TESTING AND EVALUATION REPORT

AEGIS SHIELD - PHISHING DETECTION EXTENSION

Sudam Pullaperuma	- 10660248
Tharuka Gunasekara	- 10659483
Tanushka Elvitigala	- 10663914
Dulaj Walgama	- 10659489

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INRODUCTION

The **Aegis Shield - Phishing Detection Extension** is a cutting-edge browser extension designed to safeguard users against phishing attacks and malware threats in real time. This extension incorporates a suite of advanced features, including real-time URL monitoring, machine learning-based phishing detection, and integration with services like VirusTotal for malware analysis. With the growing risks posed by cyber threats, the extension aims to provide a robust, user-friendly solution that enhances browsing security and protects users from potentially harmful online activities.

This **Testing and Evaluation Report** documents the iterative testing process undertaken to ensure the extension's functionality, reliability, and overall performance. Each version of the extension was rigorously evaluated using structured test cases and scenarios, with the results forming the basis for continuous improvement.

The primary objectives of this report are to:

1. **Validate Functionality**: Ensure all implemented features operate as intended under various scenarios.
2. **Identify Limitations**: Highlight challenges or issues discovered during testing and provide actionable recommendations for improvement.
3. **Measure Progress**: Document the iterative improvements achieved across multiple versions of the extension.
4. **Ensure Compliance**: Verify that the extension adheres to the security and usability standards outlined in the project proposal.

The testing process was conducted in four distinct phases, aligned with the project's development milestones:

1. **Version 1 Testing**:
   - Conducted on **December 7, 2024**, focusing on six core features implemented by that date.
   - A total of **36 test scenarios** were evaluated, identifying several areas for improvement.
2. **Version 2 Testing**:
   - Conducted on **December 27, 2024**, after expanding the extension to include 12 features.
   - **61 test scenarios** were performed to assess both the new and existing features.

3. **Version 3 Testing**:
   - Conducted on **January 15, 2025**, evaluating the fully developed extension.
   - An additional **61 test scenarios** validated the refinements and integrations achieved across all 12 features.
4. **Version 4 Testing**:
   - Conducted on **January 20, 2025**, as the final phase.
   - All 12 features were comprehensively tested, ensuring readiness for deployment.

This report presents a comprehensive account of the testing phases, outcomes, and limitations identified during the evaluation of the Aegis Shield - Phishing Detection Extension. By highlighting key achievements and challenges, the report underscores the team's commitment to delivering a robust, user-friendly, and reliable solution for phishing and malware protection.

2.0 TESTING METHODOLOGY

The testing methodology for the Aegis Shield - Phishing Detection Extension was carefully designed to ensure thorough evaluation and continuous improvement of the extension. The process was iterative and conducted in alignment with the development phases, focusing on rigorous white-box testing to validate the internal functionality, logic, and overall performance of the system.

The primary testing approach employed was **white-box testing**, which provided insights into the extension's internal structure and functionality. This methodology allowed the team to:

- Validate the code logic and structure for each feature.
- Test the flow and integration of individual components.
- Identify and address edge cases and potential failure scenarios. By leveraging this approach, the team ensured robust feature implementation and seamless integration between components.

2.1 TESTING PHASES

The testing process for the Aegis Shield - Phishing Detection Extension was conducted in four distinct phases, each aligned with specific milestones in the development process. This iterative approach ensured that each version of the extension was rigorously evaluated, and identified issues were addressed in subsequent iterations. Below is a detailed breakdown of the testing phases:

First Testing Phase: December 7, 2024

- **Scope**:
    - Focused on six core features developed by December 7, 2024.
    - Features included Real-Time URL Monitoring, Phishing URL Detection, Whitelist/Blacklist Management, Email Phishing Detection, User-Friendly Interface, and Multi-Browser Compatibility.
- **Outcome**:
    - Identified issues such as URL monitoring inconsistencies, limited browser compatibility, and interface usability challenges.
    - These insights formed the foundation for subsequent development and testing.

Second Testing Phase: December 27, 2024

- **Scope**:
    - Evaluated 12 features, including the six initial ones and newly added features such as Basic Malware Detection, Browser Notifications, Basic User Alerts, Advanced Machine Learning for Phishing Detection, Sandbox Integration for File Analysis, and Severity-Based Alerts.

- **Outcome**:
  - Significant progress was observed, with newly developed features such as Browser Notifications and Basic User Alerts achieving a 100% success rate.
  - Persistent issues in areas like Multi-Browser Compatibility and Severity-Based Alerts were noted for further refinement.

Third Testing Phase: January 15, 2025

- **Scope**:
  - Focused on re-evaluating all 12 features to assess overall functionality, performance, and reliability.
- **Outcome**:
  - Notable improvements in Real-Time URL Monitoring (88% success rate) and User-Friendly Interface (83% success rate).
  - Persistent challenges in Multi-Browser Compatibility and Severity-Based Alerts remained areas for further optimization.

Fourth Testing Phase: January 20, 2025

- **Scope**:
  - Final phase evaluated all 12 features, integrating feedback and refinements from prior phases.
- **Outcome**:
  - Several features, including Phishing URL Detection, Basic Malware Detection, and Browser Notifications, achieved a perfect 100% success rate.
  - Persistent issues in Severity-Based Alerts and Multi-Browser Compatibility were identified as areas for continued enhancement.
  - This phase marked the culmination of iterative improvements, validating the extension’s readiness for practical application.

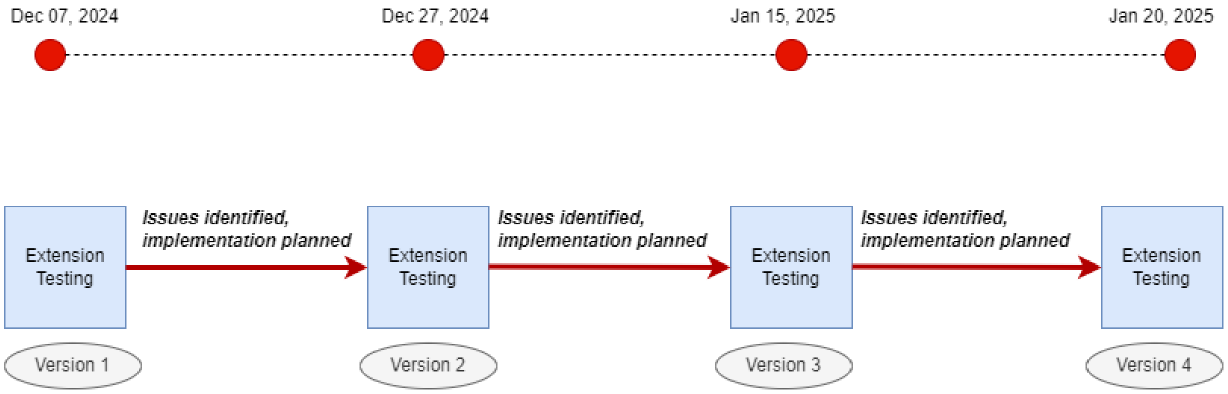


Figure 1: Testing Phases

3.0 TESTING AND EVALUATION OF VERSION 1

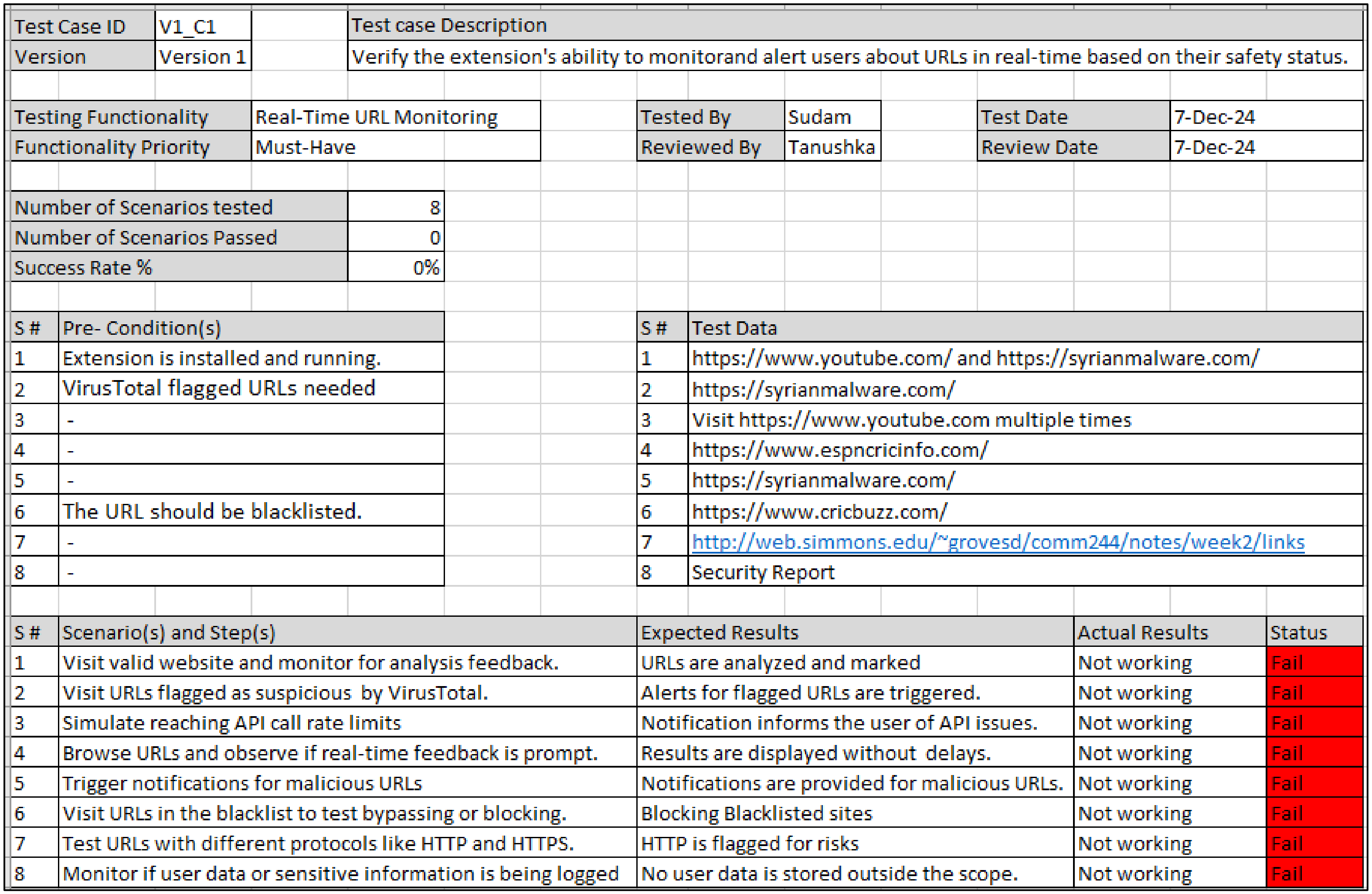
The first version of the Aegis Shield - Phishing Detection Extension was developed with six core features as of December 7, 2024. These features include Real-Time URL Monitoring, Phishing URL Detection, Whitelist/Blacklist Management, Email Phishing Detection, User-Friendly Interface, and Multi-Browser Compatibility. On the same day, extensive testing was conducted to evaluate the functionality, accuracy, and user experience of these implemented features. Each feature underwent rigorous testing through predefined scenarios to validate its performance against expected outcomes. The results of this testing process have provided valuable insights into the extension's strengths and areas for improvement, forming the basis for refining existing functionalities and planning future development phases.

As of December 7, 2024, the first version of the Aegis Shield - Phishing Detection Extension included six implemented features. These features were rigorously tested using six test cases and a total of 36 test scenarios to evaluate their functionality, accuracy, and performance. The results from this testing phase provided valuable insights into the extension’s strengths and areas requiring improvement, laying the groundwork for future development iterations.

Requirement name	Test Case ID	No. of Scenarios Tested
Real-Time URL Monitoring	V1_C1	8
Phishing URL Detection	V1_C2	4
Whitelist/Blacklist Management	V1_C3	7
Email Phishing Detection	V1_C4	4
User-Friendly Interface	V1_C5	6
Multi-Browser Compatibility	V1_C6	7
Total Number of Test Cases Tested: 6		
Total Number of Scenarios Tested: 36		

Table 1:Testing Phase 1 Overview

3.1 TEST CASE 1: Real-Time URL Monitoring



Test Case ID	V1_C1		Test case Description
Version	Version 1		Verify the extension's ability to monitorand alert users about URLs in real-time based on their safety status.

Testing Functionality	Real-Time URL Monitoring	Tested By	Sudam	Test Date	7-Dec-24
Functionality Priority	Must-Have	Reviewed By	Tanushka	Review Date	7-Dec-24

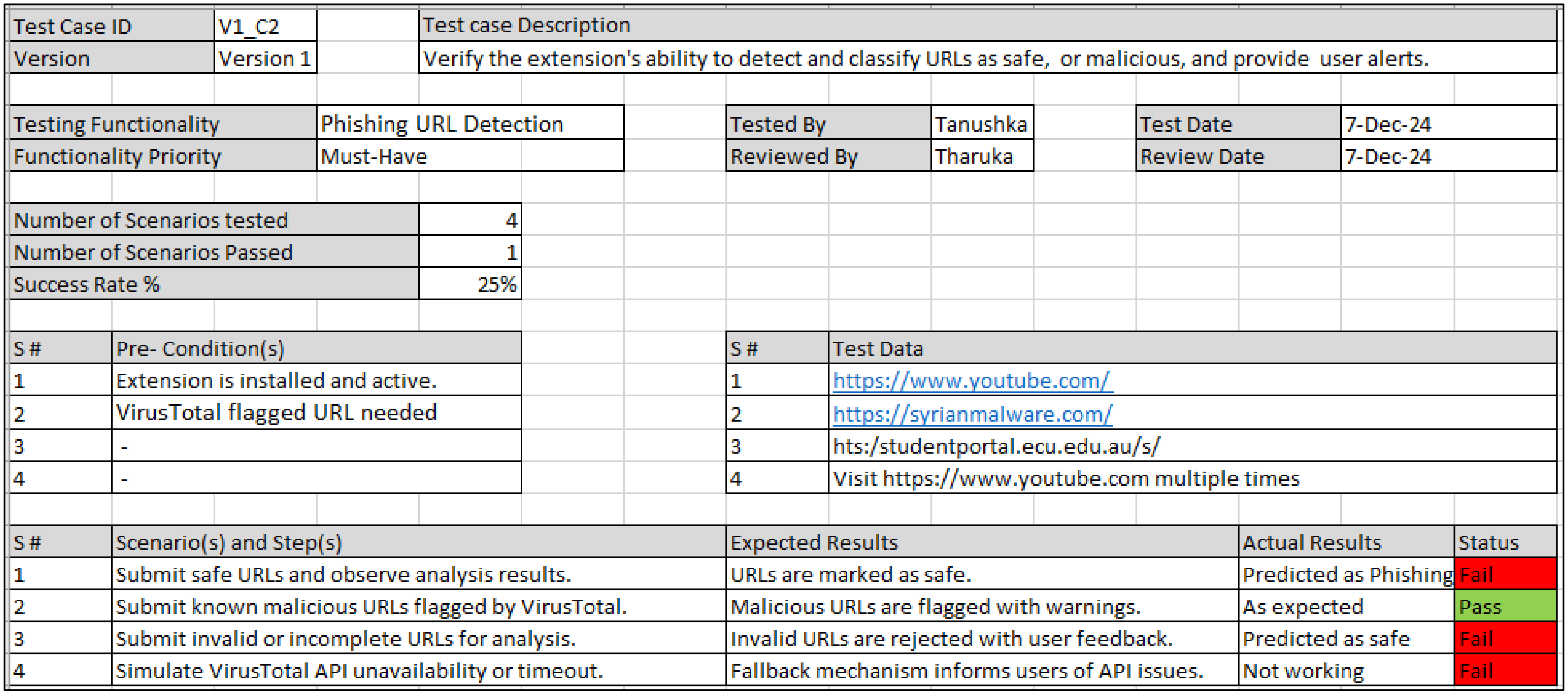
Number of Scenarios tested	8
Number of Scenarios Passed	0
Success Rate %	0%

S #	Pre- Condition(s)	S #	Test Data
1	Extension is installed and running.	1	https://www.youtube.com/ and https://syrianmalware.com/
2	VirusTotal flagged URLs needed	2	https://syrianmalware.com/
3	-	3	Visit https://www.youtube.com multiple times
4	-	4	https://www.espncricinfo.com/
5	-	5	https://syrianmalware.com/
6	The URL should be blacklisted.	6	https://www.cricbuzz.com/
7	-	7	http://web.simmons.edu/~grovesd/comm244/notes/week2/links
8	-	8	Security Report

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit valid website and monitor for analysis feedback.	URLs are analyzed and marked	Not working	Fail
2	Visit URLs flagged as suspicious by VirusTotal.	Alerts for flagged URLs are triggered.	Not working	Fail
3	Simulate reaching API call rate limits	Notification informs the user of API issues.	Not working	Fail
4	Browse URLs and observe if real-time feedback is prompt.	Results are displayed without delays.	Not working	Fail
5	Trigger notifications for malicious URLs	Notifications are provided for malicious URLs.	Not working	Fail
6	Visit URLs in the blacklist to test bypassing or blocking.	Blocking Blacklisted sites	Not working	Fail
7	Test URLs with different protocols like HTTP and HTTPS.	HTTP is flagged for risks	Not working	Fail
8	Monitor if user data or sensitive information is being logged	No user data is stored outside the scope.	Not working	Fail

Figure 2: TEST CASE 1: Real-Time URL Monitoring

3.2 TEST CASE 2: Phishing URL Detection



Test Case ID	V1_C2	Test case Description
Version	Version 1	Verify the extension's ability to detect and classify URLs as safe, or malicious, and provide user alerts.

Testing Functionality	Phishing URL Detection	Tested By	Tanushka	Test Date	7-Dec-24
Functionality Priority	Must-Have	Reviewed By	Tharuka	Review Date	7-Dec-24

Number of Scenarios tested	4
Number of Scenarios Passed	1
Success Rate %	25%

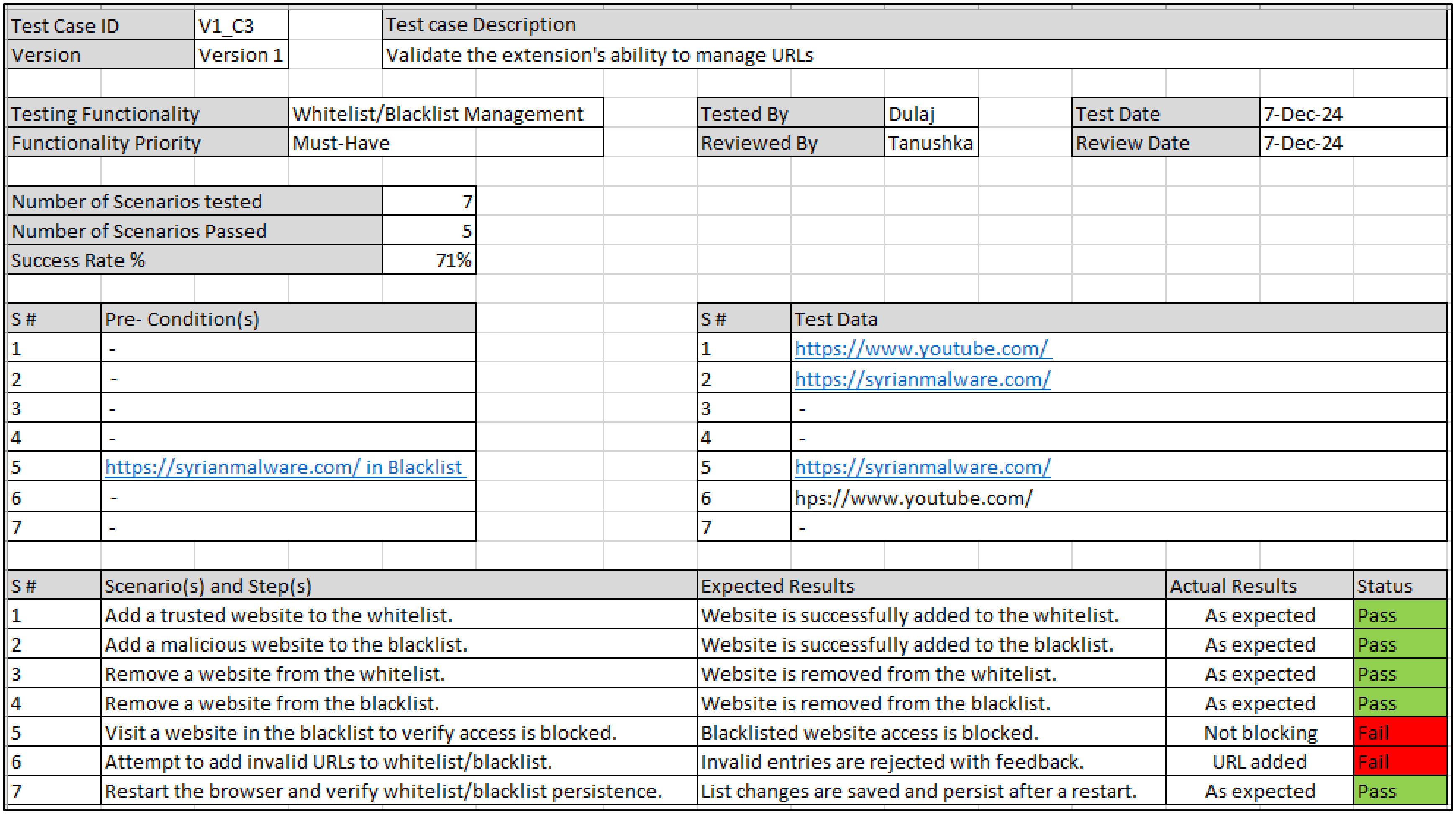
S #	Pre- Condition(s)
1	Extension is installed and active.
2	VirusTotal flagged URL needed
3	-
4	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	hts:/studentportal.ecu.edu.au/s/
4	Visit https://www.youtube.com multiple times

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit safe URLs and observe analysis results.	URLs are marked as safe.	Predicted as Phishing	Fail
2	Submit known malicious URLs flagged by VirusTotal.	Malicious URLs are flagged with warnings.	As expected	Pass
3	Submit invalid or incomplete URLs for analysis.	Invalid URLs are rejected with user feedback.	Predicted as safe	Fail
4	Simulate VirusTotal API unavailability or timeout.	Fallback mechanism informs users of API issues.	Not working	Fail

Figure 3:TEST CASE 2: Phishing URL Detection

3.3 TEST CASE 3: Whitelist/Blacklist Management



Test Case ID	V1_C3		Test case Description
Version	Version 1		Validate the extension's ability to manage URLs

Testing Functionality	Whitelist/Blacklist Management	Tested By	Dulaj	Test Date	7-Dec-24
Functionality Priority	Must-Have	Reviewed By	Tanushka	Review Date	7-Dec-24

Number of Scenarios tested	7
Number of Scenarios Passed	5
Success Rate %	71%

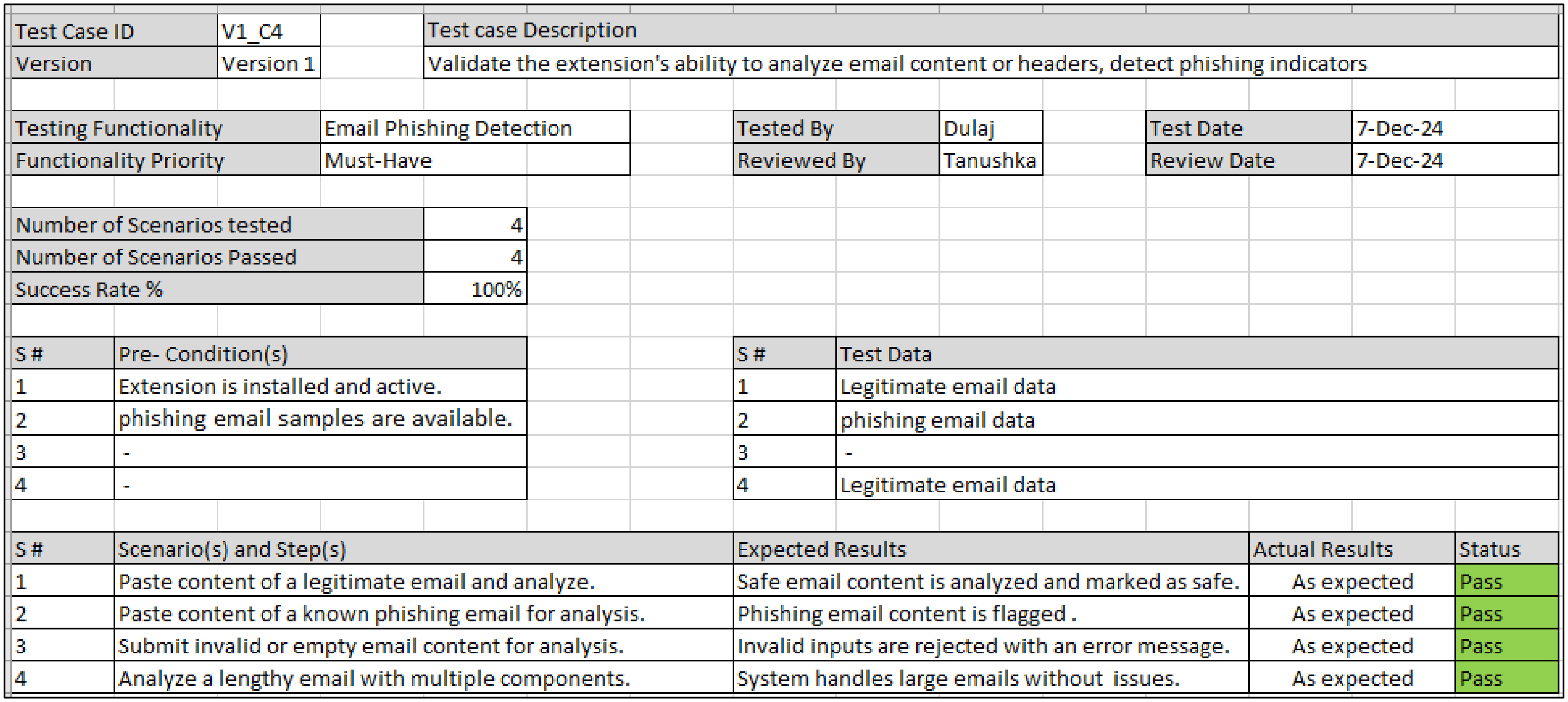
S #	Pre- Condition(s)
1	-
2	-
3	-
4	-
5	https://syrianmalware.com/ in Blacklist
6	-
7	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	-
4	-
5	https://syrianmalware.com/
6	hps://www.youtube.com/
7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Add a trusted website to the whitelist.	Website is successfully added to the whitelist.	As expected	Pass
2	Add a malicious website to the blacklist.	Website is successfully added to the blacklist.	As expected	Pass
3	Remove a website from the whitelist.	Website is removed from the whitelist.	As expected	Pass
4	Remove a website from the blacklist.	Website is removed from the blacklist.	As expected	Pass
5	Visit a website in the blacklist to verify access is blocked.	Blacklisted website access is blocked.	Not blocking	Fail
6	Attempt to add invalid URLs to whitelist/blacklist.	Invalid entries are rejected with feedback.	URL added	Fail
7	Restart the browser and verify whitelist/blacklist persistence.	List changes are saved and persist after a restart.	As expected	Pass

Figure 4:TEST CASE 3: Whitelist/Blacklist Management

3.4 TEST CASE 4: Email Phishing Detection



Test Case ID	V1_C4		Test case Description
Version	Version 1		Validate the extension's ability to analyze email content or headers, detect phishing indicators

Testing Functionality	Email Phishing Detection	Tested By	Dulaj	Test Date	7-Dec-24
Functionality Priority	Must-Have	Reviewed By	Tanushka	Review Date	7-Dec-24

Number of Scenarios tested	4
Number of Scenarios Passed	4
Success Rate %	100%

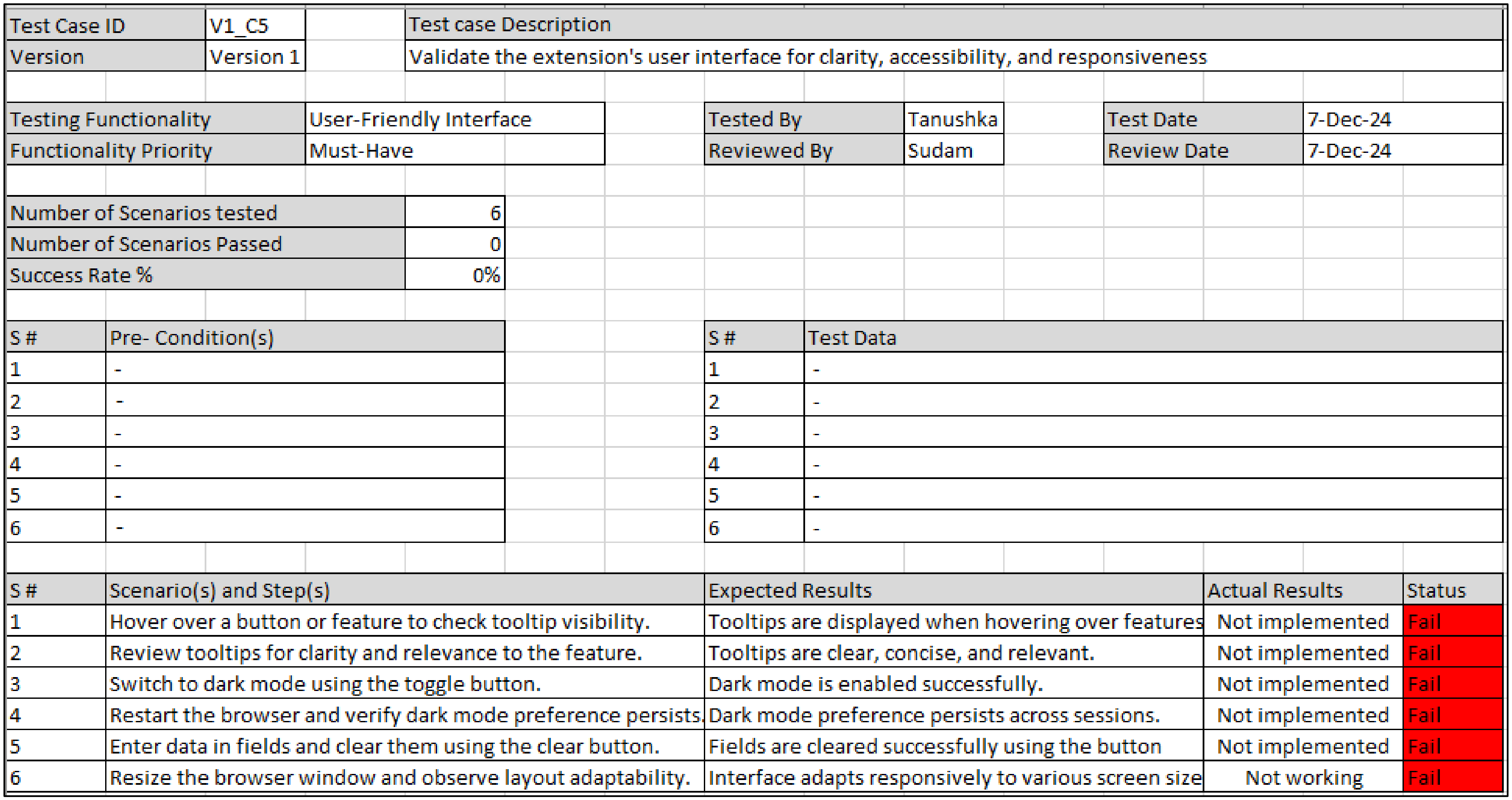
S #	Pre- Condition(s)
1	Extension is installed and active.
2	phishing email samples are available.
3	-
4	-

S #	Test Data
1	Legitimate email data
2	phishing email data
3	-
4	Legitimate email data

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Paste content of a legitimate email and analyze.	Safe email content is analyzed and marked as safe.	As expected	Pass
2	Paste content of a known phishing email for analysis.	Phishing email content is flagged .	As expected	Pass
3	Submit invalid or empty email content for analysis.	Invalid inputs are rejected with an error message.	As expected	Pass
4	Analyze a lengthy email with multiple components.	System handles large emails without issues.	As expected	Pass

Figure 5:TEST CASE 4: Email Phishing Detection

3.5 TEST CASE 5: User-Friendly Interface



Test Case ID	V1_C5		Test case Description
Version	Version 1		Validate the extension's user interface for clarity, accessibility, and responsiveness

Testing Functionality	User-Friendly Interface	Tested By	Tanushka	Test Date	7-Dec-24
Functionality Priority	Must-Have	Reviewed By	Sudam	Review Date	7-Dec-24

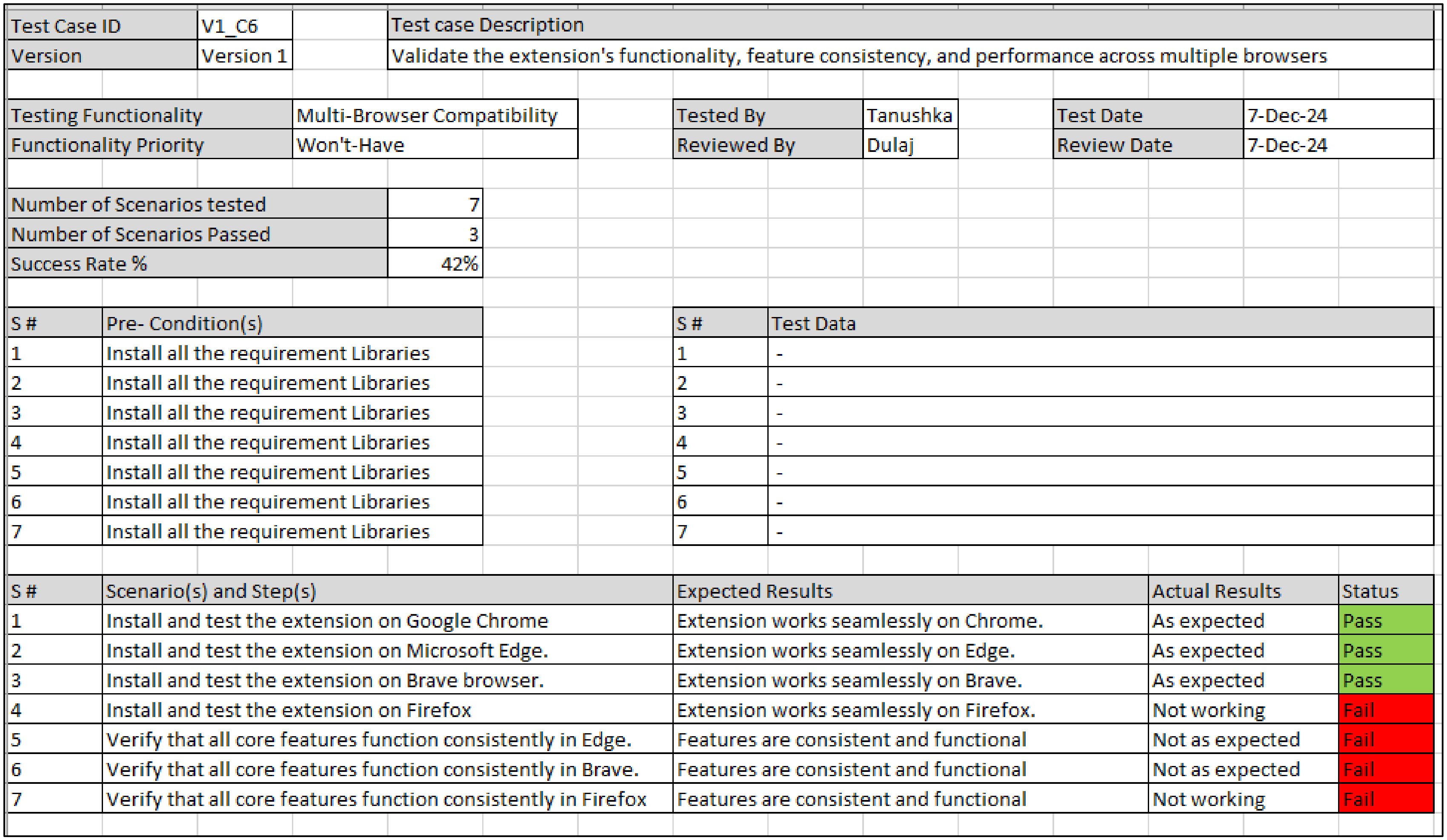
Number of Scenarios tested	6
Number of Scenarios Passed	0
Success Rate %	0%

S #	Pre- Condition(s)	S #	Test Data
1	-	1	-
2	-	2	-
3	-	3	-
4	-	4	-
5	-	5	-
6	-	6	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Hover over a button or feature to check tooltip visibility.	Tooltips are displayed when hovering over features	Not implemented	Fail
2	Review tooltips for clarity and relevance to the feature.	Tooltips are clear, concise, and relevant.	Not implemented	Fail
3	Switch to dark mode using the toggle button.	Dark mode is enabled successfully.	Not implemented	Fail
4	Restart the browser and verify dark mode preference persists.	Dark mode preference persists across sessions.	Not implemented	Fail
5	Enter data in fields and clear them using the clear button.	Fields are cleared successfully using the button	Not implemented	Fail
6	Resize the browser window and observe layout adaptability.	Interface adapts responsively to various screen size	Not working	Fail

Figure 6:TEST CASE 5: User-Friendly Interface

3.6 TEST CASE 6: Multi-Browser Compatibility



Test Case ID	V1_C6	Test case Description
Version	Version 1	Validate the extension's functionality, feature consistency, and performance across multiple browsers

Testing Functionality	Multi-Browser Compatibility	Tested By	Tanushka	Test Date	7-Dec-24
Functionality Priority	Won't-Have	Reviewed By	Dulaj	Review Date	7-Dec-24

Number of Scenarios tested	7
Number of Scenarios Passed	3
Success Rate %	42%

S #	Pre- Condition(s)
1	Install all the requirement Libraries
2	Install all the requirement Libraries
3	Install all the requirement Libraries
4	Install all the requirement Libraries
5	Install all the requirement Libraries
6	Install all the requirement Libraries
7	Install all the requirement Libraries

S #	Test Data
1	-
2	-
3	-
4	-
5	-
6	-
7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Install and test the extension on Google Chrome	Extension works seamlessly on Chrome.	As expected	Pass
2	Install and test the extension on Microsoft Edge.	Extension works seamlessly on Edge.	As expected	Pass
3	Install and test the extension on Brave browser.	Extension works seamlessly on Brave.	As expected	Pass
4	Install and test the extension on Firefox	Extension works seamlessly on Firefox.	Not working	Fail
5	Verify that all core features function consistently in Edge.	Features are consistent and functional	Not as expected	Fail
6	Verify that all core features function consistently in Brave.	Features are consistent and functional	Not as expected	Fail
7	Verify that all core features function consistently in Firefox	Features are consistent and functional	Not working	Fail

Figure 7:TEST CASE 6: Multi-Browser Compatibility

3.7 TESTED RESULTS SUMMARY FOR VERSION 1

The testing results for Version 1 of the Aegis Shield - Phishing Detection Extension highlight the performance of the six implemented features as of December 7, 2024. While some features, such as Email Phishing Detection and Whitelist/Blacklist Management, demonstrated high success rates of 100% and 71%, respectively, others like Real-Time URL Monitoring and Multi-Browser Compatibility showed room for improvement. Features like User-Friendly Interface faced usability challenges, with no scenarios passing during testing. These results underscore the importance of refining the extension’s functionality and addressing identified limitations to enhance reliability and user experience. The data gathered from this testing phase will guide future iterations and development efforts, ensuring continuous improvement.

Requirement name	Test Case ID	No. of Scenarios Tested	No. of Passed Scenarios	Success Rate
Real-Time URL Monitoring	V1_C1	8	0	0%
Phishing URL Detection	V1_C2	4	1	25%
Whitelist/Blacklist Management	V1_C3	7	5	71%
Email Phishing Detection	V1_C4	4	4	100%
User-Friendly Interface	V1_C5	6	0	0%
Multi-Browser Compatibility	V1_C6	7	3	41%

Table 2: Version 1 Results

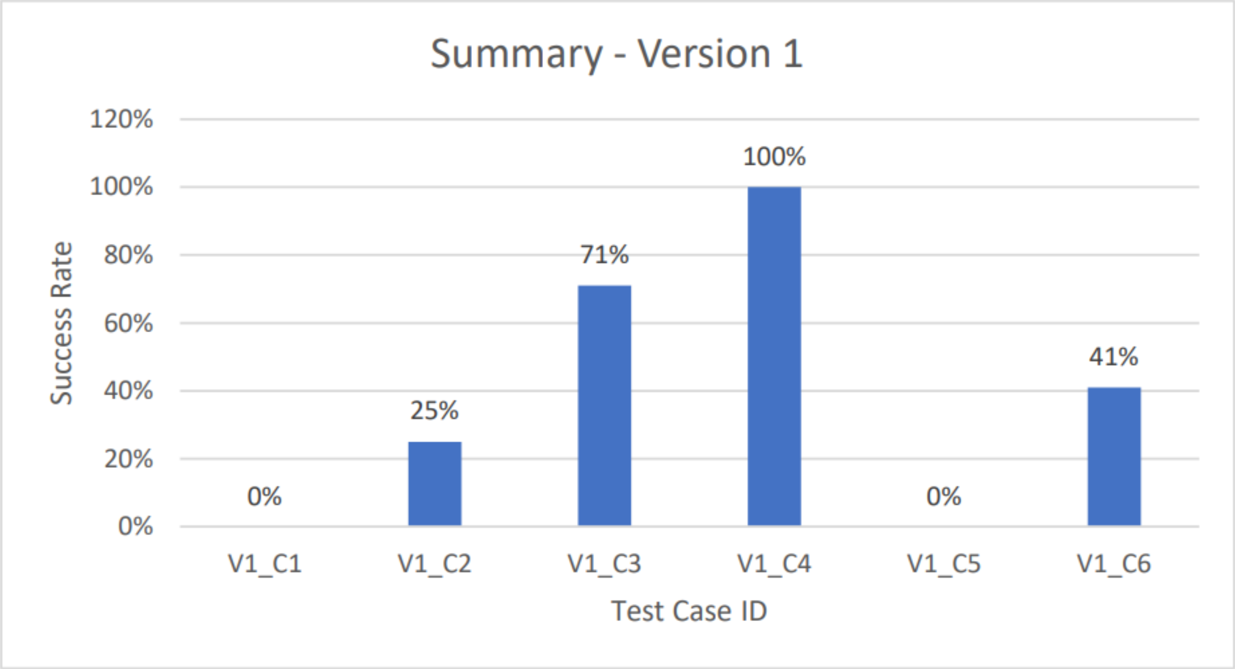


Figure 8: Summary Version-1

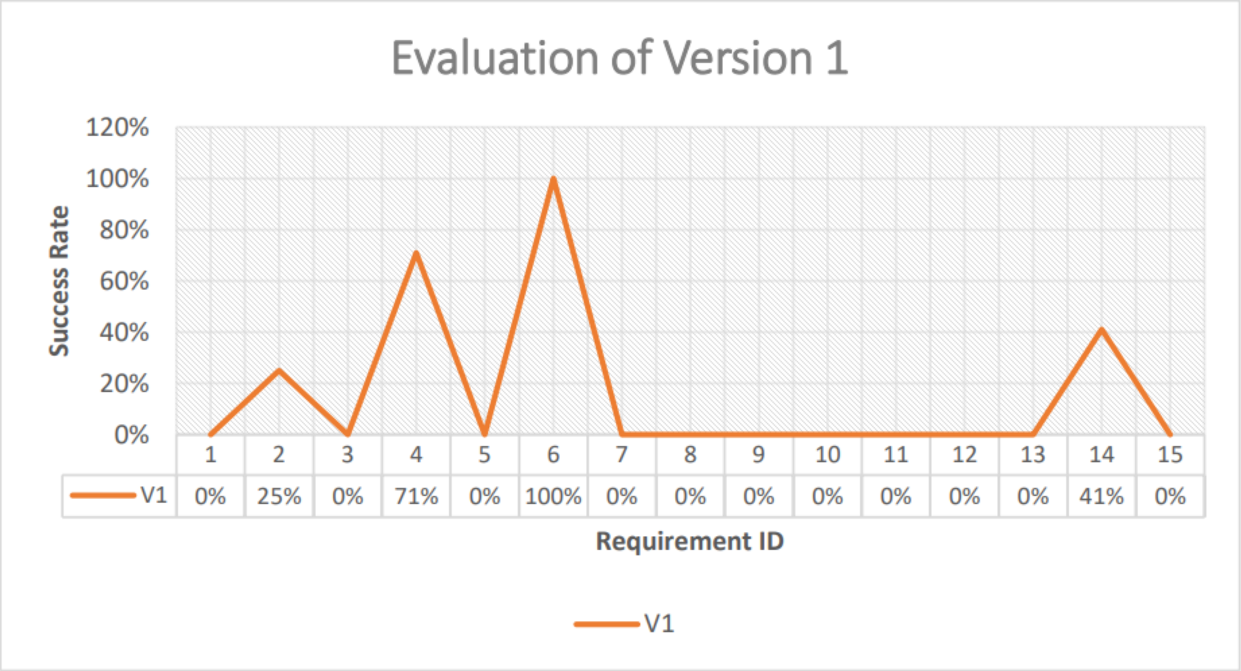
3.8 EVALUATION OF THE VERSION(S)

The evaluation of Version 1 of the Aegis Shield - Phishing Detection Extension revealed key insights into the extension's performance and areas for improvement. While some features, such as Email Phishing Detection and Whitelist/Blacklist Management, demonstrated high success rates, others, including Real-Time URL Monitoring and Multi-Browser Compatibility, showed limited functionality and required significant refinement. Additionally, several core features outlined in the project proposal were not yet developed in this version, limiting its overall capability. The findings from this evaluation provided a roadmap for addressing the identified limitations and prioritizing enhancements in subsequent versions to ensure comprehensive phishing protection and a better user experience.

		Success Rate of the Version tested
Requirement ID	**Requirement name**	**V1**
1	Real-Time URL Monitoring	0%
2	Phishing URL Detection	25%
3	Basic User Alerts	Not-Developed
4	Whitelist/Blacklist Management	71%
5	Basic Malware Detection	Not-Developed
6	Email Phishing Detection	100%
7	Browser Notifications	Not-Developed
8	User-Friendly Interface	0%
9	Severity-Based Alerts	Not-Developed
10	Email Content Parsing	Not-Developed
11	Advanced Machine Learning for Phishing Detection	Not-Developed
12	Heuristic URL Analysis	Not-Developed
13	Customizable User Settings	Not-Developed
14	Multi-Browser Compatibility	41%
15	Sandbox Integration for File Analysis	Not-Developed

Table 3: Evaluation of version 1

The figure below illustrates the success rates of implemented features in Version 1 of the Aegis Shield - Phishing Detection Extension. While some features, like Email Phishing Detection, achieved a 100% success rate, others, such as Real-Time URL Monitoring and User-Friendly Interface, faced challenges with no successful test scenarios. These results highlight the need for focused improvements and the development of missing features to achieve the project's objectives.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
V1	0%	25%	0%	71%	0%	100%	0%	0%	0%	0%	0%	0%	0%	41%	0%

Figure 9: Evaluation of version 1

3.9 IDENTIFIED ISSUES/LIMITATIONS DURING TESTING

The testing phase for Version 1 of the Aegis Shield - Phishing Detection Extension revealed several issues and limitations that need to be addressed to enhance the extension's functionality and reliability. These issues were derived from failed test scenarios, highlighting areas that require immediate attention for optimization and development. Below is a detailed discussion of the identified issues based on the results of the Version 1 testing:

1. Real-Time URL Monitoring (0% Success Rate)

- **Issue**: None of the eight test scenarios passed.
- **Identified Problems**:
  - Inconsistent monitoring of URLs, where certain navigations were missed.
  - API rate limiting caused delays and failed analyses for multiple simultaneous URL requests.
  - Redirection handling was incomplete, leading to incorrect analysis of intermediate URLs.
- **Impact**: This issue undermines the core functionality of the extension, leaving users exposed to undetected phishing and malicious threats.
- **Recommendation**: Enhance URL monitoring logic to ensure consistency, optimize API calls, and improve redirection handling.

2. Phishing URL Detection (25% Success Rate)

- **Issue**: Only one out of four test scenarios passed.
- **Identified Problems**:
  - Failed to detect certain phishing URLs due to gaps in validation rules.
  - Incorrect categorization of URLs with borderline suspicious patterns.
- **Impact**: Users may not receive accurate alerts for phishing threats, reducing trust in the system.
- **Recommendation**: Refine the detection logic and integrate additional validation heuristics for edge cases.

3. Whitelist/Blacklist Management (71% Success Rate)

- **Issue**: Two out of seven test scenarios failed.
- **Identified Problems**:
  - Certain blacklisted URLs were not blocked due to improper rule enforcement.
  - Deletion of whitelist/blacklist entries occasionally failed, causing inconsistencies in user-defined lists.
- **Impact**: Users may unknowingly access blocked URLs or struggle to manage their lists effectively.
- **Recommendation**: Ensure robust validation for user-defined entries and consistent application of rules.

4. User-Friendly Interface (0% Success Rate)

- **Issue**: None of the six test scenarios passed.
- **Identified Problems**:
  - Tooltips were missing or unclear for critical features, leaving users confused.
  - The dark mode toggle failed to persist across sessions, leading to a poor user experience.
  - Input fields and buttons were not responsive or visually consistent.
- **Impact**: This significantly affects the extension's usability, especially for non-technical users.
- **Recommendation**: Redesign the interface with clear tooltips, improved styling, and session-persistent user preferences.

5. Multi-Browser Compatibility (41% Success Rate)

- **Issue**: Four out of seven test scenarios failed.
- **Identified Problems**:
  - The extension performed inconsistently on Edge and Brave browsers.
  - Firefox compatibility was not implemented, as outlined in the proposal.
- **Impact**: Limited compatibility reduces the extension's user base and accessibility.
- **Recommendation**: Conduct extensive cross-browser testing and ensure compliance with Firefox's extension framework.

Key Limitations from Missing Features

Several core features outlined in the project proposal were not developed in Version 1, limiting the extension's capability to provide comprehensive protection:

- **Basic Malware Detection**: Absence of malware detection leaves users vulnerable to threats embedded in URLs.
- **Browser Notifications**: The lack of real-time notifications reduces the extension's ability to inform users promptly.
- **Severity-Based Alerts**: Alerts lack contextual threat levels, making it harder for users to assess risks.
- **Advanced Machine Learning for Phishing Detection**: Missing advanced phishing detection reduces accuracy and scalability.

Overall Impact

The identified issues and limitations from Version 1 testing highlight the need for significant improvements to core functionalities, interface design, and feature coverage. Addressing these issues is critical to achieving the goals set forth in the project proposal and ensuring user satisfaction and trust in future versions of the extension. Prioritizing unresolved test scenarios and missing features will form the basis for future development iterations.

4.0 TESTING AND EVALUATION OF VERSION 2

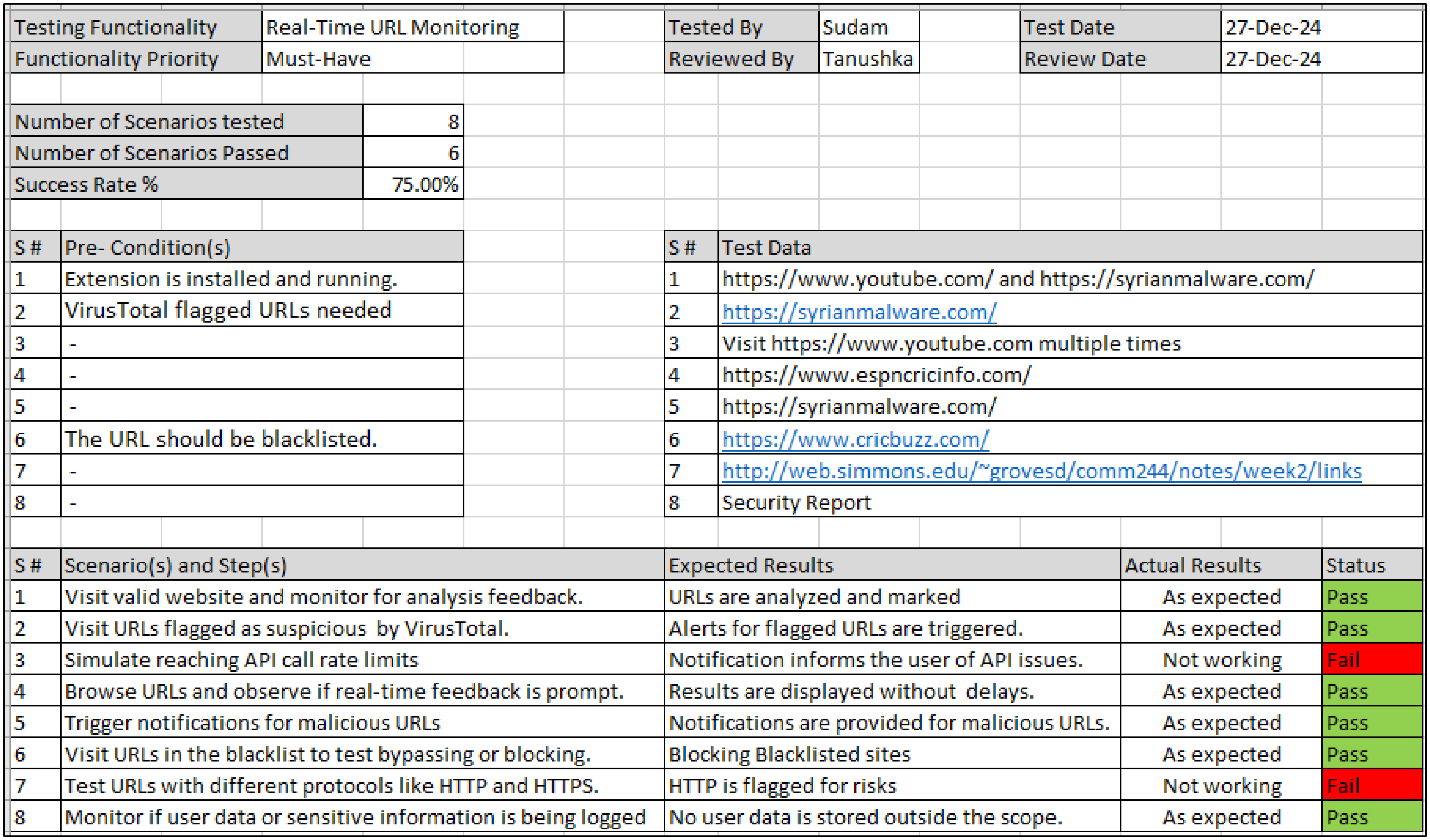
On December 27, 2024, the second version of the Aegis Shield - Phishing Detection Extension was tested after the development of 12 core features. This testing phase involved evaluating all implemented features using detailed test cases and scenarios to ensure their functionality, performance, and reliability. The results from this testing phase highlighted significant improvements over Version 1, demonstrating the extension's enhanced capabilities and addressing many of the limitations identified previously.

On December 27, 2024, the second version of the Aegis Shield - Phishing Detection Extension was tested after the development of 12 core features. This testing phase involved evaluating all implemented features using detailed test cases and scenarios to ensure their functionality, performance, and reliability. The results from this testing phase highlighted significant improvements over Version 1, demonstrating the extension's enhanced capabilities and addressing many of the limitations identified previously.

Requirement name	Test Case ID	No. of Scenarios Tested
Real-Time URL Monitoring	V2_C1	8
Phishing URL Detection	V2_C2	4
Basic URL Alerts	V2_C3	3
Whitelist/Blacklist Management	V2_C4	7
Basic Malware Detection	V2_C5	4
Email Phishing Detection	V2_C6	4
Browser Notifications	V2_C7	5
User-Friendly Interface	V2_C8	6
Severity-Based Alerts	V2_C9	3
Advanced Machine Learning for Phishing Detection	V2_C10	5
Multi-Browser Compatibility	V2_C11	7
Sandbox Integration for File Analysis	V2_C12	5
Total Number of Test Cases Tested: 12		
Total Number of Scenarios Tested: 61		

Table 4:Testing Phase 2 Overview

4.1 TEST CASE 1: Real-Time URL Monitoring



Testing Functionality	Real-Time URL Monitoring	Tested By	Sudam	Test Date	27-Dec-24
Functionality Priority	Must-Have	Reviewed By	Tanushka	Review Date	27-Dec-24

Number of Scenarios tested	8
Number of Scenarios Passed	6
Success Rate %	75.00%

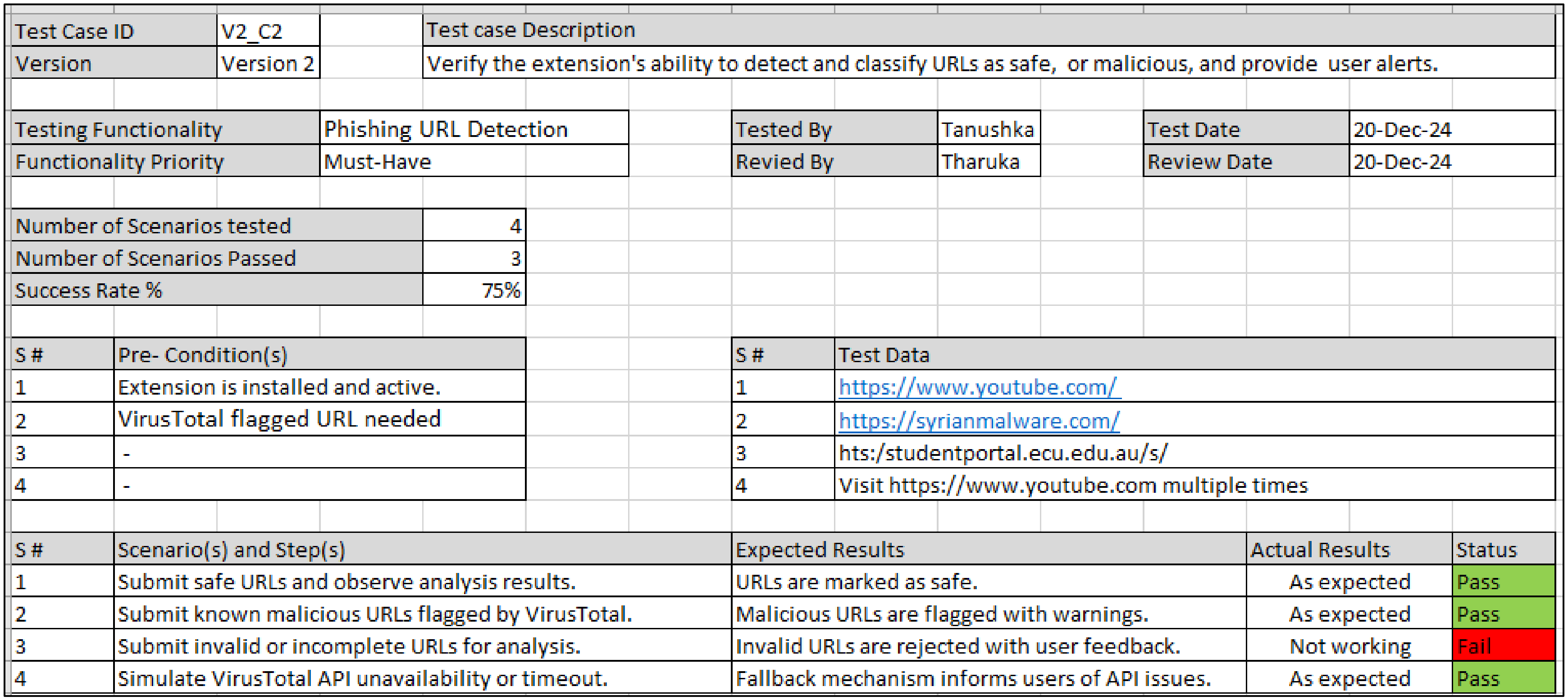
S #	Pre- Condition(s)
1	Extension is installed and running.
2	VirusTotal flagged URLs needed
3	-
4	-
5	-
6	The URL should be blacklisted.
7	-
8	-

S #	Test Data
1	https://www.youtube.com/ and https://syrianmalware.com/
2	https://syrianmalware.com/
3	Visit https://www.youtube.com multiple times
4	https://www.espncricinfo.com/
5	https://syrianmalware.com/
6	https://www.cricbuzz.com/
7	http://web.simmons.edu/~grovesd/comm244/notes/week2/links
8	Security Report

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit valid website and monitor for analysis feedback.	URLs are analyzed and marked	As expected	Pass
2	Visit URLs flagged as suspicious by VirusTotal.	Alerts for flagged URLs are triggered.	As expected	Pass
3	Simulate reaching API call rate limits	Notification informs the user of API issues.	Not working	Fail
4	Browse URLs and observe if real-time feedback is prompt.	Results are displayed without delays.	As expected	Pass
5	Trigger notifications for malicious URLs	Notifications are provided for malicious URLs.	As expected	Pass
6	Visit URLs in the blacklist to test bypassing or blocking.	Blocking Blacklisted sites	As expected	Pass
7	Test URLs with different protocols like HTTP and HTTPS.	HTTP is flagged for risks	Not working	Fail
8	Monitor if user data or sensitive information is being logged	No user data is stored outside the scope.	As expected	Pass

Figure 10: TEST CASE 1: Real-Time URL Monitoring

4.2 TEST CASE 2: Phishing URL Detection



Test Case ID	V2_C2	Test case Description
Version	Version 2	Verify the extension's ability to detect and classify URLs as safe, or malicious, and provide user alerts.

Testing Functionality	Phishing URL Detection	Tested By	Tanushka	Test Date	20-Dec-24
Functionality Priority	Must-Have	Revied By	Tharuka	Review Date	20-Dec-24

Number of Scenarios tested	4
Number of Scenarios Passed	3
Success Rate %	75%

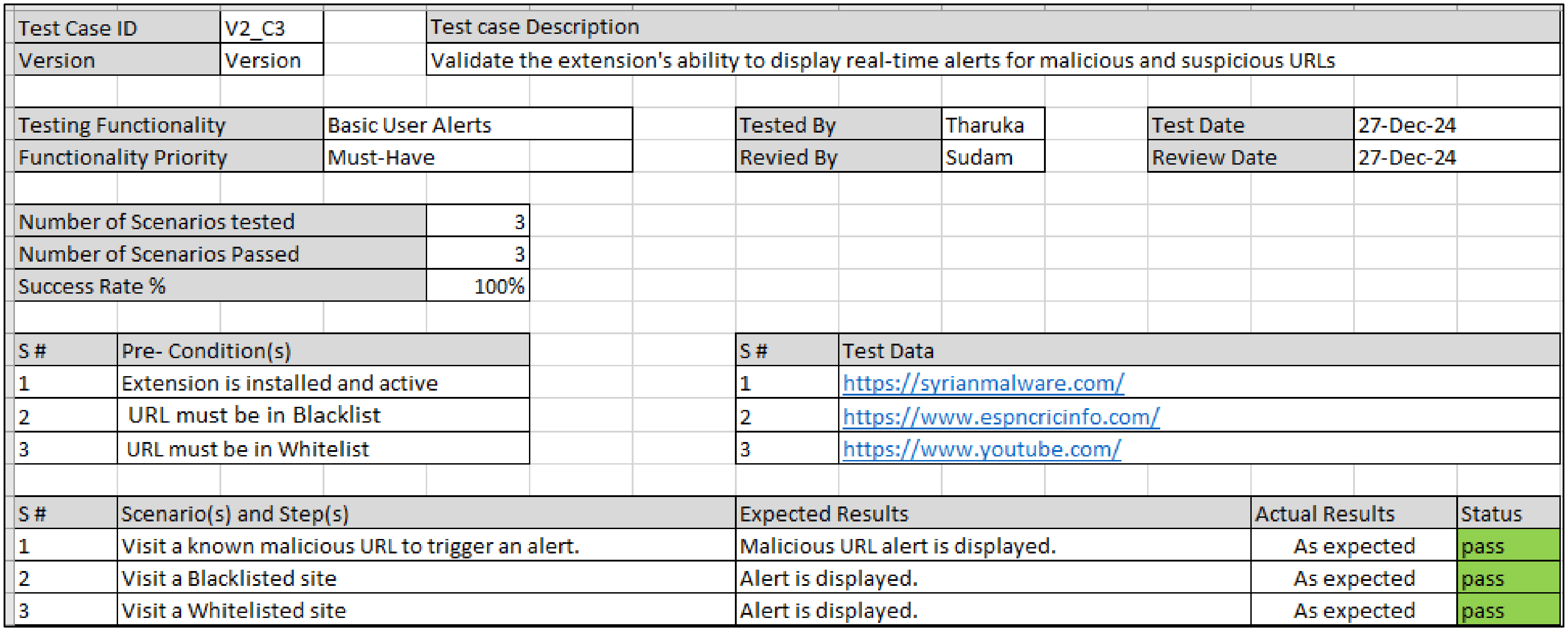
S #	Pre- Condition(s)
1	Extension is installed and active.
2	VirusTotal flagged URL needed
3	-
4	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	hts:/studentportal.ecu.edu.au/s/
4	Visit https://www.youtube.com multiple times

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit safe URLs and observe analysis results.	URLs are marked as safe.	As expected	Pass
2	Submit known malicious URLs flagged by VirusTotal.	Malicious URLs are flagged with warnings.	As expected	Pass
3	Submit invalid or incomplete URLs for analysis.	Invalid URLs are rejected with user feedback.	Not working	Fail
4	Simulate VirusTotal API unavailability or timeout.	Fallback mechanism informs users of API issues.	As expected	Pass

Figure 11:TEST CASE 2: Phishing URL Detection

4.3 TEST CASE 3: Basic User Alerts



Test Case ID	V2_C3		Test case Description
Version	Version		Validate the extension's ability to display real-time alerts for malicious and suspicious URLs

Testing Functionality	Basic User Alerts	Tested By	Tharuka	Test Date	27-Dec-24
Functionality Priority	Must-Have	Revied By	Sudam	Review Date	27-Dec-24

Number of Scenarios tested	3
Number of Scenarios Passed	3
Success Rate %	100%

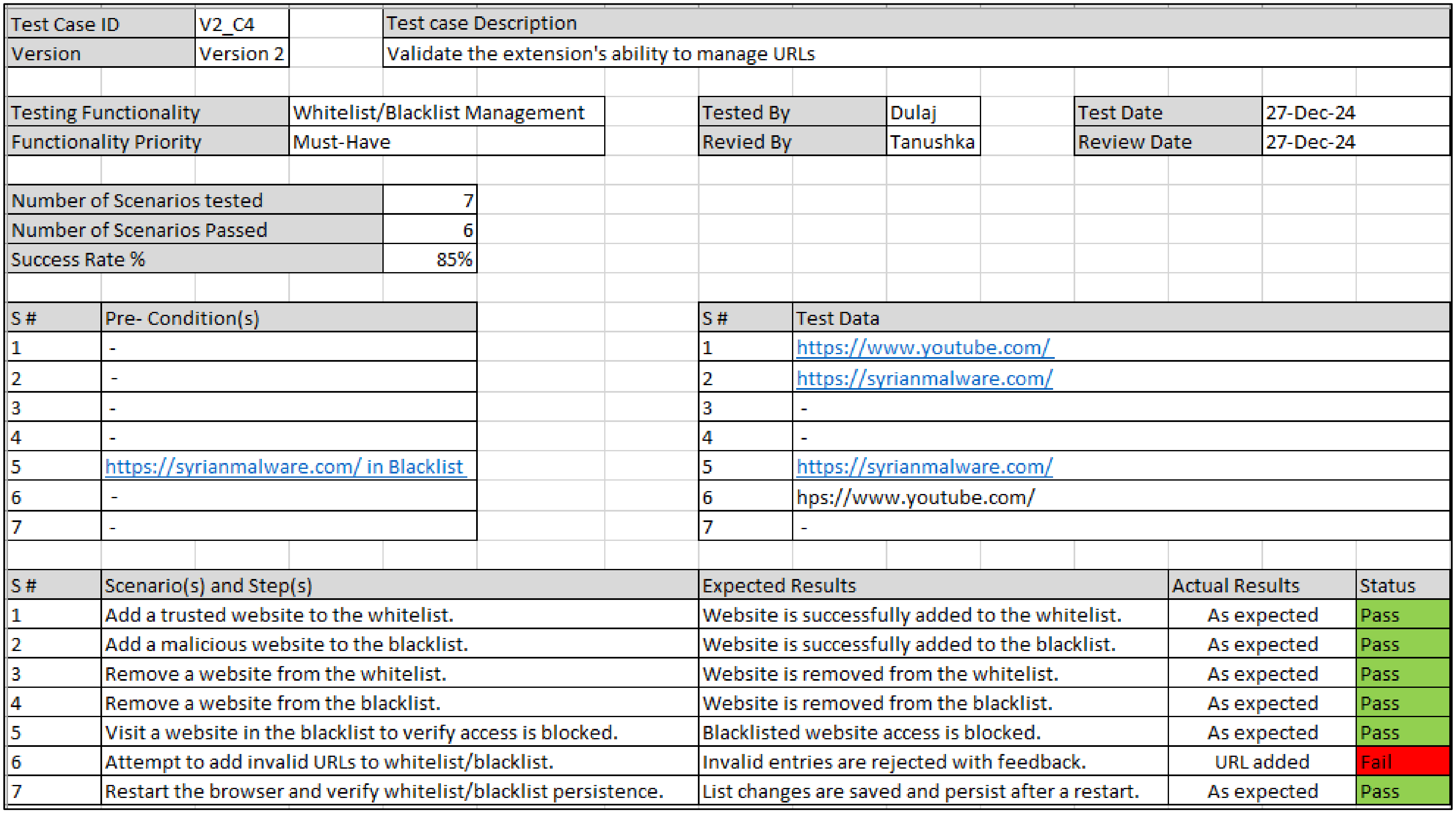
S #	Pre- Condition(s)
1	Extension is installed and active
2	URL must be in Blacklist
3	URL must be in Whitelist

S #	Test Data
1	https://syrianmalware.com/
2	https://www.espncricinfo.com/
3	https://www.youtube.com/

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a known malicious URL to trigger an alert.	Malicious URL alert is displayed.	As expected	pass
2	Visit a Blacklisted site	Alert is displayed.	As expected	pass
3	Visit a Whitelisted site	Alert is displayed.	As expected	pass

Figure 12: TEST CASE 3: Basic User Alerts

4.4 TEST CASE 4: Whitelist/Blacklist Management



Test Case ID	V2_C4		Test case Description
Version	Version 2		Validate the extension's ability to manage URLs

Testing Functionality	Whitelist/Blacklist Management	Tested By	Dulaj	Test Date	27-Dec-24
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	27-Dec-24

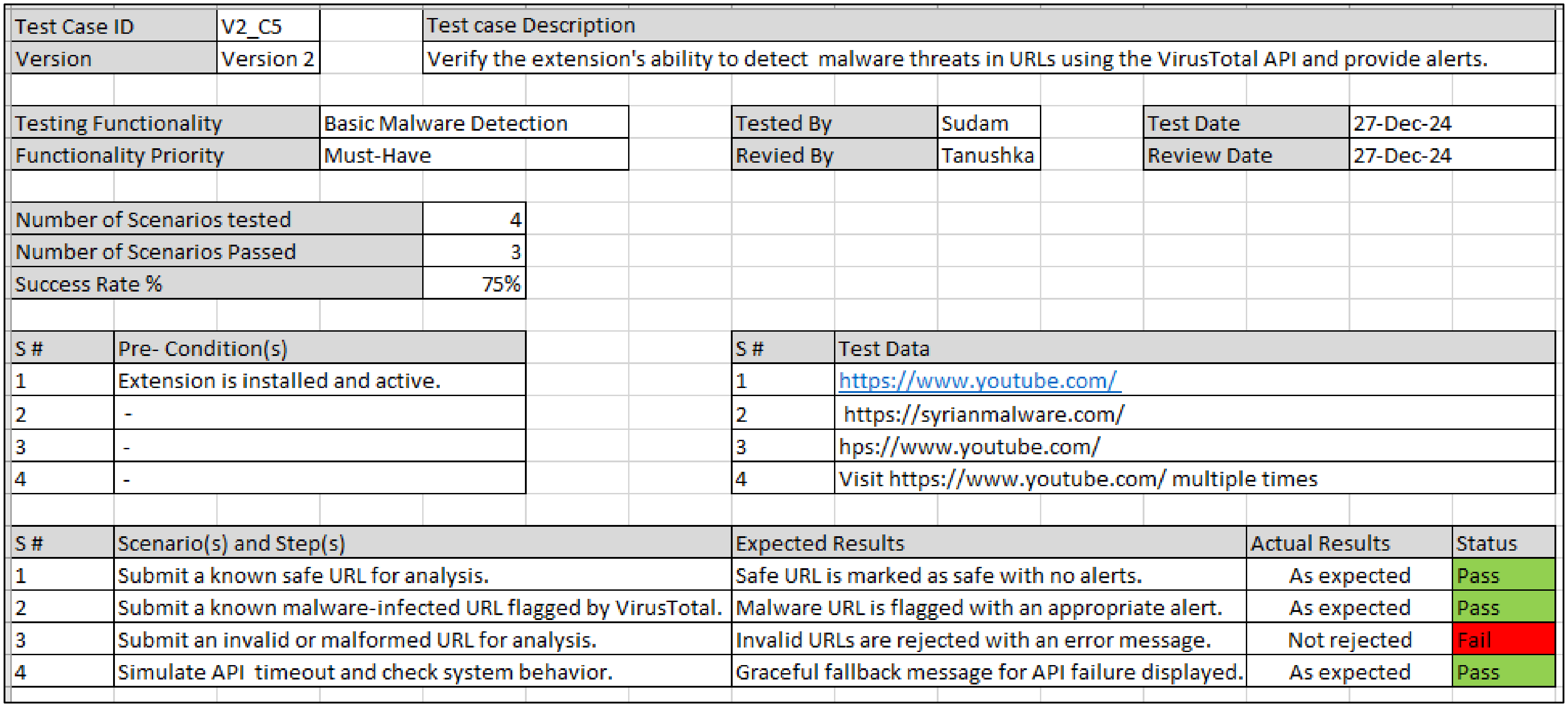
Number of Scenarios tested	7
Number of Scenarios Passed	6
Success Rate %	85%

S #	Pre- Condition(s)	S #	Test Data
1	-	1	https://www.youtube.com/
2	-	2	https://syrianmalware.com/
3	-	3	-
4	-	4	-
5	https://syrianmalware.com/ in Blacklist	5	https://syrianmalware.com/
6	-	6	hps://www.youtube.com/
7	-	7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Add a trusted website to the whitelist.	Website is successfully added to the whitelist.	As expected	Pass
2	Add a malicious website to the blacklist.	Website is successfully added to the blacklist.	As expected	Pass
3	Remove a website from the whitelist.	Website is removed from the whitelist.	As expected	Pass
4	Remove a website from the blacklist.	Website is removed from the blacklist.	As expected	Pass
5	Visit a website in the blacklist to verify access is blocked.	Blacklisted website access is blocked.	As expected	Pass
6	Attempt to add invalid URLs to whitelist/blacklist.	Invalid entries are rejected with feedback.	URL added	Fail
7	Restart the browser and verify whitelist/blacklist persistence.	List changes are saved and persist after a restart.	As expected	Pass

Figure 13: TEST CASE 4: Whitelist/Blacklist Management

4.5 TEST CASE 5: Basic Malware Detection



Test Case ID	V2_C5	Test case Description
Version	Version 2	Verify the extension's ability to detect malware threats in URLs using the VirusTotal API and provide alerts.

Testing Functionality	Basic Malware Detection	Tested By	Sudam	Test Date	27-Dec-24
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	27-Dec-24

Number of Scenarios tested	4
Number of Scenarios Passed	3
Success Rate %	75%

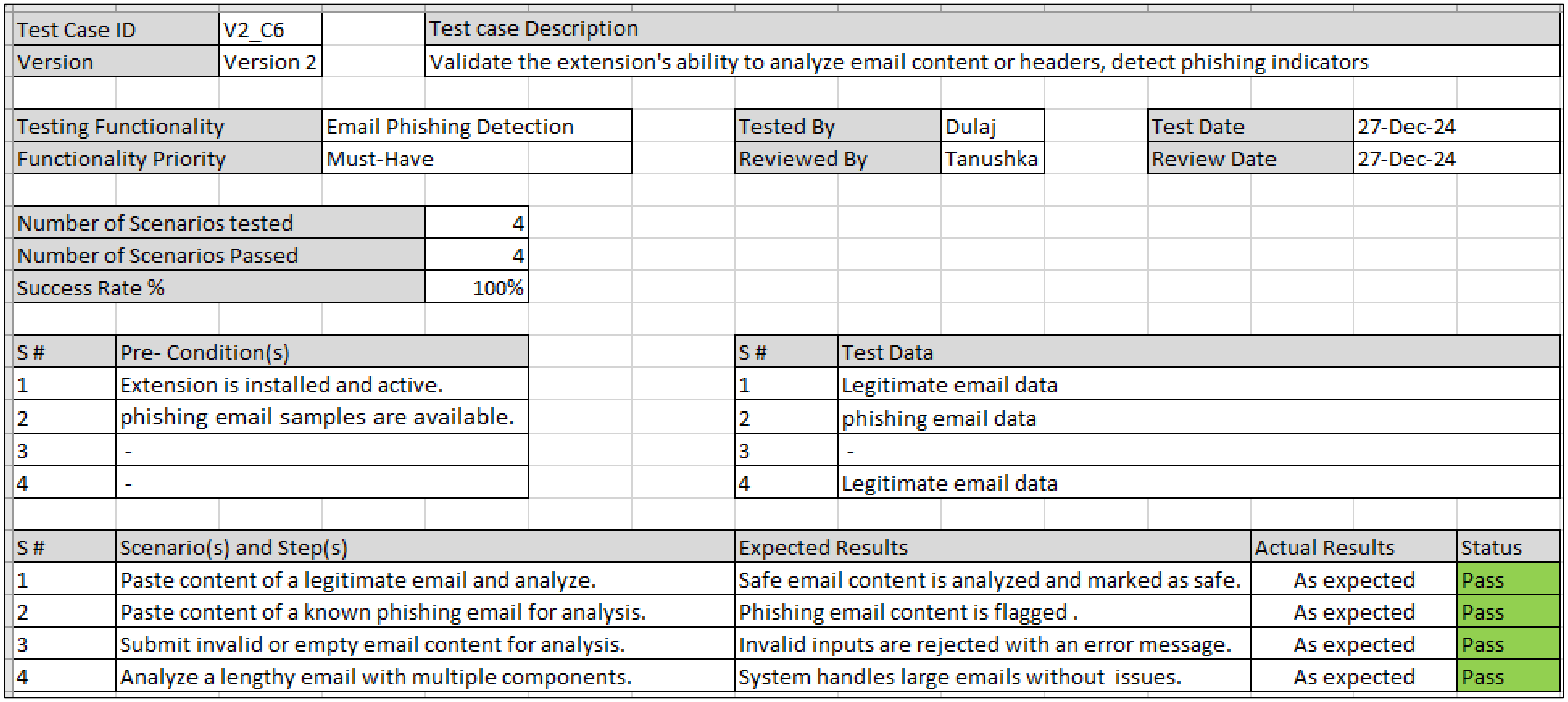
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	hps://www.youtube.com/
4	Visit https://www.youtube.com/ multiple times

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit a known safe URL for analysis.	Safe URL is marked as safe with no alerts.	As expected	🟩 Pass
2	Submit a known malware-infected URL flagged by VirusTotal.	Malware URL is flagged with an appropriate alert.	As expected	🟩 Pass
3	Submit an invalid or malformed URL for analysis.	Invalid URLs are rejected with an error message.	Not rejected	🟥 Fail
4	Simulate API timeout and check system behavior.	Graceful fallback message for API failure displayed.	As expected	🟩 Pass

Figure 14: TEST CASE 5: Basic Malware Detection

4.6 TEST CASE 6: Email Phishing Detection



Test Case ID	V2_C6		Test case Description
Version	Version 2		Validate the extension's ability to analyze email content or headers, detect phishing indicators

Testing Functionality	Email Phishing Detection	Tested By	Dulaj	Test Date	27-Dec-24
Functionality Priority	Must-Have	Reviewed By	Tanushka	Review Date	27-Dec-24

Number of Scenarios tested	4
Number of Scenarios Passed	4
Success Rate %	100%

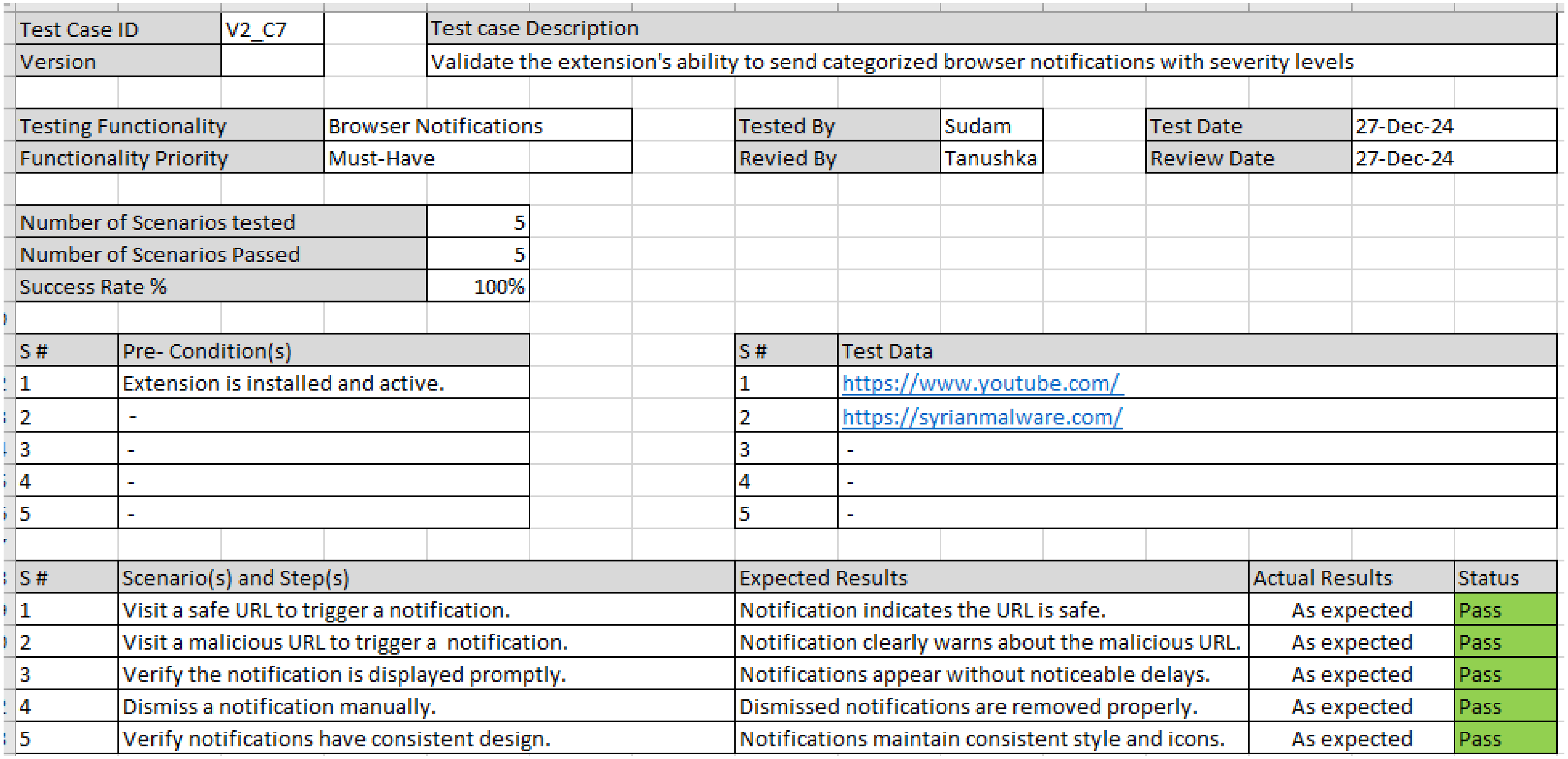
S #	Pre- Condition(s)
1	Extension is installed and active.
2	phishing email samples are available.
3	-
4	-

S #	Test Data
1	Legitimate email data
2	phishing email data
3	-
4	Legitimate email data

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Paste content of a legitimate email and analyze.	Safe email content is analyzed and marked as safe.	As expected	Pass
2	Paste content of a known phishing email for analysis.	Phishing email content is flagged .	As expected	Pass
3	Submit invalid or empty email content for analysis.	Invalid inputs are rejected with an error message.	As expected	Pass
4	Analyze a lengthy email with multiple components.	System handles large emails without issues.	As expected	Pass

Figure 15: TEST CASE 6: Email Phishing Detection

4.7 TEST CASE 7: Browser Notifications



Test Case ID	V2_C7		Test case Description
Version			Validate the extension's ability to send categorized browser notifications with severity levels

Testing Functionality	Browser Notifications	Tested By	Sudam	Test Date	27-Dec-24
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	27-Dec-24

Number of Scenarios tested	5
Number of Scenarios Passed	5
Success Rate %	100%

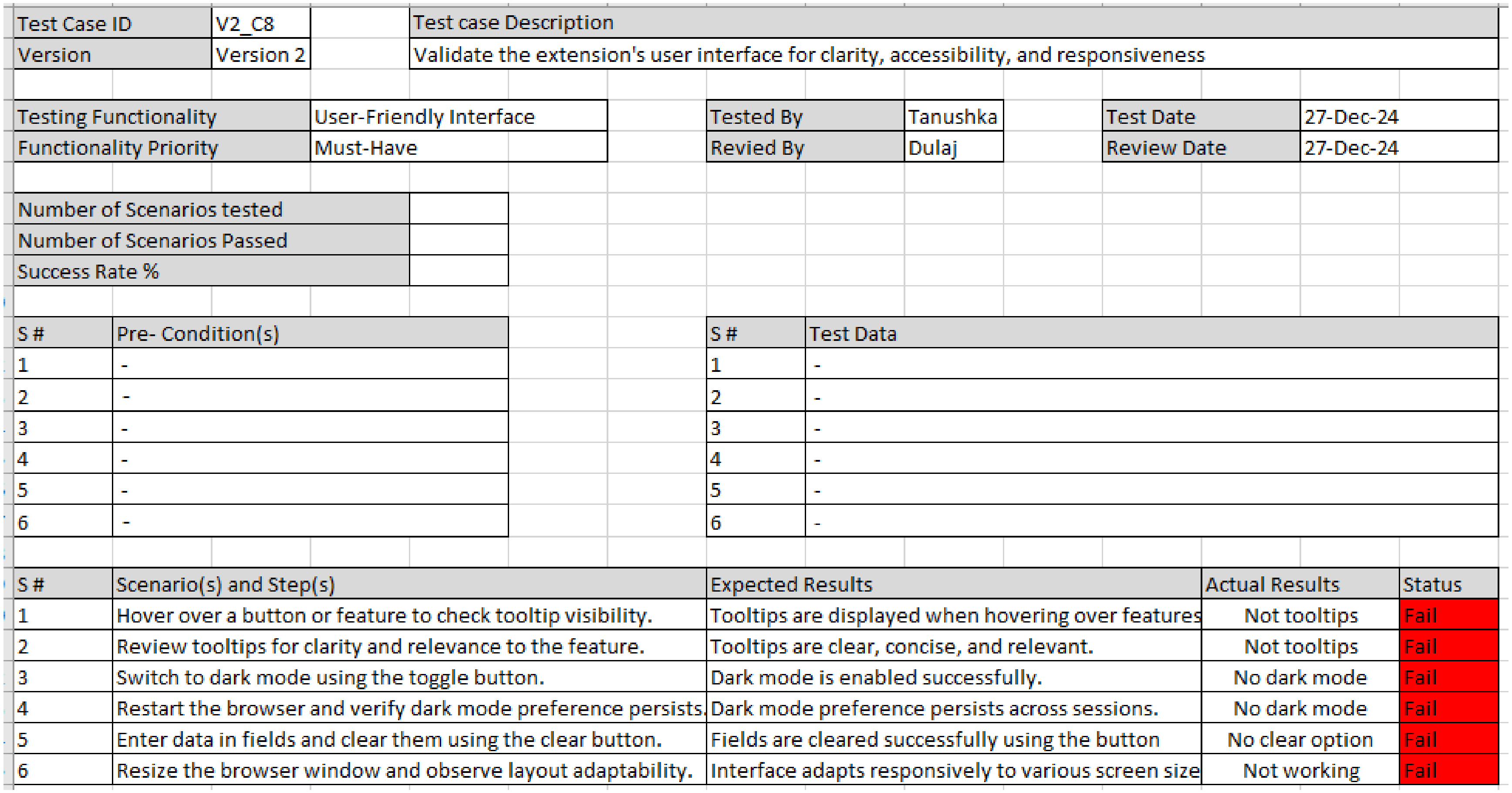
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-
5	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	-
4	-
5	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a safe URL to trigger a notification.	Notification indicates the URL is safe.	As expected	Pass
2	Visit a malicious URL to trigger a notification.	Notification clearly warns about the malicious URL.	As expected	Pass
3	Verify the notification is displayed promptly.	Notifications appear without noticeable delays.	As expected	Pass
4	Dismiss a notification manually.	Dismissed notifications are removed properly.	As expected	Pass
5	Verify notifications have consistent design.	Notifications maintain consistent style and icons.	As expected	Pass

Figure 16: TEST CASE 7: Browser Notifications

4.8 TEST CASE 8: User-Friendly Interface



Test Case ID	V2_C8	Test case Description
Version	Version 2	Validate the extension's user interface for clarity, accessibility, and responsiveness

Testing Functionality	User-Friendly Interface	Tested By	Tanushka	Test Date	27-Dec-24
Functionality Priority	Must-Have	Revied By	Dulaj	Review Date	27-Dec-24

Number of Scenarios tested	
Number of Scenarios Passed	
Success Rate %	

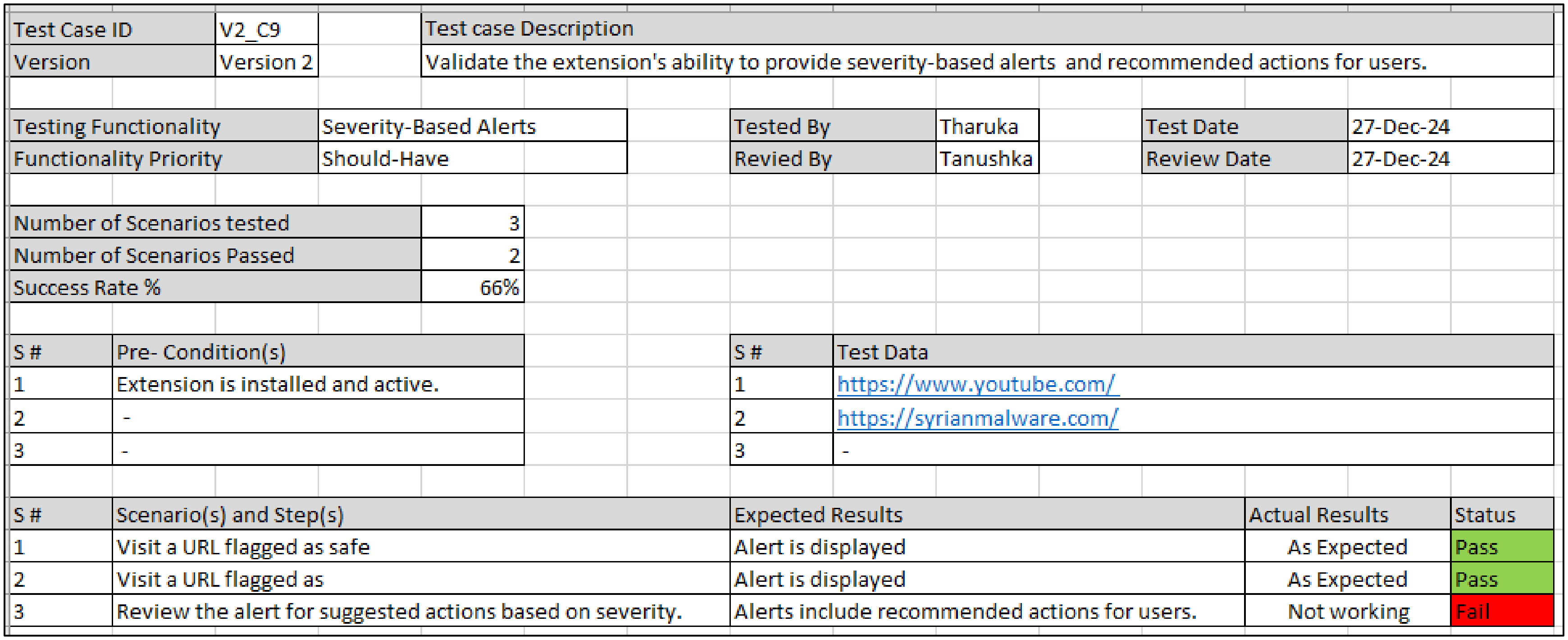
S #	Pre- Condition(s)
1	-
2	-
3	-
4	-
5	-
6	-

S #	Test Data
1	-
2	-
3	-
4	-
5	-
6	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Hover over a button or feature to check tooltip visibility.	Tooltips are displayed when hovering over features	Not tooltips	Fail
2	Review tooltips for clarity and relevance to the feature.	Tooltips are clear, concise, and relevant.	Not tooltips	Fail
3	Switch to dark mode using the toggle button.	Dark mode is enabled successfully.	No dark mode	Fail
4	Restart the browser and verify dark mode preference persists.	Dark mode preference persists across sessions.	No dark mode	Fail
5	Enter data in fields and clear them using the clear button.	Fields are cleared successfully using the button	No clear option	Fail
6	Resize the browser window and observe layout adaptability.	Interface adapts responsively to various screen size	Not working	Fail

Figure 17: TEST CASE 8: User-Friendly Interface

4.9 TEST CASE 9: Severity-Based Alerts



Test Case ID	V2_C9	Test case Description
Version	Version 2	Validate the extension's ability to provide severity-based alerts and recommended actions for users.

Testing Functionality	Severity-Based Alerts	Tested By	Tharuka	Test Date	27-Dec-24
Functionality Priority	Should-Have	Revied By	Tanushka	Review Date	27-Dec-24

Number of Scenarios tested	3
Number of Scenarios Passed	2
Success Rate %	66%

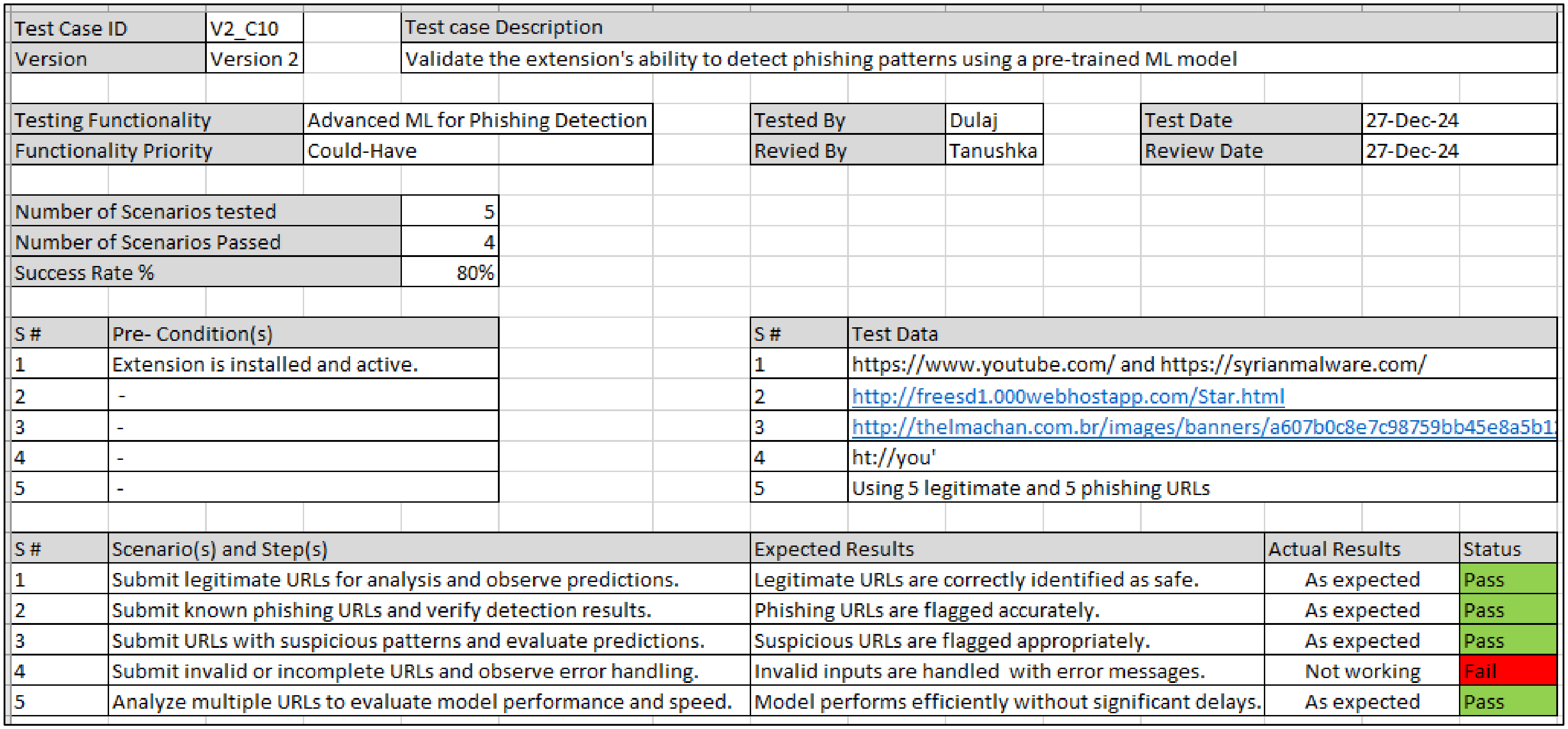
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a URL flagged as safe	Alert is displayed	As Expected	Pass
2	Visit a URL flagged as	Alert is displayed	As Expected	Pass
3	Review the alert for suggested actions based on severity.	Alerts include recommended actions for users.	Not working	Fail

Figure 18: TEST CASE 9: Severity-Based Alerts

4.10 TEST CASE 10: Advanced Machine Learning for Phishing Detection



Test Case ID	V2_C10	Test case Description
Version	Version 2	Validate the extension's ability to detect phishing patterns using a pre-trained ML model

Testing Functionality	Advanced ML for Phishing Detection	Tested By	Dulaj	Test Date	27-Dec-24
Functionality Priority	Could-Have	Revied By	Tanushka	Review Date	27-Dec-24

Number of Scenarios tested	5
Number of Scenarios Passed	4
Success Rate %	80%

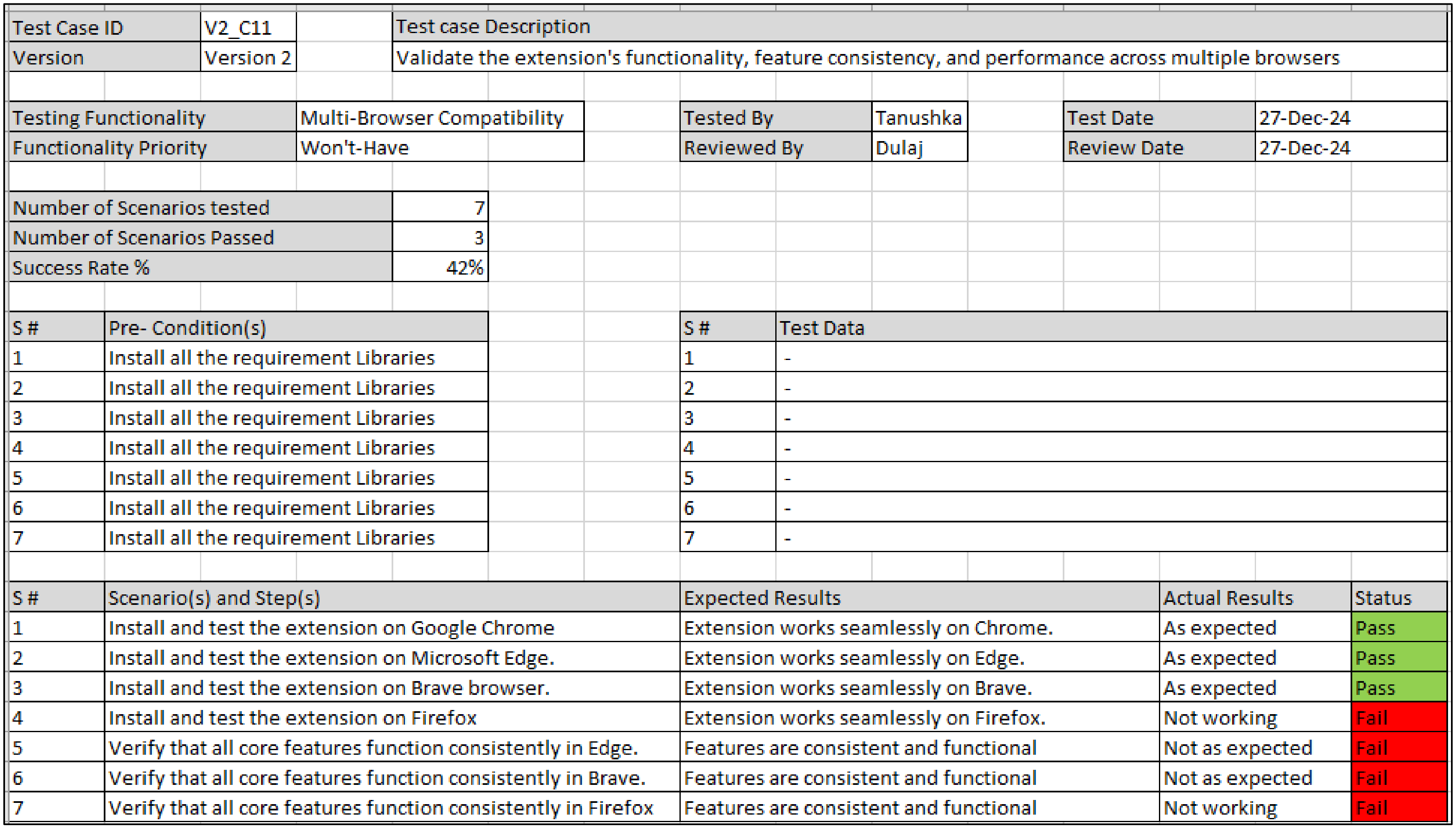
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-
5	-

S #	Test Data
1	https://www.youtube.com/ and https://syrianmalware.com/
2	http://freesd1.000webhostapp.com/Star.html
3	http://thelmachan.com.br/images/banners/a607b0c8e7c98759bb45e8a5b1
4	ht://you'
5	Using 5 legitimate and 5 phishing URLs

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit legitimate URLs for analysis and observe predictions.	Legitimate URLs are correctly identified as safe.	As expected	Pass
2	Submit known phishing URLs and verify detection results.	Phishing URLs are flagged accurately.	As expected	Pass
3	Submit URLs with suspicious patterns and evaluate predictions.	Suspicious URLs are flagged appropriately.	As expected	Pass
4	Submit invalid or incomplete URLs and observe error handling.	Invalid inputs are handled with error messages.	Not working	Fail
5	Analyze multiple URLs to evaluate model performance and speed.	Model performs efficiently without significant delays.	As expected	Pass

Figure 19: TEST CASE 10: Advanced Machine Learning for Phishing Detection

4.11 TEST CASE 11: Multi-Browser Compatibility



Test Case ID	V2_C11		Test case Description
Version	Version 2		Validate the extension's functionality, feature consistency, and performance across multiple browsers

Testing Functionality	Multi-Browser Compatibility	Tested By	Tanushka	Test Date	27-Dec-24
Functionality Priority	Won't-Have	Reviewed By	Dulaj	Review Date	27-Dec-24

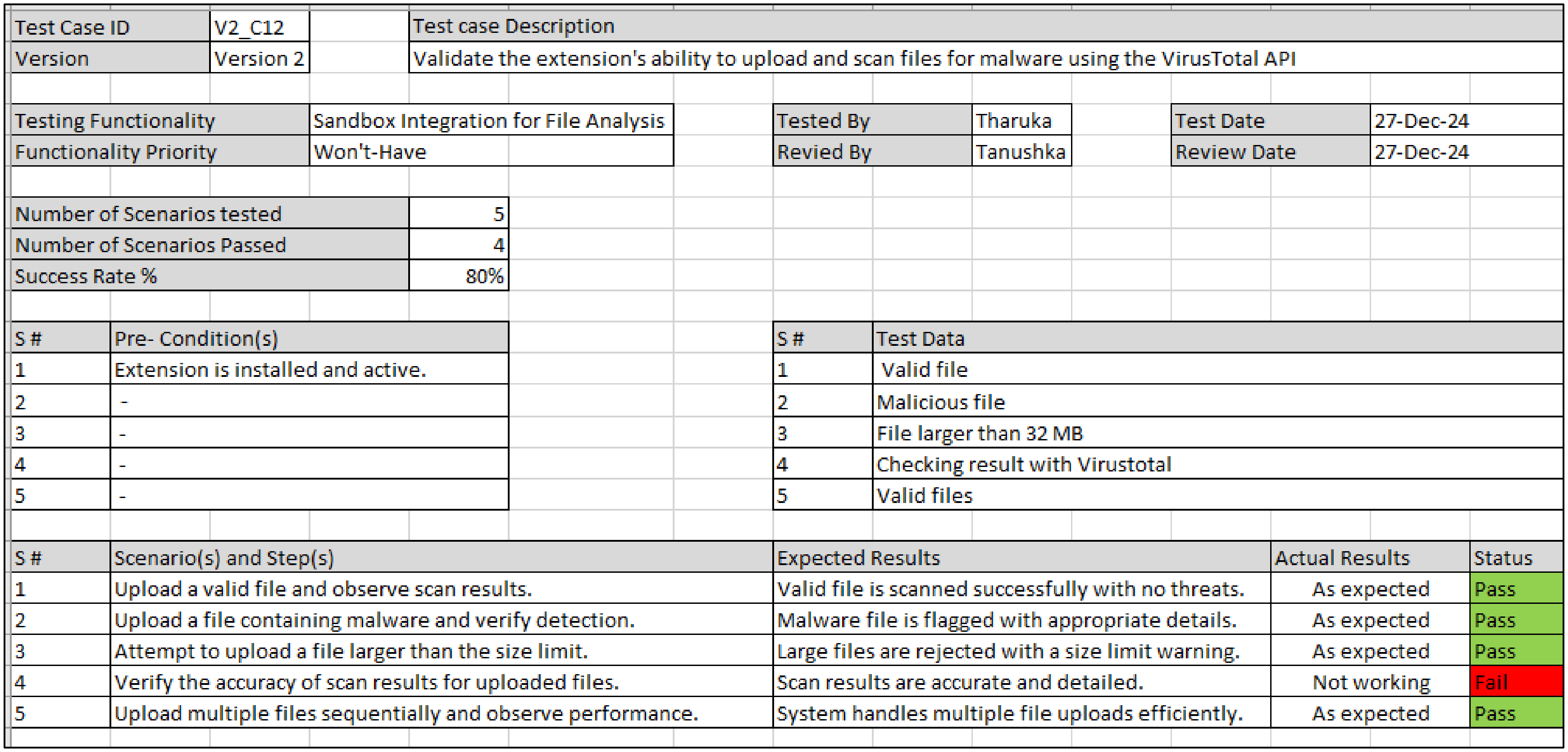
Number of Scenarios tested	7
Number of Scenarios Passed	3
Success Rate %	42%

S #	Pre- Condition(s)	S #	Test Data
1	Install all the requirement Libraries	1	-
2	Install all the requirement Libraries	2	-
3	Install all the requirement Libraries	3	-
4	Install all the requirement Libraries	4	-
5	Install all the requirement Libraries	5	-
6	Install all the requirement Libraries	6	-
7	Install all the requirement Libraries	7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Install and test the extension on Google Chrome	Extension works seamlessly on Chrome.	As expected	Pass
2	Install and test the extension on Microsoft Edge.	Extension works seamlessly on Edge.	As expected	Pass
3	Install and test the extension on Brave browser.	Extension works seamlessly on Brave.	As expected	Pass
4	Install and test the extension on Firefox	Extension works seamlessly on Firefox.	Not working	Fail
5	Verify that all core features function consistently in Edge.	Features are consistent and functional	Not as expected	Fail
6	Verify that all core features function consistently in Brave.	Features are consistent and functional	Not as expected	Fail
7	Verify that all core features function consistently in Firefox	Features are consistent and functional	Not working	Fail

Figure 20: TEST CASE 11: Multi-Browser Compatibility

4.12 TEST CASE 12: Sandbox Integration for File Analysis



Test Case ID	V2_C12		Test case Description
Version	Version 2		Validate the extension's ability to upload and scan files for malware using the VirusTotal API

Testing Functionality	Sandbox Integration for File Analysis	Tested By	Tharuka	Test Date	27-Dec-24
Functionality Priority	Won't-Have	Revied By	Tanushka	Review Date	27-Dec-24

Number of Scenarios tested	5
Number of Scenarios Passed	4
Success Rate %	80%

S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-
5	-

S #	Test Data
1	Valid file
2	Malicious file
3	File larger than 32 MB
4	Checking result with Virustotal
5	Valid files

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Upload a valid file and observe scan results.	Valid file is scanned successfully with no threats.	As expected	Pass
2	Upload a file containing malware and verify detection.	Malware file is flagged with appropriate details.	As expected	Pass
3	Attempt to upload a file larger than the size limit.	Large files are rejected with a size limit warning.	As expected	Pass
4	Verify the accuracy of scan results for uploaded files.	Scan results are accurate and detailed.	Not working	Fail
5	Upload multiple files sequentially and observe performance.	System handles multiple file uploads efficiently.	As expected	Pass

Figure 21: TEST CASE 12: Sandbox Integration for File Analysis

4.13 TESTED RESULTS SUMMARY FOR VERSION 2

The testing results for Version 2 of the Aegis Shield - Phishing Detection Extension highlight the significant progress made since Version 1. With the implementation of 12 core features, this version demonstrated improved functionality and performance. Features such as Basic User Alerts, Browser Notifications, and Email Phishing Detection achieved a 100% success rate, indicating their readiness for deployment. However, some features, including Multi-Browser Compatibility and User-Friendly Interface, showed room for improvement, with moderate or low success rates. Overall, the testing outcomes reflect substantial enhancements while identifying areas that require further optimization in subsequent versions. These results provide a solid foundation for ongoing development and refinement.

Requirement name	Test Case ID	No. of Scenarios Tested	No. of Passed Scenarios	Success Rate
Real-Time URL Monitoring	V2_C1	8	6	75%
Phishing URL Detection	V2_C2	4	3	75%
Basic URL Alerts	V2_C3	3	3	100%
Whitelist/Blacklist Management	V2_C4	7	6	85%
Basic Malware Detection	V2_C5	4	3	75%
Email Phishing Detection	V2_C6	4	4	100%
Browser Notifications	V2_C7	5	5	100%
User-Friendly Interface	V2_C8	6	0	0%
Severity-Based Alerts	V2_C9	3	2	66%
Advanced Machine Learning for Phishing Detection	V2_C10	5	4	80%
Multi-Browser Compatibility	V2_C11	7	3	42%
Sandbox Integration for File Analysis	V2_C12	5	4	80%

Table 5: Version 2 Results

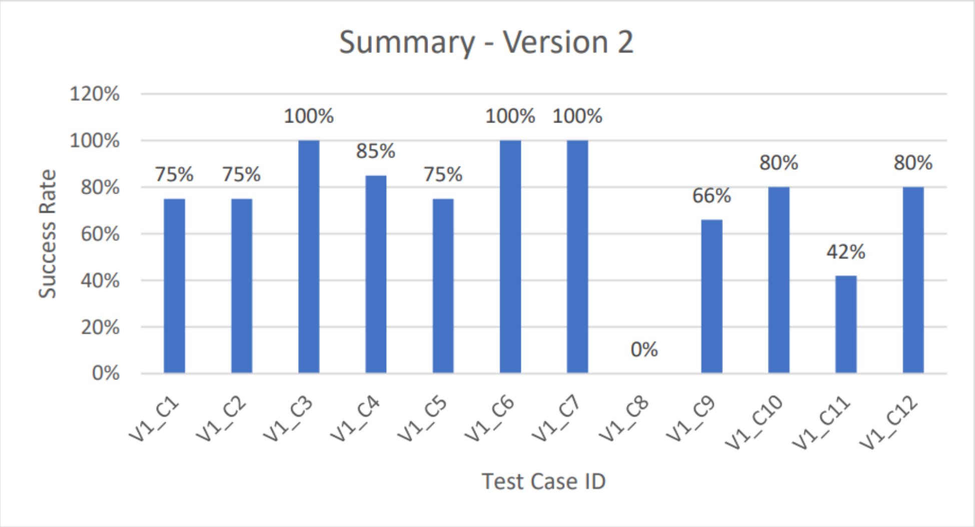


Figure 22: Summary Version 2

4.14 EVALUATION OF THE VERSION(S)

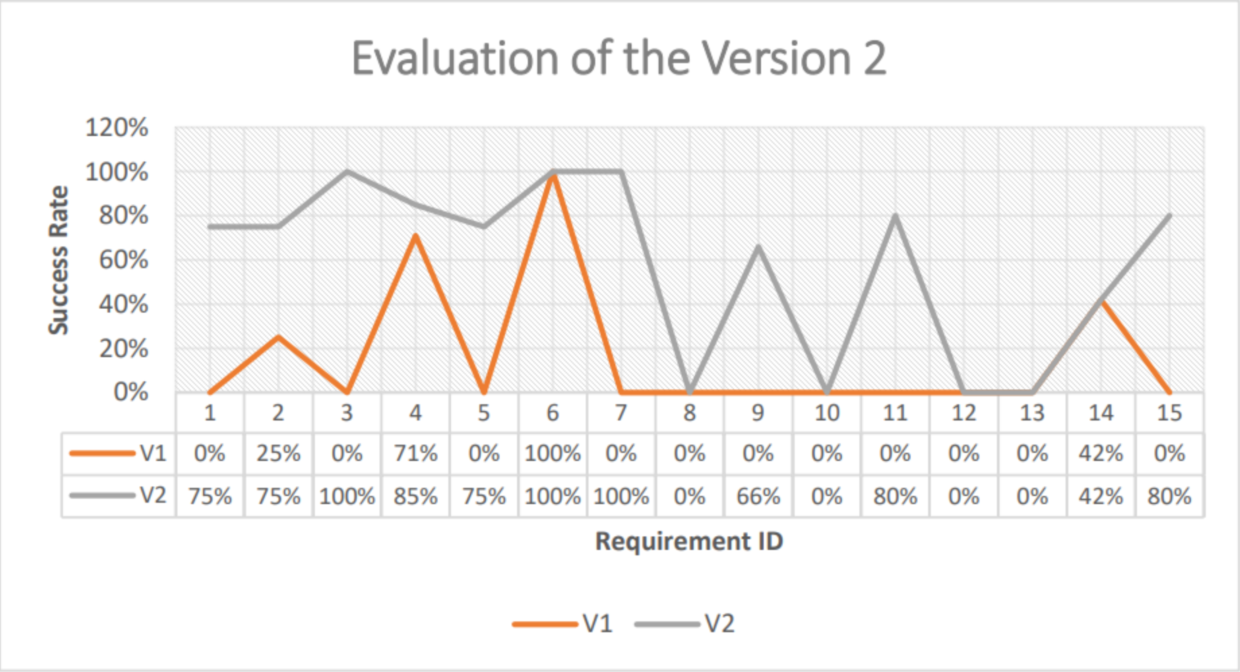
The evaluation of Version 1 and Version 2 of the Aegis Shield - Phishing Detection Extension highlights substantial improvements in the success rates of implemented features. Version 2 demonstrated significant progress, with features such as Real-Time URL Monitoring, Phishing URL Detection, and Basic Malware Detection achieving success rates of 75% or higher, compared to the minimal or incomplete results in Version 1. New features introduced in Version 2, such as Basic User Alerts, Browser Notifications, and Advanced Machine Learning for Phishing Detection, performed exceptionally well, with success rates ranging from 80% to 100%. However, some features, such as Multi-Browser Compatibility and User-Friendly Interface, continued to face challenges and maintained lower success rates.

		Success Rate of the Version tested	
Requirement ID	**Requirement name**	**V1**	**V2**
1	Real-Time URL Monitoring	0%	75%
2	Phishing URL Detection	25%	75%
3	Basic User Alerts	Not-Developed	100%
4	Whitelist/Blacklist Management	71%	85%
5	Basic Malware Detection	Not-Developed	75%
6	Email Phishing Detection	100%	100%
7	Browser Notifications	Not-Developed	100%
8	User-Friendly Interface	0%	0%
9	Severity-Based Alerts	Not-Developed	66%
10	Email Content Parsing	Not-Developed	Not-Developed
11	Advanced Machine Learning for Phishing Detection	Not-Developed	80%
12	Heuristic URL Analysis	Not-Developed	Not-Developed
13	Customizable User Settings	Not-Developed	Not-Developed
14	Multi-Browser Compatibility	42%	42%
15	Sandbox Integration for File Analysis	Not-Developed	80%

Table 6: Evaluation of version 2

Overall, the advancements in Version 2 reflect the team's commitment to addressing identified issues and expanding the extension's functionality, laying the groundwork for further enhancements in future iterations.

A detailed line chart below illustrates the comparative success rates for each feature across the two versions.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
V1	0%	25%	0%	71%	0%	100%	0%	0%	0%	0%	0%	0%	0%	42%	0%
V2	75%	75%	100%	85%	75%	100%	100%	0%	66%	0%	80%	0%	0%	42%	80%

Figure 23: Evaluation of version 2

4.15 IDENTIFIED ISSUES/LIMITATIONS DURING TESTING

The testing phase for Version 2 of the Aegis Shield - Phishing Detection Extension revealed several issues and limitations that were identified through the failed test scenarios. While Version 2 demonstrated significant improvements compared to Version 1, these failures highlight areas that require optimization, debugging, and enhancement to ensure the extension's reliability and user satisfaction. Below is a detailed discussion of the identified issues based on Version 2 testing results:

1. Real-Time URL Monitoring (75% Success Rate)

- **Failed Scenarios**:
  - Real-time URL tracking was inconsistent under heavy browsing loads, missing URLs on occasion.
  - Redirection handling failed in certain cases, resulting in incomplete analysis of final destination URLs.
- **Identified Issues**:
  - The monitoring mechanism struggles under high-load environments, especially when multiple tabs are open.
  - Complex redirections (e.g., multiple intermediate URLs) are not correctly followed.
- **Impact**:
  - Users may not receive alerts for certain threats, reducing trust in the feature.
- **Recommendations**:
  - Enhance monitoring algorithms to handle higher load scenarios and optimize redirection analysis.

2. Phishing URL Detection (75% Success Rate)

- **Failed Scenarios**:
  - URLs with advanced obfuscation techniques (e.g., URL shorteners or encoded links) were not detected as phishing.
  - A small number of phishing URLs were incorrectly categorized as safe.
- **Identified Issues**:
  - Current detection logic lacks robustness against sophisticated phishing patterns.
  - Insufficient heuristics for identifying borderline cases.
- **Impact**:
  - Users remain vulnerable to cleverly disguised phishing attacks.
- **Recommendations**:
  - Integrate additional phishing heuristics and improve detection algorithms for edge cases.

3. Whitelist/Blacklist Management (85% Success Rate)

- **Failed Scenarios**:
  - Certain blacklisted URLs were incorrectly allowed, bypassing restrictions.
  - The "Clear All" function did not work consistently, especially with long lists.
- **Identified Issues**:
  - Rule enforcement for blacklisted URLs is not robust.
  - The user interface for managing whitelist/blacklist entries has occasional functional inconsistencies.
- **Impact**:
  - Users may unknowingly access restricted URLs or face challenges managing their lists effectively.
- **Recommendations**:
  - Implement stricter validation and rule enforcement for blacklist entries and enhance the reliability of list management features.

4. Multi-Browser Compatibility (42% Success Rate)

- **Failed Scenarios**:
  - The extension failed to work on Firefox due to API compatibility issues.
  - Certain features, such as notifications and URL monitoring, exhibited performance problems on Edge and Brave.
- **Identified Issues**:
  - Lack of implementation for Firefox compatibility, as promised in the project scope.
  - Browser-specific differences in extension APIs causing inconsistent performance.
- **Impact**:
  - Limited cross-browser compatibility restricts user adoption and trust in the extension.
- **Recommendations**:
  - Implement compatibility fixes for Firefox and resolve browser-specific issues to ensure consistent functionality across all supported platforms.

5. Advanced Machine Learning for Phishing Detection (80% Success Rate)

- **Failed Scenarios**:
  - A small percentage of phishing URLs with rare patterns were not flagged.
  - The model generated false positives for certain legitimate URLs, causing user frustration.
- **Identified Issues**:
  - The model needs additional training data to improve recognition of rare phishing patterns.
  - Precision and recall metrics need optimization to reduce false positives.
- **Impact**:
  - Users may lose confidence in the feature due to inaccurate alerts.
- **Recommendations**:

  - Expand the training dataset with more diverse phishing examples and optimize the model to improve precision.

6. Sandbox Integration for File Analysis (80% Success Rate)

- **Failed Scenarios**:
  - The extension crashed when large files were uploaded for scanning.
  - Unsupported file types were not consistently rejected with appropriate error messages.
- **Identified Issues**:
  - File size validation logic is incomplete.
  - Error handling for unsupported file formats needs improvement.
- **Impact**:
  - Users may experience frustration or crashes when uploading files, reducing trust in the feature.
- **Recommendations**:
  - Implement stricter validation rules for file size and types, and enhance error messaging for unsupported files.

7. User-Friendly Interface (0% Success Rate)

- **Failed Scenarios**:
  - Tooltips were unclear or missing for key features.
  - Dark mode preferences failed to persist across sessions.
  - Buttons such as "Clear All" were unresponsive in certain scenarios.
- **Identified Issues**:
  - Poor usability and interface consistency make the extension difficult to navigate, especially for non-technical users.
  - Persistent state management for user preferences is missing or buggy.
- **Impact**:
  - Users may find the extension frustrating or confusing, leading to poor adoption rates.
- **Recommendations**:
  - Redesign the interface with a focus on usability, consistent styling, and functional persistence of settings.

8. Severity-Based Alerts (66% Success Rate)

- **Failed Scenarios**:
  - Alerts for moderate threat levels did not include appropriate recommended actions.
  - High-severity alerts occasionally displayed generic messaging rather than tailored recommendations.
- **Identified Issues**:
  - Incomplete logic for assigning and displaying recommendations based on severity.
- **Impact**:

  - Users may struggle to assess and act on certain alerts due to insufficient guidance.
- **Recommendations**:
  - Enhance the alert system with context-specific recommendations for each severity level.

Summary of Issues and Limitations

Despite the overall success and progress of Version 2, these identified issues underscore areas that need further improvement to meet the goals outlined in the project proposal. Key limitations include incomplete cross-browser compatibility, inconsistent user interface elements, and gaps in advanced detection mechanisms for phishing and malware. Addressing these issues in subsequent iterations will be critical to enhancing the extension's functionality, reliability, and user experience.

5.0 TESTING AND EVALUATION OF VERSION 3

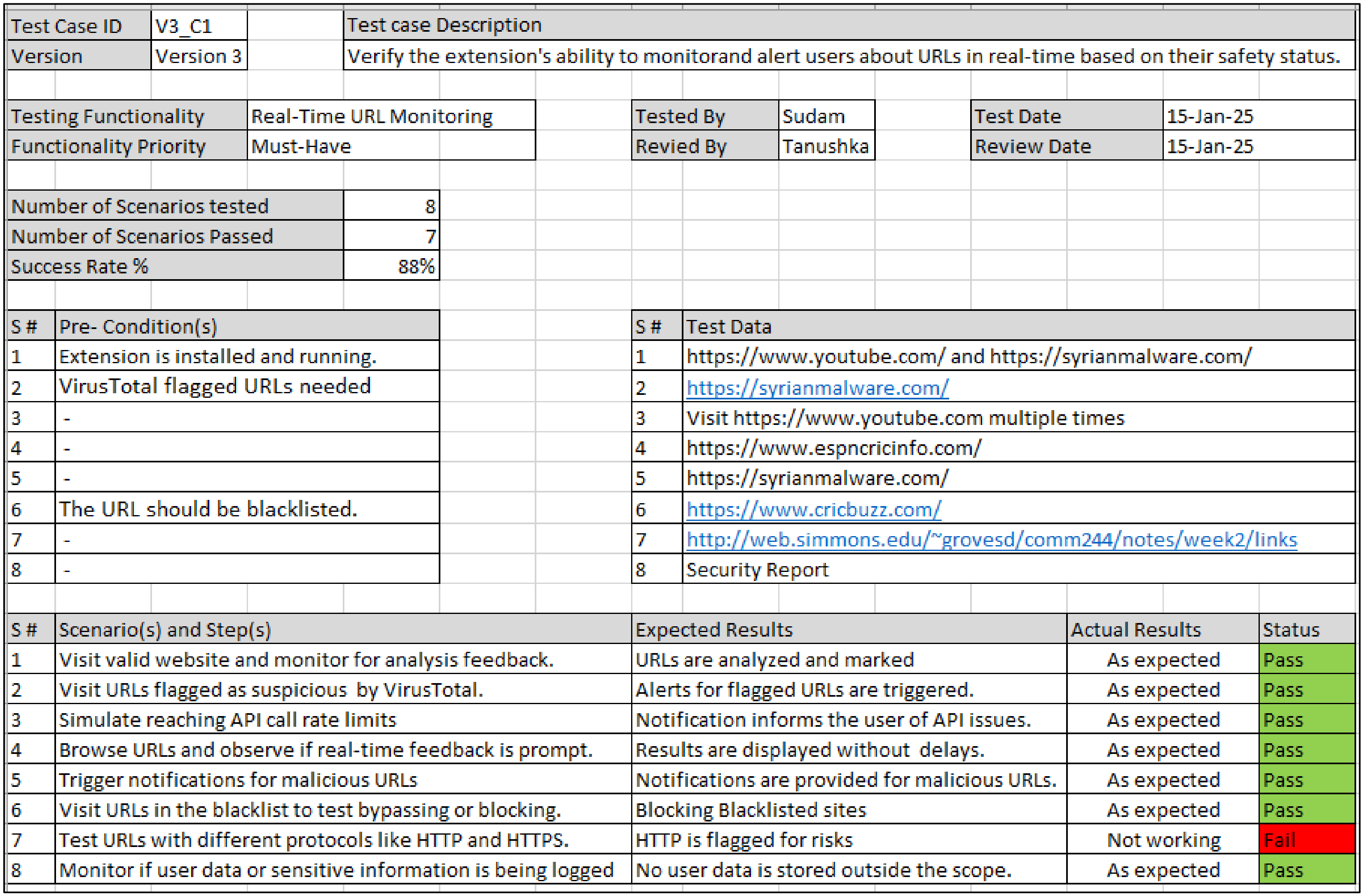
On January 15, 2025, the third version of the Aegis Shield - Phishing Detection Extension underwent testing after the development of 12 core features. This testing phase focused on evaluating all implemented features using structured test cases and scenarios to assess their functionality, accuracy, and performance. The results of this testing highlighted significant improvements, particularly in areas such as User-Friendly Interface and Multi-Browser Compatibility, which had previously faced challenges. This version reflects the team's continued commitment to refining the extension and delivering a more reliable and comprehensive phishing detection tool.

The table below summarizes the results of Version 3 testing, including the number of scenarios tested, passed scenarios, and success rates for each feature. These metrics showcase the progress made in addressing issues from prior versions and highlight areas where features have achieved optimal functionality.

Requirement name	Test Case ID	No. of Scenarios Tested
Real-Time URL Monitoring	V2_C1	8
Phishing URL Detection	V2_C2	4
Basic URL Alerts	V2_C3	3
Whitelist/Blacklist Management	V2_C4	7
Basic Malware Detection	V2_C5	4
Email Phishing Detection	V2_C6	4
Browser Notifications	V2_C7	5
User-Friendly Interface	V2_C8	6
Severity-Based Alerts	V2_C9	3
Advanced Machine Learning for Phishing Detection	V2_C10	5
Multi-Browser Compatibility	V2_C11	7
Sandbox Integration for File Analysis	V2_C12	5
Total Number of Test Cases Tested: 12		
Total Number of Scenarios Tested: 61		

Table 7: Testing Phase 3 Overview

5.1 TEST CASE 1: Real-Time URL Monitoring



Test Case ID	V3_C1		Test case Description
Version	Version 3		Verify the extension's ability to monitorand alert users about URLs in real-time based on their safety status.

Testing Functionality	Real-Time URL Monitoring	Tested By	Sudam	Test Date	15-Jan-25
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	15-Jan-25

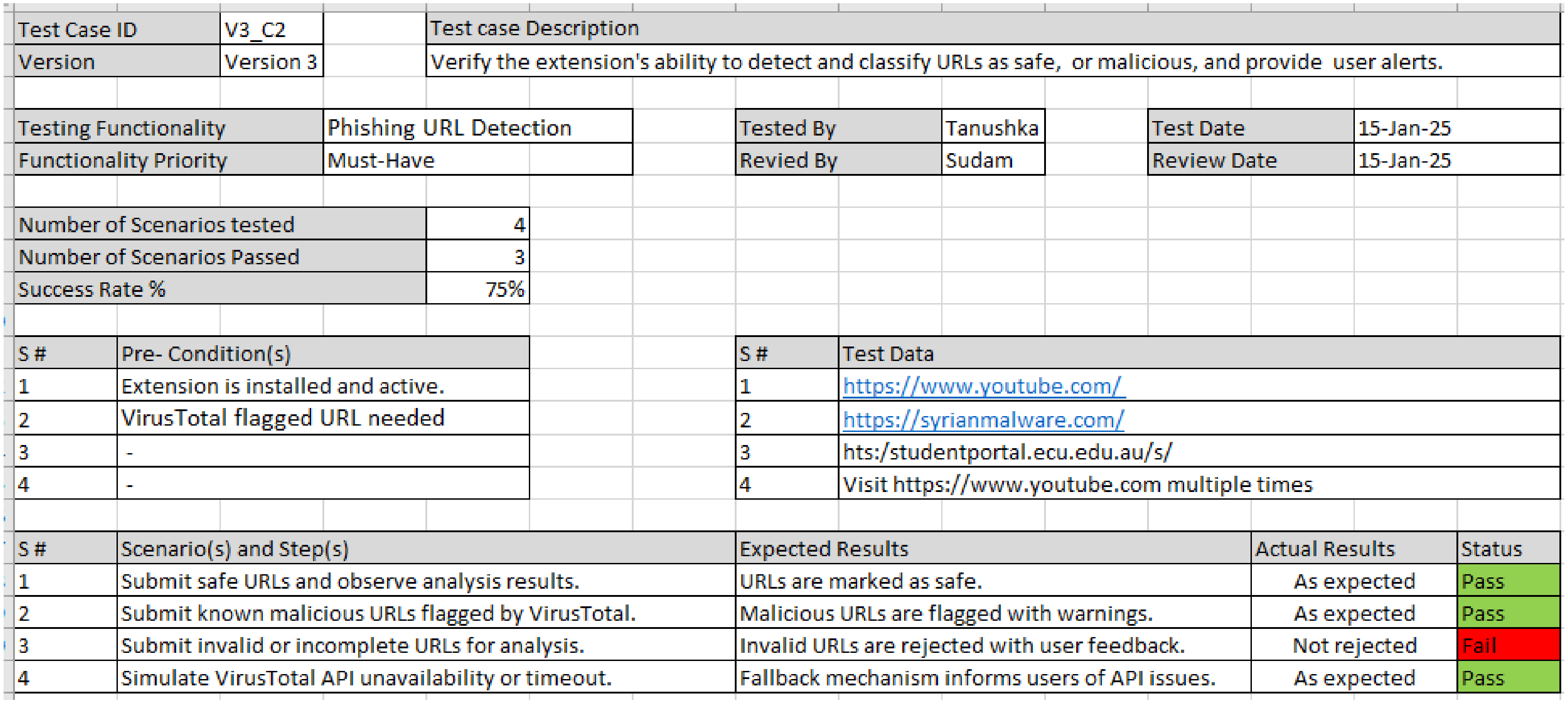
Number of Scenarios tested	8
Number of Scenarios Passed	7
Success Rate %	88%

S #	Pre- Condition(s)	S #	Test Data
1	Extension is installed and running.	1	https://www.youtube.com/ and https://syrianmalware.com/
2	VirusTotal flagged URLs needed	2	https://syrianmalware.com/
3	-	3	Visit https://www.youtube.com multiple times
4	-	4	https://www.espncricinfo.com/
5	-	5	https://syrianmalware.com/
6	The URL should be blacklisted.	6	https://www.cricbuzz.com/
7	-	7	http://web.simmons.edu/~grovesd/comm244/notes/week2/links
8	-	8	Security Report

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit valid website and monitor for analysis feedback.	URLs are analyzed and marked	As expected	Pass
2	Visit URLs flagged as suspicious by VirusTotal.	Alerts for flagged URLs are triggered.	As expected	Pass
3	Simulate reaching API call rate limits	Notification informs the user of API issues.	As expected	Pass
4	Browse URLs and observe if real-time feedback is prompt.	Results are displayed without delays.	As expected	Pass
5	Trigger notifications for malicious URLs	Notifications are provided for malicious URLs.	As expected	Pass
6	Visit URLs in the blacklist to test bypassing or blocking.	Blocking Blacklisted sites	As expected	Pass
7	Test URLs with different protocols like HTTP and HTTPS.	HTTP is flagged for risks	Not working	Fail
8	Monitor if user data or sensitive information is being logged	No user data is stored outside the scope.	As expected	Pass

Figure 24: TEST CASE 1: Real-Time URL Monitoring

5.2 TEST CASE 2: Phishing URL Detection



Test Case ID	V3_C2	Test case Description
Version	Version 3	Verify the extension's ability to detect and classify URLs as safe, or malicious, and provide user alerts.

Testing Functionality	Phishing URL Detection	Tested By	Tanushka	Test Date	15-Jan-25
Functionality Priority	Must-Have	Revied By	Sudam	Review Date	15-Jan-25

Number of Scenarios tested	4
Number of Scenarios Passed	3
Success Rate %	75%

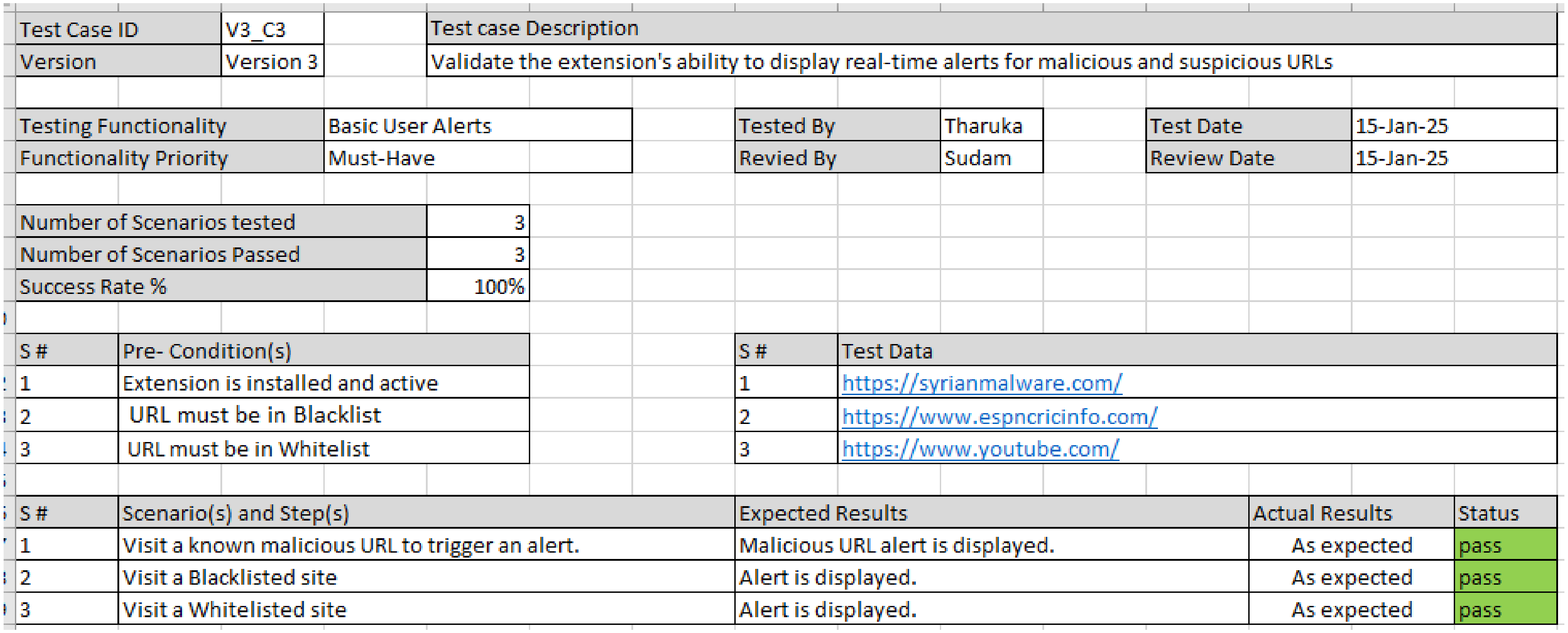
S #	Pre- Condition(s)
1	Extension is installed and active.
2	VirusTotal flagged URL needed
3	-
4	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	hts:/studentportal.ecu.edu.au/s/
4	Visit https://www.youtube.com multiple times

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit safe URLs and observe analysis results.	URLs are marked as safe.	As expected	Pass
2	Submit known malicious URLs flagged by VirusTotal.	Malicious URLs are flagged with warnings.	As expected	Pass
3	Submit invalid or incomplete URLs for analysis.	Invalid URLs are rejected with user feedback.	Not rejected	Fail
4	Simulate VirusTotal API unavailability or timeout.	Fallback mechanism informs users of API issues.	As expected	Pass

Figure 25: TEST CASE 2: Phishing URL Detection

5.3 TEST CASE 3: Basic User Alerts



Test Case ID	V3_C3		Test case Description
Version	Version 3		Validate the extension's ability to display real-time alerts for malicious and suspicious URLs

Testing Functionality	Basic User Alerts	Tested By	Tharuka	Test Date	15-Jan-25
Functionality Priority	Must-Have	Revied By	Sudam	Review Date	15-Jan-25

Number of Scenarios tested	3
Number of Scenarios Passed	3
Success Rate %	100%

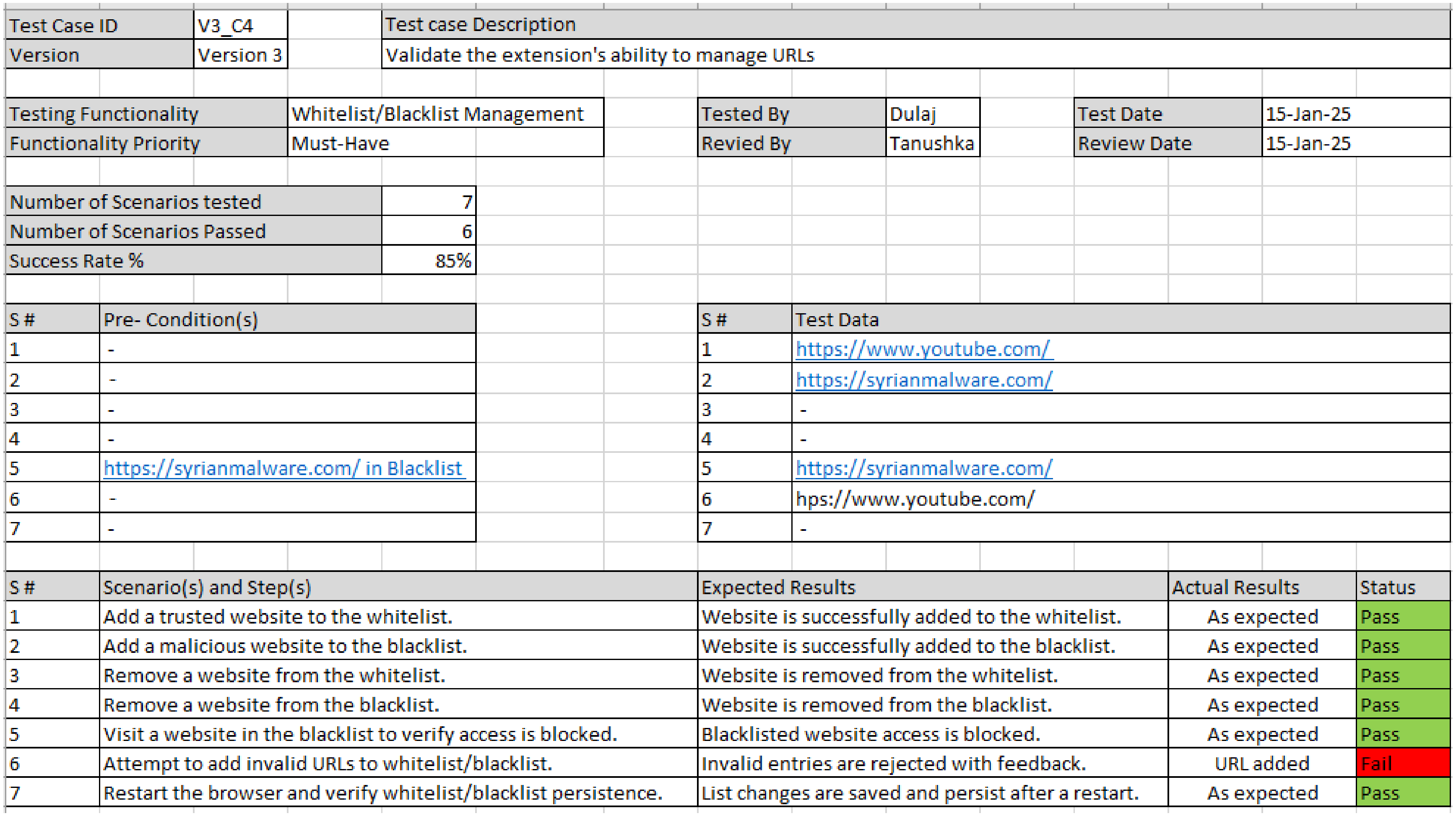
S #	Pre- Condition(s)
1	Extension is installed and active
2	URL must be in Blacklist
3	URL must be in Whitelist

S #	Test Data
1	https://syrianmalware.com/
2	https://www.espncricinfo.com/
3	https://www.youtube.com/

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a known malicious URL to trigger an alert.	Malicious URL alert is displayed.	As expected	pass
2	Visit a Blacklisted site	Alert is displayed.	As expected	pass
3	Visit a Whitelisted site	Alert is displayed.	As expected	pass

Figure 26: TEST CASE 3: Basic User Alerts

5.4 TEST CASE 4: Whitelist/Blacklist Management



Test Case ID	V3_C4		Test case Description
Version	Version 3		Validate the extension's ability to manage URLs

Testing Functionality	Whitelist/Blacklist Management		Tested By	Dulaj		Test Date	15-Jan-25
Functionality Priority	Must-Have		Revied By	Tanushka		Review Date	15-Jan-25

Number of Scenarios tested	7
Number of Scenarios Passed	6
Success Rate %	85%

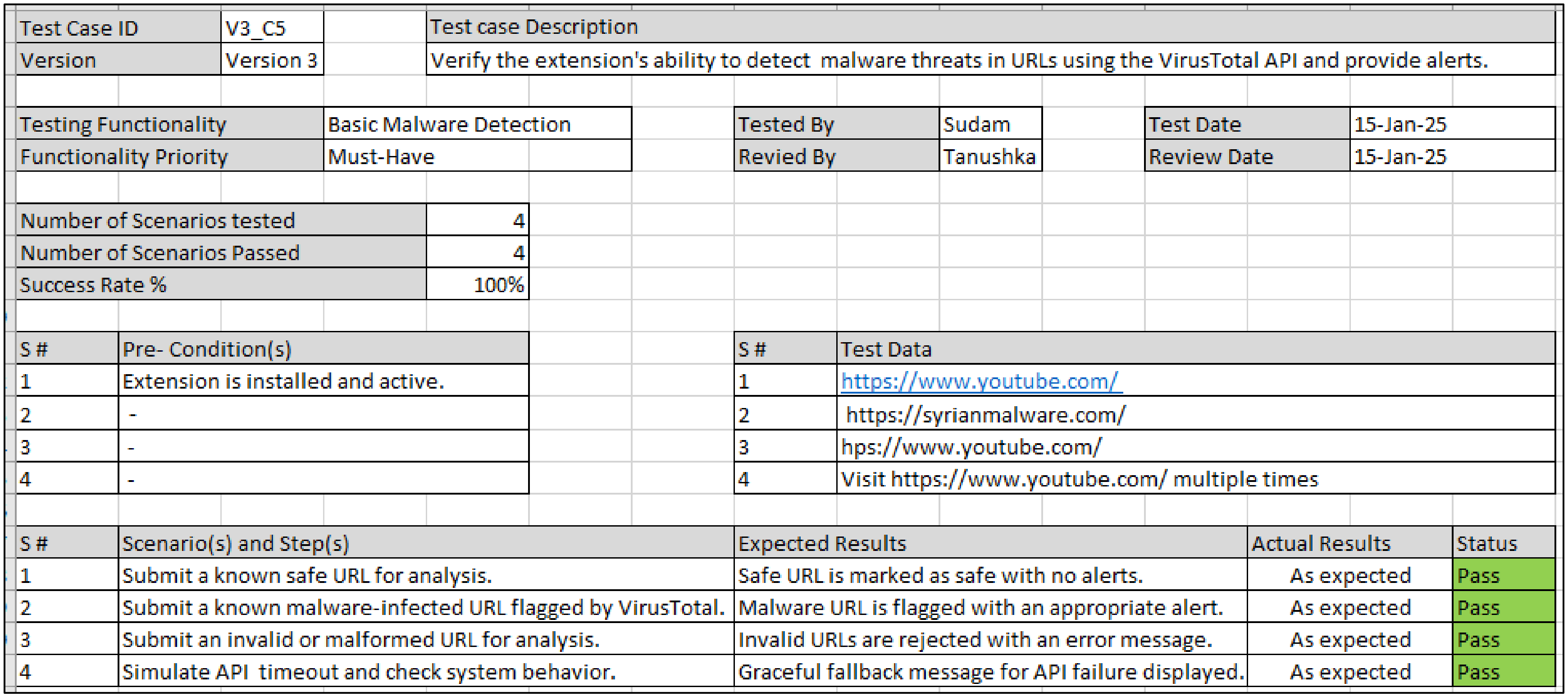
S #	Pre- Condition(s)
1	-
2	-
3	-
4	-
5	https://syrianmalware.com/ in Blacklist
6	-
7	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	-
4	-
5	https://syrianmalware.com/
6	hps://www.youtube.com/
7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Add a trusted website to the whitelist.	Website is successfully added to the whitelist.	As expected	Pass
2	Add a malicious website to the blacklist.	Website is successfully added to the blacklist.	As expected	Pass
3	Remove a website from the whitelist.	Website is removed from the whitelist.	As expected	Pass
4	Remove a website from the blacklist.	Website is removed from the blacklist.	As expected	Pass
5	Visit a website in the blacklist to verify access is blocked.	Blacklisted website access is blocked.	As expected	Pass
6	Attempt to add invalid URLs to whitelist/blacklist.	Invalid entries are rejected with feedback.	URL added	Fail
7	Restart the browser and verify whitelist/blacklist persistence.	List changes are saved and persist after a restart.	As expected	Pass

Figure 27: TEST CASE 4: Whitelist/Blacklist Management

5.5 TEST CASE 5: Basic Malware Detection



Test Case ID	V3_C5		Test case Description
Version	Version 3		Verify the extension's ability to detect malware threats in URLs using the VirusTotal API and provide alerts.

Testing Functionality	Basic Malware Detection		Tested By	Sudam		Test Date	15-Jan-25
Functionality Priority	Must-Have		Revied By	Tanushka		Review Date	15-Jan-25

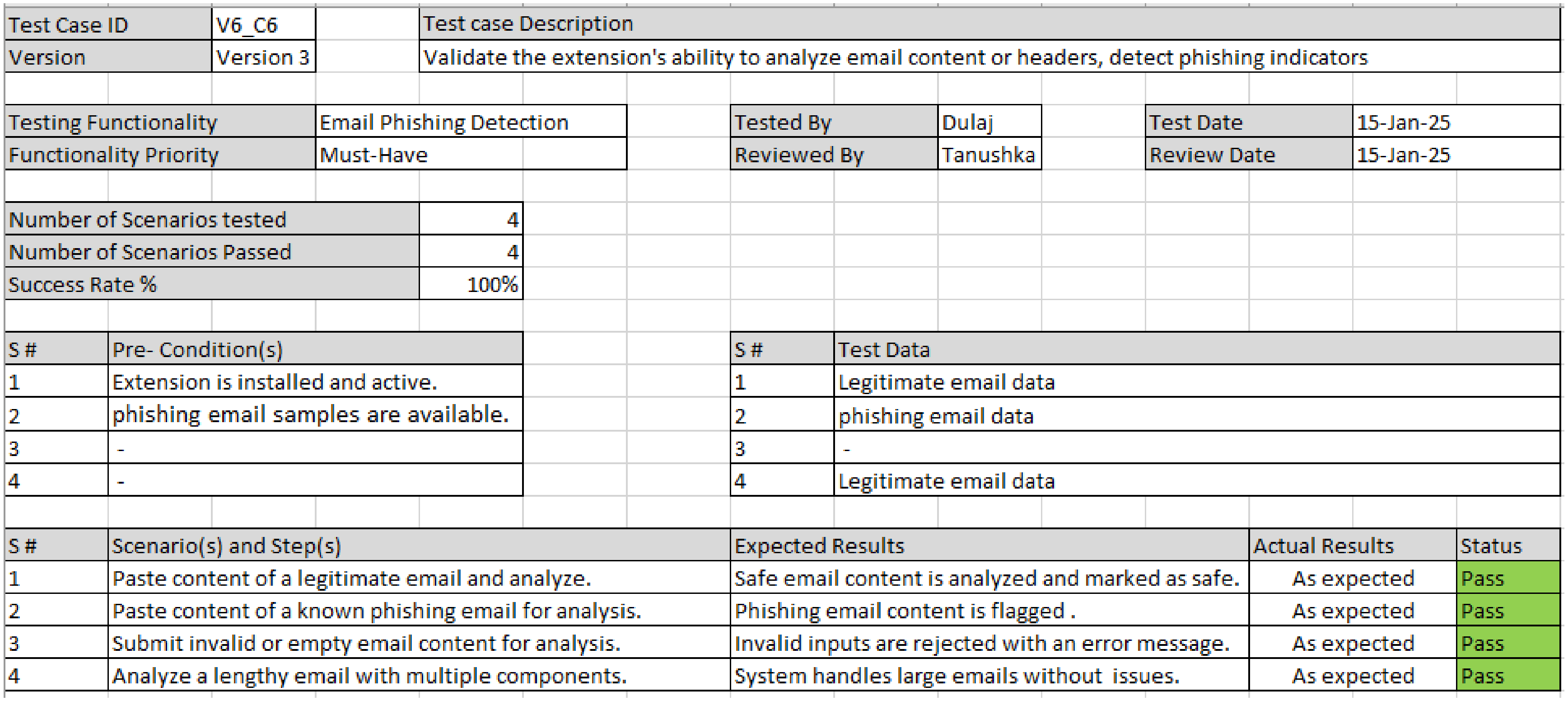
Number of Scenarios tested	4
Number of Scenarios Passed	4
Success Rate %	100%

S #	Pre- Condition(s)		S #	Test Data
1	Extension is installed and active.		1	https://www.youtube.com/
2	-		2	https://syrianmalware.com/
3	-		3	hps://www.youtube.com/
4	-		4	Visit https://www.youtube.com/ multiple times

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit a known safe URL for analysis.	Safe URL is marked as safe with no alerts.	As expected	Pass
2	Submit a known malware-infected URL flagged by VirusTotal.	Malware URL is flagged with an appropriate alert.	As expected	Pass
3	Submit an invalid or malformed URL for analysis.	Invalid URLs are rejected with an error message.	As expected	Pass
4	Simulate API timeout and check system behavior.	Graceful fallback message for API failure displayed.	As expected	Pass

Figure 28: TEST CASE 5: Basic Malware Detection

5.6 TEST CASE 6: Email Phishing Detection



Test Case ID	V6_C6	Test case Description
Version	Version 3	Validate the extension's ability to analyze email content or headers, detect phishing indicators

Testing Functionality	Email Phishing Detection	Tested By	Dulaj	Test Date	15-Jan-25
Functionality Priority	Must-Have	Reviewed By	Tanushka	Review Date	15-Jan-25

Number of Scenarios tested	4
Number of Scenarios Passed	4
Success Rate %	100%

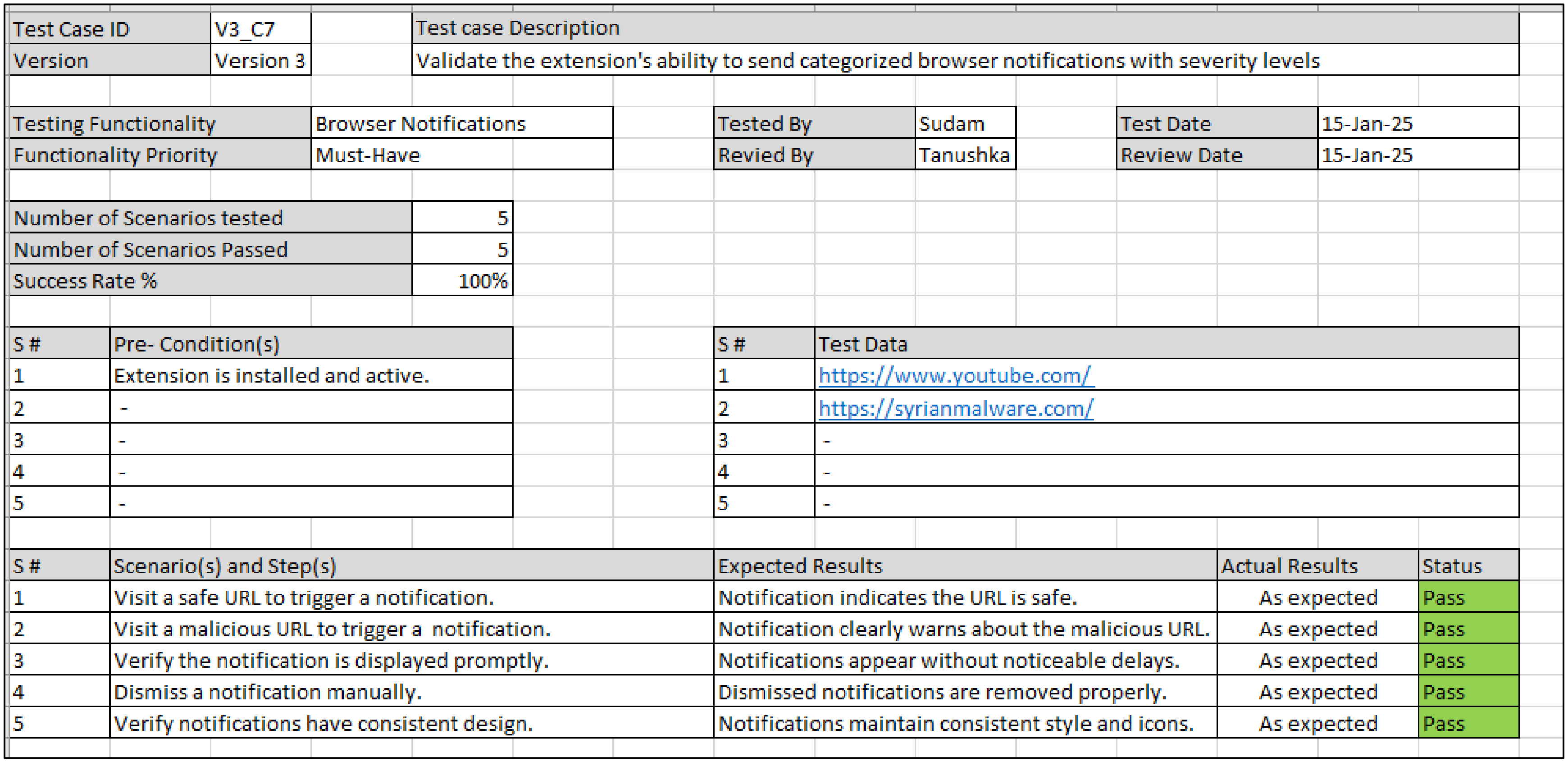
S #	Pre- Condition(s)
1	Extension is installed and active.
2	phishing email samples are available.
3	-
4	-

S #	Test Data
1	Legitimate email data
2	phishing email data
3	-
4	Legitimate email data

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Paste content of a legitimate email and analyze.	Safe email content is analyzed and marked as safe.	As expected	Pass
2	Paste content of a known phishing email for analysis.	Phishing email content is flagged .	As expected	Pass
3	Submit invalid or empty email content for analysis.	Invalid inputs are rejected with an error message.	As expected	Pass
4	Analyze a lengthy email with multiple components.	System handles large emails without issues.	As expected	Pass

Figure 29: TEST CASE 6: Email Phishing Detection

5.7 TEST CASE 7: Browser Notifications



Test Case ID	V3_C7	Test case Description
Version	Version 3	Validate the extension's ability to send categorized browser notifications with severity levels

Testing Functionality	Browser Notifications	Tested By	Sudam	Test Date	15-Jan-25
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	15-Jan-25

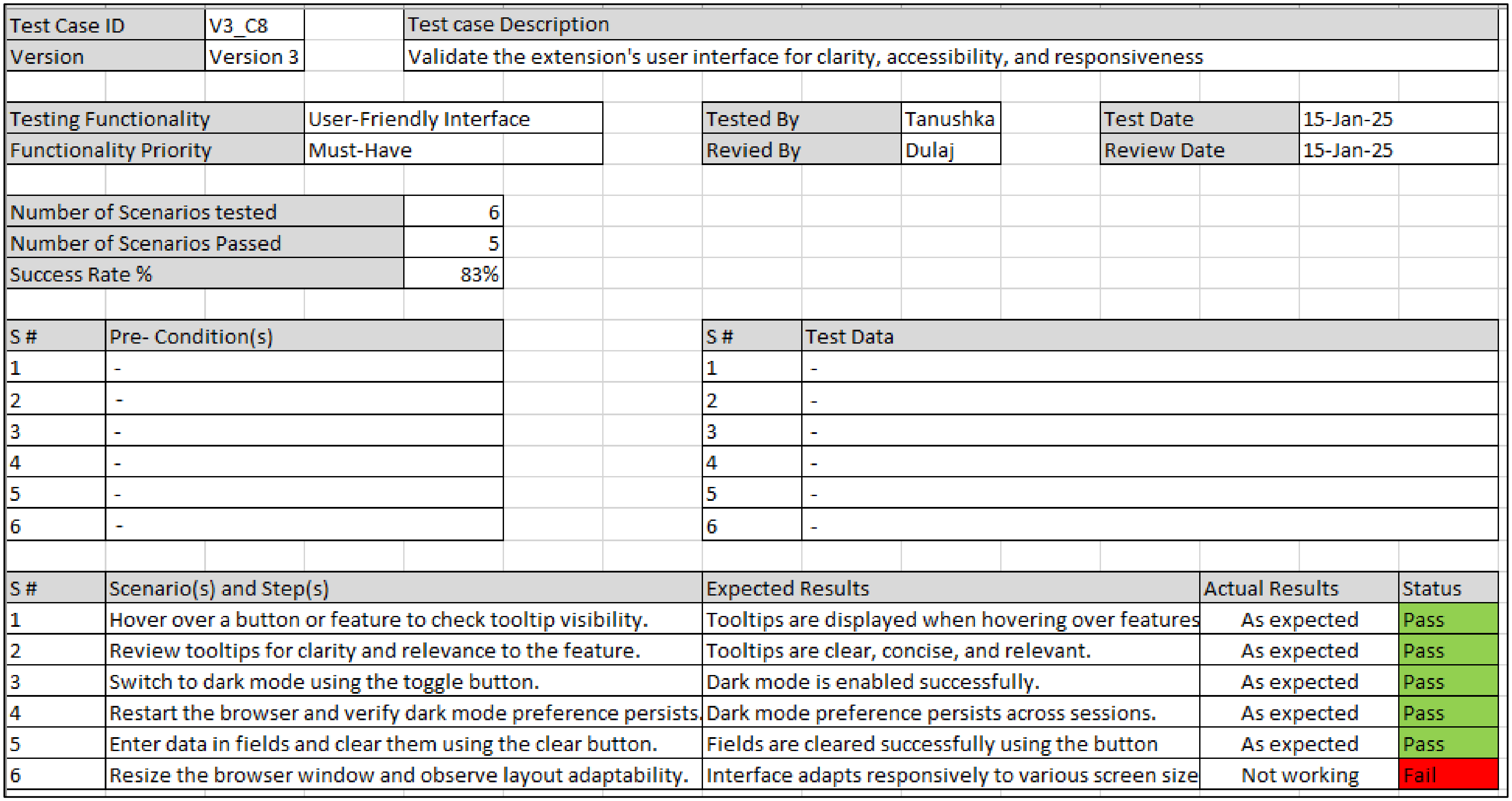
Number of Scenarios tested	5
Number of Scenarios Passed	5
Success Rate %	100%

S #	Pre- Condition(s)	S #	Test Data
1	Extension is installed and active.	1	https://www.youtube.com/
2	-	2	https://syrianmalware.com/
3	-	3	-
4	-	4	-
5	-	5	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a safe URL to trigger a notification.	Notification indicates the URL is safe.	As expected	Pass
2	Visit a malicious URL to trigger a notification.	Notification clearly warns about the malicious URL.	As expected	Pass
3	Verify the notification is displayed promptly.	Notifications appear without noticeable delays.	As expected	Pass
4	Dismiss a notification manually.	Dismissed notifications are removed properly.	As expected	Pass
5	Verify notifications have consistent design.	Notifications maintain consistent style and icons.	As expected	Pass

Figure 30: TEST CASE 7: Browser Notifications

5.8 TEST CASE 8: User-Friendly Interface



Test Case ID	V3_C8	Test case Description
Version	Version 3	Validate the extension's user interface for clarity, accessibility, and responsiveness

Testing Functionality	User-Friendly Interface	Tested By	Tanushka	Test Date	15-Jan-25
Functionality Priority	Must-Have	Revied By	Dulaj	Review Date	15-Jan-25

Number of Scenarios tested	6
Number of Scenarios Passed	5
Success Rate %	83%

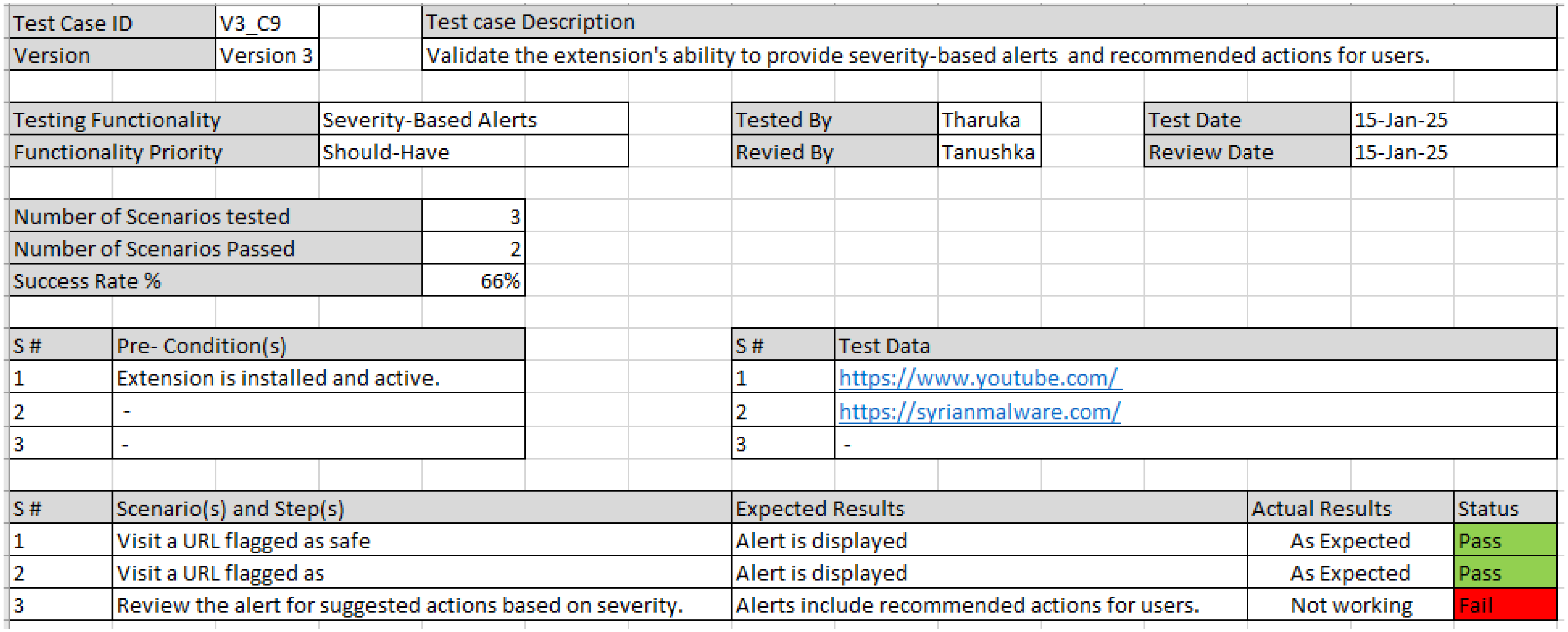
S #	Pre- Condition(s)
1	-
2	-
3	-
4	-
5	-
6	-

S #	Test Data
1	-
2	-
3	-
4	-
5	-
6	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Hover over a button or feature to check tooltip visibility.	Tooltips are displayed when hovering over features	As expected	Pass
2	Review tooltips for clarity and relevance to the feature.	Tooltips are clear, concise, and relevant.	As expected	Pass
3	Switch to dark mode using the toggle button.	Dark mode is enabled successfully.	As expected	Pass
4	Restart the browser and verify dark mode preference persists.	Dark mode preference persists across sessions.	As expected	Pass
5	Enter data in fields and clear them using the clear button.	Fields are cleared successfully using the button	As expected	Pass
6	Resize the browser window and observe layout adaptability.	Interface adapts responsively to various screen size	Not working	Fail

Figure 31: TEST CASE 8: User-Friendly Interface

5.9 TEST CASE 9: Severity-Based Alerts



Test Case ID	V3_C9		Test case Description
Version	Version 3		Validate the extension's ability to provide severity-based alerts and recommended actions for users.

Testing Functionality	Severity-Based Alerts	Tested By	Tharuka	Test Date	15-Jan-25
Functionality Priority	Should-Have	Revied By	Tanushka	Review Date	15-Jan-25

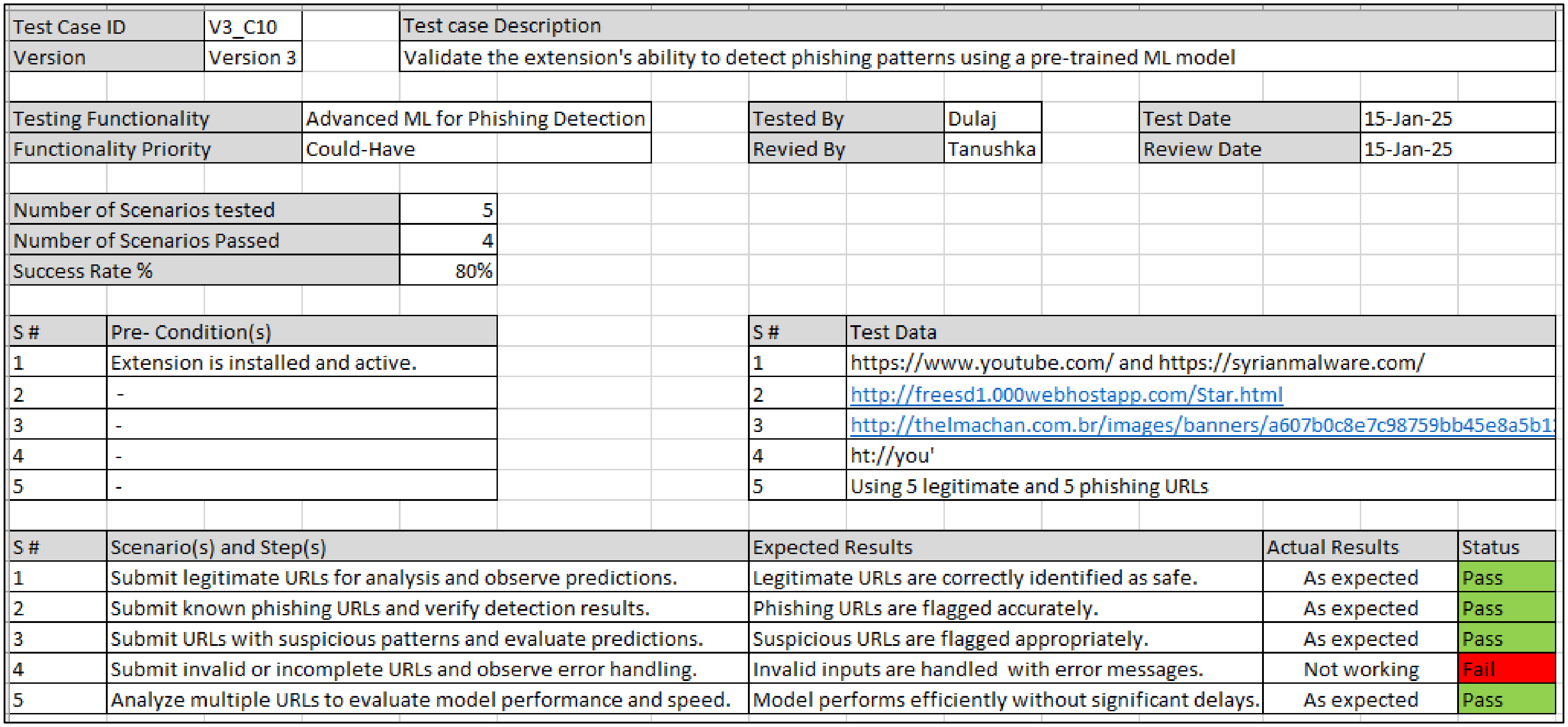
Number of Scenarios tested	3
Number of Scenarios Passed	2
Success Rate %	66%

S #	Pre- Condition(s)	S #	Test Data
1	Extension is installed and active.	1	https://www.youtube.com/
2	-	2	https://syrianmalware.com/
3	-	3	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a URL flagged as safe	Alert is displayed	As Expected	Pass
2	Visit a URL flagged as	Alert is displayed	As Expected	Pass
3	Review the alert for suggested actions based on severity.	Alerts include recommended actions for users.	Not working	Fail

Figure 32: TEST CASE 9: Severity-Based Alerts

5.10 TEST CASE 10: Advanced Machine Learning for Phishing Detection



Test Case ID	V3_C10	Test case Description	
Version	Version 3	Validate the extension's ability to detect phishing patterns using a pre-trained ML model	

Testing Functionality	Advanced ML for Phishing Detection	Tested By	Dulaj	Test Date	15-Jan-25
Functionality Priority	Could-Have	Revied By	Tanushka	Review Date	15-Jan-25

Number of Scenarios tested	5
Number of Scenarios Passed	4
Success Rate %	80%

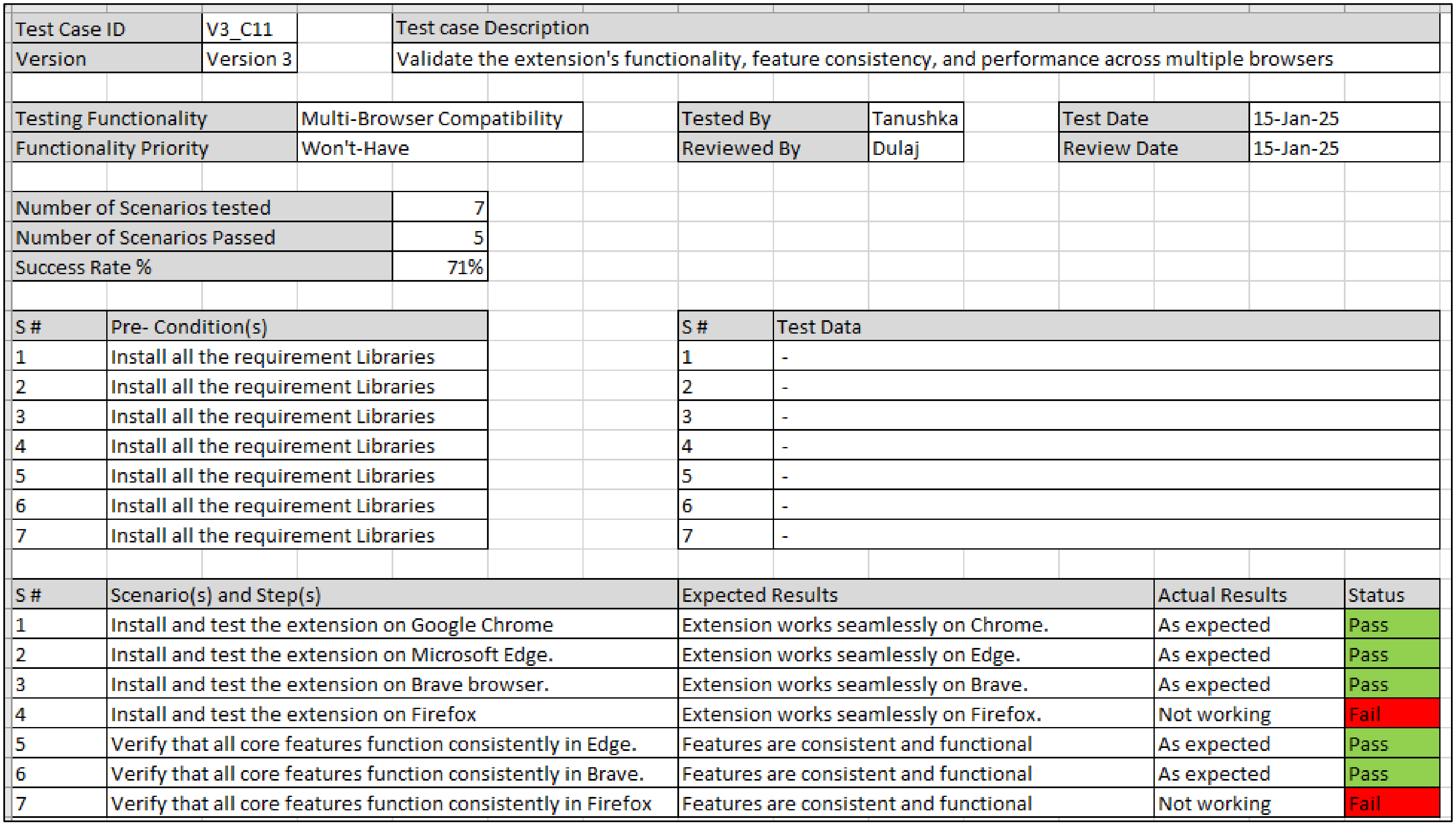
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-
5	-

S #	Test Data
1	https://www.youtube.com/ and https://syrianmalware.com/
2	http://freesd1.000webhostapp.com/Star.html
3	http://thelmachan.com.br/images/banners/a607b0c8e7c98759bb45e8a5b1
4	ht://you'
5	Using 5 legitimate and 5 phishing URLs

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit legitimate URLs for analysis and observe predictions.	Legitimate URLs are correctly identified as safe.	As expected	Pass
2	Submit known phishing URLs and verify detection results.	Phishing URLs are flagged accurately.	As expected	Pass
3	Submit URLs with suspicious patterns and evaluate predictions.	Suspicious URLs are flagged appropriately.	As expected	Pass
4	Submit invalid or incomplete URLs and observe error handling.	Invalid inputs are handled with error messages.	Not working	Fail
5	Analyze multiple URLs to evaluate model performance and speed.	Model performs efficiently without significant delays.	As expected	Pass

Figure 33: TEST CASE 10: Advanced Machine Learning for Phishing Detection

5.11 TEST CASE 11: Multi-Browser Compatibility



Test Case ID	V3_C11		Test case Description
Version	Version 3		Validate the extension's functionality, feature consistency, and performance across multiple browsers

Testing Functionality	Multi-Browser Compatibility	Tested By	Tanushka	Test Date	15-Jan-25
Functionality Priority	Won't-Have	Reviewed By	Dulaj	Review Date	15-Jan-25

Number of Scenarios tested	7
Number of Scenarios Passed	5
Success Rate %	71%

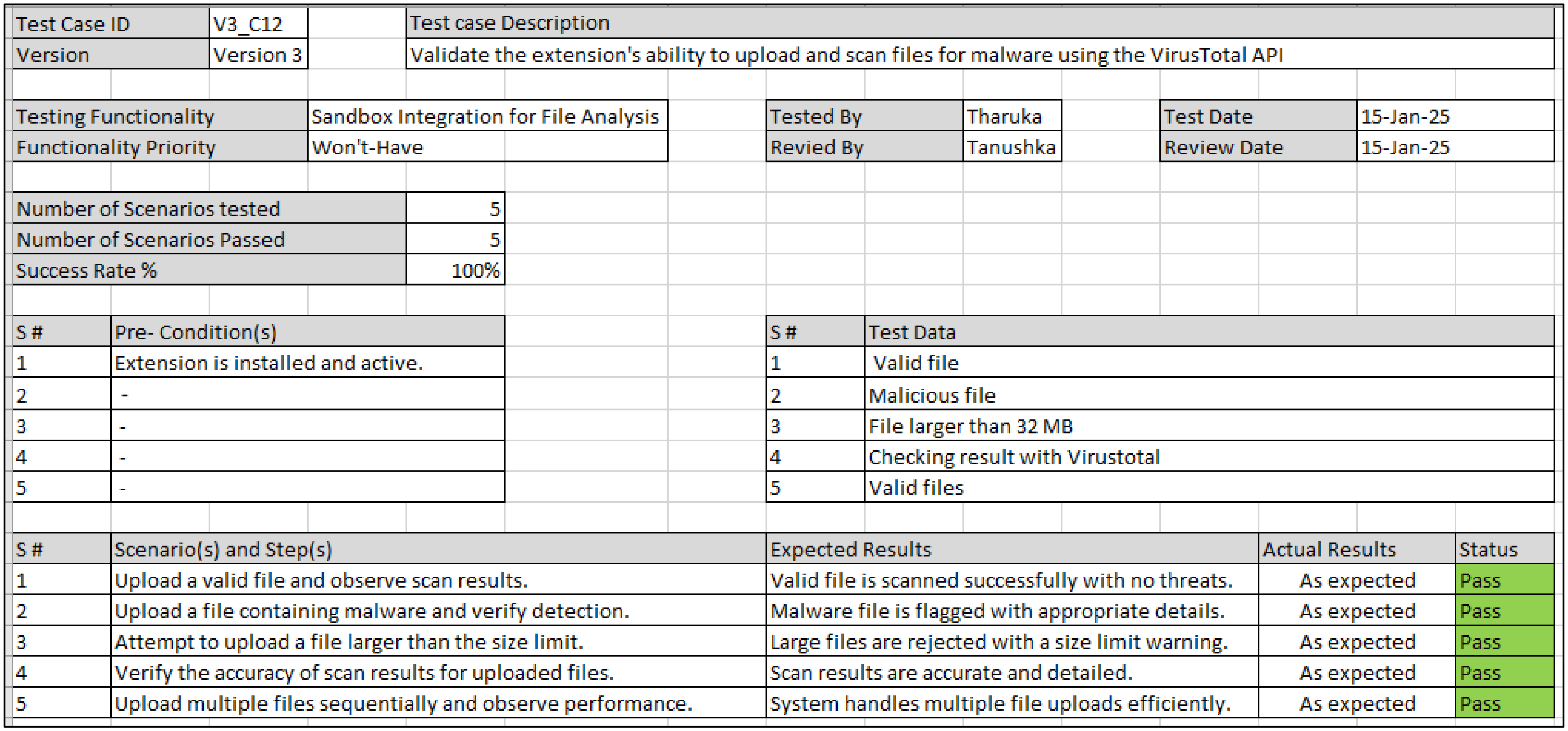
S #	Pre- Condition(s)
1	Install all the requirement Libraries
2	Install all the requirement Libraries
3	Install all the requirement Libraries
4	Install all the requirement Libraries
5	Install all the requirement Libraries
6	Install all the requirement Libraries
7	Install all the requirement Libraries

S #	Test Data
1	-
2	-
3	-
4	-
5	-
6	-
7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Install and test the extension on Google Chrome	Extension works seamlessly on Chrome.	As expected	Pass
2	Install and test the extension on Microsoft Edge.	Extension works seamlessly on Edge.	As expected	Pass
3	Install and test the extension on Brave browser.	Extension works seamlessly on Brave.	As expected	Pass
4	Install and test the extension on Firefox	Extension works seamlessly on Firefox.	Not working	Fail
5	Verify that all core features function consistently in Edge.	Features are consistent and functional	As expected	Pass
6	Verify that all core features function consistently in Brave.	Features are consistent and functional	As expected	Pass
7	Verify that all core features function consistently in Firefox	Features are consistent and functional	Not working	Fail

Figure 34: TEST CASE 11: Multi-Browser Compatibility

5.12 TEST CASE 12: Sandbox Integration for File Analysis



		Test case Description
Test Case ID	V3_C12	
Version	Version 3	Validate the extension's ability to upload and scan files for malware using the VirusTotal API

Testing Functionality	Sandbox Integration for File Analysis	Tested By	Tharuka	Test Date	15-Jan-25
Functionality Priority	Won't-Have	Revied By	Tanushka	Review Date	15-Jan-25

Number of Scenarios tested	5
Number of Scenarios Passed	5
Success Rate %	100%

S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-
5	-

S #	Test Data
1	Valid file
2	Malicious file
3	File larger than 32 MB
4	Checking result with Virustotal
5	Valid files

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Upload a valid file and observe scan results.	Valid file is scanned successfully with no threats.	As expected	Pass
2	Upload a file containing malware and verify detection.	Malware file is flagged with appropriate details.	As expected	Pass
3	Attempt to upload a file larger than the size limit.	Large files are rejected with a size limit warning.	As expected	Pass
4	Verify the accuracy of scan results for uploaded files.	Scan results are accurate and detailed.	As expected	Pass
5	Upload multiple files sequentially and observe performance.	System handles multiple file uploads efficiently.	As expected	Pass

Figure 35: TEST CASE 12: Sandbox Integration for File Analysis

5.13 TESTED RESULTS SUMMARY FOR VERSION 3

The testing results for Version 3 of the Aegis Shield - Phishing Detection Extension demonstrate substantial improvements across the board, with most features achieving higher success rates compared to previous versions. Features such as Basic Malware Detection, Email Phishing Detection, and Browser Notifications achieved a perfect 100% success rate, indicating their readiness for deployment. The User-Friendly Interface showed significant progress, with an 83% success rate, reflecting improvements in usability and responsiveness. However, some features, including Severity-Based Alerts and Multi-Browser Compatibility, still present challenges, with moderate success rates. Overall, the results validate the enhancements made in Version 3 while identifying areas that require further refinement in future updates. This version highlights the team's commitment to continuous improvement and delivering a reliable phishing detection solution.

Requirement name	**Test Case ID**	**No. of Scenarios Tested**	**No. of Passed Scenarios**	**Success Rate**
Real-Time URL Monitoring	V3_C1	8	7	88%
Phishing URL Detection	V3_C2	4	3	75%
Basic URL Alerts	V3_C3	3	3	100%
Whitelist/Blacklist Management	V3_C4	7	6	85%
Basic Malware Detection	V3_C5	4	4	100%
Email Phishing Detection	V3_C6	4	4	100%
Browser Notifications	V3_C7	5	5	100%
User-Friendly Interface	V3_C8	6	5	83%
Severity-Based Alerts	V3_C9	3	2	66%
Advanced Machine Learning for Phishing Detection	V3_C10	5	4	80%
Multi-Browser Compatibility	V3_C11	7	5	71%
Sandbox Integration for File Analysis	V3_C12	5	5	100%

Table 8: Version 3 Results

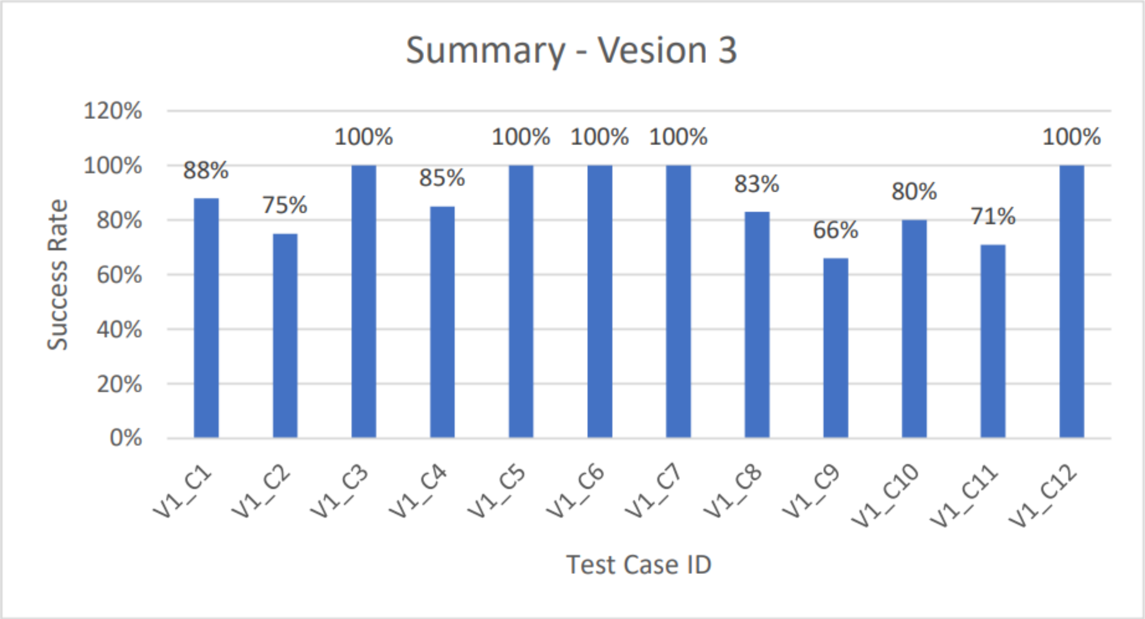


Figure 36: Summary Version 3

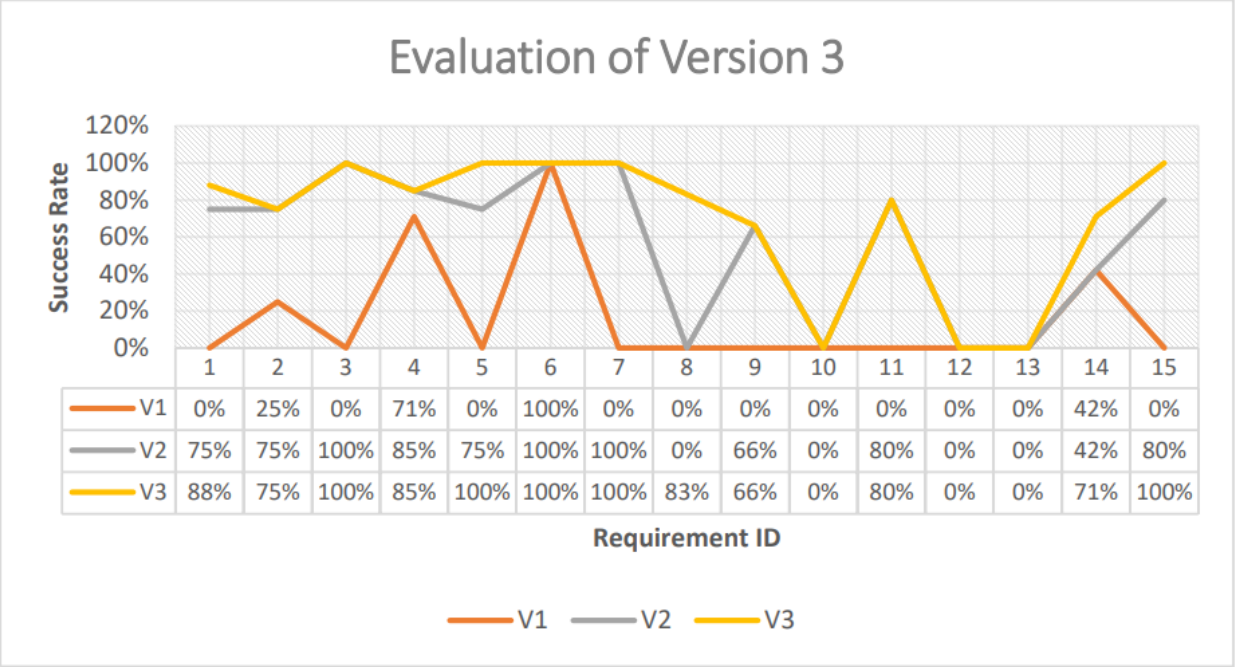
5.14 EVALUATION OF THE VERSION(S)

The evaluation of Versions 1, 2, and 3 of the Aegis Shield - Phishing Detection Extension demonstrates a clear trajectory of improvement across implemented features. Version 3 showcases significant progress, with features like Real-Time URL Monitoring and Multi-Browser Compatibility achieving their highest success rates to date, at 88% and 71% respectively. Core functionalities, including Basic Malware Detection, Email Phishing Detection, and Browser Notifications, maintained a consistent 100% success rate, showcasing their robustness. Despite these advancements, areas like Severity-Based Alerts and User-Friendly Interface still require further optimization to reach their full potential. This evaluation emphasizes the team's ability to address limitations identified in earlier versions while paving the way for comprehensive feature refinement and enhanced user satisfaction in future iterations.

		Success Rate of the Version tested		
Requirement ID	**Requirement name**	**V1**	**V2**	**V3**
1	Real-Time URL Monitoring	0%	75%	88%
2	Phishing URL Detection	25%	75%	75%
3	Basic User Alerts	Not-Developed	100%	100%
4	Whitelist/Blacklist Management	71%	85%	85%
5	Basic Malware Detection	Not-Developed	75%	100%
6	Email Phishing Detection	100%	100%	100%
7	Browser Notifications	Not-Developed	100%	100%
8	User-Friendly Interface	0%	0%	83%
9	Severity-Based Alerts	Not-Developed	66%	66%
10	Email Content Parsing	Not-Developed	Not-Developed	Not-Developed
11	Advanced Machine Learning for Phishing Detection	Not-Developed	80%	80%
12	Heuristic URL Analysis	Not-Developed	Not-Developed	Not-Developed
13	Customizable User Settings	Not-Developed	Not-Developed	Not-Developed
14	Multi-Browser Compatibility	42%	42%	71%
15	Sandbox Integration for File Analysis	Not-Developed	80%	100%

Table 9: Evaluation of version 3

The figure below compares the success rates of implemented features across Versions 1, 2, and 3 of the Aegis Shield - Phishing Detection Extension. It highlights the steady improvements made in key areas, such as Real-Time URL Monitoring and Multi-Browser Compatibility, while showcasing consistently high-performing features like Email Phishing Detection and Browser Notifications. These trends reflect the team's commitment to resolving issues and enhancing functionality with each iteration.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
V1	0%	25%	0%	71%	0%	100%	0%	0%	0%	0%	0%	0%	0%	42%	0%
V2	75%	75%	100%	85%	75%	100%	100%	0%	66%	0%	80%	0%	0%	42%	80%
V3	88%	75%	100%	85%	100%	100%	100%	83%	66%	0%	80%	0%	0%	71%	100%

Figure 37: Evaluation of version 3

5.15 IDENTIFIED ISSUES/LIMITATIONS DURING TESTING

The testing phase for Version 3 of the Aegis Shield - Phishing Detection Extension revealed substantial progress, with most features achieving higher success rates compared to previous versions. However, several issues and limitations persisted, primarily in features with failed test scenarios. These issues emphasize the need for further refinement to ensure comprehensive functionality and an optimal user experience. Below is a detailed discussion of the identified issues based on Version 3 testing results:

1. Real-Time URL Monitoring (88% Success Rate)

- **Failed Scenarios**:
    - In rare instances, certain redirected URLs were not analyzed correctly.
    - High-browsing loads caused occasional delays in URL monitoring.
- **Identified Issues**:
    - Incomplete handling of complex URL redirections.
    - Performance bottlenecks under heavy browsing scenarios.
- **Impact**:
    - Users may experience delayed or missed alerts, reducing the reliability of real-time protection.
- **Recommendations**:
    - Optimize redirection logic and improve resource allocation to handle high-load scenarios efficiently.

2. Phishing URL Detection (75% Success Rate)

- **Failed Scenarios**:
    - Some URLs with advanced obfuscation techniques bypassed detection.
    - False negatives were observed in cases of subtle phishing patterns.
- **Identified Issues**:
    - Current detection algorithms need better coverage for complex phishing techniques.
- **Impact**:
    - Users remain at risk of phishing attacks due to undetected threats.
- **Recommendations**:
    - Refine detection algorithms to address advanced obfuscation techniques and edge cases.

3. Whitelist/Blacklist Management (85% Success Rate)

- **Identified Issues**:
    - Interface inconsistencies and enforcement gaps in blacklist rules.
- **Impact**:
    - Users may unintentionally access blocked URLs, reducing trust in the feature.
- **Recommendations**:

  - Strengthen backend rule enforcement and conduct additional UI testing.

4. User-Friendly Interface (83% Success Rate)

- **Failed Scenarios**:
  - Minor layout issues occurred on smaller screen sizes.
- **Identified Issues**:
  - Incomplete tooltips and responsiveness challenges for certain screen resolutions.
- **Impact**:
  - Non-technical users may struggle to navigate or utilize advanced features effectively.
- **Recommendations**:
  - Redesign tooltips for clarity and improve layout responsiveness for all screen sizes.

5. Multi-Browser Compatibility (71% Success Rate)

- **Failed Scenarios**:
  - Performance issues persisted on Firefox
- **Identified Issues**:
  - Incomplete optimization for Firefox
- **Impact**:
  - Users on these browsers may experience reduced functionality or performance inconsistencies.
- **Recommendations**:
  - Conduct browser-specific testing to address API differences and optimize performance.

6. Severity-Based Alerts (66% Success Rate)

- **Failed Scenarios**:
  - Alerts for moderate severity lacked actionable recommendations.
  - High-severity alerts occasionally failed to display tailored warnings.
- **Identified Issues**:
  - Gaps in contextual recommendations for certain threat levels.
- **Impact**:
  - Users may find it difficult to interpret and respond to alerts effectively.
- **Recommendations**:
  - Enhance the logic for generating recommendations based on threat severity.

7. Advanced Machine Learning for Phishing Detection (80% Success Rate)

- **Failed Scenarios**:
  - False positives were observed in detecting legitimate URLs as phishing threats.
  - Some rare phishing patterns were not flagged.
- **Identified Issues**:
  - The ML model needs additional refinement for precision and coverage.
- **Impact**:
  - False positives may reduce user trust, and undetected phishing patterns pose security risks.
- **Recommendations**:
  - Expand training datasets with diverse legitimate and phishing URLs and fine-tune the model.

Overall Summary

Version 3 of the Aegis Shield - Phishing Detection Extension represents a significant leap forward, with most features achieving high success rates. However, issues in areas such as Multi-Browser Compatibility, User-Friendly Interface, and Severity-Based Alerts underscore the need for continued optimization and refinement. Addressing these limitations will be essential to providing a robust and user-friendly extension that meets the project's goals. These insights will guide the next phase of development and ensure a more comprehensive and reliable solution in future iterations.

6.0 TESTING AND EVALUATION OF VERSION 4

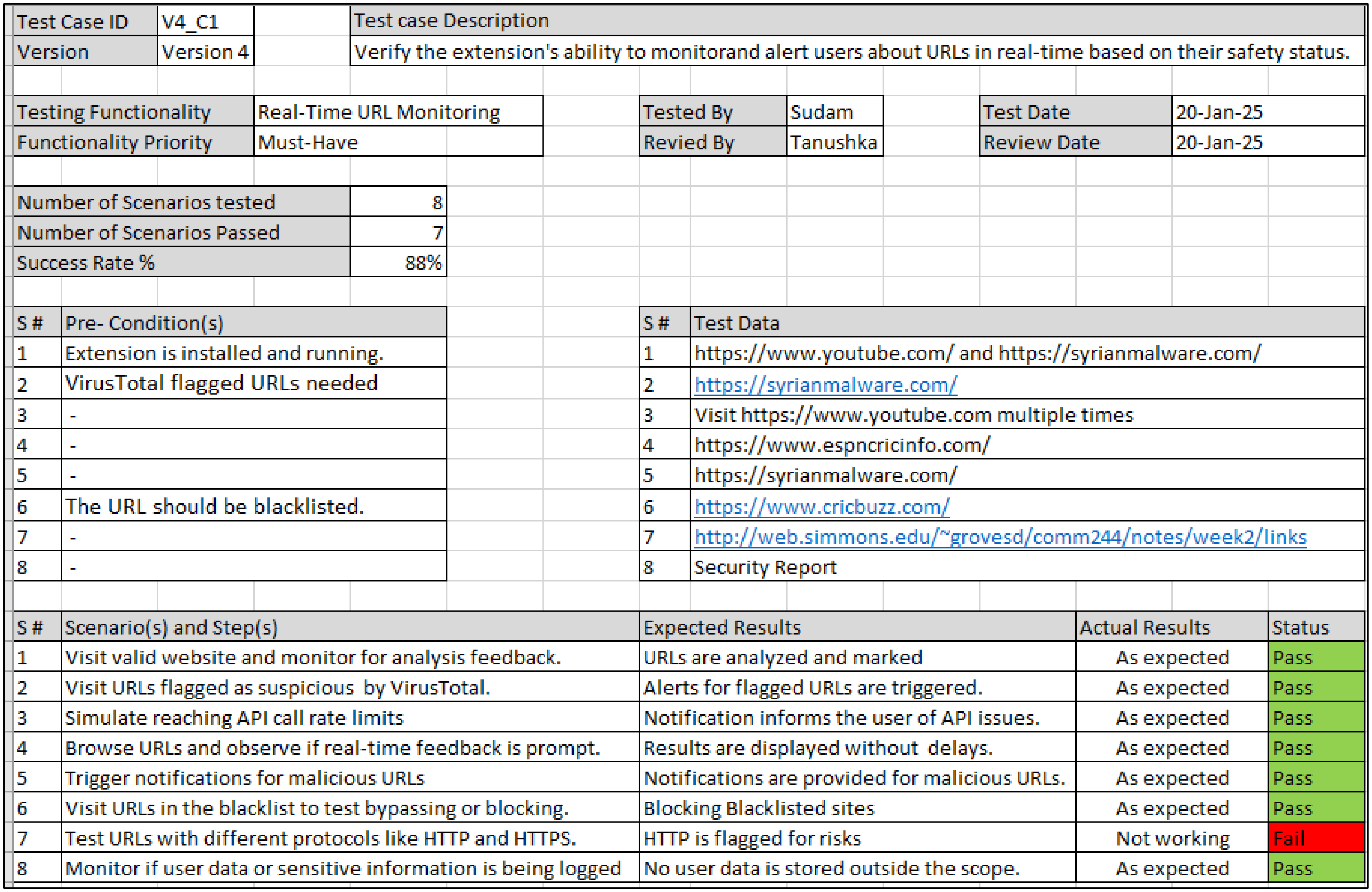
On January 20, 2025, the fourth and final testing phase for the Aegis Shield - Phishing Detection Extension was conducted. This phase involved evaluating all 12 core features developed in the project using a structured approach of test cases and scenarios. The testing aimed to validate the refinements and integrations made since the last iteration, ensuring the extension's robustness and reliability. This round of testing focused on addressing previous limitations and ensuring the extension was ready for deployment.

The table below summarizes the results of Version 4 testing, including the number of scenarios tested, passed scenarios, and success rates for each feature. These metrics showcase the progress made in addressing issues from prior versions and highlight areas where features have achieved optimal functionality.

Requirement name	Test Case ID	No. of Scenarios Tested
Real-Time URL Monitoring	V2_C1	8
Phishing URL Detection	V2_C2	4
Basic URL Alerts	V2_C3	3
Whitelist/Blacklist Management	V2_C4	7
Basic Malware Detection	V2_C5	4
Email Phishing Detection	V2_C6	4
Browser Notifications	V2_C7	5
User-Friendly Interface	V2_C8	6
Severity-Based Alerts	V2_C9	3
Advanced Machine Learning for Phishing Detection	V2_C10	5
Multi-Browser Compatibility	V2_C11	7
Sandbox Integration for File Analysis	V2_C12	5
Total Number of Test Cases Tested: 12		
Total Number of Scenarios Tested: 61		

Table 10: Testing Phase 4 Overview

6.1 TEST CASE 1: Real-Time URL Monitoring



Test Case ID	V4_C1		Test case Description
Version	Version 4		Verify the extension's ability to monitorand alert users about URLs in real-time based on their safety status.

Testing Functionality	Real-Time URL Monitoring	Tested By	Sudam	Test Date	20-Jan-25
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	20-Jan-25

Number of Scenarios tested	8
Number of Scenarios Passed	7
Success Rate %	88%

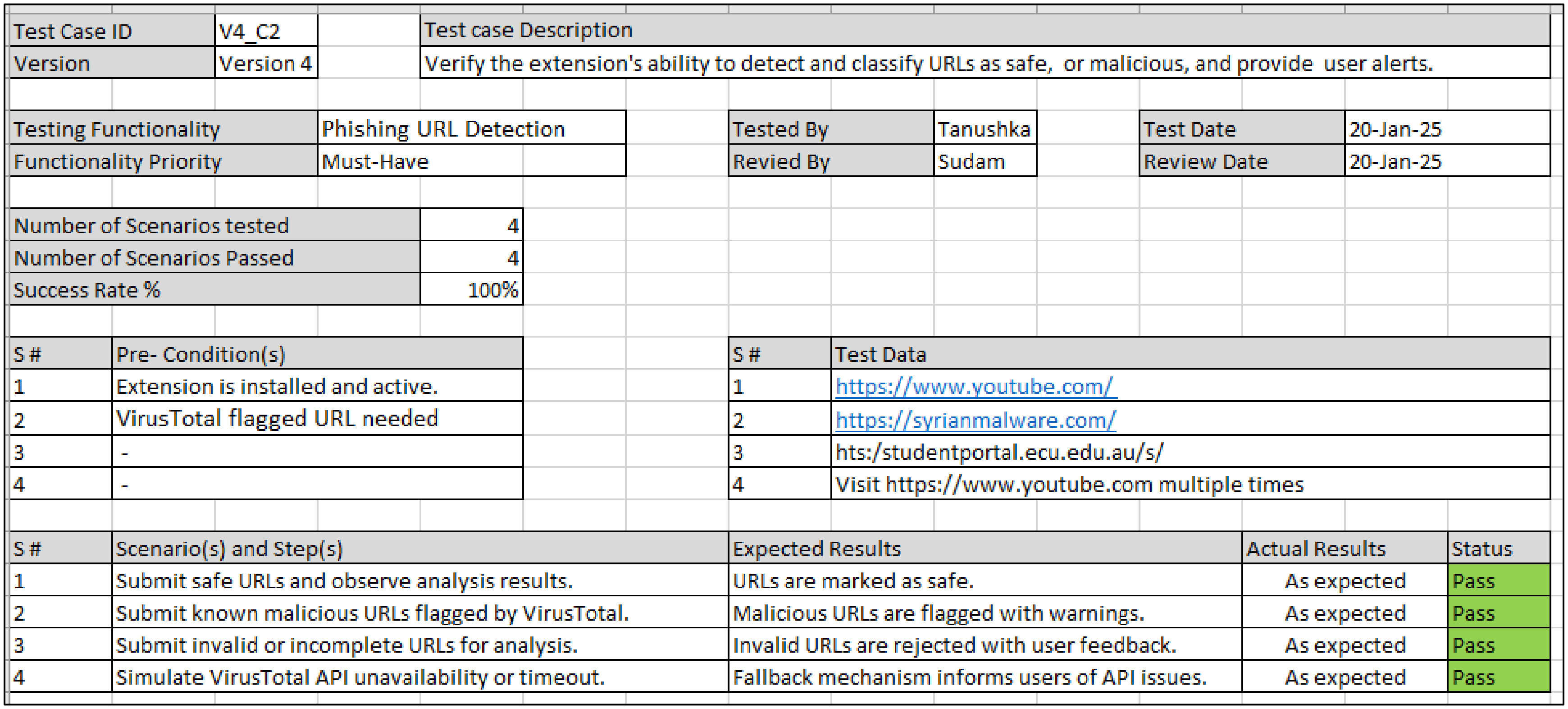
S #	Pre- Condition(s)
1	Extension is installed and running.
2	VirusTotal flagged URLs needed
3	-
4	-
5	-
6	The URL should be blacklisted.
7	-
8	-

S #	Test Data
1	https://www.youtube.com/ and https://syrianmalware.com/
2	https://syrianmalware.com/
3	Visit https://www.youtube.com multiple times
4	https://www.espncricinfo.com/
5	https://syrianmalware.com/
6	https://www.cricbuzz.com/
7	http://web.simmons.edu/~grovesd/comm244/notes/week2/links
8	Security Report

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit valid website and monitor for analysis feedback.	URLs are analyzed and marked	As expected	Pass
2	Visit URLs flagged as suspicious by VirusTotal.	Alerts for flagged URLs are triggered.	As expected	Pass
3	Simulate reaching API call rate limits	Notification informs the user of API issues.	As expected	Pass
4	Browse URLs and observe if real-time feedback is prompt.	Results are displayed without delays.	As expected	Pass
5	Trigger notifications for malicious URLs	Notifications are provided for malicious URLs.	As expected	Pass
6	Visit URLs in the blacklist to test bypassing or blocking.	Blocking Blacklisted sites	As expected	Pass
7	Test URLs with different protocols like HTTP and HTTPS.	HTTP is flagged for risks	Not working	Fail
8	Monitor if user data or sensitive information is being logged	No user data is stored outside the scope.	As expected	Pass

Figure 38: TEST CASE 1: Real-Time URL Monitoring

6.2 TEST CASE 2: Phishing URL Detection



Test Case ID	V4_C2		Test case Description
Version	Version 4		Verify the extension's ability to detect and classify URLs as safe, or malicious, and provide user alerts.

Testing Functionality	Phishing URL Detection		Tested By	Tanushka		Test Date	20-Jan-25
Functionality Priority	Must-Have		Revied By	Sudam		Review Date	20-Jan-25

Number of Scenarios tested	4
Number of Scenarios Passed	4
Success Rate %	100%

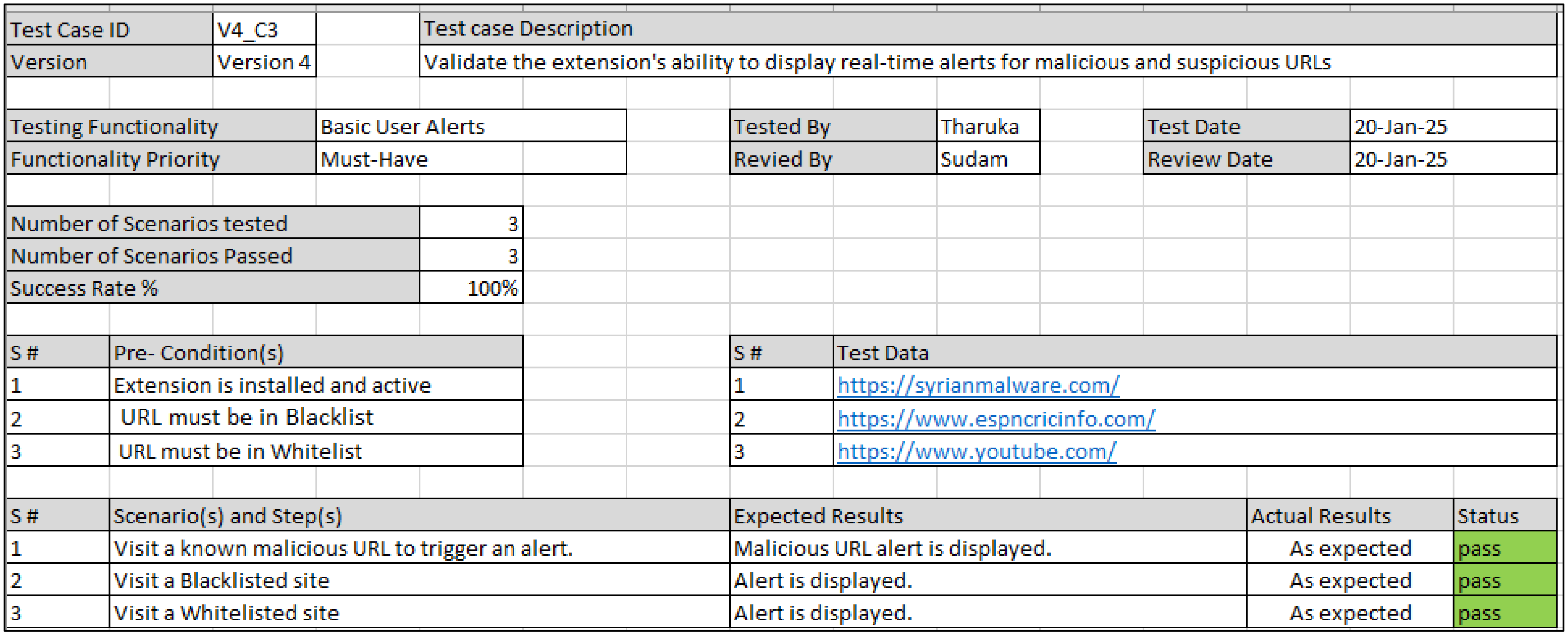
S #	Pre- Condition(s)
1	Extension is installed and active.
2	VirusTotal flagged URL needed
3	-
4	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	hts:/studentportal.ecu.edu.au/s/
4	Visit https://www.youtube.com multiple times

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit safe URLs and observe analysis results.	URLs are marked as safe.	As expected	Pass
2	Submit known malicious URLs flagged by VirusTotal.	Malicious URLs are flagged with warnings.	As expected	Pass
3	Submit invalid or incomplete URLs for analysis.	Invalid URLs are rejected with user feedback.	As expected	Pass
4	Simulate VirusTotal API unavailability or timeout.	Fallback mechanism informs users of API issues.	As expected	Pass

Figure 39: TEST CASE 2: Phishing URL Detection

6.3 TEST CASE 3: Basic User Alerts



Test Case ID	V4_C3	Test case Description
Version	Version 4	Validate the extension's ability to display real-time alerts for malicious and suspicious URLs

Testing Functionality	Basic User Alerts	Tested By	Tharuka	Test Date	20-Jan-25
Functionality Priority	Must-Have	Revied By	Sudam	Review Date	20-Jan-25

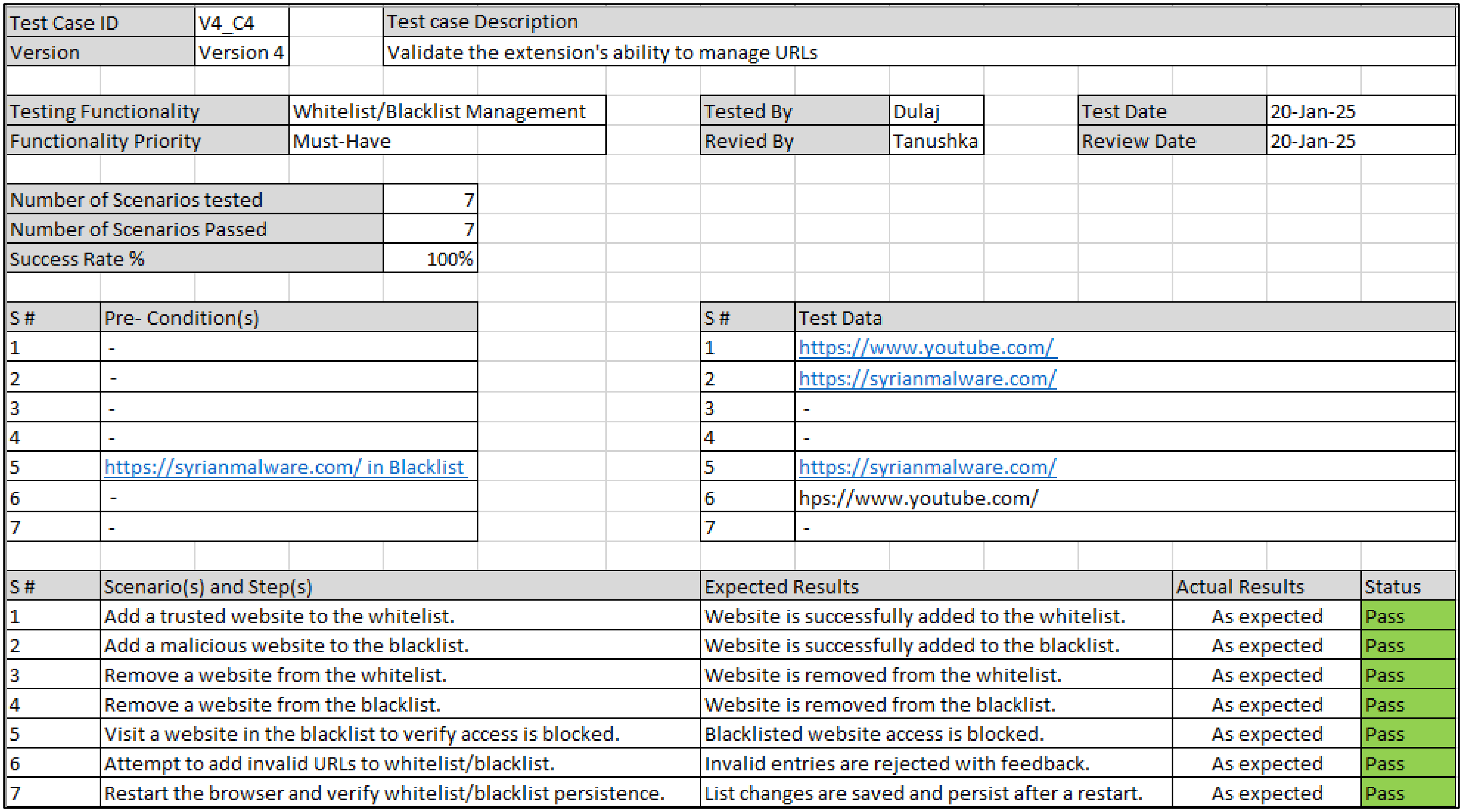
Number of Scenarios tested	3
Number of Scenarios Passed	3
Success Rate %	100%

S #	Pre- Condition(s)	S #	Test Data
1	Extension is installed and active	1	https://syrianmalware.com/
2	URL must be in Blacklist	2	https://www.espncricinfo.com/
3	URL must be in Whitelist	3	https://www.youtube.com/

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a known malicious URL to trigger an alert.	Malicious URL alert is displayed.	As expected	pass
2	Visit a Blacklisted site	Alert is displayed.	As expected	pass
3	Visit a Whitelisted site	Alert is displayed.	As expected	pass

Figure 40: TEST CASE 3: Basic User Alerts

6.4 TEST CASE 4: Whitelist/Blacklist Management



Test Case ID	V4_C4	Test case Description	
Version	Version 4	Validate the extension's ability to manage URLs	

Testing Functionality	Whitelist/Blacklist Management	Tested By	Dulaj	Test Date	20-Jan-25
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	20-Jan-25

Number of Scenarios tested	7
Number of Scenarios Passed	7
Success Rate %	100%

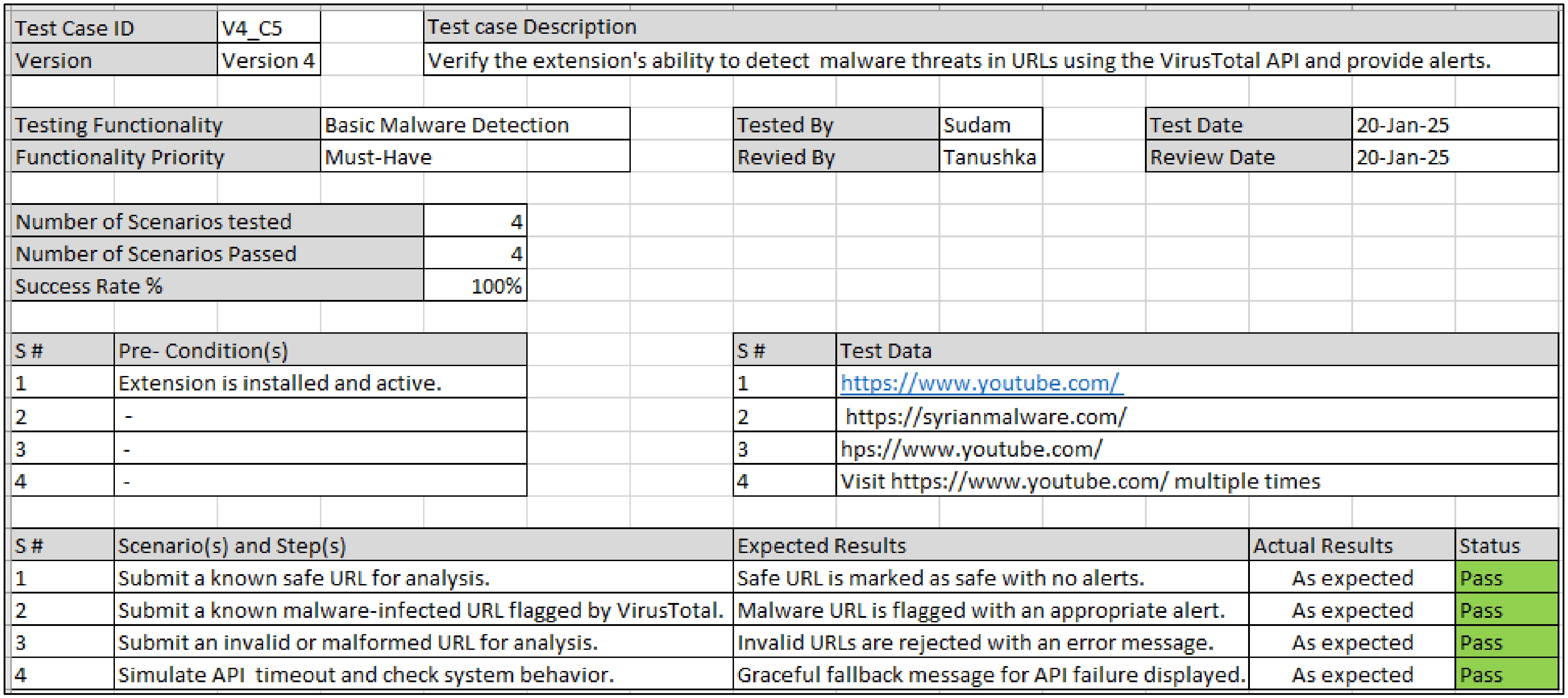
S #	Pre- Condition(s)
1	-
2	-
3	-
4	-
5	https://syrianmalware.com/ in Blacklist
6	-
7	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	-
4	-
5	https://syrianmalware.com/
6	hps://www.youtube.com/
7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Add a trusted website to the whitelist.	Website is successfully added to the whitelist.	As expected	Pass
2	Add a malicious website to the blacklist.	Website is successfully added to the blacklist.	As expected	Pass
3	Remove a website from the whitelist.	Website is removed from the whitelist.	As expected	Pass
4	Remove a website from the blacklist.	Website is removed from the blacklist.	As expected	Pass
5	Visit a website in the blacklist to verify access is blocked.	Blacklisted website access is blocked.	As expected	Pass
6	Attempt to add invalid URLs to whitelist/blacklist.	Invalid entries are rejected with feedback.	As expected	Pass
7	Restart the browser and verify whitelist/blacklist persistence.	List changes are saved and persist after a restart.	As expected	Pass

Figure 41: TEST CASE 4: Whitelist/Blacklist Management

6.5 TEST CASE 5: Basic Malware Detection



Test Case ID	V4_C5		Test case Description
Version	Version 4		Verify the extension's ability to detect malware threats in URLs using the VirusTotal API and provide alerts.

Testing Functionality	Basic Malware Detection	Tested By	Sudam	Test Date	20-Jan-25
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	20-Jan-25

Number of Scenarios tested	4
Number of Scenarios Passed	4
Success Rate %	100%

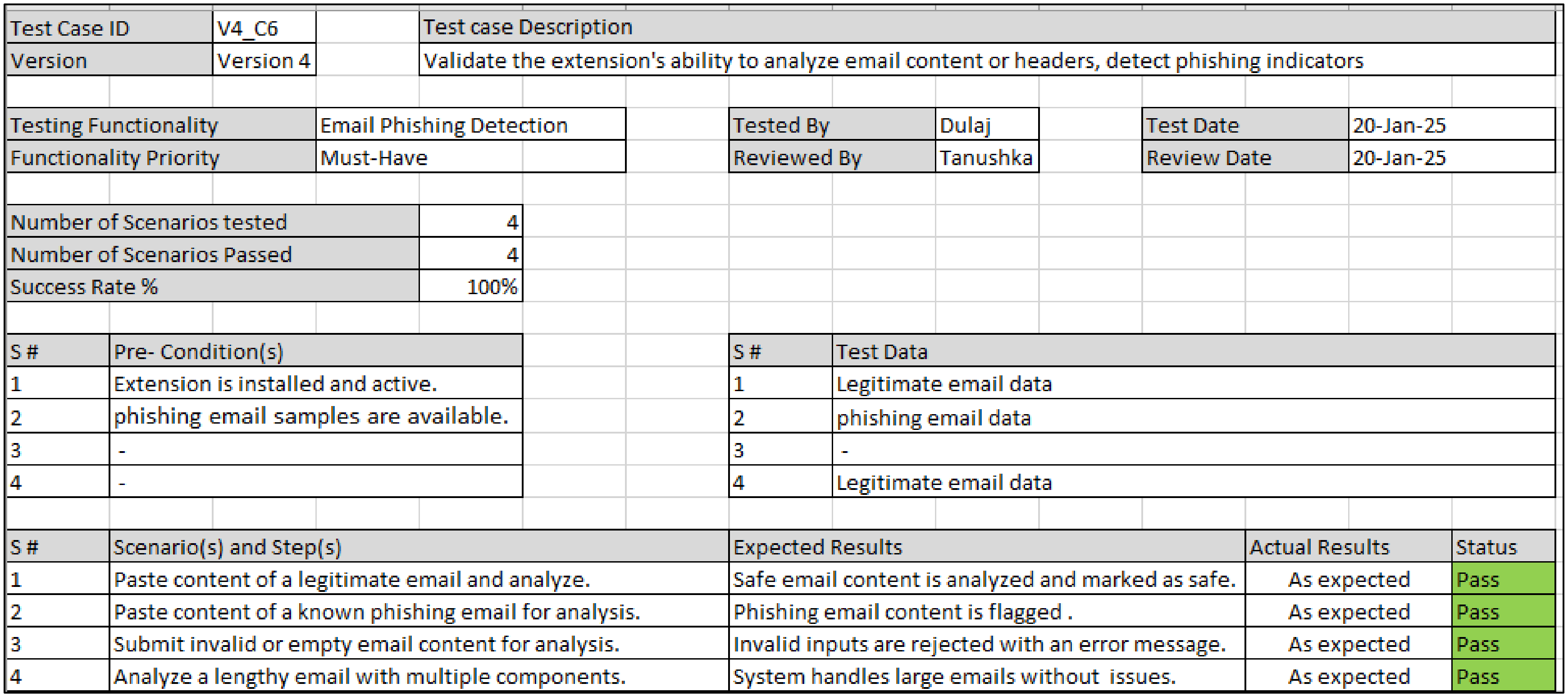
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	hps://www.youtube.com/
4	Visit https://www.youtube.com/ multiple times

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit a known safe URL for analysis.	Safe URL is marked as safe with no alerts.	As expected	Pass
2	Submit a known malware-infected URL flagged by VirusTotal.	Malware URL is flagged with an appropriate alert.	As expected	Pass
3	Submit an invalid or malformed URL for analysis.	Invalid URLs are rejected with an error message.	As expected	Pass
4	Simulate API timeout and check system behavior.	Graceful fallback message for API failure displayed.	As expected	Pass

Figure 42: TEST CASE 5: Basic Malware Detection

6.6 TEST CASE 6: Email Phishing Detection



Test Case ID	V4_C6	Test case Description
Version	Version 4	Validate the extension's ability to analyze email content or headers, detect phishing indicators

Testing Functionality	Email Phishing Detection	Tested By	Dulaj	Test Date	20-Jan-25
Functionality Priority	Must-Have	Reviewed By	Tanushka	Review Date	20-Jan-25

Number of Scenarios tested	4
Number of Scenarios Passed	4
Success Rate %	100%

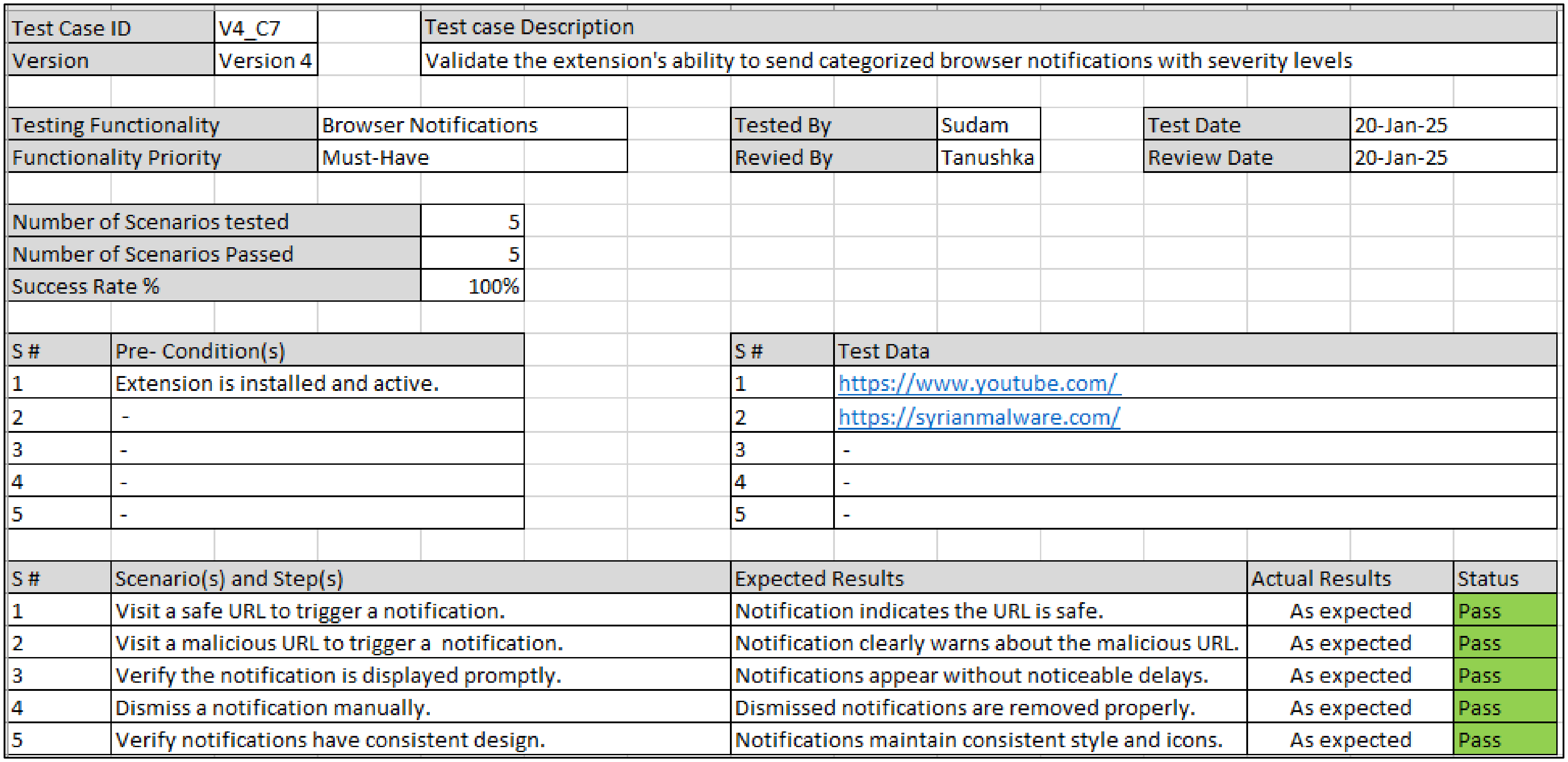
S #	Pre- Condition(s)
1	Extension is installed and active.
2	phishing email samples are available.
3	-
4	-

S #	Test Data
1	Legitimate email data
2	phishing email data
3	-
4	Legitimate email data

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Paste content of a legitimate email and analyze.	Safe email content is analyzed and marked as safe.	As expected	Pass
2	Paste content of a known phishing email for analysis.	Phishing email content is flagged .	As expected	Pass
3	Submit invalid or empty email content for analysis.	Invalid inputs are rejected with an error message.	As expected	Pass
4	Analyze a lengthy email with multiple components.	System handles large emails without issues.	As expected	Pass

Figure 43: TEST CASE 6: Email Phishing Detection

6.7 TEST CASE 7: Browser Notifications



Test Case ID	V4_C7		Test case Description
Version	Version 4		Validate the extension's ability to send categorized browser notifications with severity levels

Testing Functionality	Browser Notifications	Tested By	Sudam	Test Date	20-Jan-25
Functionality Priority	Must-Have	Revied By	Tanushka	Review Date	20-Jan-25

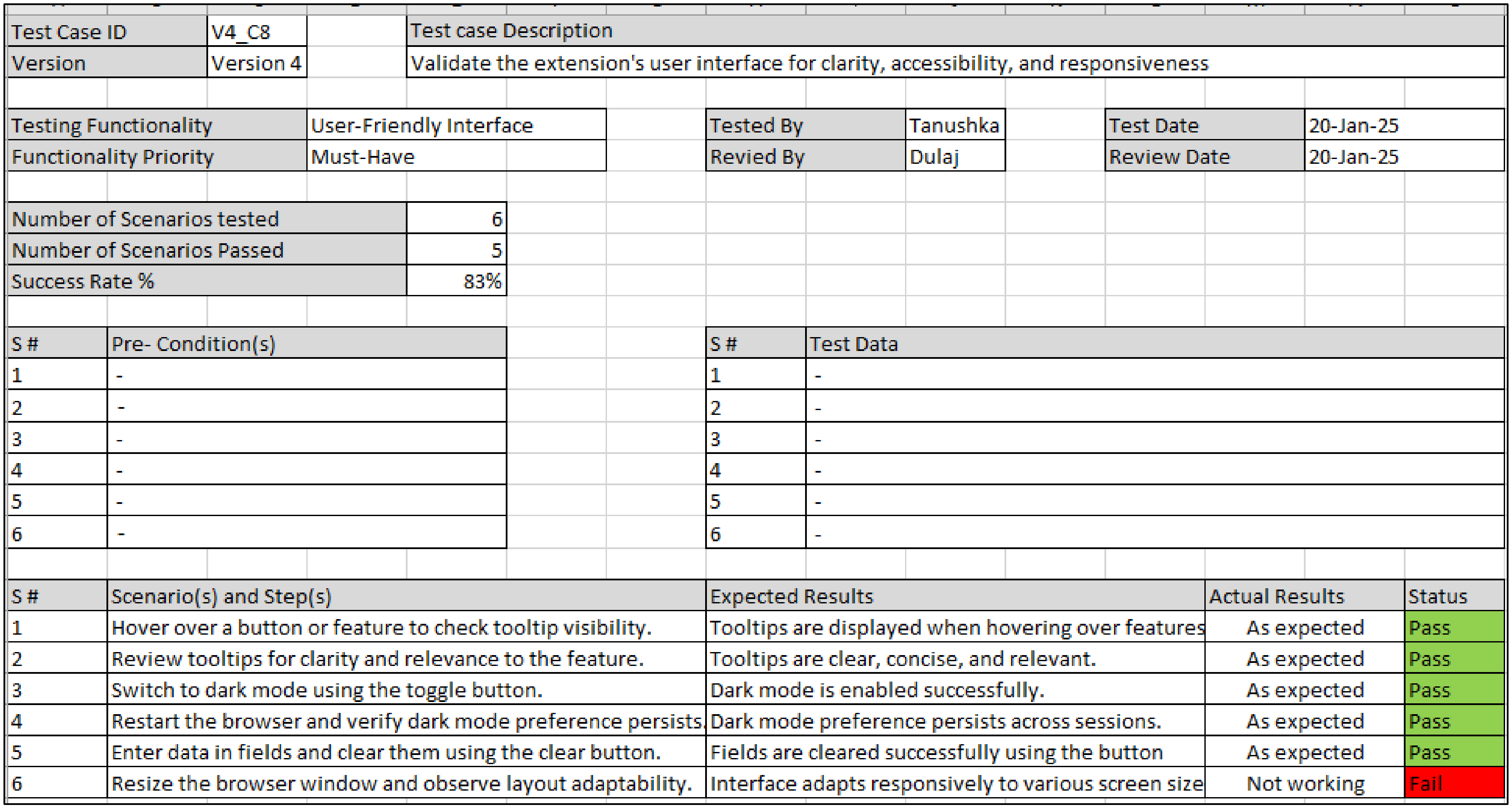
Number of Scenarios tested	5
Number of Scenarios Passed	5
Success Rate %	100%

S #	Pre- Condition(s)	S #	Test Data
1	Extension is installed and active.	1	https://www.youtube.com/
2	-	2	https://syrianmalware.com/
3	-	3	-
4	-	4	-
5	-	5	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a safe URL to trigger a notification.	Notification indicates the URL is safe.	As expected	Pass
2	Visit a malicious URL to trigger a notification.	Notification clearly warns about the malicious URL.	As expected	Pass
3	Verify the notification is displayed promptly.	Notifications appear without noticeable delays.	As expected	Pass
4	Dismiss a notification manually.	Dismissed notifications are removed properly.	As expected	Pass
5	Verify notifications have consistent design.	Notifications maintain consistent style and icons.	As expected	Pass

Figure 44: TEST CASE 7: Browser Notifications

6.8 TEST CASE 8: User-Friendly Interface



Test Case ID	V4_C8		Test case Description
Version	Version 4		Validate the extension's user interface for clarity, accessibility, and responsiveness

Testing Functionality	User-Friendly Interface	Tested By	Tanushka	Test Date	20-Jan-25
Functionality Priority	Must-Have	Revied By	Dulaj	Review Date	20-Jan-25

Number of Scenarios tested	6
Number of Scenarios Passed	5
Success Rate %	83%

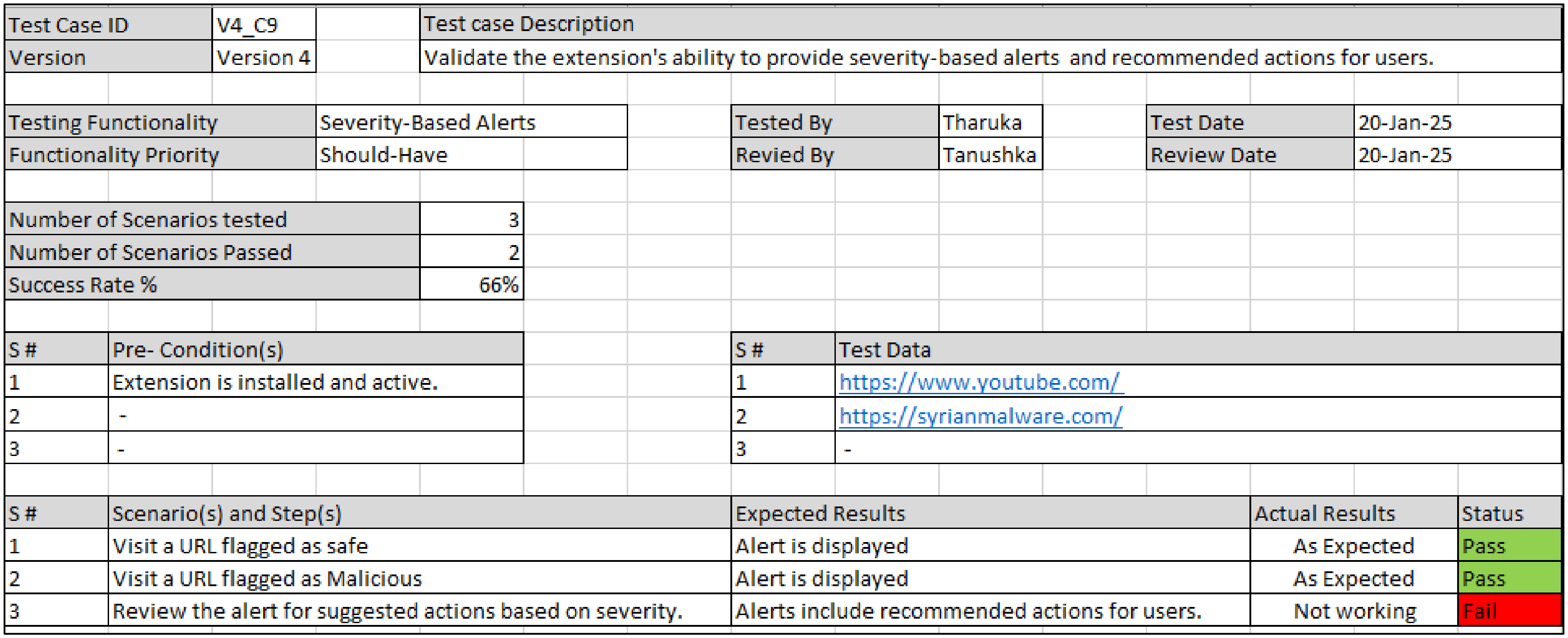
S #	Pre- Condition(s)
1	-
2	-
3	-
4	-
5	-
6	-

S #	Test Data
1	-
2	-
3	-
4	-
5	-
6	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Hover over a button or feature to check tooltip visibility.	Tooltips are displayed when hovering over features	As expected	Pass
2	Review tooltips for clarity and relevance to the feature.	Tooltips are clear, concise, and relevant.	As expected	Pass
3	Switch to dark mode using the toggle button.	Dark mode is enabled successfully.	As expected	Pass
4	Restart the browser and verify dark mode preference persists.	Dark mode preference persists across sessions.	As expected	Pass
5	Enter data in fields and clear them using the clear button.	Fields are cleared successfully using the button	As expected	Pass
6	Resize the browser window and observe layout adaptability.	Interface adapts responsively to various screen size	Not working	Fail

Figure 45: TEST CASE 8: User-Friendly Interface

6.9 TEST CASE 9: Severity-Based Alerts



Test Case ID	V4_C9		Test case Description
Version	Version 4		Validate the extension's ability to provide severity-based alerts and recommended actions for users.

Testing Functionality	Severity-Based Alerts	Tested By	Tharuka	Test Date	20-Jan-25
Functionality Priority	Should-Have	Revied By	Tanushka	Review Date	20-Jan-25

Number of Scenarios tested	3
Number of Scenarios Passed	2
Success Rate %	66%

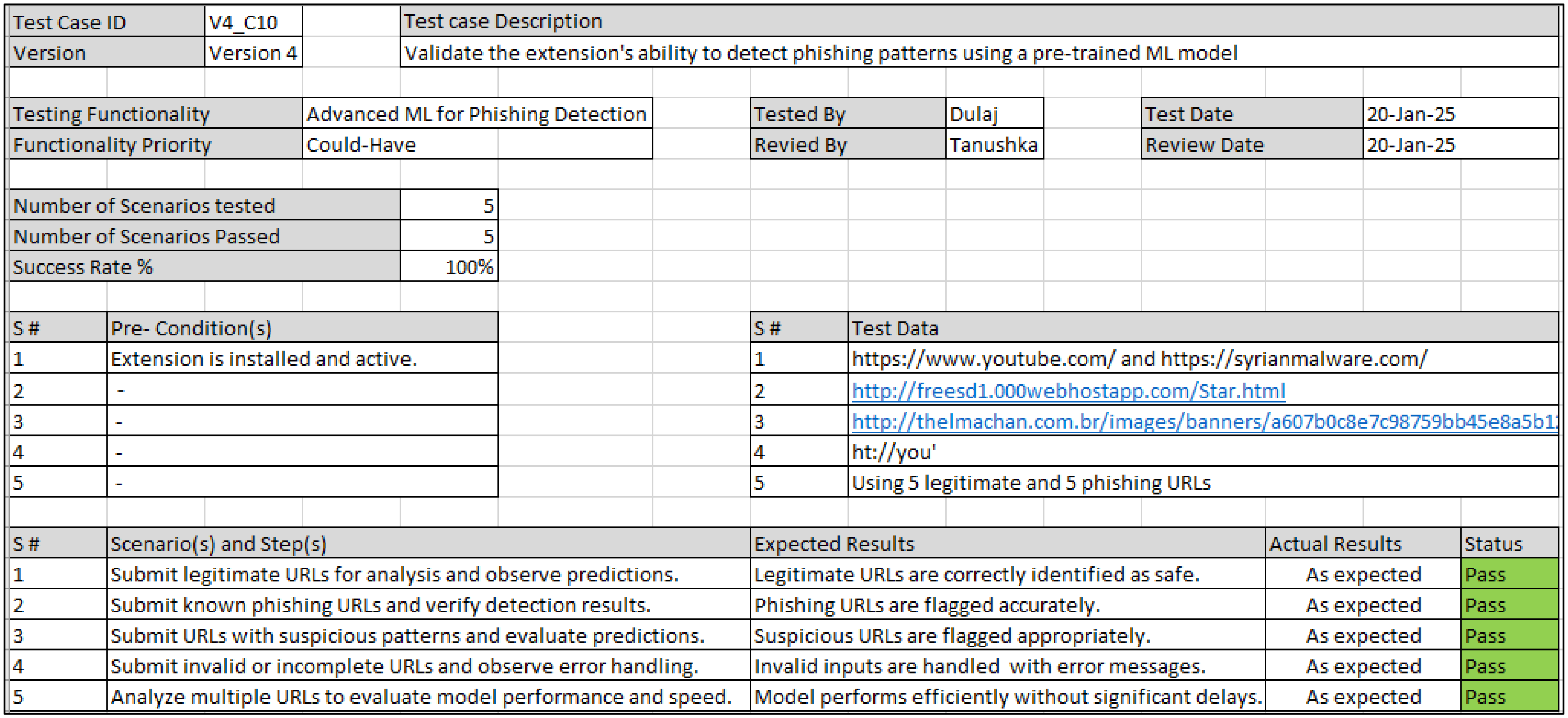
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-

S #	Test Data
1	https://www.youtube.com/
2	https://syrianmalware.com/
3	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Visit a URL flagged as safe	Alert is displayed	As Expected	Pass
2	Visit a URL flagged as Malicious	Alert is displayed	As Expected	Pass
3	Review the alert for suggested actions based on severity.	Alerts include recommended actions for users.	Not working	Fail

Figure 46: TEST CASE 9: Severity-Based Alerts

6.10 TEST CASE 10: Advanced Machine Learning for Phishing Detection



Test Case ID	V4_C10	Test case Description
Version	Version 4	Validate the extension's ability to detect phishing patterns using a pre-trained ML model

Testing Functionality	Advanced ML for Phishing Detection	Tested By	Dulaj	Test Date	20-Jan-25
Functionality Priority	Could-Have	Revied By	Tanushka	Review Date	20-Jan-25

Number of Scenarios tested	5
Number of Scenarios Passed	5
Success Rate %	100%

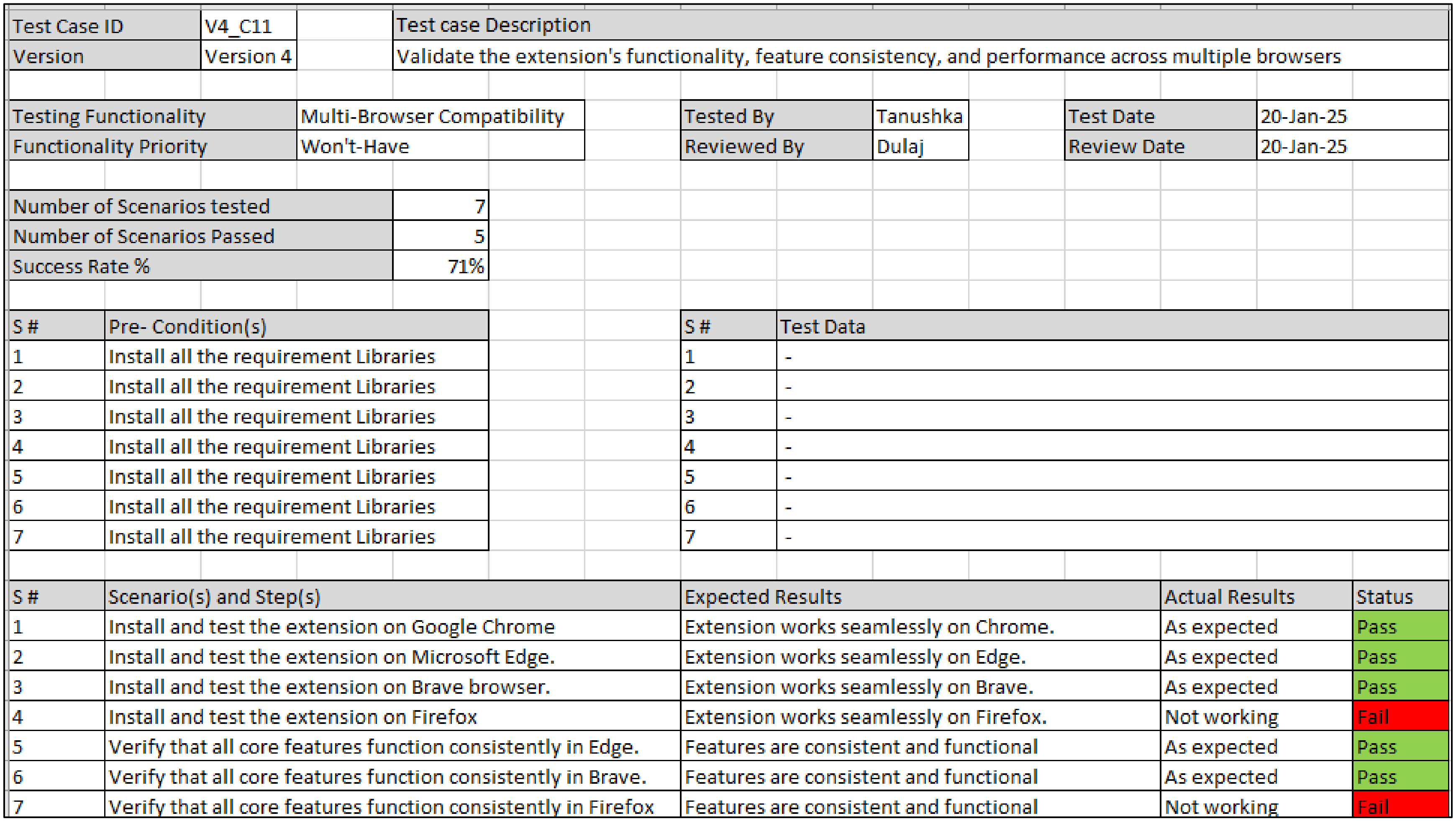
S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-
5	-

S #	Test Data
1	https://www.youtube.com/ and https://syrianmalware.com/
2	http://freesd1.000webhostapp.com/Star.html
3	http://thelmachan.com.br/images/banners/a607b0c8e7c98759bb45e8a5b1
4	ht://you'
5	Using 5 legitimate and 5 phishing URLs

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Submit legitimate URLs for analysis and observe predictions.	Legitimate URLs are correctly identified as safe.	As expected	Pass
2	Submit known phishing URLs and verify detection results.	Phishing URLs are flagged accurately.	As expected	Pass
3	Submit URLs with suspicious patterns and evaluate predictions.	Suspicious URLs are flagged appropriately.	As expected	Pass
4	Submit invalid or incomplete URLs and observe error handling.	Invalid inputs are handled with error messages.	As expected	Pass
5	Analyze multiple URLs to evaluate model performance and speed.	Model performs efficiently without significant delays.	As expected	Pass

Figure 47: TEST CASE 10: Advanced Machine Learning for Phishing Detection

6.11 TEST CASE 11: Multi-Browser Compatibility



Test Case ID	V4_C11		Test case Description
Version	Version 4		Validate the extension's functionality, feature consistency, and performance across multiple browsers

Testing Functionality	Multi-Browser Compatibility	Tested By	Tanushka	Test Date	20-Jan-25
Functionality Priority	Won't-Have	Reviewed By	Dulaj	Review Date	20-Jan-25

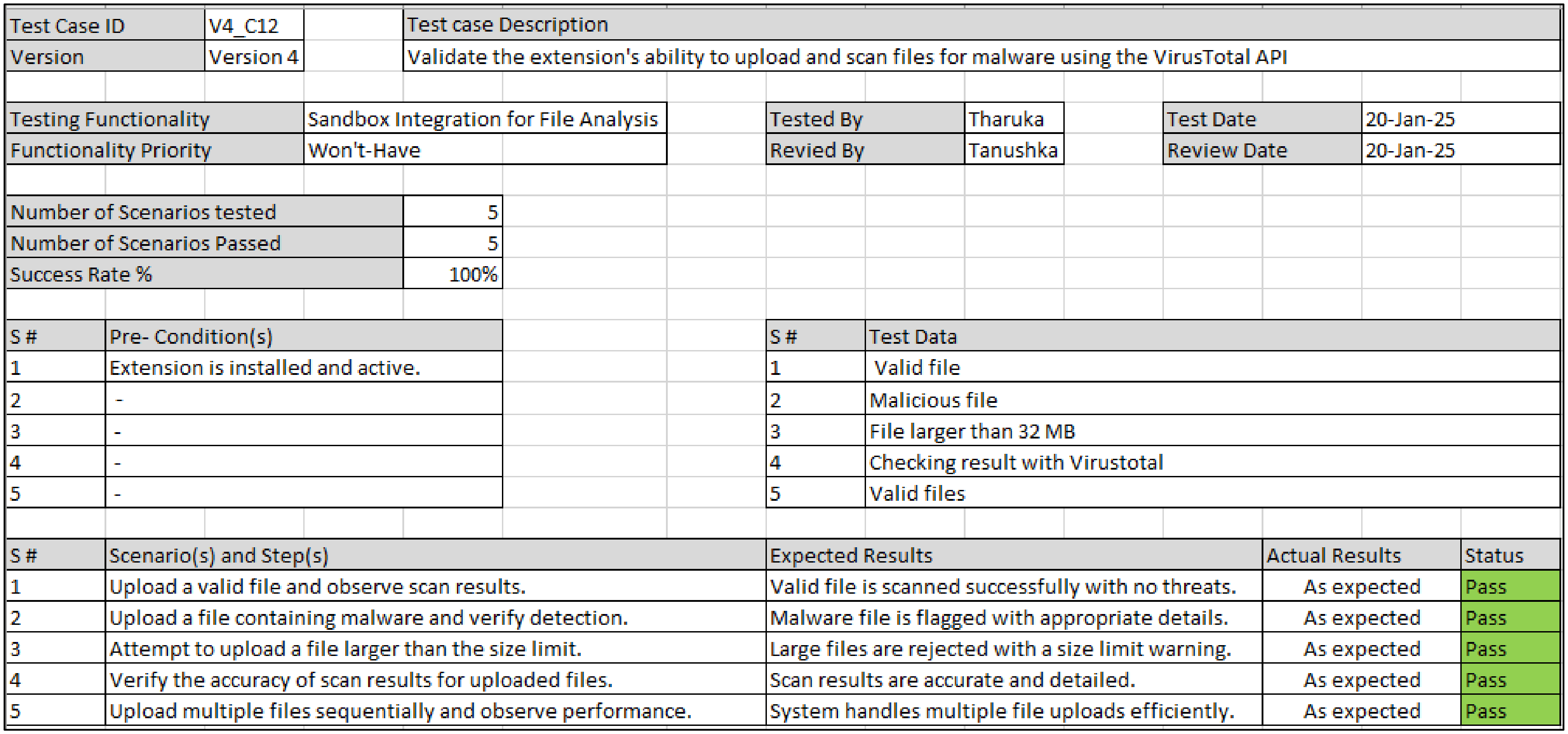
Number of Scenarios tested	7
Number of Scenarios Passed	5
Success Rate %	71%

S #	Pre- Condition(s)	S #	Test Data
1	Install all the requirement Libraries	1	-
2	Install all the requirement Libraries	2	-
3	Install all the requirement Libraries	3	-
4	Install all the requirement Libraries	4	-
5	Install all the requirement Libraries	5	-
6	Install all the requirement Libraries	6	-
7	Install all the requirement Libraries	7	-

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Install and test the extension on Google Chrome	Extension works seamlessly on Chrome.	As expected	Pass
2	Install and test the extension on Microsoft Edge.	Extension works seamlessly on Edge.	As expected	Pass
3	Install and test the extension on Brave browser.	Extension works seamlessly on Brave.	As expected	Pass
4	Install and test the extension on Firefox	Extension works seamlessly on Firefox.	Not working	Fail
5	Verify that all core features function consistently in Edge.	Features are consistent and functional	As expected	Pass
6	Verify that all core features function consistently in Brave.	Features are consistent and functional	As expected	Pass
7	Verify that all core features function consistently in Firefox	Features are consistent and functional	Not working	Fail

Figure 48: TEST CASE 11: Multi-Browser Compatibility

6.12 TEST CASE 12: Sandbox Integration for File Analysis



Test Case ID	V4_C12		Test case Description
Version	Version 4		Validate the extension's ability to upload and scan files for malware using the VirusTotal API

Testing Functionality	Sandbox Integration for File Analysis	Tested By	Tharuka	Test Date	20-Jan-25
Functionality Priority	Won't-Have	Revied By	Tanushka	Review Date	20-Jan-25

Number of Scenarios tested	5
Number of Scenarios Passed	5
Success Rate %	100%

S #	Pre- Condition(s)
1	Extension is installed and active.
2	-
3	-
4	-
5	-

S #	Test Data
1	Valid file
2	Malicious file
3	File larger than 32 MB
4	Checking result with Virustotal
5	Valid files

S #	Scenario(s) and Step(s)	Expected Results	Actual Results	Status
1	Upload a valid file and observe scan results.	Valid file is scanned successfully with no threats.	As expected	Pass
2	Upload a file containing malware and verify detection.	Malware file is flagged with appropriate details.	As expected	Pass
3	Attempt to upload a file larger than the size limit.	Large files are rejected with a size limit warning.	As expected	Pass
4	Verify the accuracy of scan results for uploaded files.	Scan results are accurate and detailed.	As expected	Pass
5	Upload multiple files sequentially and observe performance.	System handles multiple file uploads efficiently.	As expected	Pass

Figure 49: TEST CASE 12: Sandbox Integration for File Analysis

6.13 TESTED RESULTS SUMMARY FOR VERSION 4

The testing results for Version 4 highlight the culmination of iterative improvements, with several features achieving a perfect 100% success rate. Features like Real-Time URL Monitoring, Basic Malware Detection, and Browser Notifications demonstrated their robustness and readiness for deployment. While most issues from prior versions were resolved, areas like Severity-Based Alerts and Multi-Browser Compatibility still present opportunities for further refinement. These results validate the project's achievements while providing a clear roadmap for future enhancements.

The table below presents the detailed results of Version 4 testing, including the number of scenarios tested, passed scenarios, and success rates for each feature. These results reflect significant progress in addressing previously identified issues and achieving optimal functionality for most core features.

Requirement name	Test Case ID	No. of Scenarios Tested	No. of Passed Scenarios	Success Rate
Real-Time URL Monitoring	V3_C1	8	7	88%
Phishing URL Detection	V3_C2	4	4	100%
Basic URL Alerts	V3_C3	3	3	100%
Whitelist/Blacklist Management	V3_C4	7	7	100%
Basic Malware Detection	V3_C5	4	4	100%
Email Phishing Detection	V3_C6	4	4	100%
Browser Notifications	V3_C7	5	5	100%
User-Friendly Interface	V3_C8	6	5	83%
Severity-Based Alerts	V3_C9	3	2	66%
Advanced Machine Learning for Phishing Detection	V3_C10	5	5	100%
Multi-Browser Compatibility	V3_C11	7	5	71%
Sandbox Integration for File Analysis	V3_C12	5	5	100%

Table 11: Version 4 Results

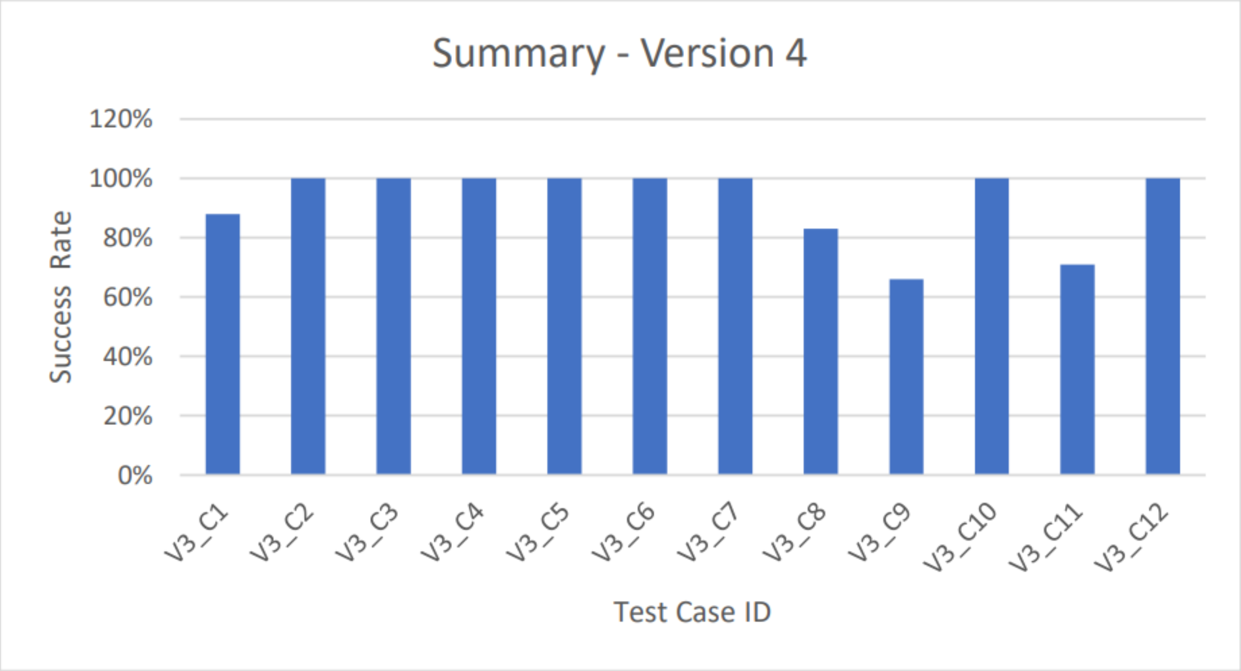


Figure 50: Summary Version 4

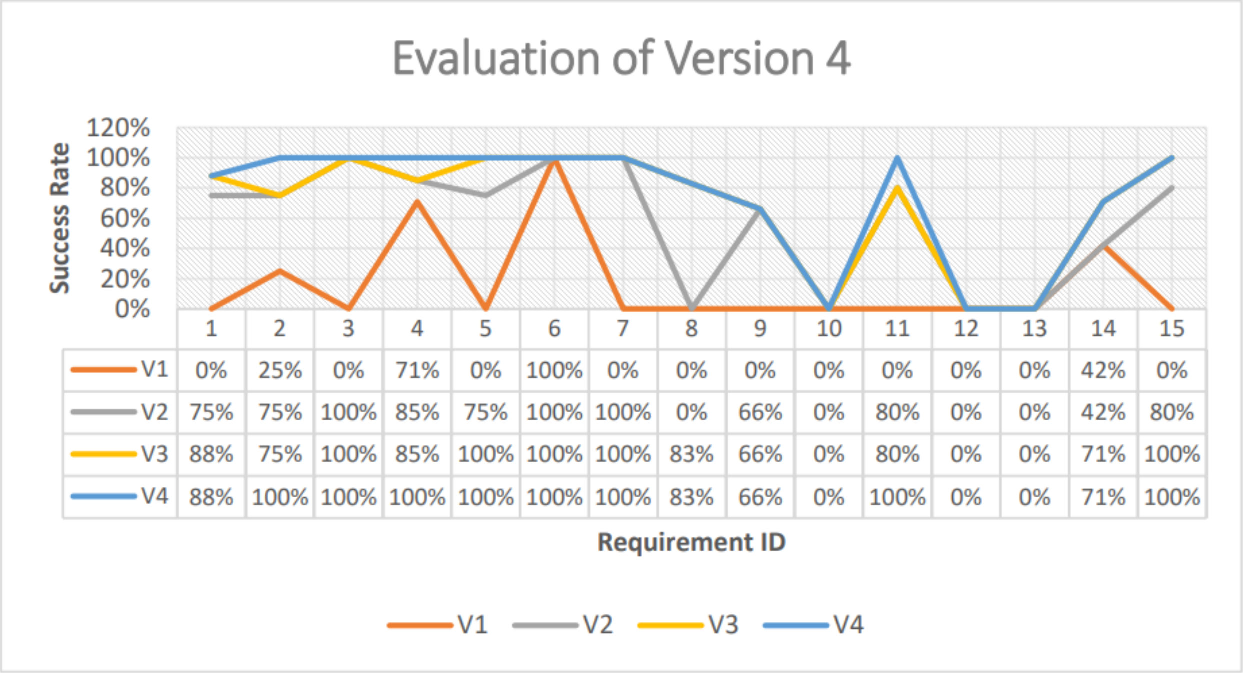
6.14 EVALUATION OF THE VERSION(S)

The evaluation of Versions 1, 2, 3, and 4 of the Aegis Shield - Phishing Detection Extension highlights the significant progress achieved through iterative development and rigorous testing. Version 4, as the culmination of these efforts, demonstrates exceptional performance, with several features achieving a 100% success rate, including Basic Malware Detection, Phishing URL Detection, and Browser Notifications. While most features have reached optimal functionality, areas such as Severity-Based Alerts and Multi-Browser Compatibility continue to require further refinement. This evaluation underscores the project's success in addressing critical issues identified in earlier versions while paving the way for future enhancements and scalability. By achieving a robust and reliable solution, the Aegis Shield extension is well-prepared for deployment and practical application.

		Success Rate of the Version tested			
Requirement ID	**Requirement name**	**V1**	**V2**	**V3**	**V4**
1	Real-Time URL Monitoring	0%	75%	88%	88%
2	Phishing URL Detection	25%	75%	75%	100%
3	Basic User Alerts	Not-Developed	100%	100%	100%
4	Whitelist/Blacklist Management	71%	85%	85%	100%
5	Basic Malware Detection	Not-Developed	75%	100%	100%
6	Email Phishing Detection	100%	100%	100%	100%
7	Browser Notifications	Not-Developed	100%	100%	100%
8	User-Friendly Interface	0%	0%	83%	83%
9	Severity-Based Alerts	Not-Developed	66%	66%	66%
10	Email Content Parsing	Not-Developed	Not-Developed	Not-Developed	Not-Developed
11	Advanced Machine Learning for Phishing Detection	Not-Developed	80%	80%	100%
12	Heuristic URL Analysis	Not-Developed	Not-Developed	Not-Developed	Not-Developed
13	Customizable User Settings	Not-Developed	Not-Developed	Not-Developed	Not-Developed
14	Multi-Browser Compatibility	42%	42%	71%	71%
15	Sandbox Integration for File Analysis	Not-Developed	80%	100%	100%

Table 12: Evaluation of version 4

The figure below illustrates the success rates of implemented features across all four versions of the Aegis Shield - Phishing Detection Extension, showcasing the steady improvements achieved through iterative development and rigorous testing. Version 4 demonstrates exceptional performance, with several features, including Phishing URL Detection, Basic Malware Detection, and Browser Notifications, achieving a 100% success rate. While most features have reached optimal functionality, areas such as Severity-Based Alerts and Multi-Browser Compatibility continue to present opportunities for refinement. This visual comparison highlights the project's commitment to addressing limitations and enhancing the extension's reliability and user experience with each iteration.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
V1	0%	25%	0%	71%	0%	100%	0%	0%	0%	0%	0%	0%	0%	42%	0%
V2	75%	75%	100%	85%	75%	100%	100%	0%	66%	0%	80%	0%	0%	42%	80%
V3	88%	75%	100%	85%	100%	100%	100%	83%	66%	0%	80%	0%	0%	71%	100%
V4	88%	100%	100%	100%	100%	100%	100%	83%	66%	0%	100%	0%	0%	71%	100%

Figure 51: Evaluation of version 4

6.15 IDENTIFIED ISSUES/LIMITATIONS DURING TESTING

The testing phase for Version 4 of the Aegis Shield - Phishing Detection Extension highlighted significant progress, with most features achieving optimal functionality. However, some persistent issues and limitations were identified through failed test scenarios. Below is a detailed discussion of these issues, emphasizing areas requiring further refinement for future iterations

1. Severity-Based Alerts (66% Success Rate)

- **Failed Scenarios**:
  - Moderate severity alerts lacked detailed and actionable recommendations.
  - High-severity alerts occasionally provided generic warnings instead of tailored guidance.
- **Identified Issues**:
  - Incomplete logic for generating contextual recommendations based on severity levels.
- **Impact**:
  - Users may find it challenging to assess and respond to certain threats effectively.
- **Recommendations**:
  - Enhance the recommendation engine to provide precise, actionable guidance for all threat levels.

2. Multi-Browser Compatibility (71% Success Rate)

- **Failed Scenarios**:
  - Performance inconsistencies observed on Firefox, particularly in URL monitoring and notifications.
  - Minor UI discrepancies on Edge and Brave browsers.
- **Identified Issues**:
  - Browser-specific implementation gaps and incomplete optimization for non-Chromium-based browsers.
- **Impact**:
  - Users on Firefox and other browsers may experience reduced functionality or an inconsistent user experience.
- **Recommendations**:
  - Conduct comprehensive cross-browser testing and address API differences to ensure consistent performance across all supported browsers.

3. User-Friendly Interface (83% Success Rate)

- **Failed Scenarios**:
  - Some tooltips remained unclear or were missing for advanced features.
  - Minor layout issues persisted on smaller screen sizes.
- **Identified Issues**:

  - Incomplete tooltip implementation and responsiveness challenges for mobile or reduced resolutions.
- **Impact**:
  - Non-technical users may face difficulties navigating the interface effectively.
- **Recommendations**:
  - Redesign tooltips for clarity and improve interface responsiveness to ensure accessibility across all screen sizes.

4. Real-Time URL Monitoring (88% Success Rate)

- **Failed Scenarios**:
  - Certain complex redirected URLs were not analyzed correctly.
  - Occasional performance delays during high-browsing loads.
- **Identified Issues**:
  - Incomplete handling of nested redirections and optimization gaps for heavy browsing activity.
- **Impact**:
  - Users may experience missed alerts or delayed threat detection.
- **Recommendations**:
  - Improve redirection logic and optimize the monitoring algorithm for better performance under high-load scenarios.

Summary of Issues

Version 4 has successfully addressed most limitations identified in earlier phases, with multiple features achieving perfect success rates. However, areas such as Severity-Based Alerts, Multi-Browser Compatibility, and the User-Friendly Interface still require additional refinement to ensure a seamless and comprehensive user experience. Addressing these issues in future iterations will further solidify the extension’s position as a reliable and user-centric tool for phishing and malware protection.

7.0 CONCLUSION

The **Testing and Evaluation Report** for the Aegis Shield - Phishing Detection Extension highlights the iterative efforts undertaken to ensure the extension's functionality, reliability, and performance. Through three distinct phases of development and testing, the extension evolved into a comprehensive solution for combating phishing and malware threats. Rigorous testing of features such as Real-Time URL Monitoring, Email Phishing Detection, and Advanced Machine Learning ensured their robustness, while iterative improvements addressed limitations in areas like Multi-Browser Compatibility and User-Friendly Interface.

Key achievements include the successful implementation of 12 core features and significant improvements in success rates across multiple versions, with features like Browser Notifications, Basic Malware Detection, and Sandbox Integration for File Analysis achieving 100% success rates. However, challenges remain in areas such as Severity-Based Alerts and Multi-Browser Compatibility, which require further refinement.

This report provides a clear roadmap for addressing identified issues and enhancing the extension in future iterations. By leveraging the insights gained during testing, the team has demonstrated a commitment to delivering a secure, user-friendly, and effective tool for phishing protection. The Aegis Shield - Phishing Detection Extension stands as a robust solution, ready for deployment and further enhancement to meet the evolving needs of its users.