Client Side Testing

1. Introduction

Client-side testing focuses on vulnerabilities that can be exploited in the user's browser. These vulnerabilities often arise from the improper handling of user-supplied input in the client-side code, and can lead to attacks such as Cross-Site Scripting (XSS), clickjacking, and the manipulation of client-side resources. This testing category covers a wide range of client-side vulnerabilities, including DOM-based XSS, JavaScript execution, HTML injection, and more.

2. CVSS Score Summary

Test Case	Vulnerability	CVSS v3.1 Score	CVSS Vector	Severity
OTG-CLIENT-001	DOM-based Cross-Site Scripting	6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	Medium
OTG-CLIENT-002	JavaScript Execution	6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	Medium
OTG-CLIENT-003	HTML Injection	6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	Medium
OTG-CLIENT-004	Client-Side URL Redirect	5.4	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N	Medium
OTG-CLIENT-005	CSS Injection	0.0	N/A	Informational
OTG-CLIENT-006	Client Side Resource Manipulation	0.0	N/A	Informational

OTG-CLIENT-007	Cross Origin Resource Sharing (CORS)	0.0	N/A	Informational
OTG-CLIENT-008	Cross Site Flashing	0.0	N/A	Informational
OTG-CLIENT-009	Clickjacking	6.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	Medium
OTG-CLIENT-010	WebSocket Testing	0.0	N/A	Informational
OTG-CLIENT-011	Web Messaging Testing	0.0	N/A	Informational
OTG-CLIENT-012	Client-Side Storage Testing	0.0	N/A	Informational

3. Summary of Findings

The most significant finding in this category is the presence of multiple client-side injection vulnerabilities. The application is vulnerable to DOM-based XSS, JavaScript execution, and HTML injection, all of which could be used to execute malicious code in the user's browser. Additionally, the application is vulnerable to clickjacking, which could be used to trick users into performing unintended actions.

A key challenge in this testing category was the lack of a dedicated client-side testing page. This made it difficult to test for certain vulnerabilities, such as those related to Web Messaging and Local Storage. While the tests that were performed revealed several significant vulnerabilities, the inability to fully assess the application's client-side security leaves a potential gap in the assessment. It is recommended that a dedicated client-side testing page be created to allow for a more thorough evaluation of the application's client-side security.