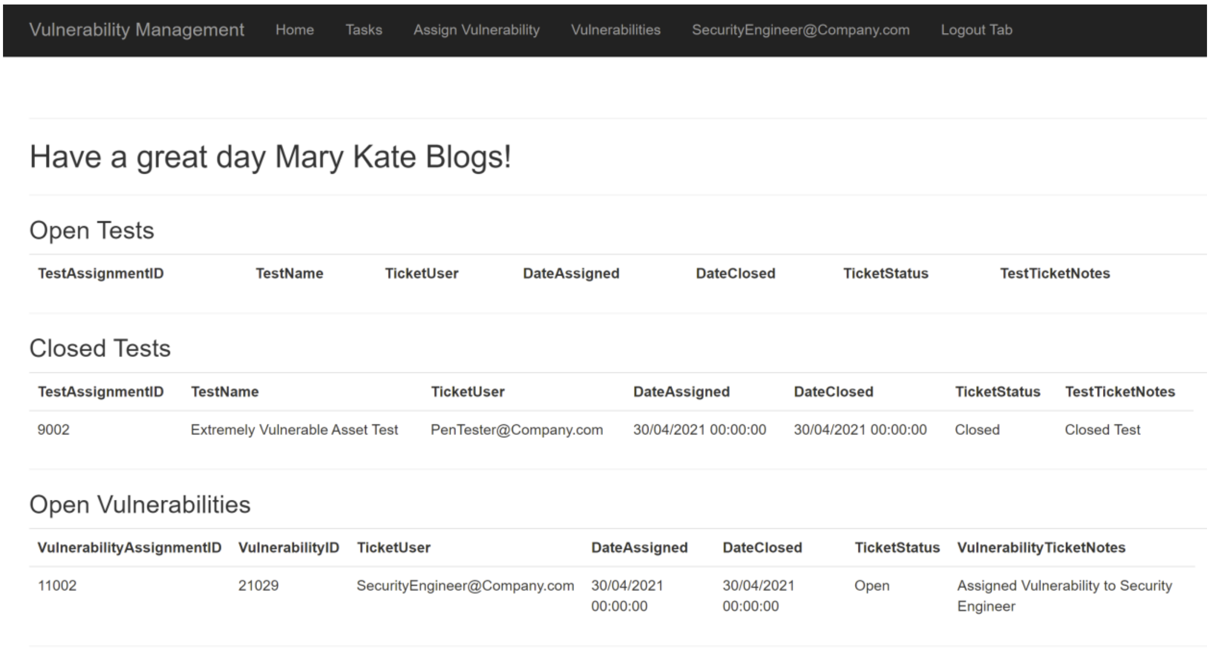
Login

Username: SecurityEngineer@Company.com

Password: ••••••

© 2021 - Vulnerability Management

When the Security Engineer logs in notice they have less privileges than the other roles, this can be seen in the nav bar links which appear as shown below, they have access only to their Tasks the Assigned Vulnerabilities and the Vulnerabilities:



Have a great day Mary Kate Blogs!

Open Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes

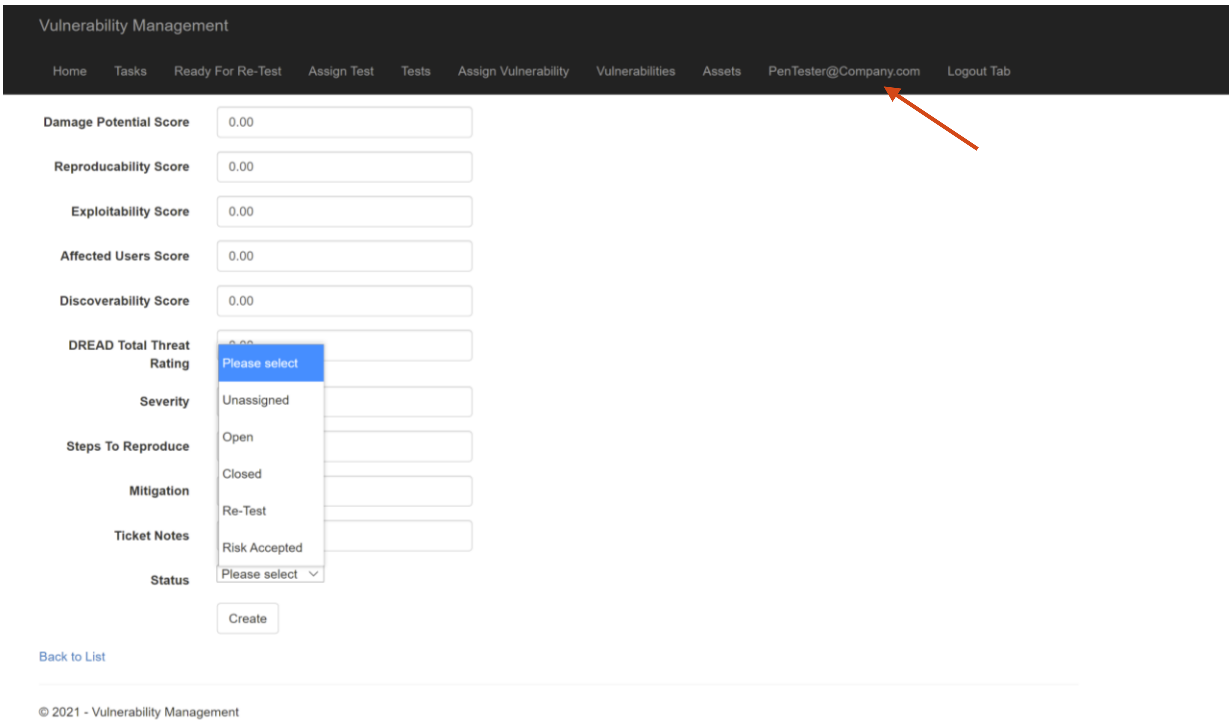
Closed Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes
9002	Extremely Vulnerable Asset Test	PenTester@Company.com	30/04/2021 00:00:00	30/04/2021 00:00:00	Closed	Closed Test

Open Vulnerabilities

VulnerabilityAssignmentID	VulnerabilityID	TicketUser	DateAssigned	DateClosed	TicketStatus	VulnerabilityTicketNotes
11002	21029	SecurityEngineer@Company.com	30/04/2021 00:00:00	30/04/2021 00:00:00	Open	Assigned Vulnerability to Security Engineer

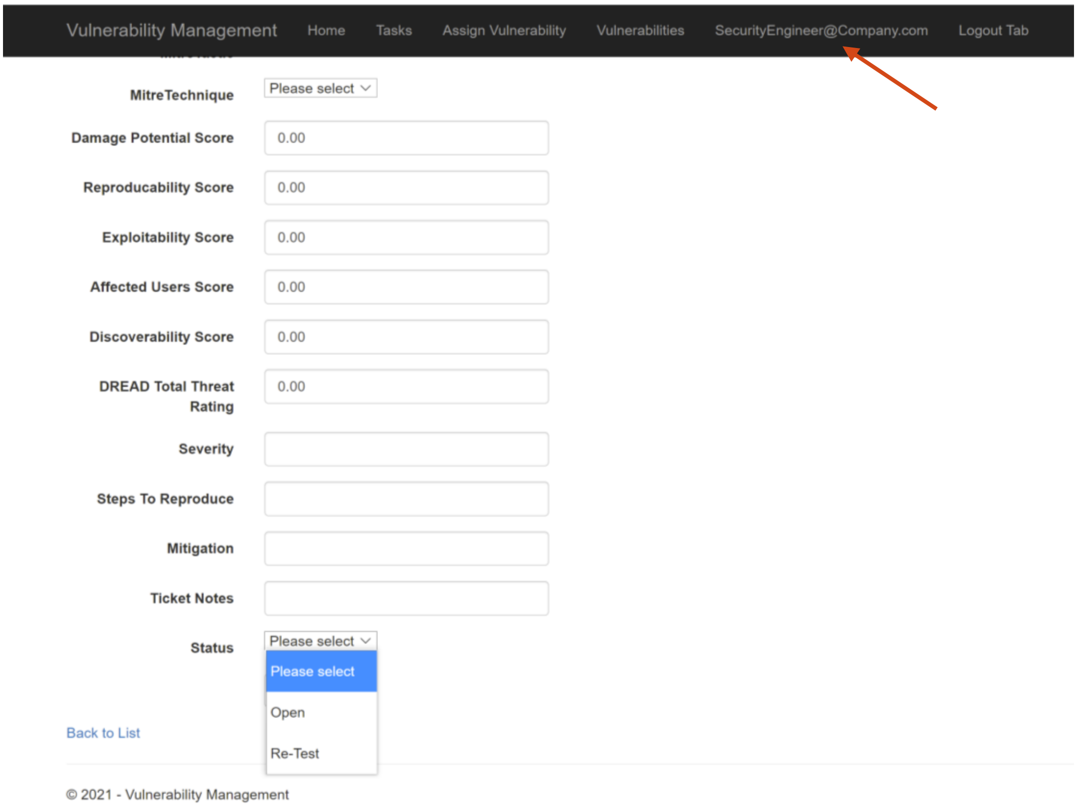
These privilege restrictions can be seen also when adding vulnerabilities, as the Penetration Tester is the only person allowed to set the vulnerability to closed the status drop down for the Penetration Tester is as follows in add vulnerability:



Damage Potential Score	0.00
Reproducability Score	0.00
Exploitability Score	0.00
Affected Users Score	0.00
Discoverability Score	0.00
DREAD Total Threat Rating	0.00
Severity	
Steps To Reproduce	
Mitigation	
Ticket Notes	
Status	Please select

© 2021 - Vulnerability Management

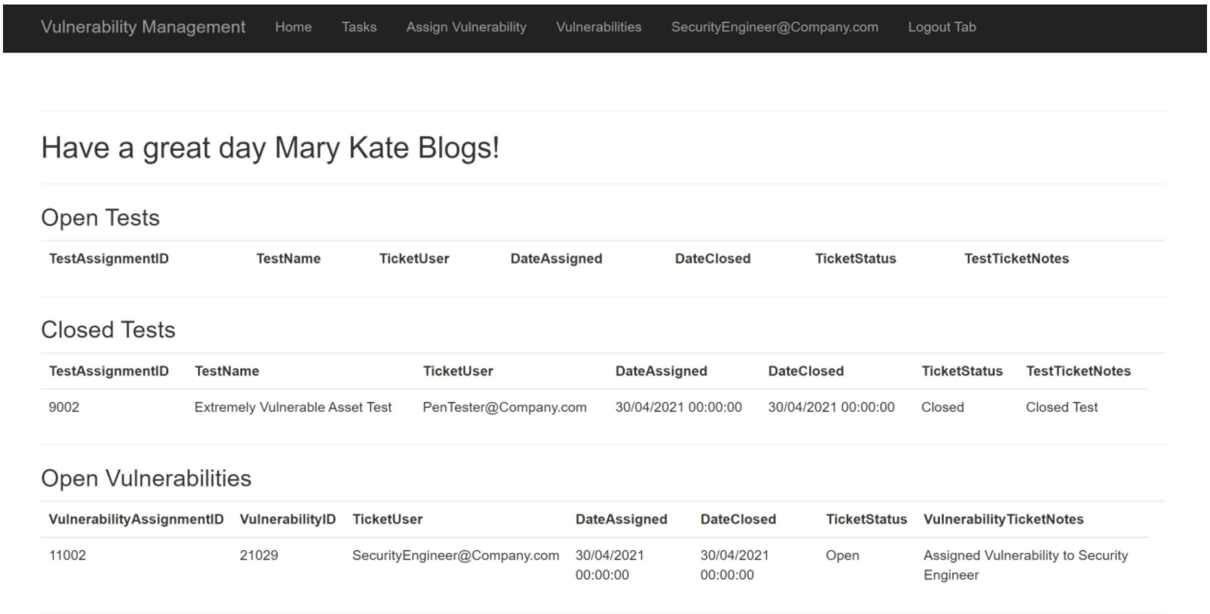
For the Security Engineer the status list is as follows:



MitreTechnique	Please select
Damage Potential Score	0.00
Reproducability Score	0.00
Exploitability Score	0.00
Affected Users Score	0.00
Discoverability Score	0.00
DREAD Total Threat Rating	0.00
Severity	
Steps To Reproduce	
Mitigation	
Ticket Notes	
Status	Please select

© 2021 - Vulnerability Management

Now when the Security Engineer is logged in the dashboard also displays the test from earlier as closed and the new vulnerability from above as it dynamically updates:



Have a great day Mary Kate Blogs!

Open Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes

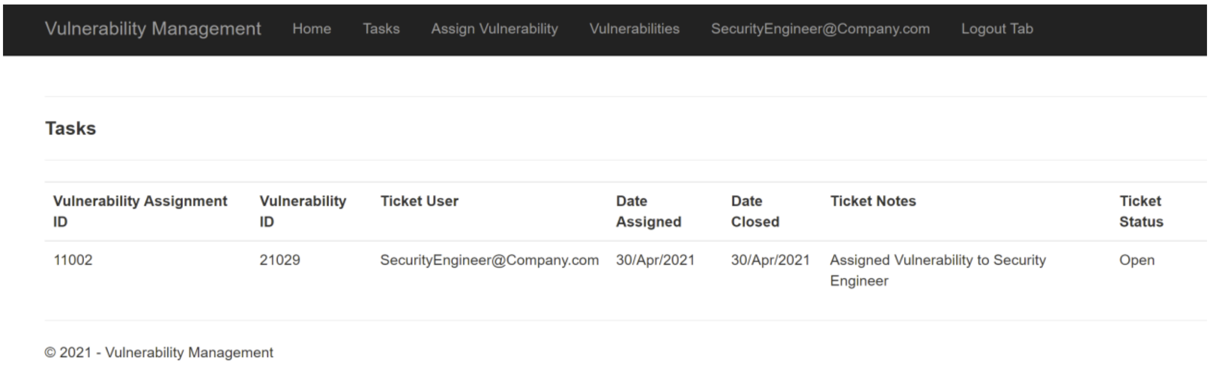
Closed Tests

TestAssignmentID	TestName	TicketUser	DateAssigned	DateClosed	TicketStatus	TestTicketNotes
9002	Extremely Vulnerable Asset Test	PenTester@Company.com	30/04/2021 00:00:00	30/04/2021 00:00:00	Closed	Closed Test

Open Vulnerabilities

VulnerabilityAssignmentID	VulnerabilityID	TicketUser	DateAssigned	DateClosed	TicketStatus	VulnerabilityTicketNotes
11002	21029	SecurityEngineer@Company.com	30/04/2021 00:00:00	30/04/2021 00:00:00	Open	Assigned Vulnerability to Security Engineer

The Security Engineer can now see the vulnerability has been assigned to them in their Tasks box:

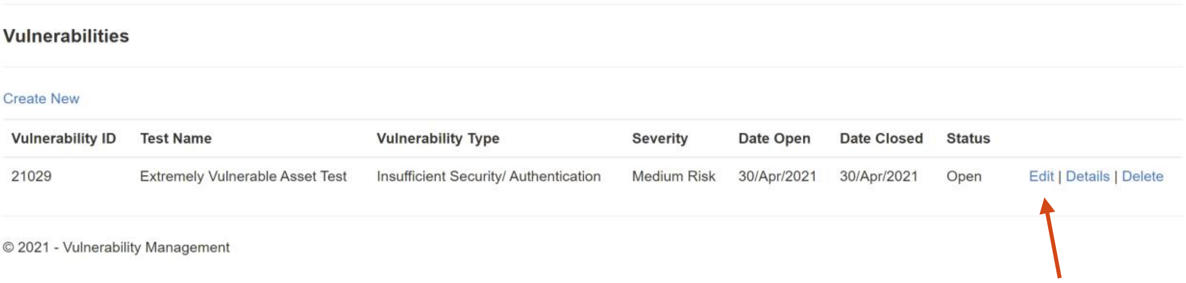


Tasks

Vulnerability Assignment ID	Vulnerability ID	Ticket User	Date Assigned	Date Closed	Ticket Notes	Ticket Status
11002	21029	SecurityEngineer@Company.com	30/Apr/2021	30/Apr/2021	Assigned Vulnerability to Security Engineer	Open

© 2021 - Vulnerability Management

The Security Engineer will then perform mitigation for the vulnerability and when complete they will edit the assigned vulnerability and set it to Re-Test and they do not have privileges to close off the vulnerability.



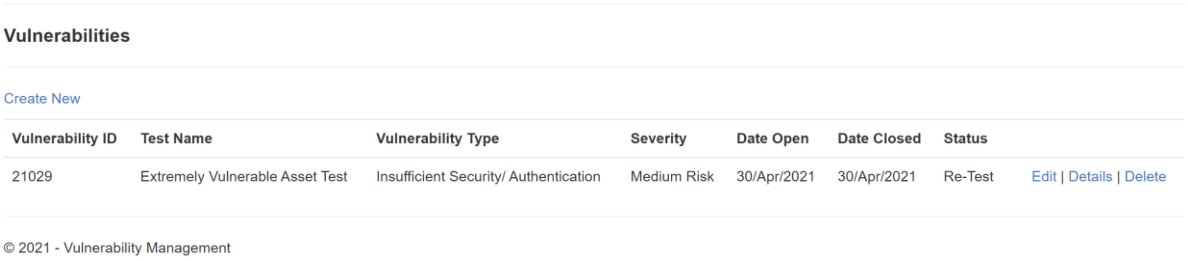
Vulnerabilities

Create New

Vulnerability ID	Test Name	Vulnerability Type	Severity	Date Open	Date Closed	Status	
21029	Extremely Vulnerable Asset Test	Insufficient Security/ Authentication	Medium Risk	30/Apr/2021	30/Apr/2021	Open	Edit | Details | Delete

© 2021 - Vulnerability Management

Vulnerability set to Re-Test



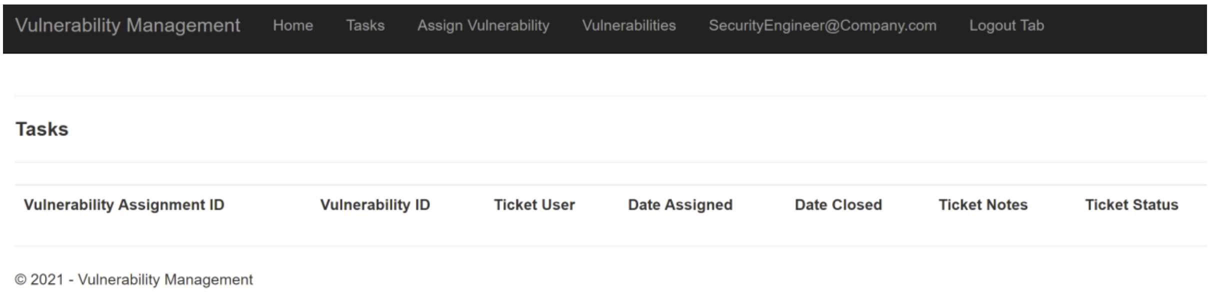
Vulnerabilities

Create New

Vulnerability ID	Test Name	Vulnerability Type	Severity	Date Open	Date Closed	Status	
21029	Extremely Vulnerable Asset Test	Insufficient Security/ Authentication	Medium Risk	30/Apr/2021	30/Apr/2021	Re-Test	Edit | Details | Delete

© 2021 - Vulnerability Management

The Tasks are now empty as the assignment on the Security Engineers part is complete

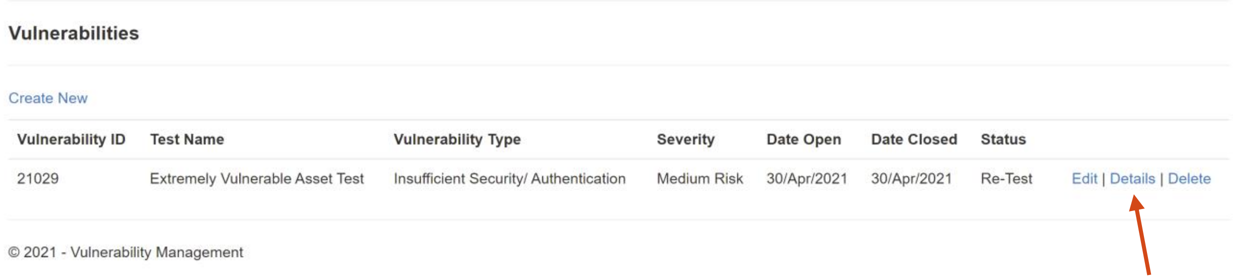


Tasks

Vulnerability Assignment ID	Vulnerability ID	Ticket User	Date Assigned	Date Closed	Ticket Notes	Ticket Status

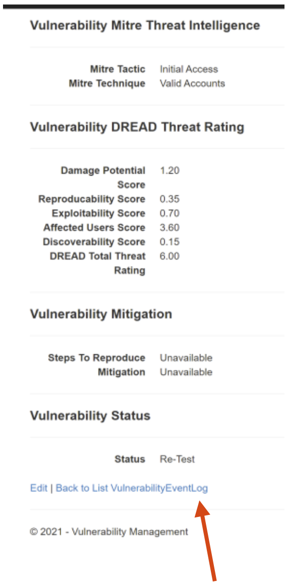
© 2021 - Vulnerability Management

The action performed by the Security Engineer and the associated ticket notes will be logged in this time the vulnerability event log and for each individual vulnerability the event log information can be found on the event log link within the details of the individual vulnerability as follows:


Vulnerabilities

Vulnerability ID	Test Name	Vulnerability Type	Severity	Date Open	Date Closed	Status	
21029	Extremely Vulnerable Asset Test	Insufficient Security/ Authentication	Medium Risk	30/Apr/2021	30/Apr/2021	Re-Test	Edit | Details | Delete

© 2021 - Vulnerability Management


Vulnerability Mitre Threat Intelligence

Mitre Tactic	Initial Access
Mitre Technique	Valid Accounts

Vulnerability DREAD Threat Rating

Damage Potential Score	1.20
Reproducability Score	0.35
Exploitability Score	0.70
Affected Users Score	3.60
Discoverability Score	0.15
DREAD Total Threat Rating	6.00

Vulnerability Mitigation

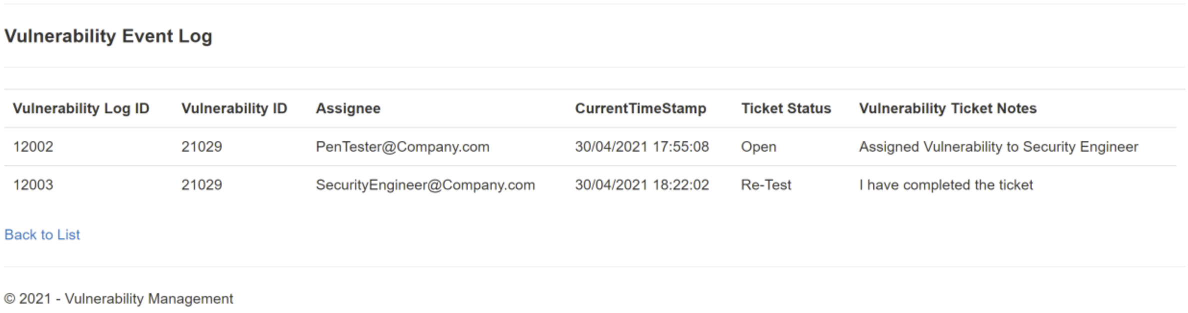
Steps To Reproduce	Unavailable
Mitigation	Unavailable

Vulnerability Status

Status	Re-Test

© 2021 - Vulnerability Management

Vulnerability Event Log for Vulnerability 21029:

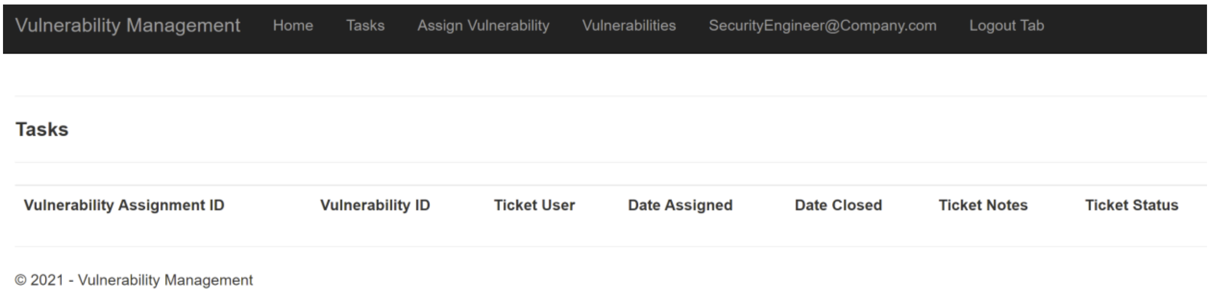


Vulnerability Event Log

Vulnerability Log ID	Vulnerability ID	Assignee	CurrentTimeStamp	Ticket Status	Vulnerability Ticket Notes
12002	21029	PenTester@Company.com	30/04/2021 17:55:08	Open	Assigned Vulnerability to Security Engineer
12003	21029	SecurityEngineer@Company.com	30/04/2021 18:22:02	Re-Test	I have completed the ticket

© 2021 - Vulnerability Management

When set to Re-Test status the assigned vulnerability will no longer be shown in the Security Engineers Tasks box as they have completed their duty. Only open assigned vulnerabilities will display in the task box as per the individual they are assigned to.

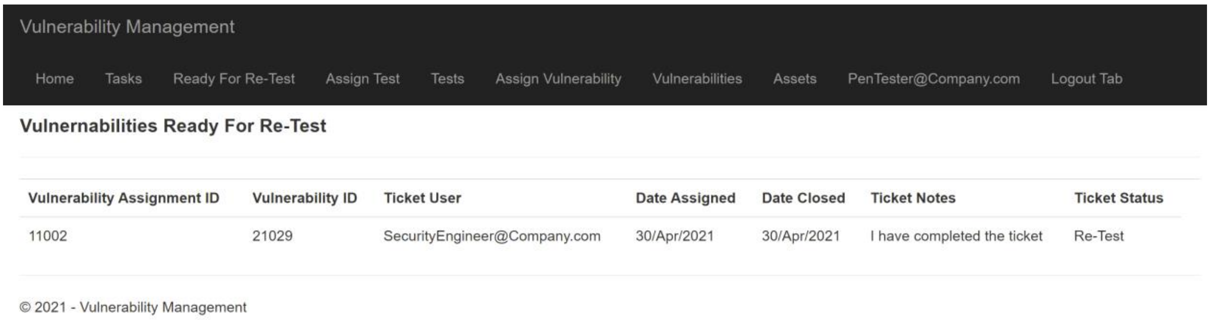


Tasks

Vulnerability Assignment ID	Vulnerability ID	Ticket User	Date Assigned	Date Closed	Ticket Notes	Ticket Status

© 2021 - Vulnerability Management

The Penetration Tester also has a task box for vulnerabilities which are set to Re-Test as they will have to be re-tested any vulnerabilities to make sure they are completely securely mitigated before setting their status to closed. The following is the Penetration Testers Task box after they log in:

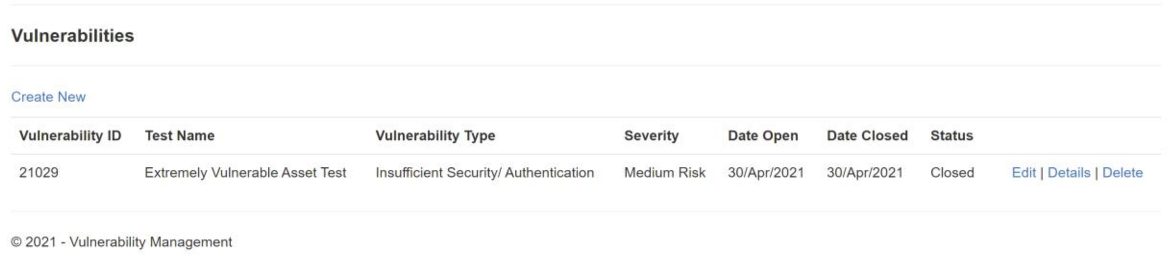


Vulnernabilities Ready For Re-Test

Vulnerability Assignment ID	Vulnerability ID	Ticket User	Date Assigned	Date Closed	Ticket Notes	Ticket Status
11002	21029	SecurityEngineer@Company.com	30/Apr/2021	30/Apr/2021	I have completed the ticket	Re-Test

© 2021 - Vulnerability Management

The Penetration Tester will then Re-test the vulnerability and either re- assign the vulnerability to the Security Engineer if it is not completely mitigated or more vulnerabilities have arisen within it, or they will set the vulnerability to closed, or if the severity is not of worry they will set the Vulnerability to Risk Accepted. The following is the Vulnerability Edited by the Penetration Tester and set to Closed:



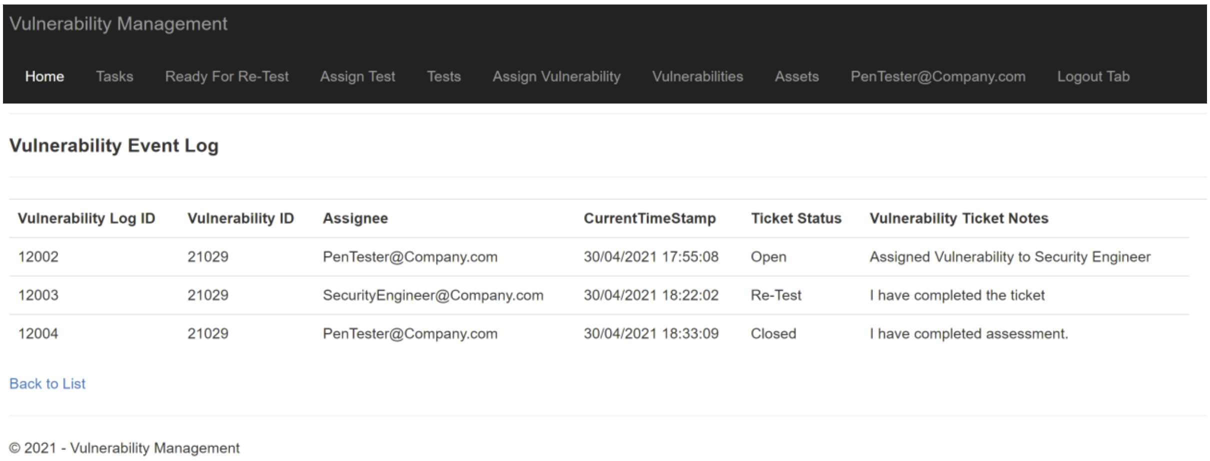
Vulnerabilities

Create New

Vulnerability ID	Test Name	Vulnerability Type	Severity	Date Open	Date Closed	Status	
21029	Extremely Vulnerable Asset Test	Insufficient Security/ Authentication	Medium Risk	30/Apr/2021	30/Apr/2021	Closed	Edit | Details | Delete

© 2021 - Vulnerability Management

This information and the ticket event notes will be updated in the event log and can be found in the individual vulnerabilities event log link as below:



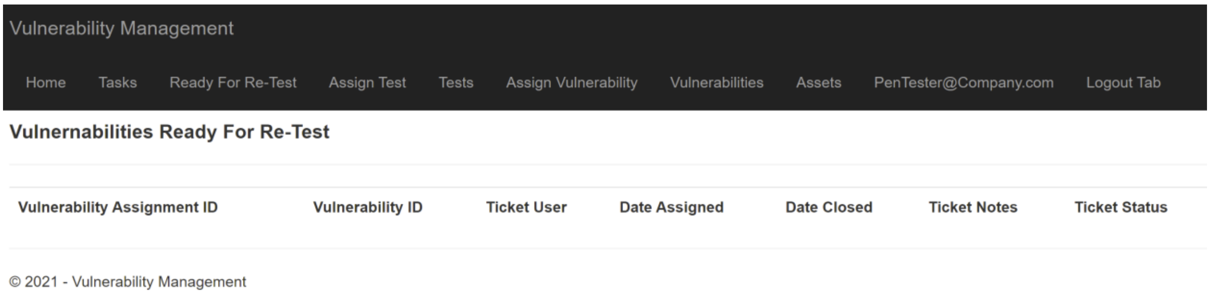
Vulnerability Event Log

Vulnerability Log ID	Vulnerability ID	Assignee	CurrentTimeStamp	Ticket Status	Vulnerability Ticket Notes
12002	21029	PenTester@Company.com	30/04/2021 17:55:08	Open	Assigned Vulnerability to Security Engineer
12003	21029	SecurityEngineer@Company.com	30/04/2021 18:22:02	Re-Test	I have completed the ticket
12004	21029	PenTester@Company.com	30/04/2021 18:33:09	Closed	I have completed assessment.

Back to List

© 2021 - Vulnerability Management

When the status of the vulnerability is changed from Re-Test it is updated to its set status and will no longer be present in the Ready for Re-Test task box.



Vulnernabilities Ready For Re-Test

Vulnerability Assignment ID	Vulnerability ID	Ticket User	Date Assigned	Date Closed	Ticket Notes	Ticket Status

© 2021 - Vulnerability Management

This is the full vulnerability management cycle within the application flow which conveys how each event is logged in the cycle and how the management system is handled, historically tracking every step of the test, vulnerability and mitigation process to provide an in depth vulnerability management solution.

Comparison to Original Design and Specification

Vulnerability Management had developed significantly during implementation and design. Originally the project was meant to be a desktop application however the more it was discussed I had decided with my tutor that the project would be better as a web application, as the pros outweighed the cons and it was a platform which would provide much more accessibility should the application be placed into production.

Further into Development there were changes with the way the system would be designed and developed. Originally the application was going to be an asp.net application however I felt this would not suit the data and the system that was going to be implemented. Through research I had found the Model View Controller framework and although this had proven to be significantly more challenging in implementation, it turned out to be a much better fit for separation of the data.

As the project grew significantly in depth in the production process and more realizations about how for example the vulnerability event log or the vulnerability assignments and updating everything dynamically would work, the database has grown and changed significantly compared to the original plan.

The project ideas also grew in development, I had wanted to incorporate threat intelligence into the application and decided incorporating the MITRE tactic and techniques information would be a complimentary addition to the vulnerability mitigation. The idea of the vulnerability severity calculation through the DREAD matrix was also discovered in the development process. Each of these additions provide the platform and the vulnerabilities with a more textural in depth vulnerability intelligence using frameworks which are already being used in enterprises globally today.

Learning Outcomes

The opportunity to partake and develop this project has been an invaluable journey. Developing the project has allowed me to flourish my software development capabilities. During this project several new languages were learned and others further expanded on. I wanted to push my development skills when creating this project and take on the challenge of MVC, C#, JavaScript, jQuery, Ajax and advanced SQL.

Technology Learning Outcomes

Developing the project has instilled a completely new mindset regarding software development in me. Initially development would not have been my strongest point and through research, applying knowledge and repeatedly trying my own solutions, I have grown a vast interest in the subject. Learning the MVC framework allowed me to push my boundaries with development. On multiple occasions I found myself engrossed in the complexity of its theory. Further into development watching the data as it flowed through the application from data access objects capturing data in the database which flows through functions to be stored into models and weaving that back into controllers and forward to views really made me appreciate value in that last piece of data that arrived at the screen. Learning about the path that data takes allowed me to combine that knowledge with the research I had been partaking regarding vulnerability management and that cycle of data too, enabling me to combine both areas into one and create a final product which delves into the depth of vulnerability management data.

Personal Outcomes

Creating a system which handles a significant process has taught me hugely about managing my own system of carrying out a process. In my final year I had spent the majority of my time either on college work or work, I had found any spare time I had, even at work on a lunch break I would be watching a video on how to code something or trying to figure out how something works so I was ready to go for the next challenge that arose. I had learned how to optimize time and make the most of the value in every minute. Developing the project has allowed me to believe that anything is possible with perseverance, enthusiasm and the willingness to learn.

Achievement Review

Vulnerability Management had successfully reached all functionality that it was set to achieve in the original speculation. The following are the items in the speculation:

	Description
Achieved	A tool that captures the attributes of validated vulnerabilities by a penetration tester and manages the process and timeline of each vulnerability within an organisation.
Achieved	Provide a management interface to facilitate all aspects of vulnerability management for an organisation.
Achieved	The capture and management of vulnerability data through its lifecycle.
Achieved	A GUI that allows users to store all attributes of vulnerabilities and provide a dashboard displaying the current security status of an organisation.
Achieved	App runs across multiple platforms (Android, PC, Mac)
Achieved	System contains management software to allow for multiple users.
Achieved	Relevant and useful information is extracted from the raw data and shown in a user friendly manner.

Acknowledgements

I would like to sincerely thank my supervisor Richard Butler whose continual support, guidance, enthusiasm, expertise, energy and advice has been invaluable to the development and creation of this project at every step of the process. Additionally I would like to thank all other lecturers who had provided insight, advice and feedback during various stages of the project development. I would like to thank all my lecturers over my four years at IT Carlow, who have been so supportive and kind since first year making me become the best student I could be, their efforts, support and assistance has been greatly appreciated. Finally I would like to thank my family and friends especially Katie, Hazel and Sarah for their friendship, support, feedback and pushing me to do my best throughout the development process and the college years.

Plagiarism Declaration

I declare that all material in this submission is entirely my own work except where duly acknowledged. I have cited the sources of all quotations, paraphrases, summaries of information, tables, diagrams or other material; including software and other electronic media in which intellectual property rights may reside. I have provided a complete bibliography of all works and sources used in the preparation of this submission. I understand that failure to comply with the Institute's regulations governing plagiarism constitute a serious offence.

Student Name: Síne Doheny

Student Number: C00226237

Signature: Síne Doheny

Date: 30/04/2021