Scam Buster Application & Extension - Testing Report

Project Overview

Project Name: Scam Buster Application and Browser Extension
Domain: Cyber Security
Duration: 1 Months (4 weeks)
Role: Test Engineer
Objective: To validate the functionality, accuracy, and reliability of a cyber security tool designed to protect users from fraudulent websites and phishing attempts

Application Overview

Scam Buster is a browser extension with an accompanying application designed to protect users from malicious websites, phishing attacks, and scam messages. The tool provides real-time threat analysis and assigns risk scores to websites based on multiple security parameters.

Key Features:

- Real-time website threat assessment
- Risk score calculation (0-100 scale)
- Phishing and scam detection
- User account management

- Free trial model with 5 complimentary scans

Application Workflow

1. **Installation Phase:** User downloads and installs the browser extension from the official store
2. **Free Trial Access:** Upon installation, users receive 5 free threat assessments without account creation
3. **Account Creation:** After exhausting free trials, users must create an account to continue using the service
4. **Unlimited Access:** Registered users gain unlimited access to all security features
5. **Active Protection:** The extension actively monitors and alerts users about potentially dangerous websites and suspicious messages

Testing Approach & Methodology

Test Strategy:

I employed a combination of **functional testing**, **usability testing**, and **exploratory testing** to ensure comprehensive coverage of the application's critical features.

Testing Phases:

Phase 1: Free Trial Testing (Week 1-2)

- Validated the 5-scan limitation mechanism
- Tested threat detection accuracy using known malicious and legitimate websites
- Evaluated user experience during the trial period
- Verified scoring algorithm consistency

Phase 2: Account Management Testing (Week 3-4)

- Tested registration flow with multiple email providers (Gmail, Outlook, Yahoo)
- Validated authentication mechanisms
- Tested session management and token handling
- Verified the transition from trial to registered user

Phase 3: Core Functionality Testing (Week 5-6)

- Conducted extensive testing with various website categories (e-commerce, banking, social media, phishing sites)
- Validated threat detection accuracy across different threat levels
- Tested edge cases and boundary conditions
- Performance testing under various network conditions

Phase 4: Regression & Integration Testing (Week 7-8)

- Retested all critical functionalities after bug fixes
- Validated integration with different browsers (Chrome, Firefox, Edge)

- Cross-platform compatibility testing
- Final user acceptance scenarios

Test Environment

Browsers Tested: Chrome (v120+), Firefox (v118+), Edge (v119+)
Operating Systems: Windows 10/11, macOS Ventura, Ubuntu 22.04
Network Conditions: High-speed broadband, 4G mobile, Throttled connections
Test Websites: 50+ legitimate sites, 30+ known phishing/scam sites from public databases

Defects Identified

Defect #1: Connectivity Error for Accessible Websites

Severity: High
Priority: P1
Category: Functional Defect

Description:
The extension incorrectly displayed "Site could not be accessible" error messages for legitimate, fully operational websites during threat assessment.

Steps to Reproduce:

1. Install Scam Buster extension
2. Navigate to known legitimate websites (tested with amazon.com, wikipedia.org, github.com)
3. Trigger security scan
4. Observe error message

Expected Result: Extension should successfully scan the website and provide an accurate risk score

Actual Result: Error message displayed: "Site could not be accessible" despite websites being fully operational

Impact: This defect undermines user trust and renders the tool unreliable for legitimate browsing activities. Users may abandon the product due to false connectivity errors.

Root Cause Analysis: Potential issues with DNS resolution, timeout configurations, or network request handling in the extension's backend API calls

Defect #2: Inaccurate High Score for Known Malicious Websites

Severity: Critical
Priority: P2
Category: Security/Algorithm Defect

Description:
The extension assigned high safety scores (approximately

90/100) to verified phishing and scam websites, indicating them as "safe" when they should be flagged as dangerous.

Steps to Reproduce:

1. Navigate to known phishing sites from PhishTank database
2. Activate Scam Buster scan
3. Review the assigned risk score
4. Compare with actual threat level

Expected Result: Known malicious sites should receive low scores (0-30 range) with clear warning indicators

Actual Result: Malicious websites received scores around 90/100, suggesting they are safe for users

Impact: This is a critical security flaw that defeats the primary purpose of the application. Users relying on this tool may fall victim to scams, leading to financial loss, data theft, and severe reputation damage for the product.

Examples Tested:

- Fake banking login pages: Score 88-92
- Cryptocurrency phishing sites: Score 85-90
- E-commerce scam sites: Score 87-93

Recommendation: Immediate review of the threat detection algorithm, integration with updated threat intelligence databases, and implementation of multi-layered verification mechanisms

Defect #3: Zero Score Assignment for Legitimate Websites

Severity: Minor
Priority: P1
Category: Functional/Algorithm Defect

Description:
Certain legitimate and trusted websites received a risk score of 0/100, which should theoretically indicate maximum safety but was displayed without any contextual information, causing user confusion.

Steps to Reproduce:

1. Navigate to well-established websites (tested with government domains, educational institutions)
2. Run security assessment
3. Observe score of 0 displayed

Expected Result: Legitimate websites should receive high safety scores (80-100) with clear "Safe" or "Trusted" indicators

Actual Result: Score displayed as 0 with no contextual messaging, leading to ambiguity about whether this means "safest possible" or "no data available"

Impact: Users may misinterpret a score of 0 as indicating either no threat assessment was performed or that the site is extremely dangerous. This creates confusion and reduces confidence in the product.

Additional Observations:

- No distinction between "score 0 = safest" vs "score 0 = error/no data"
- Missing visual indicators (color coding, icons) to clarify the meaning
- Inconsistent scoring methodology across different website categories

Recommendation: Implement clear UI/UX indicators, adopt industry-standard scoring conventions (higher score = safer), and add contextual tooltips explaining score meanings

Defect #4: Account Creation Failure with Gmail Authentication

Severity: Major
Priority: P0
Category: Authentication/Integration Defect

Description:
Users are unable to create accounts using Gmail authentication despite successful OAuth connection, preventing access to unlimited features after free trial expiration.

Steps to Reproduce:

1. Exhaust all 5 free trial scans
2. Click on "Create Account" or "Sign Up"
3. Select "Sign in with Google" option
4. Complete Gmail authentication flow
5. Grant requested permissions
6. Observe account creation failure

Expected Result: Account should be created successfully, and user should be redirected to the dashboard with unlimited access

Actual Result:

- Authentication appears successful
- User is returned to the application
- Error message displayed: "Unable to create account" or generic failure message
- No account is created in the backend system
- User remains locked out after free trials