|  |
| --- |
|  |
| Testing Documentation |
| Men’s Shed Web Application - 2023 |

|  |
| --- |
| SOC09109 2022-3 TR2 001 - Group Project |

Contents

[Testing Overview 2](#_Toc133234054)

[Functionality Testing 3](#_Toc133234055)

[User Experience Testing 5](#_Toc133234056)

[Site Visitor 5](#_Toc133234057)

[Standard Member 6](#_Toc133234058)

[Heightened-Risk Member 6](#_Toc133234059)

[Administrator 6](#_Toc133234060)

[Security Testing 7](#_Toc133234061)

[Checklist 7](#_Toc133234062)

[Vulnerability Scan 8](#_Toc133234063)

[Nikto Scan 8](#_Toc133234064)

[Nmap 9](#_Toc133234065)

[Dynamic Testing 10](#_Toc133234066)

[Remediation Log 10](#_Toc133234067)

# Testing Overview

The Men’s Shed web application will need to undergo thorough testing approached from several different angles in order to ensure that it provides the requested functionality, performs as expected and satisfies the requested requirements before being presented to the client. Evaluating the application from different angles will maximise the chance of spotting errors/flaws that can be addressed so that the final application is of good quality.

The testing phase will therefore contain the following objectives:

* **Functionality/Stress Testing** **–** Does the application provide the desired/requested functionality as agreed with the client? How will the application handle unexpected input/user behaviour?
* **User Experience Testing** **–** From the perspective of a user, how does the application perform/will the application be suitable for the desired target user? This will include evaluating the application as a standard user and from the administrator’s point of view as they use the application.
* **Security Testing** **–** From the perspective of a threat actor, are there any obvious security issues that stand out? Does the product contain the necessary safeguards to protect user personal information? Can the application be exploited or used as a platform to deliver exploits?
* **Remediation Phase –** Any issues or bugs that are identified during the testing will be addressed and removed/fixed.

**Note – The test build was deployed using PythonAnywhere, it was pointed out to me before testing that there may be some issues with this particular platform.**

# Functionality Testing

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Area** | **Expected Result** | **Actual Result** | **Actions Required (Moving Forward)** |
| Resource database | Categorised, populated, searchable, safety/PPE requirement.  Availability, training required, restricted view. | Database skeleton is in-place, appropriate categories, item classifications are in place with a Boolean value.  Tool Database is populated at least partially, searching requires input, images are currently not displayed in the test version.  Books and board games libraries are currently not populated. | Book and board game libraries need populated.  Images of the tools could be displayed and scrolled through as thumbnails in addition to an input search.  A little extra spacing between search result headings to accommodate longer entries and enhance readability. |
| User system | User classification – standard / admin.  User restricted view permission, user creation and detail storage.  Admin management section. | User admin classification is working as a Boolean value.  Users have a Boolean value to allow/hide restricted items as well as a training done Boolean.  User login function operational. User signup page contains all necessary inputs, new user creation is operational.  User sign-in with created accounts was not currently operational. | Admin management section still to be implemented.  Created user sign-in needs to be completed. |
| Booking System | Member ability to view available tools, select and book available tools in timeslots.  Tracked log of booking history. | Booking page visible to logged in member (test admin).  Booking form is implemented with suitable input fields.  A log skeleton was visible when logged in as the test admin user.  Booking functionality was currently not operational when evaluated. **(I have been advised this is an issue with the test deployment environment)** | Booking functionality needs to be completed.  **(Due to test environment issues, this functionality will need to be re-assessed after the next development/testing cycle)**  Log implementation needs to be done and checked alongside functionality implementation. |
| Contact and Support  Functionality | Working, easy to use links to further MS pages.  Operational contact page for members + non-members to receive support. | Working links to the Men’s Shed social media and phone/email are provided in the footer.  A support page is implemented that provides phone details, meeting details and a user form to submit questions to the team.  Support page is submitting information however this is not currently manageable or visible to the logged in test admin. | Support request functionality could be implemented when the admin management features are added. |

# User Experience Testing

## Site Visitor

**From the viewpoint of a site visitor with no prior user account.**

Upon landing on the homepage, the initial impression is that it is a little bare content-wise. This is something that would be improved with further iterations of development but was worth mentioning.

The navigation is clear so there is no trouble moving through the site pages for even the most basic of web user, however the navigation positioning does stand out as being off-centre at larger screen widths.

\*(**Interestingly, this off-centre positioning appears as slightly too far right on 24” displays and reverses to just off-left on 27” screens.)**

The navigation displays clearly on smaller screen sizes and collapses into a toggle menu on the smallest of screens. As a visitor unfamiliar with this site or not particularly web experienced, it may be difficult to work out where the navigation is at smallest screens. This is due to the navbar colour and lack of contrast with the nav button.

Although the menu button has a useful hover fill effect, on a mobile screen this may be confusing at first due to most mobile user’s not using a pointer input device. These potential issues are only applicable to visitors and members unfamiliar with the site, after use this is not an issue.

The initial hero banner does grab attention when first landing on the site and provides some movement/interactivity, the white text however on the first background image does make it shine a little/harder to make out clearly, but this is minimal.

The about page provides good images of the local area and provides good background information that a visitor would find useful, as a potential member or interested party this page is easy to read and find out more about the committee of this particular shed group. The committee members about-text was informative but there was a typo in the section about Mike Rowlinson.

**\*(Nobody is immune to typos however they have quite a significant impact on the impression and experience of the reader and should be rectified before going live.)**

Two of the committee members images did not load on the test visit.

**\*(This could very possibly be an issue with the test environment but needs investigating.)**

As a visitor without a logged in account, the only pages available to navigate to are the landing page, about page and support page to contact, this is the ideal scenario.

Full social media navigation buttons available on the footer are beneficial to a visitor who may be interested in learning more about the organisation.

The support and signup pages are clear and easy to use, they provide the visitor with everything they need.

**Notes - \*Useful or interesting observations for the team made while testing as a user, but not necessarily something a user would notice or care about.**

## Standard Member

While the ability to create a new standard member appears functional, I was unable to login with my newly created user.

**\*(This may be due to the development platform or newly created users requiring manual admin approval before becoming active, regardless it is not possible to evaluate the experience from this point of view at the current build due to the admin management portal still being in development.)**

## Heightened-Risk Member

Similarly with the standard member, this user account was not available for evaluation at this time.

**\*(There is groundwork laid out for assigning this member classification in the database code).**

## Administrator

Upon logging in as the test admin account, three additional navigation tabs are available. The booking tab and resource library tab should also be available to the logged in standard and heightened risk members \***(was unable to verify this)**.

The admin tab is currently a placeholder with no options, after future development this will contain the admin management controls for the app.

# Security Testing

## Checklist

|  |  |
| --- | --- |
| The application enforces HTTPS | Not at application level - The application has not arrived at the required stage to implement this correctly. This should be re-evaluated after future development-testing cycles. |
| Passwords are stored hashed with acceptable algorithm | Yes – Bcrypt was implemented by the team to provide user password hashing. |
| Input validation in-play | Partially – There appears to be some native input validation on the choices the team made to develop the app, or the host of the test deployment is providing this.  There is limited input validation on user signup fields as I can successfully sign-up with any information as well as pass any inputs in, however the login fields are enforcing strict validation on case-sensitivity, requiring exact matches to accepted entries.  There is no password policy enforcement on user signup. **This is something that needs to be implemented in future development-testing cycles.**  This check is hard to accurately assess as the test input fields are resistant to common SQL injection inputs, despite no clear evidence of deliberate defence against them, the test host environment may be providing protection that was not written in by the team by using current and updated infrastructure. |
| Member information stored is encrypted | N/A – At this stage of the app development. |
| Administrator has access to user log data | Not currently – Admin management features have not made it in the limited development cycle the team had this time around. **Future work on the project should address this.** |
| User password policy is enforced | No – **As previously mentioned this will need to be implemented in future development.** |

## Vulnerability Scan

**NOTE – Due to the unfinished nature of the application and the legalities surrounding scanning infrastructure that is owned and hosted on a public server without the owner’s permission, scanning is as far as the security testing can proceed at this stage of the development and is already skirting the grey area.**

**NOTE – Due to the test environment not being like the final deployment environment (if at all), the results of these scans should be taken as informational moving forward.**

**Vulnerability scanning and especially dynamic testing will need to be re-done completely once the application is deployed on its intended infrastructure and before it goes live.**

### Nikto Scan

Text

Description automatically generated

Figure - Nikto Vulnerability Scan

As can be seen from the screenshot the scanner managed to gather some information before it reached an error limit and terminated. **(I suspect that the scanning was detected and blocked as Nikto is a very loud tool, this would be due to security on the public network).**

In this deployment on the python anywhere server, the scan has identified the lack of specific security headers that identify a possible attack vector. Secure headers were mentioned in the security considerations section of the PIR. **(During future development, these security headers could be implemented per html page to mitigate this risk once the basic functionality is complete).**

The clacks overhead message is something of an easter egg, it is a header that contains a tribute to Terry Pratchett and serves no other purpose than to exist.

This was as far as Nikto managed to get before getting stonewalled and this should not be pushed further **(for legality purposes)**, however by simply entering the domain name it managed to pull the server IP and identify the header vulnerabilities.

### Nmap

Text

Description automatically generated

As can be seen from this simple nmap scan, there is a huge array of open ports on this deployment and I terminated this scan very quickly, there was a lot more to come.

\***(This is not unusual as this is a public server)**

This scan simply provides the port number and protocol for the server IP and shows the huge potential for exploring attack vectors, more aggressive scanning could be done to try and determine more information about each of the open ports and server software, however this cannot be done on the current test deployment. \***(This absolutely should be done if the deployed app is being hosted on owned infrastructure and could be explored by future development teams)**

## Dynamic Testing

As mentioned previously, dynamic testing cannot be explored currently as the server and network infrastructure is public.

# Remediation Log

**Due to the limited time available left and the iterative nature of the project, the remediation log will consist of only the errors spotted in the work we have done already.**

**The list of pressing issues that needs attention will be shared with the team in the teams channel.**