

AEGIS SHIELD - PHISHING DETECTION EXTENSION

Sudam Pullaperuma - 10660248

Tharuka Gunasekara - 10659483

Tanushka Elvitigala - 10663914

Dulaj Walgama - 10659489

TABLE OF CONTENTS

1	0 Inroduction	6
2	0 Testing Methodology	8
	2.1 Testing Phases	8
3	0 Testing And Evaluation Of Version 1	10
	3.1 Test Case 1: Real-Time Url Monitoring	11
	3.2 Test Case 2: Phishing Url Detection	12
	3.3 Test Case 3: Whitelist/Blacklist Management	13
	3.4 Test Case 4: Email Phishing Detection	14
	3.5 Test Case 5: User-Friendly Interface	15
	3.6 Test Case 6: Multi-Browser Compatibility	16
	3.7 Tested Results Summary For Version 1	17
	3.8 Evaluation Of The Version(S)	18
	3.9 Identified Issues/Limitations During Testing	20
4	0 Testing And Evaluation Of Version 2	22
	4.1 Test Case 1: Real-Time Url Monitoring	23
	4.2 Test Case 2: Phishing Url Detection	24
	4.3 Test Case 3: Basic User Alerts	25
	4.4 Test Case 4: Whitelist/Blacklist Management	26
	4.5 Test Case 5: Basic Malware Detection	27
	4.6 Test Case 6: Email Phishing Detection	28
	4.7 Test Case 7: Browser Notifications	29
	4.8 Test Case 8: User-Friendly Interface	30
	4.9 Test Case 9: Severity-Based Alerts	31
	4.10 Test Case 10: Advanced Machine Learning For Phishing Detection	32
	4.11 Test Case 11: Multi-Browser Compatibility	33
	4.12 Test Case 12: Sandbox Integration For File Analysis	34
	4.13 Tested Results Summary For Version 2	35
	4.14 Evaluation Of The Version(S)	36
	4.15 Identified Issues/Limitations During Testing	38
5	0 Testing And Evaluation Of Version 3	42
	5.1 Test Case 1: Real-Time Url Monitoring	43
	5.2 Test Case 2: Phishing Url Detection	44

5.3 Test Case 3: Basic User Alerts	45
5.4 Test Case 4: Whitelist/Blacklist Management	46
5.5 Test Case 5: Basic Malware Detection	47
5.6 Test Case 6: Email Phishing Detection	48
5.7 Test Case 7: Browser Notifications	49
5.8 Test Case 8: User-Friendly Interface	50
5.9 Test Case 9: Severity-Based Alerts	51
5.10 Test Case 10: Advanced Machine Learning For Phishing Detection	52
5.11 Test Case 11: Multi-Browser Compatibility	53
5.12 Test Case 12: Sandbox Integration For File Analysis	54
5.13 Tested Results Summary For Version 3	55
5.14 Evaluation Of The Version(S)	57
5.15 Identified Issues/Limitations During Testing	59
6.0 Testing And Evaluation Of Version 4	62
6.1 Test Case 1: Real-Time Url Monitoring	63
6.2 Test Case 2: Phishing Url Detection	64
6.3 Test Case 3: Basic User Alerts	65
6.4 Test Case 4: Whitelist/Blacklist Management	66
6.5 Test Case 5: Basic Malware Detection	67
6.6 Test Case 6: Email Phishing Detection	68
6.7 Test Case 7: Browser Notifications	69
6.8 Test Case 8: User-Friendly Interface	70
6.9 Test Case 9: Severity-Based Alerts	71
6.10 Test Case 10: Advanced Machine Learning For Phishing Detection	72
6.11 Test Case 11: Multi-Browser Compatibility	73
6.12 Test Case 12: Sandbox Integration For File Analysis	74
6.13 Tested Results Summary For Version 4	75
6.14 Evaluation Of The Version(S)	77
6.15 Identified Issues/Limitations During Testing	79
7.0 Conclusion	81

LIST OF FIGURES

Figure 1: Testing Phases	9
Figure 2: TEST CASE 1: Real-Time URL Monitoring	11
Figure 3:TEST CASE 2: Phishing URL Detection	12
Figure 4:TEST CASE 3: Whitelist/Blacklist Management	13
Figure 5:TEST CASE 4: Email Phishing Detection	14
Figure 6:TEST CASE 5: User-Friendly Interface	15
Figure 7:TEST CASE 6: Multi-Browser Compatibility	16
Figure 8: Summary Version-1	17
Figure 9: Evaluation of version 1	19
Figure 10: TEST CASE 1: Real-Time URL Monitoring	23
Figure 11:TEST CASE 2: Phishing URL Detection	24
Figure 12: TEST CASE 3: Basic User Alerts	25
Figure 13: TEST CASE 4: Whitelist/Blacklist Management	26
Figure 14: TEST CASE 5: Basic Malware Detection	27
Figure 15: TEST CASE 6: Email Phishing Detection	28
Figure 16: TEST CASE 7: Browser Notifications	29
Figure 17: TEST CASE 8: User-Friendly Interface	30
Figure 18: TEST CASE 9: Severity-Based Alerts	31
Figure 19: TEST CASE 10: Advanced Machine Learning for Phishing Detection	32
Figure 20: TEST CASE 11: Multi-Browser Compatibility	33
Figure 21: TEST CASE 12: Sandbox Integration for File Analysis	34
Figure 22: Summary Version 2	35
Figure 23: Evaluation of version 2	37
Figure 24: TEST CASE 1: Real-Time URL Monitoring	43
Figure 25: TEST CASE 2: Phishing URL Detection	44
Figure 26: TEST CASE 3: Basic User Alerts	45
Figure 27: TEST CASE 4: Whitelist/Blacklist Management	46
Figure 28: TEST CASE 5: Basic Malware Detection	47
Figure 29: TEST CASE 6: Email Phishing Detection	48
Figure 30: TEST CASE 7: Browser Notifications	49
Figure 31: TEST CASE 8: User-Friendly Interface	50
Figure 32: TEST CASE 9: Severity-Based Alerts	51

Figure 33: TEST CASE 10: Advanced Machine Learning for Phishing Detection	52
Figure 34: TEST CASE 11: Multi-Browser Compatibility	53
Figure 35: TEST CASE 12: Sandbox Integration for File Analysis	54
Figure 36: Summary Version 3	56
Figure 37: Evaluation of version 3	58
Figure 38: TEST CASE 1: Real-Time URL Monitoring	63
Figure 39: TEST CASE 2: Phishing URL Detection	64
Figure 40: TEST CASE 3: Basic User Alerts	65
Figure 41: TEST CASE 4: Whitelist/Blacklist Management	66
Figure 42: TEST CASE 5: Basic Malware Detection	67
Figure 43: TEST CASE 6: Email Phishing Detection	68
Figure 44: TEST CASE 7: Browser Notifications	69
Figure 45: TEST CASE 8: User-Friendly Interface	70
Figure 46: TEST CASE 9: Severity-Based Alerts	71
Figure 47: TEST CASE 10: Advanced Machine Learning for Phishing Detection	72
Figure 48: TEST CASE 11: Multi-Browser Compatibility	73
Figure 49: TEST CASE 12: Sandbox Integration for File Analysis	74
Figure 50: Summary Version 4	76
Figure 51: Evaluation of version 4	78

LIST OF TABLES

Table 1:Testing Phase 1 Overview	10
Table 2: Version 1 Results	17
Table 3: Evaluation of version 1	18
Table 4:Testing Phase 2 Overview	22
Table 5: Version 2 Results	35
Table 6: Evaluation of version 2	36
Table 7: Testing Phase 3 Overview	42
Table 8: Version 3 Results	55
Table 9: Evaluation of version 3	57
Table 10: Testing Phase 4 Overview	62
Table 11: Version 4 Results	75
Table 12: Evaluation of version 4	77

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.
- o **61 test scenarios** were performed to assess both the new and existing features.

3. **Version 3 Testing**:

- o 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:

- o Conducted on **January 20, 2025**, as the final phase.
- o 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:

- o 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:

- o Identified issues such as URL monitoring inconsistencies, limited browser compatibility, and interface usability challenges.
- o 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:

o 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.

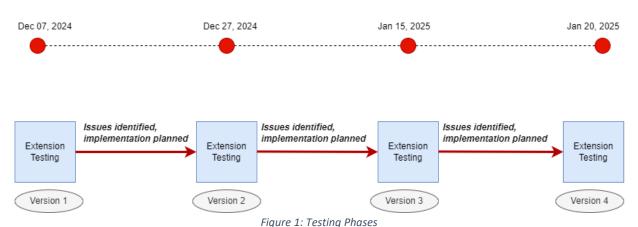
Fourth Testing Phase: January 20, 2025

• 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.



AEGIS SHIELD - PHISHING DETECTION EXTENSION

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 Cas	es Tested: 6	
Total Number of Scenario	s Tested: 36	

Table 1:Testing Phase 1 Overview

3.1 TEST CASE 1: Real-Time URL Monitoring

Test	Case ID	V1_C1		Test case I	Descriptio	n							1	
Vers	ion	Version 1		Verify the	extension	n's ability t	o moi	nitorand al	ert users ak	out URLs i	n real-tim	e based o	n their saf	ety status.
Testi	ng Functio	nality	Real-Time	URL Monit	toring		Test	ed By	Sudam		Test Date		7-Dec-24	
_	tionality F		Must-Have		toring			ewed By	Tanushka		Review D	ate	7-Dec-24	
	, , ,	,		_										
Num	ber of Sce	narios test	ed	8										
Num	ber of Sce	narios Pass	sed	0										
Succ	ess Rate %	5		0%										
S#	Pre- Cond	dition(s)					S#	Test Data						
1		is installe					1	https://w	ww.youtub	e.com/ an	d https://	syrianmal	ware.com/	/
2	VirusTota	al flagged	URLs need	led			2		rianmalwa					
3	-						3		s://www.yo			times		
4	-						4		ww.espncr		/			
5	-						5		rianmalwa					
6	The URL	should be	blackliste	d.			6		ww.cricbuz					
7	-						7		b.simmons	.edu/~gro	vesd/com	m244/not	es/week2	/links
8	-						8	Security R	eport				_	
							-	cted Resul				Actual Re		Status
1						ck.	_		ed and mai			Not work		Fail
2				-	otal.				ed URLs are			Not work		Fail
3					-111		+		orms the u			Not work		Fail
4					араск із р	rompt.	+		olayed with			Not work		Fail
					a or block	ina	_		re provided	for malici	ous UKLS.	Not work		Fail Fail
	6 Visit URLs in the blacklist to test bypassing or blocking.							king Blackli				Not work	Fail	
8	Visit valid website and monitor for analysis feedback. Visit URLs flagged as suspicious by VirusTotal. Simulate reaching API call rate limits Browse URLs and observe if real-time feedback is proi Trigger notifications for malicious URLs Visit URLs in the blacklist to test bypassing or blocking Test URLs with different protocols like HTTP and HTTP							is flagged	stored out	ido tho so	000	Not work		Fail
ő	MOUNTOL	i user data	or sensitiv	e iniormat	ion is bell	ig rogged	INO U	ser data is	Stored out	side the SO	ope.	Not work	ing	rali

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

3.2 TEST CASE 2: Phishing URL Detection

Test Cas	se ID	V1_C2		Test case	Descriptio	n								
Version		Version 1		Verify the	fy the extension's ability to detect and classify URLs as safe, or malicious, and provide user alerts.									
Testing	Functionalit	у	Phishing	URL Detec	tion		Tested By	,	Tanushka		Test Date		7-Dec-24	
Functio	mber of Scenarios tested mber of Scenarios Passed cess Rate % Pre- Condition(s) Extension is installed and			ve			Reviewed	Reviewed By Tharu			Review D	ate	7-Dec-24	
Numbe	r of Scenario	s tested		4										
Numbe	r of Scenario	s Passed		1										
Number of Scenarios tested Number of Scenarios Passed Success Rate % S # Pre- Condition(s)			25%											
0.11		1 / >					o							
S#	_						S#	Test Data						
1							1 https://www.youtube.com/							
2	VirusTota	al flagged	URL need	ed			2	https://syrianmalware.com/						
3	-						3	hts:/stud	entportal.e	cu.edu.aı	ı/s/			
4	-						4	Visit http	s://www.yo	outube.co	m multipl	e times		
S#	Scenario(s) and Step	o(s)				Expected	Results				Actual Re	esults	Status
1	Submit sa	fe URLs an	d observe	analysis re	sults.		URLs are r	marked as	safe.			Predicte	d as Phishin	g Fail
2	Submit kr	nown malic	ious URLs	flagged by	VirusTotal	l.	Malicious	URLs are f	flagged with	n warning	s.	As exped	ted	Pass
3	Submit in	valid or inc	complete l	JRLs for and	alysis.		Invalid UF	RLs are reje	ected with (user feed	back.	Predicte	Fail	
4	Simulate	VirusTotal	API unavai	ilability or	timeout.		Fallback n	nechanism	n informs us	ers of AP	l issues.	Not working		Fail

Figure 3:TEST CASE 2: Phishing URL Detection

3.3 TEST CASE 3: Whitelist/Blacklist Management

Test Cas	e ID	V1 C3		Test case	Description												
Version		Version 1			he extension's	s ability to	manage UI	RLs									
						,											
Testing	unctionalit	у	Whitelist	/Blacklist N	/lanagement		Tested By		Dulaj		Test Date		7-Dec-24				
Function	ality Priorit	у	Must-Hav	e			Reviewed	Ву	Tanushka		Review D	Date 7-Dec-24					
Number	of Scenario	s tested		7													
Number	of Scenario	s Passed		5													
Success	# Pre- Condition(s)			71%													
S #	Pre- Cond	lition(s)					S#	Test Data									
1	-						1	https://w	ww.youtub	e.com/							
2	-						2	https://sy	rianmalwar	e.com/							
3	3 -						3	-									
4	4 -						4	-									
5	https://sy	<u>rianmalwa</u>	re.com/ in	Blacklist			5	https://syrianmalware.com/									
6	-						6	hps://ww	/w.youtube.	com/							
7	-						7	-									
S #	Scenario(s) and Step	(s)				Expected	Results				Actual Re	sults	Status			
1	Add a tru	sted websi	te to the w	hitelist.			Website i	s successfu	ully added to	o the whit	elist.	As ex	pected	Pass			
2	Add a ma	licious web	site to the	blacklist.			Website i	s successfu	ully added to	o the blac	klist.	As ex	pected	Pass			
3	Remove a	website f	rom the w	hitelist.			Website i	s removed	from the w	hitelist.		As ex	pected	Pass			
4	Remove a	website f	rom the bl	acklist.			Website i	s removed	from the bl	lacklist.		As ex	pected	Pass			
5	_				ccess is blocke	d.	Blackliste	d website	access is blo	ocked.		Not b	locking	Fail			
6	Attempt t	o add inva	lid URLs to	whitelist/	blacklist.		Invalid entries are rejected with feedback.					URL	Fail				
7	Restart th	e browser	and verify	whitelist/	blacklist persi:	stence.	List chang	es are sav	ed and persi	ist after a	restart.	As expected Pa		Pass			

Figure 4:TEST CASE 3: Whitelist/Blacklist Management

3.4 TEST CASE 4: Email Phishing Detection

Test Cas	se ID	V1_C4		Test case I	Description						I			
Version		Version 1		Validate t	he extensio	n's ability	y to analyz	e email co	ntent or hea	aders, det	ect phishi	ng indicato	rs	
Tosting	Eunctionalit	v	Email Bhi	ching Doto	ction		Tostad Pu	,	Dulai		Tost Data		7-Dec-24	
		•			ction				Tanushka				7-Dec-24 7-Dec-24	
Number	r of Scenario	s tested		4										
Number	r of Scenario	s Passed		4										
Success	Rate %			100%										
S#	Pre- Cond	dition(s)					S#	Test Data	1					
1				re.			1 Legitimate email data							
2	phishing	email sam	ples are a	vailable.			2 phishing email data							
3	-						3	-						
4	-						4	Legitimat	te email data	a				
S#	Scenario(s) and Step	(s)				Expected	Results				Actual Re	sults	Status
1	Paste con	tent of a le	gitimate e	mail and a	nalyze.		Safe ema	il content	is analyzed a	and marke	ed as safe.	As ex	pected	Pass
Testing Functionality Email Phishing Detection Tested By Dulaj Test Date Reviewed By Tanushka Review Date 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 Legitimate email data 2 phishing email samples are available. 2 phishing email data 3 - 4 - 4 Legitimate email data S# Scenario(s) and Step(s) Expected Results Safe email content is analyzed and marked as safe. Actual Paste content of a legitimate email for analysis. Phishing email content is flagged.				As expected Pass		Pass								
3	Submit in	valid or en	npty email	content fo	r analysis.		Invalid in	puts are re	ejected with	an error r	nessage.	As ex	pected	Pass
4	Analyze a	lengthy er	nail with r	nultiple co	mponents.		System h	andles larg	ge emails wi	thout issu	ues.	As expected P		Pass

Figure 5:TEST CASE 4: Email Phishing Detection

3.5 TEST CASE 5: User-Friendly Interface

Test Cas	e ID	V1_C5		Test case [Description									
Version		Version 1		Validate t	he extensior	n's user i	nterface fo	or clarity, a	ccessibility	, and resp	onsivenes	s		
			User-Frier	ndly Interfa	ace		Tested By	'	Tanushka		Test Date		7-Dec-24	
Function	nality Priorit	у	Must-Hav	e		Reviewed By Sudam Review D					ate	7-Dec-24		
	•			_										
				6										
		s Passed		0										
Success	ersion Version 1 esting Functionality User- unctionality Priority Must umber of Scenarios tested umber of Scenarios Passed uccess Rate % # Pre- Condition(s) Scenario(s) and Step(s) Hover over a button or fea Review tooltips for clarity Switch to dark mode using Restart the browser and v			0%										
S#	Pre- Cond	lition(s)					S #	Test Data						
1	-						1	-						
2	-						2	-						
3	-						3	-						
4	-						4	-						
5	S # Pre- Condition(s) 1						5	-						
6	-						6	-						
S#	Scenario(s) and Step	(s)				Expected	Results				Actual Re	sults	Status
1	Hover ove	er a button	or feature	to check to	ooltip visibili	ity.	Tooltips a	re display	ed when ho	overing ov	er features	Not imp	lemented	Fail
2	Review to	oltips for	clarity and	relevance t	to the featur	re.	Tooltips a	re clear, c	oncise, and	relevant.		Not imp	lemented	Fail
3	Switch to	dark mode	using the	toggle but	ton.		Dark mod	e is enable	ed successf	ully.		Not imp	lemented	Fail
Testing Functionality Functionality Priority Number of Scenarios tested Number of Scenarios Passed Success Rate % S# Pre- Condition(s) 1 - 2 - 3 - 4 - 5 - 6 - S# Scenario(s) and Ste 1 Hover over a butto 2 Review tooltips for 3 Switch to dark mod		e browser	and verify	dark mode	preference	Dark mod	e preferer	nce persists	across se	ssions.	Not imp	lemented	Fail	
5	Enter data	in fields a	nd clear th	nem using t	he clear but	ton.	. Fields are cleared successfully using the button Not imple					lemented	Fail	
6	Resize the	e browser v	window an	d observe	layout adapt	tability.	lity. Interface adapts responsively to various screen size Not working						orking/	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	1				1			1
Version		Version 1		Validate t	he extension's funct	ionality, fe	ature cons	sistency, an	d perform	ance acros	s multiple	browsers	
Testing Fu	ınctionalit	у	Multi-Bro	wser Comp	atibility	Tested By		Tanushka		Test Date		7-Dec-24	
Functiona	lity Priorit	у	Won't-Ha	ve		Reviewed	Ву	Dulaj		Review D	ate	7-Dec-24	
Number o	f Scenario	s tested		7									
Number o	f Scenario	s Passed		3									
Success Ra	ate %			42%									
S#	Pre- Cond	lition(s)				S#	Test Data						
1	Install all	the require	ement Libr	aries		1	-						
2	Install all	the require	ement Libr	aries		2	-						
3	Install all	the require	ement Libr	aries		3	-						
4	Install all	the require	ement Libr	aries		4 -							
5	Install all	the require	ement Libr	aries		5 -							
6	Install all	the require	ement Libr	aries		6	-						
7	Install all	the require	ement Libr	aries		7	-						
S#	Scenario(s) and Step	(s)			Expected	Results				Actual Re	sults	Status
1	Install and	d test the e	extension o	n Google (Chrome	Extension	works sea	amlessly on	Chrome.		As expect	ed	Pass
2	Install and	d test the e	extension o	n Microso	ft Edge.	Extension	works sea	amlessly on	Edge.		As expect	ed	Pass
3	Install and	d test the e	extension	n Brave br	owser.	Extension	works sea	amlessly on	Brave.		As expect	ed	Pass
4	Install and	d test the e	extension o	n Firefox		Extension	works sea	amlessly on	Firefox.		Not work	ing	Fail
5	Verify tha	t all core f	eatures fur	nction cons	istently in Edge.	Features a	are consist	tent and fur	nctional		Not as ex	pected	Fail
6	Verify tha	t all core f	eatures fui	nction cons	istently in Brave.	Features a	re consist	tent and fur	nctional		Not as ex	pected	Fail
7	Verify tha	t all core f	eatures fui	nction cons	istently in Firefox	Features are consistent and functional Not working Fai							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

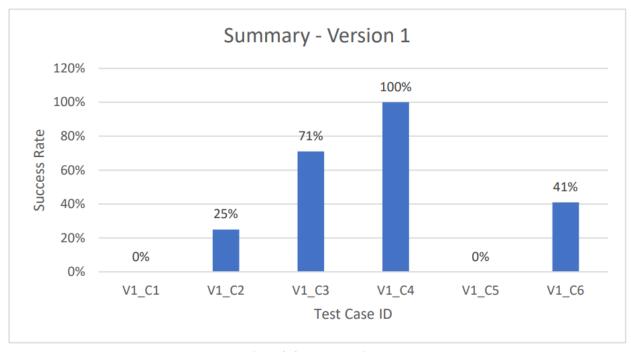


Figure 8: Summary Version-1

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.

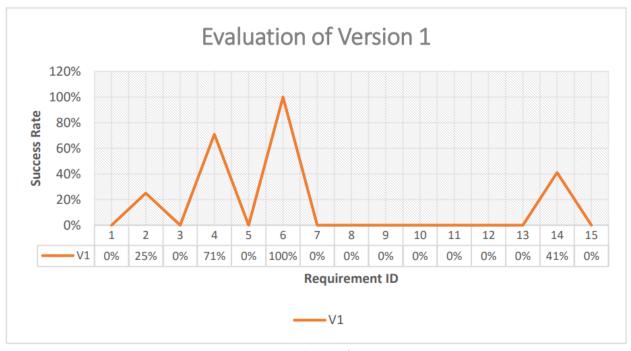


Figure 9: Evaluation of version 1

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:
 - o 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:
 - o Failed to detect certain phishing URLs due to gaps in validation rules.
 - o 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:
 - o 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:
 - o 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.
 - o 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:
 - o The extension performed inconsistently on Edge and Brave browsers.
 - o 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 Case	es Tested: 12	
Total Number of Scenario	s Tested: 61	

Table 4:Testing Phase 2 Overview

4.1 TEST CASE 1: Real-Time URL Monitoring

Testi	ing Functionality	Real-Time	URL Monit	toring		Test	ed By	Sudam	Test Date		27-Dec-2	4	
Func	tionality Priority	Must-Have	e			Revi	ewed By	Tanushka	Review D	ate	27-Dec-2	4	
Num	ber of Scenarios tes	ited	8										
Num	ber of Scenarios Pa	ssed	6										
Succ	ess Rate %		75.00%										
S#	Pre- Condition(s)					S#	Test Data						
1	Extension is install	ed and runn	ing.			1	https://w	ww.youtube.c	om/ and https://s	syrianmal	ware.com/	/	
2	VirusTotal flagged	URLs need	ded			2							
3	-				1 https://www.youtube.com/ and https://syrianma 2 https://syrianmalware.com/ 3 Visit https://www.youtube.com multiple times 4 https://www.espncricinfo.com/ 5 https://syrianmalware.com/ 6 https://syrianmalware.com/ 7 http://web.simmons.edu/~grovesd/comm244/no 8 Security Report Expected Results Actual R dback. URLs are analyzed and marked As e Alerts for flagged URLs are triggered. As e								
4	-					4							
5	-					5	https://sy						
6	The URL should be	e blackliste	d.			6	https://w	ww.cricbuzz.co					
7	-					7	http://we	b.simmons.ed	/links				
8	-				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/week 8 Security Report Expected Results ck. URLs are analyzed and marked Actual Results As expected								
S#	Scenario(s) and Ste	p(s)				Expe	cted Resul	lts		Actual Re	sults	Status	
1	Visit valid website	and monito	r for analys	is feedba	ck.	URLs	are analyz	ed and marked	d	As ex	pected	Pass	
2	Visit URLs flagged a	s suspicious	s by VirusT	otal.		Aler	ts for flagg	ed URLs are trig	ggered.	As ex	pected	Pass	
3	Simulate reaching A	API call rate	limits			Noti	fication inf	forms the user	of API issues.	Not v	vorking	Fail	
4	Simulate reaching API call rate limits Browse URLs and observe if real-time feedback is pro					Resu	ılts are disp	olayed without	delays.	As ex	pected	Pass	
5	Trigger notifications for malicious URLs					Noti	fications a	re provided for	malicious URLs.	As ex	pected	Pass	
6	7,500						Blocking Blacklisted sites As expected Pass						
7							is flagged	for risks		Not v	orking	Fail	
8	Monitor if user data	ion is beir	ng logged	No u	iser data is	stored outside	the scope.	As ex	pected	Pass			

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

4.2 TEST CASE 2: Phishing URL Detection

Test Ca	se ID	V2_C2		Test case	Descriptio	n								
Version	1	Version 2		Verify the	extension	n's ability to	detect ar	d classify	URLs as saf	e, or mal	icious, and	provide u	ser alerts.	
Tosting	Functionalit		Dhiching	URL Detec	tion		Tested By		Tanushka		Test Date		20-Dec-2	4
	Functionalit nality Priorit	-	Must-Hav		tion		Revied By		Tharuka		Review D		20-Dec-2	
Numbe	r of Scenario	s tested		4										
Numbe	r of Scenario	s Passed		3										
Success	ccess Rate % Pre- Condition(s)			75%										
S#	Pre- Cond	dition(s)					S#	Test Data						
1	Extension	n is installe	d and activ	/e.			1	https://w	/ww.youtul	oe.com/				
2	VirusTota	al flagged	URL need	ed			2	https://sy	yrianmalwa	re.com/				
3	-						3	hts:/stud	entportal.e	cu.edu.a	u/s/			
4	-						4	Visit http	s://www.y	outube.co	om multiple	times		
S#	Scenario(s) and Step)(s)				Expected	Results				Actual Re	sults	Status
1	Submit sa	afe URLs an	d observe	analysis re	sults.		URLs are r	narked as	safe.			As ex	pected	Pass
2	Submit kı	nown malic	ious URLs	flagged by	VirusTotal		Malicious	URLs are f	lagged witl	n warning	s.	As ex	pected	Pass
3	Submit invalid or incomplete URLs for analysis.					Invalid UR	Ls are reje	ected with	user feed	back.	Not v	orking	Fail	
4	Simulate VirusTotal API unavailability or timeout.					Fallback n	nechanism	n informs us	sers of AP	l issues.	As ex	pected	Pass	

Figure 11:TEST CASE 2: Phishing URL Detection

4.3 TEST CASE 3: Basic User Alerts

Test Ca	ase ID	V2_C3		Test case Descriptio	n							
Versio	n	Version		Validate the extens	ion's ability to disp	lay real-tim	e alerts for n	nalicious	and suspic	ious URLs		
	g Functional	-	Basic Use	r Alerts	Tested	Ву	Tharuka		Test Date		27-Dec-24	ļ
Function	onality Prior	ity	Must-Hav	/e	Revied	Ву	Sudam		Review D	ate	27-Dec-24	ļ
Numbe	er of Scenari	os tested		3								
Numbe	er of Scenari	os Passed		3								
Succes	s Rate %			100%								
S#	Pre- Cor	dition(s)			S#	Test Data	9					
1	Extensio	n is installe	ed and activ	ve	1	https://s	yrianmalwa	re.com/				
2	URL mu	ıst be in Bl	acklist		2	https://v	www.espncri	icinfo.con	m/			
3	URL mu	st be in Wh	itelist		3	https://v	www.youtub	e.com/				
S#	Scenario	(s) and Ste	p(s)		Expect	ed Results				Actual Re	sults	Status
1				trigger an alert.			is displayed			As ex	pected	pass
2		lacklisted s				displayed.				 	pected	pass
3	Visit a Blacklisted site Visit a Whitelisted site			Alert is	displayed.				As ex	pected	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				<u>'</u>				'	
Version		Version 2		Validate t	he extension's	s ability to	manage U	RLs						
Testing F	unctionalit	у	Whitelist	/Blacklist N	lanagement		Tested By	1	Dulaj	Т	est Date		27-Dec-24	ļ
Function	ality Priorit	:у	Must-Hav	e			Revied By	/	Tanushka	R	Review Da	ate	27-Dec-24	
	of Scenario			7										
	of Scenario	s Passed		6										
Success R	Rate %			85%										
S #	Pre- Cond	dition(s)					S #	Test Data						
1	-						1		/ww.youtub					
2	-						2	https://sv	yrianmalwar	re.com/				
3	-						3	-						
4	-						4	-						
5	https://sv	<u>rianmalwa</u>	re.com/ ir	n Blacklist			5	https://sv	yrianmalwar	re.com/				
6	-						6	hps://ww	vw.youtube.	.com/				
7	-						7	-						
S#	Scenario(s) and Step	(s)				Expected	Results				Actual Re	sults	Status
1	Add a tru	sted websi	te to the w	hitelist.			Website i	s successf	ully added to	o the white	list.	As ex	pected	Pass
2	Add a ma	licious web	site to the	blacklist.			Website i	s successf	ully added to	o the blackl	list.	As ex	pected	Pass
3	Remove a website from the whitelist.					Website i	s removed	d from the w	hitelist.		As ex	pected	Pass	
4						Website i	s removed	d from the bl	lacklist.		As ex	pected	Pass	
5	5 Visit a website in the blacklist to verify access is blocked				d.	Blackliste	d website	access is blo	ocked.		As ex	pected	Pass	
6	6 Attempt to add invalid URLs to whitelist/blacklist.						Invalid er	tries are r	ejected with	n feedback.	ı	URL	added	Fail
7						stence.	List chang	es are sav	ed and persi	ist after a re	estart.	As ex	pected	Pass

Figure 13: TEST CASE 4: Whitelist/Blacklist Management

4.5 TEST CASE 5: Basic Malware Detection

١	Version 2			Description								
			Verify the	extension's ability	to detect r	nalware th	reats in UR	Ls using th	ne VirusTota	al API and	provide al	erts.
ctionality		Basic Malv	vare Detec	tion	Tested By	/	Sudam		Test Date		27-Dec-24	4
ty Priority	,	Must-Have	2		Revied B	/	Tanushka		Review Da	ate	27-Dec-24	1
Scenarios	tested		4									
			3									
:e %			75%									
re- Condit	tion(s)				S#	Test Data						
Pre- Condition(s) Extension is installed and active.					1	https://www.youtube.com/						
-					2	https://syrianmalware.com/						
_					3	hps://ww	/w.youtube	c.com/				
-					4	Visit http	s://www.y	outube.co	m/ multipl	e times		
cenario(s)) and Step	(s)			Expected	Results				Actual Re	sults	Status
Submit a kr	nown safe	URL for ar	alysis.		Safe URL	is marked a	as safe with	no alerts		As ex	pected	Pass
Submit a kr	nown mal	ware-infe	ted URL fla	agged by VirusTota	I. Malware	URL is flag	ged with ar	appropri	ate alert.	As ex	pected	Pass
Submit an invalid or malformed URL for analysis.				Invalid U	RLs are reje	ected with a	an error m	essage.	Not re	ejected	Fail	
Simulate API timeout and check system behavior.					Graceful							
	Scenarios Scenarios e % Pre- Condi Extension Coenario(s Submit a k Submit a k	Scenarios tested Scenarios Passed e % Pre- Condition(s) Extension is installed Comparison of the compa	Scenarios tested Scenarios Passed e % Pre- Condition(s) Extension is installed and active Comparison of the second	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) Extension is installed and active. Scenario(s) and Step(s) Extension is a known safe URL for analysis. Extension is a known malware-infected URL flates	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) Extension is installed and active. Scenario(s) and Step(s) Eubmit a known safe URL for analysis. Eubmit a known malware-infected URL flagged by VirusTota submit an invalid or malformed URL for analysis.	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) S # Extension is installed and active. 1 2 3 4 Scenario(s) and Step(s) Expected Submit a known safe URL for analysis. Safe URL flagged by VirusTotal. Malware Submit an invalid or malformed URL for analysis. Invalid UR	Scenarios tested Scenarios Passed e % 75% Pre- Condition(s) Statension is installed and active. 1 https://w 2 https://s 3 hps://ww 4 Visit http Indicate a known safe URL for analysis. Submit a known malware-infected URL flagged by VirusTotal. Malware URL is flagged by Univalid URLs are rejected univalid URLs are rejected to the state of the s	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) S# Test Data Extension is installed and active. 1 https://www.youtule 2 https://syrianmalwate. 3 hps://www.youtule 4 Visit https://www.youtule 5 Usit https://www.youtule 6 Usit https://www.youtule 7 Usit https://www.youtule 8 Usit https://www.youtule 9	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) S # Test Data Extension is installed and active. 1 https://www.youtube.com/ 2 https://syrianmalware.com/ 3 hps://www.youtube.com/ 4 Visit https://www.youtube.com/ 5 Expected Results 5 Submit a known safe URL for analysis. 5 Safe URL is marked as safe with no alerts 5 Submit a known malware-infected URL flagged by VirusTotal. 6 Malware URL is flagged with an appropri	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) S# Test Data Extension is installed and active. 1 https://www.youtube.com/ 2 https://syrianmalware.com/ 3 hps://www.youtube.com/ 4 Visit https://www.youtube.com/ multiple.cenario(s) and Step(s) Expected Results Extension is installed and active. 2 https://www.youtube.com/ 4 Visit https://www.youtube.com/ multiple.cenario(s) and Step(s) Expected Results Extension is installed and active. Safe URL is marked as safe with no alerts. Extension is installed and active. A Wisit https://www.youtube.com/ Malware URL is flagged with an appropriate alert. Extension is installed and active. Invalid URLs are rejected with an error message.	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) S# Test Data Extension is installed and active. 1 https://www.youtube.com/ 2 https://syrianmalware.com/ 3 hps://www.youtube.com/ 4 Visit https://www.youtube.com/ multiple times Excenario(s) and Step(s) Expected Results Expected Re	Scenarios tested 4 Scenarios Passed 3 e % 75% Pre- Condition(s) S # Test Data https://www.youtube.com/ 2 https://syrianmalware.com/ 3 hps://www.youtube.com/ 4 Visit https://www.youtube.com/ multiple times scenario(s) and Step(s) Expected Results Actual Results Safe URL is marked as safe with no alerts. As expected submit a known malware-infected URL flagged by VirusTotal. Submit a known malware-infected URL for analysis. Malware URL is flagged with an appropriate alert. As expected invalid or malformed URL for analysis. Not rejected

Figure 14: TEST CASE 5: Basic Malware Detection

4.6 TEST CASE 6: Email Phishing Detection

Test Ca	se ID	V2_C6		Test case I	Description							
Version	1	Version 2		Validate t	he extension's abilit	ty to analyz	e email co	ntent or he	aders, detect ph	ishing indicat	ors	
Testing	Functionalit	у	Email Phis	shing Dete	ction	Tested By	/	Dulaj	Test [Date	27-Dec-2	4
Functio	nality Priorit	у	Must-Hav	e		Reviewed	d By	Tanushka	Revie	w Date	27-Dec-2	4
Numbe	r of Scenario	s tested		4								
Numbe	r of Scenario	s Passed		4								
Success	Rate %			100%								
S#	Pre- Cond	lition(s)				S#	Test Data	1				
1	Extension	is installe	d and activ	e.		1	Legitimat	te email dat	ta			
2	phishing	email sam	ples are a	vailable.		2	phishing	email data				
3	-					3	-					
4	-					4	Legitimat	te email dat	ta			
S#	Scenario	s) and Step	o(s)			Expected	Results			Actual R	esults	Status
1				mail and a	nalyze.	-		is analyzed	and marked as s		xpected	Pass
2			_		for analysis.			ent is flagg			xpected	Pass
3	Submit invalid or empty email content for analysis.										Pass	
4	Analyze a lengthy email with multiple componer			<u> </u>			•	ithout issues.		xpected	Pass	

Figure 15: TEST CASE 6: Email Phishing Detection

4.7 TEST CASE 7: Browser Notifications

Test Ca	ase ID	V2_C7		Test case Desc	ription				1				
Versio	n			Validate the e	xtension's abili	ty to send c	ategorize	d browser n	otificatio	ns with sev	erity level	s	
Testing	g Functionali	ity	Browser N	Notifications		Tested By		Sudam		Test Date		27-Dec-24	
Function	ber of Scenarios tested 5 ber of Scenarios Passed 5 ess Rate % 100% Pre- Condition(s) Extension is installed and active.			Revied By	1	Tanushka		Review D	ate	27-Dec-24	ı		
Numbe	er of Scenari	os tested		5									
Numbe	er of Scenari	os Passed		5									
Succes	s Rate %			100%									
S#	Pre- Con	dition(s)				S #	Test Data	a					
1	Extensio	n is installe	d and activ	re.		1	https://v	vww.youtul	be.com/				
2	-					2	https://s	yrianmalwa	re.com/				
3	-					3	-						
4	-					4	-						
5	-					5	-						
S#	Scenario	(s) and Ste	o(s)			Expected	Results				Actual Re	sults	Status
1	Visit a sa	fe URL to tr	igger a not	ification.		Notificati	on indicat	es the URL	is safe.		As ex	pected	Pass
2	Visit a m	alicious UR	L to trigger	a notification.		Notificati	on clearly	warns abou	ut the mal	icious URL.	As ex	pected	Pass
3	Verify th	ne notificati	on is displa	yed promptly.		Notificati	ons appea	ar without n	oticeable	delays.	As ex	pected	Pass
4	Dismiss a notification manually.				Dismissed	d notificat	ions are rer	noved pro	perly.	As ex	pected	Pass	
5	Verify the notification is displayed promptly. Dismiss a notification manually. Verify notifications have consistent design.					Notificati	ons maint	ain consiste	ent style a	nd icons.	As ex	pected	Pass

Figure 16: TEST CASE 7: Browser Notifications

4.8 TEST CASE 8: User-Friendly Interface

Test Ca	ase ID	V2_C8		Test case	Description	า								
Versio	n	Version 2		Validate t	he extensi	on's user i	nterface fo	or clarity, a	accessibility	, and resp	onsivenes	s		
Testing	g Functiona	ality	User-Frie	ndly Interf	ace		Tested By	,	Tanushka		Test Date		27-Dec-2	4
	onality Pric		Must-Hav	e			Revied By	1	Dulaj		Review D	ate	27-Dec-2	4
Numbe	er of Scena	rios tested												
Numbe	er of Scena	rios Passed												
Succes	s Rate %													
S #	Pre- Co	ondition(s)					S#	Test Data	ı					
1	-						1	-						
2	-						2	-						
3	-						3	-						
4	-						4	-						
5	-						5	-						
6	-						6	-						
S#	Scenar	io(s) and Step	o(s)				Expected	Results				Actual Re	sults	Status
1	Hover	over a button	or feature	to check to	ooltip visib	ility.	Tooltips a	re display	ed when ho	vering ov	er features	Not to	ooltips	Fail
2	Reviev	v tooltips for	clarity and	relevance	to the feat	ure.	Tooltips a	re clear, c	oncise, and	relevant.		Not to	ooltips	Fail
3	Switch	to dark mode	using the	toggle but	ton.		Dark mod	e is enable	ed successfu	ılly.		No dar	k mode	Fail
4	Restart the browser and verify dark mode preference pers				ce persists	Dark mod	e preferer	nce persists	across se	ssions.	No dar	k mode	Fail	
5	Enter data in fields and clear them using the clear button.					utton.	Fields are	cleared s	uccessfully	using the	button	No clea	r option	Fail
6	Resize the browser window and observe layout adaptable					ptability.	Interface	adapts res	ponsively t	o various	screen size	Not w	orking	Fail

Figure 17: TEST CASE 8: User-Friendly Interface

4.9 TEST CASE 9: Severity-Based Alerts

Test Ca	ase ID	V2_C9		Test case Descri	ption								
Versio	Functionality Severity phality Priority Should-Fer of Scenarios tested er of Scenarios Passed s Rate %			Validate the ext	ension's abili	ty to provid	le severity	-based aler	ts and re	commende	d actions f	or users.	
			Severity-	Based Alerts		Tested By	/	Tharuka		Test Date		27-Dec-2	4
Function	onality Prio	rity	Should-H	ave		Revied By	/	Tanushka		Review D	ate	27-Dec-2	4
Numbe	er of Scena	rios tested		3									
Numbe	er of Scena	rios Passed		2									
Succes	access Rate % 66%												
S#	Pre- Co	ndition(s)				S#	Test Data	9					
1	Extensi	ion is installe	d and activ	ve.		1	1 https://www.youtube.com/						
2	-					2	https://s	yrianmalwa	re.com/				
3	-					3	-						
S#	Scenari	io(s) and Step	o(s)			Expected	Results				Actual Re	sults	Status
1 Visit a URL flagged as safe			Alert is di	isplayed				As Ex	pected	Pass			
2	Visit a URL flagged as				Alert is di	isplayed				As Ex	pected	Pass	
3	Review the alert for suggested actions based on severity.				n severity.	Alerts inc	lude reco	mmended a	ctions for	users.	Not v	orking/	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											
Versio	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				
Function	Functionality Priority Coul		Could-Hav	Could-Have			Revied By		Tanushka		Review Date		27-Dec-24	
Numbe	er of Scenario	s tested		5										
	Number of Scenarios Passed 4													
	Success Rate %			80%										
S#	Pre- Cond	Pre- Condition(s)						Test Data						
1	Extension	Extension is installed and active.					1	https://www.youtube.com/ and https://syrianmalware.com/						
2	-	-				2	http://freesd1.000webhostapp.com/Star.html							
3	-	-					3	http://thelmachan.com.br/images/banners/a607b0c8e7c98759bb45e8a5b1						
4	-						4	ht://you'						
5	-						5	Using 5 legitimate and 5 phishing URLs						
S#	Scenario(s) and Step	(s)				Expected Results					Actual Re	sults	Status
1	Submit le	Submit legitimate URLs for analysis and observe predictions.						Legitimate URLs are correctly identified as safe.					As expected	
2	Submit kn	Submit known phishing URLs and verify detection results.						Phishing URLs are flagged accurately.					As expected	
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 m	Analyze multiple URLs to evaluate model performance and speed.						Model performs efficiently without significant delays. As expected Pass						Pass

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

4.11 TEST CASE 11: Multi-Browser Compatibility

Test Ca	se ID	V2_C11		Test case I	Description				<u> </u>					
Versio	Version 2			Validate the extension's functionality, feature consistency, and performance across multiple browsers										
Testing	g Functionalit	ty	Multi-Bro	wser Comp	atibility	Tested B	у	Tanushka	Test Date	2	27-Dec-2	4		
Functionality Priority Won't-Ha			/e		Reviewed By		Dulaj	Review [Date	27-Dec-24				
Number of Scenarios tested				7										
Numbe	Number of Scenarios Passed			3										
Succes	Success Rate %			42%										
S#	Pre- Cond	dition(s)				S#	Test Data							
1	Install all	Install all the requirement Libraries					-							
2	Install all	Install all the requirement Libraries				2	2 -							
3	Install all	Install all the requirement Libraries				3	-							
4	Install all	Install all the requirement Libraries				4	-							
5	Install all	Install all the requirement Libraries				5	5 -							
6	Install all	Install all the requirement Libraries					-							
7	Install all	the requir	ement Libr	aries		7	-							
S#	Scenario(s) and Step	(s)			Expected	Results		Actual Re	sults	Status			
1	Install an	Install and test the extension on Google Chrome						amlessly on Chr	As expected		Pass			
2	Install an	Install and test the extension on Microsoft Edge.						amlessly on Edg	As expected		Pass			
3	Install an	Install and test the extension on Brave browser.						amlessly on Bra	As expected		Pass			
4	Install an	Install and test the extension on Firefox						amlessly on Fire	Not working Fail		Fail			
5	Verify th	Verify that all core features function consistently in Edge.						tent and function	Not as expected Fail		Fail			
6	Verify th	Verify that all core features function consistently in Brave.						tent and function	Not as expected Fail		Fail			
7	Verify th	at all core f	eatures fu	nction cons	istently 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	n	Version 2		Validate t	ne extension's abili	ty to upload ar	nd scan files f	or malware u	ising the VirusTota	I API			
Testing	g Functional	ty	Sandbox I	ntegration	for File Analysis	Teste	d By	Tharuka	Test Dat	e	27-Dec-2	4	
	Functionality Priority Won't-Hav					Revie	Revied By		Tanushka Review D		ate 27-Dec-24		
Numbe	er of Scenari	os tested		5									
Numbe	Number of Scenarios Passed 4												
Succes	Success Rate % 80%												
S#	Pre- Con	ndition(s) S# Test Data											
1	Extensio	Extension is installed and active.					Valid fil	Valid file					
2	-	-					Maliciou	Malicious file					
3	-	-					File large	File larger than 32 MB					
4	-					4	Checking	Checking result with Virustotal					
5	-					5	Valid file	Valid files					
S#	Scenario	(s) and Step	o(s)			Exped	Expected Results Sta						
1	Upload a	Upload a valid file and observe scan results.						Valid file is scanned successfully with no threats. As expected					
2	Upload a	Upload a file containing malware and verify detection.						Malware file is flagged with appropriate details. As expected					
3	Attempt to upload a file larger than the size limit.						Large files are rejected with a size limit warning. As expected Par					Pass	
4	Verify th	Verify the accuracy of scan results for uploaded files.						Scan results are accurate and detailed.					
5	Upload r	Upload multiple files sequentially and observe performance.					m handles mu	ıltiple file up	oloads efficiently.	As ex	pected	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

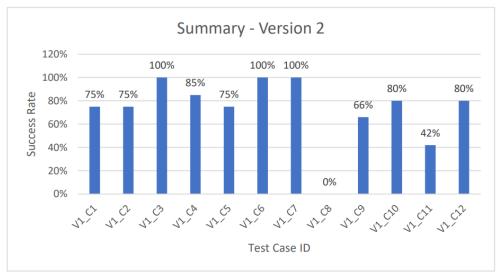


Figure 22: Summary Version 2

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 o	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.

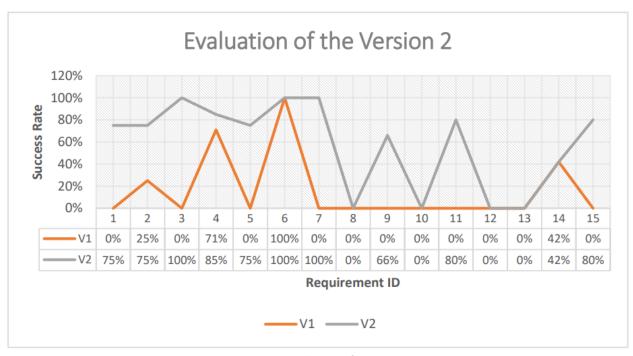


Figure 23: Evaluation of version 2

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.
- o 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.
- o A small number of phishing URLs were incorrectly categorized as safe.

• Identified Issues:

- o Current detection logic lacks robustness against sophisticated phishing patterns.
- o Insufficient heuristics for identifying borderline cases.

• Impact:

o 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:

- o Certain blacklisted URLs were incorrectly allowed, bypassing restrictions.
- o The "Clear All" function did not work consistently, especially with long lists.

• Identified Issues:

- o 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:

o 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:

- o 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:

- o Lack of implementation for Firefox compatibility, as promised in the project scope.
- o Browser-specific differences in extension APIs causing inconsistent performance.

• Impact:

o Limited cross-browser compatibility restricts user adoption and trust in the extension.

Recommendations:

o 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:

- o A small percentage of phishing URLs with rare patterns were not flagged.
- o 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.
- o Precision and recall metrics need optimization to reduce false positives.

• Impact:

o 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:

- o The extension crashed when large files were uploaded for scanning.
- Unsupported file types were not consistently rejected with appropriate error messages.

• Identified Issues:

- o File size validation logic is incomplete.
- o Error handling for unsupported file formats needs improvement.

• Impact:

 Users may experience frustration or crashes when uploading files, reducing trust in the feature.

• Recommendations:

o 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.
- o Dark mode preferences failed to persist across sessions.
- o 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.
- o 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:

- o Alerts for moderate threat levels did not include appropriate recommended actions.
- High-severity alerts occasionally displayed generic messaging rather than tailored recommendations.

• Identified Issues:

o Incomplete logic for assigning and displaying recommendations based on severity.

• Impact:

o Users may struggle to assess and act on certain alerts due to insufficient guidance.

• Recommendations:

o 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 Scenario	s 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									
Vers	ion	Version 3		Verify the	extension!	s ability t	o mor	nitorand al	ert users al	bout URLs	n real-tim	e based or	their safe	ety status.
Testi	ing Functio	onality	Real-Time	URL Monit	toring		Test	ed By	Sudam		Test Date		15-Jan-25)
Func	tionality P	riority	Must-Hav	e			Revi	ed By	Tanushka		Review Da	ate	15-Jan-25	
Num	ber of Sce	narios test	ed	8										
Num	ber of Sce	narios Pass	ed	7										
Succ	ess Rate %	5		88%										
S#	Pre- Cond						S#	Test Data						
1		is installe					1	https://w	ww.youtul	oe.com/ ar	d https://	syrianmaly	vare.com/	'
2	VirusTota	al flagged	URLs need	ded			2		<u>rianmalwa</u>					
3	-						3	Visit https	s://www.y	outube.co	m multiple	times		
4	-						4		ww.espnc		ı/			
5	-						5		rianmalwa					
6	The URL	should be	blackliste	d.			6	https://w	ww.cricbu	zz.com/				
7	-						7	http://we	b.simmon	s.edu/~gro	vesd/com	m244/note	es/week2/	links
8	-						8	Security R	Report					
S#		s) and Step					Expe	cted Resul	ts			Actual Re	sults	Status
1					is feedbac	k.	_		ed and ma			As ex	pected	Pass
2				s by VirusT	otal.		_		ed URLs are			As ex	pected	Pass
3		reaching A					-		orms the u			As ex	pected	Pass
4	Browse URLs and observe if real-time feedback is promp						_		olayed with			As ex	pected	Pass
5	Trigger notifications for malicious URLs						_		re provided	d for malici	ous URLs.		pected	Pass
6	Visit URLs in the blacklist to test bypassing or blocking.						_	king Blackli				As ex	pected	Pass
7	Test URLs with different protocols like HTTP and HTTPS.						_	is flagged					orking	Fail
8	Monitor i	f user data	or sensitiv	e informat	ion is being	glogged	No u	ser data is	stored out	side the so	ope.	As ex	pected	Pass

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

5.2 TEST CASE 2: Phishing URL Detection

Test Ca	se ID	V3_C2		Test case I	Descriptio	n							
Version	า	Version 3		Verify the	extension	's ability to de	tect and clas	sify URLs as saf	e, or mal	icious, and	provide u	ser alerts.	
Testina	Functiona	lity	Phiching	URL Detec	tion	Tes	ted By	Tanushka		Test Date	<u> </u>	15-Jan-25	
	nality Pric		Must-Hav		LIOII		ied By	Sudam		Review D		15-Jan-25	
unctic	manty File	птсу	IVIUSCITIAV			IVE	ieu by	Sudam		Neview D	ate	15-Jan-25	,
Numbe	er of Scena	rios tested		4									
Numbe	r of Scena	rios Passed		3									
Succes	s Rate %			75%									
S#	Pre- Co	ndition(s)				S#	Test	Data					
1	Extensi	ion is installe	d and activ	re.		1	https	://www.youtu	be.com/				
2	VirusTo	otal flagged	URL need	ed		2	https	://syrianmalwa	are.com/				
3	-					3	hts:/	studentportal.e	ecu.edu.a	u/s/			
4	-					4	Visit	https://www.y	outube.co	om multiple	e times		
S#	Scenari	io(s) and Step)(s)			Exp	ected Resul	ts			Actual Re	sults	Status
1	Submit	safe URLs an	d observe	analysis re	sults.	URI	s are marke	d as safe.			As ex	pected	Pass
2	Submit	known malic	ious URLs	flagged by	VirusTotal	. Ma	icious URLs	are flagged wit	h warning	s.	As ex	pected	Pass
3	Submit invalid or incomplete URLs for analysis.						alid URLs are	rejected with	user feed	back.	Not r	ejected	Fail
4	Simula	te VirusTotal	API unava	ilability or t	timeout.	Fal	back mecha	nism informs u	sers of AP	l issues.	As ex	pected	Pass

5.3 TEST CASE 3: Basic User Alerts

Test Ca	ase ID	V3_C3		Test case Description	n							
Versio	n	Version 3		Validate the extensi	on's ability to disp	lay real-tim	e alerts for ma	alicious	and suspic	ious URLs		
Testing	g Functionalit	ty	Basic Use	r Alerts	Tested	Ву	Tharuka		Test Date		15-Jan-25	5
Function	onality Priori	ty	Must-Hav	/e	Revied	Ву	Sudam		Review D	ate	15-Jan-25	5
Numbe	er of Scenario	os tested		3								
Numbe	er of Scenario	s Passed		3								
Succes	s Rate %	e % 100%										
S#	Pre- Cond	dition(s)			S #	Test Data	a					
1	Extension	n is installe	d and activ	ve	1	https://s	yrianmalware	e.com/				
2	URL mu	st be in Bla	acklist		2	https://v	www.espncric	info.co	m/			
3	URL mus	t be in Whi	telist		3	https://v	vww.youtube	.com/				
S#	Scenario	(c) and Stan	\(c\		Evnecte	ed Results				Actual Re	sculte	Status
3π 1		Scenario(s) and Step(s) Visit a known malicious URL to trigger an alert.					is displayed.				pected	pass
2		acklisted sit				displayed.	1 /			+	pected	pass
3	Visit a W	hitelisted s	ite			displayed.					pected	pass

Figure 26: TEST CASE 3: Basic User Alerts

5.4 TEST CASE 4: Whitelist/Blacklist Management

Test Case	ID	V3 C4		Test case I	Description			1					
Version		Version 3		Validate t	he extension's	ability to	manage UI	RLs			e 15-Jan-25		
						-							
Testing Fu	unctionalit	у	Whitelist/	/Blacklist N	lanagement		Tested By		Dulaj	Test Date		15-Jan-25	
Functiona	ality Priorit	у	Must-Hav	e			Revied By	,	Tanushka	Review D	ate	15-Jan-25	
Number o	of Scenario	s tested		7									
	of Scenario	s Passed		6									
Success R	ate %			85%									
S#	Pre- Cond	lition(s)					S#	Test Data					
1	-						1		ww.youtube				
2	-						2	https://sy	yrianmalware	.com/			
3	-						3	-					
4	-						4	-					
5	https://sy	<u>rianmalwa</u>	re.com/ in	Blacklist			5	https://sy	yrianmalware	.com/			
6	-						6	hps://ww	/w.youtube.c	om/			
7	-						7	-					
S#	Scenario(s) and Step	(s)				Expected	Results			Actual Re	sults	Status
1	Add a trus	sted websit	te to the w	hitelist.			Website i	s successf	ully added to	the whitelist.	As ex	pected	Pass
2	Add a ma	licious web	site to the	blacklist.			Website i	s successf	ully added to	the blacklist.	As ex	pected	Pass
3	Remove a	website fr	rom the wi	nitelist.			Website i	s removed	from the wh	itelist.	As ex	pected	Pass
4	Remove a	website fr	rom the bla	acklist.			Website i	s removed	from the bla	cklist.	As ex	pected	Pass
5					ccess is blocked.		Blackliste	d website	access is bloc	ked.	As ex	pected	Pass
6		o add inval							ejected with		URL	added	Fail
7	Restart th	e browser	and verify	whitelist/l	blacklist persist	tence.	List chang	es are sav	ed and persis	t after a restart.	As ex	pected	Pass

Figure 27: TEST CASE 4: Whitelist/Blacklist Management

5.5 TEST CASE 5: Basic Malware Detection

Test Ca	se ID	V3_C5		Test case	Description									
Version	n	Version 3		Verify the	extension's	ability t	o detect m	nalware th	reats in UR	Ls using t	he VirusTot	al API and	provide a	erts.
Testing	Functionalit	V	Basic Malv	ware Detec	ction		Tested By	,	Sudam		Test Date		15-Jan-25	5
	nality Priorit		Must-Hav	e			Revied By		Tanushka		Review D	ate	15-Jan-25	5
Numbe	er of Scenario	s tested		4										
Numbe	er of Scenario	s Passed		4										
Succes	cess Rate %			100%										
S#	Pre- Cond	lition(s)					S#	Test Data	1					
1	Extension	is installe	d and activ	e.			1	https://w	/ww.youtul	be.com/				
2	-						2	https://s	yrianmalw	are.com/				
3	-						3	hps://ww	vw.youtube	e.com/				
4	-						4	Visit http	s://www.y	outube.co	om/ multip	le times		
S#	Scenario(Scenario(s) and Step(s)					Expected	Results				Actual Re	sults	Status
1	Submit a	Submit a known safe URL for analysis.						is marked a	as safe with	no alert	5.	As ex	pected	Pass
2	Submit a	Submit a known malware-infected URL flagged by VirusTo						URL is flag	ged with ar	appropri	iate alert.	As ex	pected	Pass
3	Submit ar	Submit an invalid or malformed URL for analysis.						RLs are reje	ected with	an error n	nessage.	As ex	pected	Pass
4	Simulate	API timeou	ck system b		Graceful f	allback me	essage for A	API failure	e displayed.	. As ex	pected	Pass		

Figure 28: TEST CASE 5: Basic Malware Detection

5.6 TEST CASE 6: Email Phishing Detection

Test Cas	se ID	V6_C6		Test case	Descriptio	tension's ability to analyze email content or headers, detect phishing indicators Tested By Dulaj Test Date 15-Jan-25 Reviewed By Tanushka Review Date 15-Jan-25											
Version		Version 3		Validate t	he extensi	ion's abilit	y to analyz	e email co	ntent or he	aders, det	tect phishir	ng indicato	rs				
Testing	Functionalit	у	Email Phis	shing Dete	ction		Tested By	/	Dulaj		Test Date		15-Jan-25				
Functio	nality Priorit	у	Must-Hav	e			Reviewe	d By	Tanushka		Review D	ate	15-Jan-25				
Numbe	r of Scenario	s tested		4													
Numbe	r of Scenario	s Passed		4													
Success	Rate %			100%													
S#	Pre- Cond	lition(s)					S#	Test Data									
1	Extension	is installe	d and activ	/e.			1	Legitimat	te email dat	ta							
2	phishing	email sam	ples are a	available.			2	phishing	email data								
3	-						3	-									
4	-						4	Legitimat	te email dat	ta							
S#	Scenario(s) and Step	(s)				Expected	Results				Actual Re	sults	Status			
1	Paste content of a legitimate email and analyze.						Safe ema	il content	is analyzed	and mark	ed as safe.	As ex	pected	Pass			
2	Paste content of a known phishing email for analysis.						Phishing	email cont	ent is flagg	ed.		As ex	pected	Pass			
3	Submit in	Submit invalid or empty email content for analysis.						puts are re	ejected with	an error	message.	As ex	pected	Pass			
4	Analyze a	lengthy er	nail with n	nultiple co	mponents		System h	andles larg	ge emails w	ithout iss	ues.	As ex	pected	Pass			

Figure 29: TEST CASE 6: Email Phishing Detection

5.7 TEST CASE 7: Browser Notifications

Test Ca	se ID	V3_C7		Test case [Description	·							
Versior	1	Version 3		Validate t	he extension's a	ability to send o	ategorized	browser n	otification	ns with sev	erity level	5	
Testing	Functionali	ty	Browser I	Notification	15	Tested By	,	Sudam		Test Date		15-Jan-2	5
	nality Priori	•	Must-Hav	e		Revied By		Tanushka		Review D	ate	15-Jan-2	5
Numbe	r of Scenario	os tested		5									
	r of Scenario			5									
Success	Rate %			100%									
S#	Pre- Con	dition(s)				S #	Test Data						
1	_	n is installe	d and activ	/e.		1	https://w	ww.youtub	e.com/				
2	-					2		yrianmalwa					
3	-					3	-						
4	-					4	-						
5	-					5	-						
S#	Scenario	(s) and Step	o(s)			Expected	Results				Actual Re	sults	Status
1		fe URL to tr		ification.		-		es the URL i	s safe.		As ex	pected	Pass
2				a notificat	ion.	Notificati	on clearly	warns abou	it the mal	icious URL.	As ex	pected	Pass
3	Verify the notification is displayed promptly.					Notificati	ons appea	r without n	oticeable	delays.	As ex	pected	Pass
4	Dismiss a	notificatio	n manuall	у.		Dismissed	l notificati	ons are ren	noved pro	perly.	As ex	pected	Pass
5	Verify no	tifications	have consi	stent desig	ın.	Notificati	ons maint	ain consiste	nt style a	nd icons.	As ex	pected	Pass

Figure 30: TEST CASE 7: Browser Notifications

5.8 TEST CASE 8: User-Friendly Interface

Test Cas	ie ID	V3_C8		Test case	Description	1								
Version		Version 3		Validate t	he extensi	on's user i	nterface fo	r clarity, a	ccessibility	, and resp	onsivenes	s		
Testing	Functionalit	/	User-Frier	ndly Interfa	ace		Tested By		Tanushka		Test Date		15-Jan-25	
Function	nality Priorit	У	Must-Hav	9			Revied By		Dulaj		Review Da	ate	15-Jan-25	
	of Scenario			6										
Number	of Scenario	s Passed		5										
Success	Rate %			83%										
S#	Pre- Cond	ition(s)					S#	Test Data						
1	-						1	-						
2	-						2	-						
3	-						3	-						
4	-						4	-						
5	-						5	-						
6	-						6	-						
S#		s) and Step					Expected I	Results				Actual Re	sults	Status
1	Hover ove	r a button	or feature	to check to	ooltip visib	ility.	Tooltips a	re display	ed when ho	overing ov	er features	As ex	pected	Pass
2	Review tooltips for clarity and relevance to the featur						Tooltips a	re clear, co	oncise, and	relevant.		As ex	pected	Pass
3	Switch to dark mode using the toggle button.						Dark mode	e is enable	ed successf	ully.		As ex	pected	Pass
4	Restart th	e browser	and verify	dark mode	e preferenc	e persists.	Dark mode	e preferer	nce persists	across se	ssions.	As ex	pected	Pass
5	Enter data	in fields a	nd clear th	em using t	the clear bu	utton.	Fields are	cleared su	uccessfully	using the	button	As ex	pected	Pass
6	Resize the	browser v	window an	d observe	layout ada	ptability.	Interface a	adapts res	ponsively t	o various	screen size	Not w	orking	Fail

Figure 31: TEST CASE 8: User-Friendly Interface

5.9 TEST CASE 9: Severity-Based Alerts

Test Ca	ise ID	V3_C9		Test case Description	n								
Versio	n	Version 3		Validate the extensi	on's abil	ity to provid	le severity	/-based alert	s and rec	ommende	d actions f	or users.	
Testing	g Functiona	ality	Severity-E	Based Alerts		Tested By	1	Tharuka		Test Date		15-Jan-2	5
Functio	onality Pric	ority	Should-Ha	ave		Revied By	/	Tanushka		Review D	ate	15-Jan-2	5
Numbe	or of Scopa	rios tested		2									
		rios lested		2									
Succes	ccess Rate % 66%												
C #	D C-					C #	T+ D-+-	_					
S#		ondition(s) ion is installe	d and activ	10		S#	Test Data	ww.youtube	o com/				
2	-	ion is mstane	u anu activ	e.		2		yrianmalwar					
3	-					3	-						
S#	Scenari	io(s) and Step	o(s)			Expected	Results				Actual Re	sults	Status
1		Visit a URL flagged as safe					isplayed				As Ex	pected	Pass
2	Visit a	Visit a URL flagged as					isplayed				As Ex	pected	Pass
3	Review	v the alert for	suggested	actions based on sev	erity.	Alerts inc	lude reco	mmended ac	tions for	users.	Not v	vorking	Fail

Figure 32: TEST CASE 9: Severity-Based Alerts

5.10 TEST CASE 10: Advanced Machine Learning for Phishing Detection

Test Cas	se ID	V3_C10		Test case I	Description								
Version	1	Version 3		Validate t	he extension's abi	ility to de	etect phish	ing patter	ns using a pre-t	rained ML model			
Tosting	Functionalit	,	Advanced	MI for Dhi	ching Detection		Tested By		Dulai	Test Date		15-Jan-25	<u> </u> :
	Functionalit				shing Detection		,		,				
Functio	nality Priorit	У	Could-Hav	/e			Revied By	/	Tanushka	Review Date	e	15-Jan-25	<u> </u>
Numbe	r of Scenario	s tested		5									
Numbe	r of Scenario	s Passed		4									
Success	Rate %			80%									
S#	Pre- Cond	lition(s)					S#	Test Data	3				
1	_		d and activ	e.			1	https://w	vww.youtube.c	om/ and https://sy	rianmalwa	re.com/	
2	-						2			ostapp.com/Star.h			
3	-						3	http://th	elmachan.com.	.br/images/banner	s/a607b0c8	e7c98759b	b45e8a5b1
4	-						4	ht://you'	1				
5	-						5	Using 5 le	egitimate and 5	phishing URLs			
S #	Scenario(s) and Step)(s)				Expected	Results			Actual Re	sults	Status
1	Submit le	gitimate U	RLs for ana	lysis and o	bserve prediction	s.	Legitimat	e URLs are	correctly ident	tified as safe.	As ex	pected	Pass
2	Submit kr	Submit known phishing URLs and verify detection results.						URLs are fl	lagged accurate	ly.	As ex	pected	Pass
3	Submit UI	Submit URLs with suspicious patterns and evaluate predictions.						s URLs are	flagged approp	oriately.	As ex	pected	Pass
4	Submit in	valid or inc	omplete U	IRLs and ob	serve error handl	ing.	Invalid in	puts are h	andled with er	ror messages.	Not v	vorking	Fail
5	Analyze n	nultiple UR	Ls to evalu	ate model	performance and	speed.	Model pe	rforms eff	ficiently withou	ıt significant delays	. As ex	pected	Pass

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

5.11 TEST CASE 11: Multi-Browser Compatibility

Test Ca	ise ID	V3_C11		Test case	Description									
Versio	n	Version 3		Validate t	he extension's f	functio	nality, fe	ature con	sistency, an	d perforr	nance acro	ss multiple	browsers	
	g Functionalit			wser Comp	patibility		Tested By		Tanushka		Test Date		15-Jan-25	
Functio	onality Priorit	У	Won't-Ha	ve		F	Reviewed	Ву	Dulaj		Review [Date	15-Jan-25	5
Numbe	er of Scenario	s tested		7										
Numbe	er of Scenario	s Passed		5										
Succes	s Rate %			71%										
S#	Pre- Cond					5	6#	Test Data	1					
1		the require				1	l	-						
2		the require				2	2	-						
3	Install all	the require	ement Libr	aries		3	3	-						
4	Install all	the require	ement Libr	aries		4	1	-						
5	Install all	the require	ement Libr	aries		5	5	-						
6	Install all	the require	ement Libr	aries		6	5	-						
7	Install all	the require	ement Libr	aries		7	7	-						
S#	Scenario(s) and Step	(s)			E	xpected	Results				Actual Re	sults	Status
1	Install an	d test the e	xtension o	on Google (Chrome	E	extension	works se	amlessly on	Chrome.		As expec	ted	Pass
2	Install an	d test the e	xtension o	on Microso	ft Edge.	E	xtension	works se	amlessly on	Edge.		As expec	ted	Pass
3	Install an	d test the e	xtension o	on Brave br	owser.	E	xtension	works se	amlessly on	Brave.		As expec	ted	Pass
4	Install and test the extension on Firefox			E	extension	works se	amlessly on	Firefox.		Not work	ing	Fail		
5	Verify that all core features function consistently in Edge.				e. Features are consistent and functional As expected Pa					Pass				
6	Verify that all core features function consistently in Brave					e. F	eatures a	are consis	tent and fur	nctional		As expec	ted	Pass
7	Verify that all core features function consistently in Fire					ox F	eatures	are consis	tent and fur	nctional		Not work	ing	Fail

Figure 34: TEST CASE 11: Multi-Browser Compatibility

5.12 TEST CASE 12: Sandbox Integration for File Analysis

Test Ca	ase ID	V3_C12		Test case [Description	·						
Versio	n	Version 3		Validate t	he extension's ability	to upload and s	can files fo	r malware us	ing the VirusTota	I API		
Tostin	- Functionalit		Candhay	Integration	for File Analysis	Tostad D		Tharuka	Test Dat		15-Jan-25	
	g Functionalit	•			for File Analysis	Tested B						
Function	onality Priorit	ty	Won't-Ha	ve		Revied B	У	Tanushka	Review	Date	15-Jan-25	
Numb	er of Scenario	s tested		5								
Numb	er of Scenario	s Passed		5								
Succes	s Rate %			100%								
S#	Pre- Cond	dition(s)				S #	Test Data	<u> </u>				
1	Extension	n is installe	d and activ	ve.		1	Valid file	2				
2	-					2	Malicious	s file				
3	-					3	File large	r than 32 MB				
4	-					4	Checking	result with V	'irustotal			
5	-					5	Valid file	S				
S #	Scenario(s) and Step	(s)			Expected	Results			Actual Re	sults	Status
1	Upload a	valid file ar	nd observe	e scan resul	ts.	Valid file	is scanned	d successfully	with no threats.	As ex	pected	Pass
2	Upload a	file contair	ning malwa	are and veri	ify detection.	Malware	file is flag	ged with appr	opriate details.	As ex	pected	Pass
3	Attempt	to upload a	file larger	than the si	ze limit.	Large file	es are rejec	ted with a siz	e limit warning.	As ex	pected	Pass
4	Verify the accuracy of scan results for uploaded files.			oaded files.	Scan resu	ults are acc	urate and det	ailed.	As ex	pected	Pass	
5	Upload m	ultiple file	s sequent	ially and ob	serve performance.	System h	andles mu	ltiple file upl	oads efficiently.	As ex	pected	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

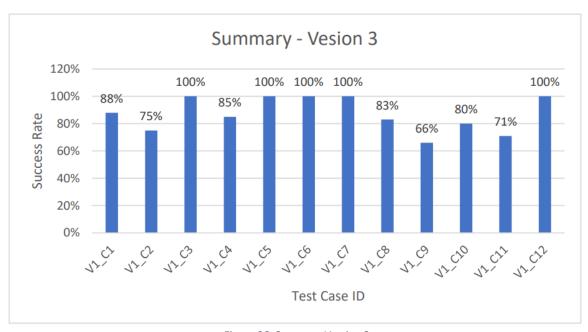


Figure 36: Summary Version 3

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	f the Version teste	d
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.

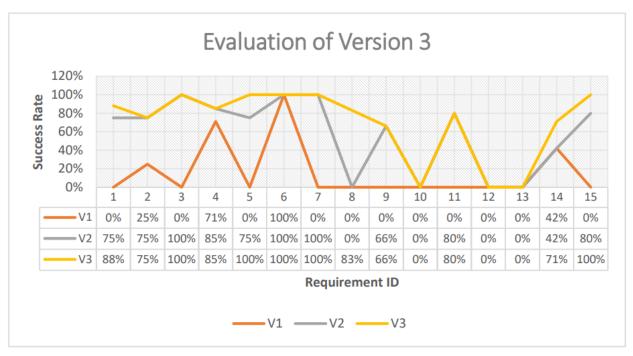


Figure 37: Evaluation of version 3

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:

- o In rare instances, certain redirected URLs were not analyzed correctly.
- o High-browsing loads caused occasional delays in URL monitoring.

• Identified Issues:

- o Incomplete handling of complex URL redirections.
- o 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.
- o False negatives were observed in cases of subtle phishing patterns.

• Identified Issues:

 Current detection algorithms need better coverage for complex phishing techniques.

• Impact:

o 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:

o Interface inconsistencies and enforcement gaps in blacklist rules.

• Impact:

Users may unintentionally access blocked URLs, reducing trust in the feature.

Recommendations:

o Strengthen backend rule enforcement and conduct additional UI testing.

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

• Failed Scenarios:

o Minor layout issues occurred on smaller screen sizes.

• Identified Issues:

o Incomplete tooltips and responsiveness challenges for certain screen resolutions.

• Impact:

o Non-technical users may struggle to navigate or utilize advanced features effectively.

• Recommendations:

o 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:

- o Alerts for moderate severity lacked actionable recommendations.
- o High-severity alerts occasionally failed to display tailored warnings.

Identified Issues:

o Gaps in contextual recommendations for certain threat levels.

• Impact:

o Users may find it difficult to interpret and respond to alerts effectively.

Recommendations:

o Enhance the logic for generating recommendations based on threat severity.

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

• Failed Scenarios:

- o False positives were observed in detecting legitimate URLs as phishing threats.
- o Some rare phishing patterns were not flagged.

• Identified Issues:

o The ML model needs additional refinement for precision and coverage.

• Impact:

o 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 Case	es Tested: 12	
Total Number of Scenario	s 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									
Vers	ion	Version 4		Verify the	extension's ability t	to moi	nitorand al	ert users al	out URLs in real-tir	ne based o	n their saf	ety status.		
		•												
	ing Function			URL Monit	oring		ed By	Sudam	Test Dat		20-Jan-2			
Fund	tionality F	Priority	Must-Hav	e		Revi	ed By	Tanushka	Review	Date	20-Jan-2	5		
Num	hor of Sco	enarios test	od	8										
		narios test		7										
			seu	88%										
Succ	ess Rate %	0		88%										
S#	Pre- Cond	dition(s)				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/								
1		n is installe	d and runn	ing.		1	1							
2	VirusTota	al flagged	URLs need	led		2								
3	-					3	Visit https://www.youtube.com multiple times							
4	-					4	https://w	ww.espncr	icinfo.com/					
5	-					5	https://sy	yrianmalwa	re.com/					
6	The URL	should be	blackliste	d.		6	https://w	ww.cricbuz	z.com/					
7	-					7	http://we	eb.simmons	.edu/~grovesd/cor	nm244/not	es/week2	/links		
8	-					8	Security F	Report						
S#	Scenario(s) and Step	o(s)			Expe	cted Resu	lts		Actual Re	sults	Status		
1					is feedback.	_		zed and mai		As ex	pected	Pass		
2				by VirusT	otal.	_		ed URLs are		As ex	pected	Pass		
3	Simulate reaching API call rate limits								ser of API issues.	As ex	pected	Pass		
4	Browse URLs and observe if real-time feedback is prompt					_			out delays.		pected	Pass		
5		otifications				_			for malicious URLs		pected	Pass		
6					g or blocking.	-		isted sites		As ex	pected	Pass		
7			•		TP and HTTPS.	_	is flagged			+	vorking	Fail		
8	Monitor i	f user data	or sensitiv	e informati	ion is being logged	No u	ser data is	stored out	side the scope.	As ex	pected	Pass		

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

6.2 TEST CASE 2: Phishing URL Detection

Test Ca	se ID	V4_C2		Test case I	Description	n								
Version	n	Version 4			•		o detect ar	nd classify	URLs as saf	e, or mal	icious, and	provide u	ser alerts.	
Testing	Functionali	ty	Phishing	URL Detec	tion		Tested By	,	Tanushka		Test Date	20-Jan-25		<u> </u>
	nality Priori	•	Must-Hav				Revied By		Sudam		Review D	ate	20-Jan-25	
Numbe	er of Scenario	os tested		4										
	er of Scenarions	4 100%												
3ucces:	s nate 70			100%										
S#	Pre- Condition(s)					S#	Test Data							
1	Extensio	n is installe	d and activ	e.			1	https://w	/ww.youtul	oe.com/				
2	VirusTot	tal flagged	URL need	ed			2	https://syrianmalware.com/						
3	-						3	hts:/stud	entportal.e	cu.edu.a	u/s/			
4	-						4	Visit http	s://www.y	outube.co	om multiple	e times		
S#	Scenario	(s) and Step	o(s)				Expected	Results				Actual Re	sults	Status
1	L Submit safe URLs and observe analysis results.				URLs are r	marked as	safe.			As ex	pected	Pass		
2	Submit known malicious URLs flagged by VirusTotal.				Malicious URLs are flagged with warnings. As expected Pass					Pass				
3	Submit invalid or incomplete URLs for analysis.					Invalid URLs are rejected with user feedback. As expected Pass						Pass		
4	Simulate VirusTotal API unavailability or timeout.						Fallback mechanism informs users of API issues. As expected Pass						Pass	

Figure 39: TEST CASE 2: Phishing URL Detection

6.3 TEST CASE 3: Basic User Alerts

Test Ca	se ID	V4_C3		Test case Description	on							
Version	n	Version 4		Validate the extens	sion's ability to di	splay real-t	time alerts for	malicious	and suspic	ious URLs		
_	g Functiona		Basic Use		Teste		Tharuka		Test Date		20-Jan-2	
Functio	onality Prio	rity	Must-Hav	ve	Revie	d By	Sudam		Review D	ate	20-Jan-2	5
Numbe	er of Scenar	ios tested		3								
Numbe	er of Scenar	ios Passed		3								
Succes	s Rate %			100%								
S#	Pre- Co	ndition(s)			S#	Test [Data					
1	Extensi	on is installe	d and acti	ve	1	https	://syrianmalw	are.com/				
2	URL m	ust be in Bla	acklist		2	https	://www.espno	ricinfo.co	m/			
3	URL mu	ıst be in Whi	telist		3	https	://www.youtu	be.com/				
S#	Scenario	o(s) and Step	n(s)		Fxner	ted Result	ts			Actual Re	sults	Status
1				o trigger an alert.			lert is displaye	d.			pected	pass
2	Visit a Blacklisted site									pass		
3	Visit a Whitelisted site			Alert	is displaye	ed.			As ex	pected	pass	

Figure 40: TEST CASE 3: Basic User Alerts

6.4 TEST CASE 4: Whitelist/Blacklist Management

Test Cas	e ID	V4_C4		Test case	Description										
Version		Version 4		Validate t	he extension's a	ability to	manage U	RLs							
Testing	unctionalit	у	Whitelist,	/Blacklist N	lanagement		Tested By	,	Dulaj	Test Da	te	20-Jan-25	j		
Function	Version 4 Validate the extension of Scenarios tested rof Scenarios Passed 7 Rate % 100% Pre- Condition(s)						Revied By	1	Tanushka	Review	Date	20-Jan-25	5		
				_											
		s Passed		/											
Success	Rate %			100%											
S#	Pre- Conc	lition(s)					S#	Test Data							
3 π 1	-	artion(s)					1		ww.youtube	com/					
2	1-						2		https://syrianmalware.com/						
2		-					2	- IIII	ymammanware	:.com/					
4	-						4	-							
5	- https://syrianmalware.com/ in Blacklist						5	https://sv	tps://syrianmalware.com/						
6	-	, ridiiiiidiwa	reroomy n	Bidditist			6		hps://www.youtube.com/						
7	-						7	-	wyoutubere	o,					
S#	Scenario(s) and Step	(s)				Expected	Results			Actual Re	esults	Status		
1	Add a trus	sted websit	te to the w	hitelist.			Website i	s successf	ully added to	the whitelist.	As ex	xpected	Pass		
2	Add a malicious website to the blacklist.						Website i	s successf	ully added to	the blacklist.	As ex	xpected	Pass		
3	Remove a website from the whitelist.					Website i	s removed	from the wh	itelist.	As ex	xpected	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.						Blackliste	d website	access is bloo	ked.	As ex	xpected	Pass		
6	Attempt to add invalid URLs to whitelist/blacklist.						Invalid er	tries are r	ejected with	feedback.	As ex	xpected	Pass		
7	Restart the browser and verify whitelist/blacklist persis					ence.	List chang	es are sav	ed and persis	t after a restart.	As ex	xpected	Pass		

Figure 41: TEST CASE 4: Whitelist/Blacklist Management

6.5 TEST CASE 5: Basic Malware Detection

Test Cas	e ID	V4_C5		Test case	Descriptio	n								
Version		Version 4		Verify the	extension	n's ability t	o detect m	nalware th	reats in UR	Ls using th	ne VirusTot	al API and	provide al	erts.
Testing	Functionalit	V	Basic Mal	ware Detec	ction		Tested By	,	Sudam		Test Date		20-Jan-25	<u> </u>
	nality Priorit		Must-Hav				Revied By		Tanushka		Review D	ate	20-Jan-25	
Number	of Scenario	s tested		4										
Number	of Scenario	s Passed		4										
Success	ess Rate % Pre- Condition(s)			100%										
S#	Pre- Cond	dition(s)					S#	Test Data						
1	Extension	is installe	d and activ	e.			1	https://w	/ww.youtul	be.com/				
2	-						2	https://s	yrianmalw	are.com/				
3	-						3	hps://ww	vw.youtube	e.com/				
4	-						4	Visit http	s://www.y	outube.co	m/ multipl	e times		
S#	Scenario(s) and Step	(s)				Expected	Results				Actual Re	sults	Status
1	Submit a known safe URL for analysis.				Safe URL i	is marked a	as safe with	no alerts		As ex	pected	Pass		
2	Submit a known malware-infected URL flagged by VirusTo			/irusTotal.	Malware I	URL is flag	ged with ar	appropri	ate alert.	As ex	pected	Pass		
3	Submit an invalid or malformed URL for analysis.				Invalid URLs are rejected with an error message. As expected Pass					Pass				
4	Simulate	API timeo	ut and che	ck system l	ehavior.		Graceful f	allback me	essage for A	API failure	displayed.	As ex	pected	Pass

Figure 42: TEST CASE 5: Basic Malware Detection

6.6 TEST CASE 6: Email Phishing Detection

Test Cas	o ID	VA CE		Tost caso	Description	n							
	e 10	V4_C6			<u> </u>								
Version		Version 4		Validate t	he extensi	on's abilit	y to analyz	e email co	ntent or hea	ders, detect phish	ing indicate	ors	
			- 151	1. 5.									
	Functionalit	-	Email Phi	shing Dete	ction		Tested By		Dulaj	Test Date	2	20-Jan-25)
Function	ality Priorit	у	Must-Hav	e			Reviewed	Ву	Tanushka	Review [Date	20-Jan-25	5
Number	of Scenario	s tested		4									
Number	of Scenario	s Passed		4									
Success	ess Rate %			100%									
S#	Pre- Cond	lition(s)					S#	Test Data	ì				
1	Extension	is installe	d and activ	e.			1	Legitimat	te email data	1			
2	phishing	email sam	ples are a	vailable.			2 phishing email data						
3	-						3	-					
4	-						4	Legitimat	te email data	1			
S#	Scenario(s) and Step	(s)				Expected	Results			Actual Re	sults	Status
1	Paste content of a legitimate email and analyze.				Safe ema	il content	is analyzed a	nd marked as safe	. As ex	pected	Pass		
2	Paste content of a known phishing email for analysis.			s.	Phishing email content is flagged . As expected Pass					Pass			
3	Submit invalid or empty email content for analysis.					Invalid in	puts are re	ejected with	an error message.	As ex	pected	Pass	
4	Analyze a lengthy email with multiple components.					System ha	andles larg	ge emails wit	thout issues.	As ex	pected	Pass	

Figure 43: TEST CASE 6: Email Phishing Detection

6.7 TEST CASE 7: Browser Notifications

Test Ca	se ID	V4_C7		Test case	Description								
Version	1	Version 4		Validate t	he extension's abilit	y to send o	ategorized	d browser not	tification	s with sev	erity level	s	
Testing	Functionalit	у	Browser N	Votification	ıs	Tested By	1	Sudam		Test Date		20-Jan-25)
Functio	nality Priorit	у	Must-Hav	e		Revied By	/	Tanushka		Review D	ate	20-Jan-25	1
Numbe	r of Scenario	s tested		5									
	r of Scenario			5									
Success	Rate %			100%									
S#	Pre- Cond	lition(s)				S#	Test Data	1					
1	Extension	is installe	d and activ	e.		1	https://w	ww.youtube	.com/				
2	-					2	https://s	yrianmalware	e.com/				
3	-					3	-						
4	-					4	-						
5	-					5	-						
S#	Scenario(s) and Step	(s)			Expected	Results				Actual Re	sults	Status
1	Visit a saf	e URL to tri	gger a not	ification.		Notificati	on indicat	es the URL is	safe.		As ex	pected	Pass
2	Visit a ma	licious URL	to trigger	a notificat	ion.	Notificati	on clearly	warns about	the mali	cious URL.	As ex	pected	Pass
3	Verify the notification is displayed promptly.			otly.	Notifications appear without noticeable delays. As expected Par					Pass			
4	Dismiss a notification manually.				Dismissed notifications are removed properly. As expected Pass							Pass	
5	Verify notifications have consistent design.				ŗn.	Notificati	ons maint	ain consisten	t style ar	d icons.	As ex	pected	Pass

Figure 44: TEST CASE 7: Browser Notifications

6.8 TEST CASE 8: User-Friendly Interface

Test Ca	ase ID	V4 C8		Test case I	Description	1				<u> </u>				
Versio	n	Version 4		Validate the extension's user interface for clarity, accessibility, and responsiveness										
										·				
Testing	Testing Functionality User-Friendly			ndly Interfa	ace		Tested By		Tanushka	Test Date	20-Jan-25		;	
Function	onality Priori	ty	Must-Hav	e			Revied By		Dulaj	Review D	ite 20-Jan-25		j	
Numbe	er of Scenario	os tested		6										
Numbe	er of Scenario	os Passed		5										
Succes	s Rate %			83%										
S#	Pre- Con	dition(s)					S#	Test Data	1					
1	-						1	-						
2	-						2	-						
3	-						3 -							
4	-						4 -							
5	-						5	-						
6	-						6	-						
S#	Scenario	(s) and Step	(s)				Expected	Results			Actual Res	sults	Status	
1		er a button					Tooltips a	are display	ed when hov	ering over features	As exp	pected	Pass	
2		ooltips for	<u> </u>			ure.			oncise, and re		As exp	pected	Pass	
3		dark mode					Dark mode is enabled successfully.				As expected Pass		Pass	
4	_	Restart the browser and verify dark mode preference persists					Dark mode preference persists across sessions.				As expected Pass		Pass	
5	_	Enter data in fields and clear them using the clear button.					Fields are cleared successfully using the button As expected				pected	Pass		
6	Resize th	e browser	window an	d observe	layout adap	otability.	Interface adapts responsively to various screen size Not working Fai					Fail		

Figure 45: TEST CASE 8: User-Friendly Interface

6.9 TEST CASE 9: Severity-Based Alerts

Test Ca	se ID V4_C9 Test case Description													
Version 4			Validate the extension's ability to provide severity-based alerts and recommended actions for users.											
Testing	Testing Functionality Severity-		Severity-l	Based Aler	ts	Teste	d By	1	Tharuka		Test Date	20-Jan-25		i
Functio	Functionality Priority Should		Should-H	ave		Revie	d By	/	Tanushka		Review D	ate 20-Jan-25		i
Numbe	Number of Scenarios tested 3													
Numbe	Number of Scenarios Passed 2													
Success	Rate %			66%										
S#	Pre- Cond	lition(s)				S#	S # Test Data							
1	Extension	is installe	d and activ	re.		1		https://www.youtube.com/						
2	-					2		https://syrianmalware.com/						
3	-					3		-						
S #	Scenario(s) and Step	o(s)			Expe	Expected Results					Actual Re	sults	Status
1	Visit a UR	Visit a URL flagged as safe					Alert is displayed					As Expected		Pass
2	Visit a URL flagged as Malicious					Alert	Alert is displayed					As Expected		Pass
3	Review the alert for suggested actions based on severity.					ty. Alert	Alerts include recommended actions for users. Not					Not v	vorking	Fail

Figure 46: TEST CASE 9: Severity-Based Alerts

6.10 TEST CASE 10: Advanced Machine Learning for Phishing Detection

Test Ca	se ID	V4_C10		Test case [Description									
Version	n	Version 4		Validate t	he extension's a	bility to de	tect phish	ing patter	ns using a pr	e-traine	d ML model			
Testing	Testing Functionality Advanced ML for Phishing Detection		Tested By		Dulaj		Test Date	20-Jan-25						
Functio	nality Priorit	у	Could-Hav	/e			Revied By	1	Tanushka		Review Date		20-Jan-25	
				_										
	Number of Scenarios tested 5													
	er of Scenario	s Passed		5										
Succes	s Rate %	1		100%										
S#	Pre- Cond	lition(s)					S #	Test Data						
3#		is installe	d and activ	_			3#				nd between / /enum	ian maluus		
1	Extension	i is installe	u anu activ	e.			1				nd https://syr		e.com/	
2	-						2 http://freesd1.000webhostapp.com/Star.html							
3	-						3	http://thelmachan.com.br/images/banners/a607b0c8e7c98759bb45e8a5b1						
4	-						4	ht://you'						
5	-		I				5	Using 5 le	gitimate an	d 5 phish	ing URLs			
S#		s) and Step					Expected Results					Actual Re	sults	Status
1	Submit le	gitimate U	RLs for ana	lysis and o	bserve predictio	ns.	Legitimat	e URLs are	correctly id	entified	as safe.	As ex	pected	Pass
2	Submit kr	nown phish	ing URLs a	nd verify d	etection results.		Phishing URLs are flagged accurately.					As expected		Pass
3	Submit U	Submit URLs with suspicious patterns and evaluate predictions.					Suspicious URLs are flagged appropriately.				As expected		Pass	
4	Submit in	Submit invalid or incomplete URLs and observe error handling.					Invalid inputs are handled with error messages.				As expected P		Pass	
5	Analyze n	Analyze multiple URLs to evaluate model performance and speed.					Model performs efficiently without significant delays. As expected Pass						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 I	Description		<u>'</u>				<u> </u>			
Version		Version 4		Validate t	he extensio	n's functi	ionality, fe	ature con	sistency, an	d perforn	nance acros	s multiple	browsers	
Testing F	unctionalit	V	Multi-Bro	wser Comp	atibility		Tested By		Tanushka		Test Date		20-Jan-25	5
	ality Priorit		Won't-Ha		,		Reviewed		Dulaj		Review D	ate	20-Jan-25	
Number	of Scenario	s tested		7										
Number	of Scenario	s Passed		5										
Success R	Rate %			71%										
S#	Pre- Cond	lition(s)					S#	Test Data						
1	Install all	the require	ement Libr	aries			1	-						
2	Install all	the require	ement Libr	aries			2	-						
3	Install all	the require	ement Libr	aries			3	-						
4	Install all	the require	ement Libr	aries			4 -							
5	Install all	the require	ement Libr	aries			5 -							
6	Install all	the require	ement Libr	aries			6 -							
7	Install all	the require	ement Libr	aries			7	-						
S#	Scenario(s) and Step	(s)				Expected	Results				Actual Re	sults	Status
1	Install and	d test the e	xtension o	n Google (Chrome		Extension	works sea	amlessly on	Chrome.		As expect	ted	Pass
2	Install and	d test the e	xtension o	n Microsof	ft Edge.		Extension	works sea	amlessly on	Edge.		As expect	ted	Pass
3	Install and	d test the e	xtension o	n Brave br	owser.		Extension works seamlessly on Brave. As					As expect	ted	Pass
4	Install and	d test the e	xtension o	n Firefox			Extension works seamlessly on Firefox. Not work					Not work	ing	Fail
5	Verify tha	t all core f	eatures fui	nction cons	istently in E	dge.	Features are consistent and functional As expected					ted	Pass	
6	Verify tha	t all core f	eatures fui	nction cons	istently in B	Brave.	Features are consistent and functional As expected					ted	Pass	
7	Verify tha	t all core f	eatures fui	nction cons	istently in F	irefox	Features are consistent and functional Not working Fa					Fail		

Figure 48: TEST CASE 11: Multi-Browser Compatibility

6.12 TEST CASE 12: Sandbox Integration for File Analysis

Test Cas	ie ID	V4_C12		Test case [Description									
Version 4			Validate the extension's ability to upload and scan files for malware using the VirusTotal API											
	Functionalit				for File Analysis	Tested B	<u> </u>	Tharuka	Test Date	20-Jan-25				
Functio	nality Priorit	У	Won't-Ha	ve		Revied B	У	Tanushka	Review D	ate	20-Jan-25	i 		
Numbe	r of Scenario	s tested		5										
Numbe	r of Scenario	s Passed		5										
Success	Success Rate % 100%													
S#	Pre- Cond					S #	Test Data	ı						
1	Extension	is installe	d and activ	e.		1	Valid file	2						
2	-					2	Malicious file							
3	-					3	File larger than 32 MB							
4	-					4	Checking result with Virustotal							
5	-					5	Valid files							
S#	Scenario(s) and Step	(s)			Expected	Expected Results Actual Results Status							
1	Upload a	valid file ar	nd observe	scan result	ts.	Valid file	is scanned	d successfully v	vith no threats.	As ex	pected	Pass		
2	Upload a	file contain	ing malwa	re and veri	fy detection.	Malware	file is flag	ged with appro	priate details.	As ex	pected	Pass		
3				than the si		Large file	Large files are rejected with a size limit warning. As expected Pass							
4	Verify the	Verify the accuracy of scan results for uploaded files.					Scan results are accurate and detailed. As expected Pas					Pass		
5	Upload multiple files sequentially and observe performance.					System h	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

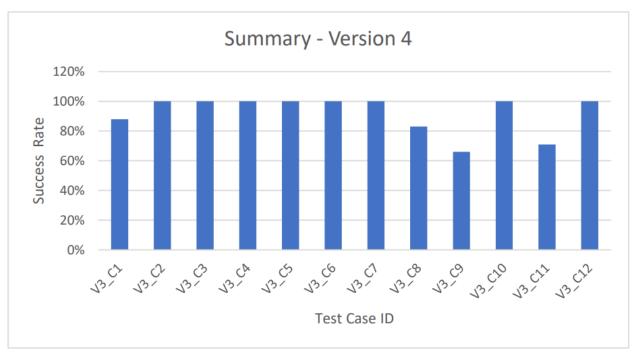


Figure 50: Summary Version 4

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.

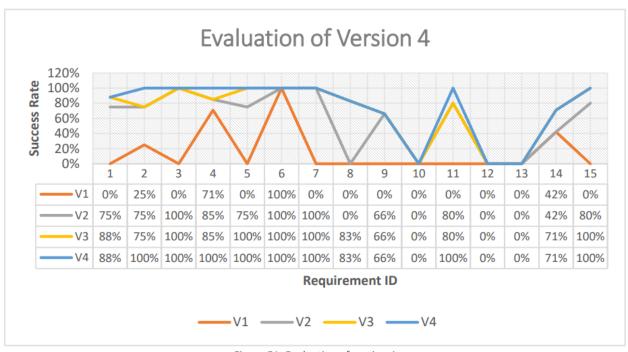


Figure 51: Evaluation of version 4

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:

- o 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:

o 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:

o 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:

- o Some tooltips remained unclear or were missing for advanced features.
- o Minor layout issues persisted on smaller screen sizes.

• Identified Issues:

 Incomplete tooltip implementation and responsiveness challenges for mobile or reduced resolutions.

• Impact:

o 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:

- o Certain complex redirected URLs were not analyzed correctly.
- o Occasional performance delays during high-browsing loads.

• Identified Issues:

o Incomplete handling of nested redirections and optimization gaps for heavy browsing activity.

• Impact:

o Users may experience missed alerts or delayed threat detection.

• Recommendations:

o 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.