Business Logic Testing

1. Introduction

Business logic testing focuses on identifying flaws in the application's intended workflow and business rules. These vulnerabilities are often unique to the application and its specific domain, and can be difficult to detect with automated scanners. This testing category covers a wide range of business logic flaws, including data validation issues, the ability to forge requests, and the circumvention of workflows.

2. CVSS Score Summary

Test Case	Vulnerability	CVSS v3.1 Score	CVSS Vector	Severity
OTG-BUSLOGIC-001	Business Logic Data Validation	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	Medium
OTG-BUSLOGIC-002	Ability to Forge Requests	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	High
OTG-BUSLOGIC-003	Integrity Checks	8.8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	High
OTG-BUSLOGIC-004	Process Timing	5.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	Medium
OTG-BUSLOGIC-005	Function Usage Limits	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High
OTG-BUSLOGIC-006	Circumvention of Workflows	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	Medium
OTG-BUSLOGIC-007	Defenses Against	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	High

	Application Mis-use			
OTG-BUSLOGIC-008	Upload of Unexpected File Types	0.0	N/A	Informational
OTG-BUSLOGIC-009	Upload of Malicious Files	0.0	N/A	Informational

3. Summary of Findings

The most significant finding in this category is the application's susceptibility to business logic data validation flaws. The application fails to properly validate user input, allowing for the submission of invalid data, such as negative prices and zero quantities. Additionally, the application is vulnerable to request forgery, allowing an attacker to enable debug and other hidden parameters. The application also fails to properly enforce integrity checks, allowing for the modification of hidden fields and the potential for privilege escalation.

A key challenge in this testing category was the lack of a clear understanding of the application's intended business logic. This made it difficult to determine whether certain behaviors were intentional or the result of a vulnerability. The tests for process timing also revealed a significant difference in response times for valid and invalid SQL queries, which could be used to infer the validity of a query. The test for circumventing workflows also revealed that it is possible to set the security level to an invalid value, which could have unintended consequences.