# Business Logic Vulnerabilities

Flaws in the application's flow or logic that allow attackers to bypass intended behaviors (e.g., order manipulation, discount abuse).

## Example:

| Scenario | Description |
| --- | --- |
| Discount Abuse | Apply a coupon multiple times using API calls, even after it’s marked used in UI |
| Race Condition | Submitting two requests simultaneously to transfer double the amount |
| Order Manipulation | Change item prices or order total in intercepted request |
| Authorization Bypass | Cancelling a payment request after download link is triggered |
| Cart Tampering | Modify shipping price, quantity, or SKU in cart APIs |

## Impact

| Type | Impact |
| --- | --- |
| Financial Loss | Free products, refunds, coupon abuse |
| Service Abuse | Bypass payment, upload limits, rate limits |
| Reputation Damage | Business rule broken = user trust lost |
| Compliance Risk | Can lead to logic-based data leakage |

## Common Types of Business Logic Flaws

**Race Conditions**

* **Definition: Exploiting timing gaps between concurrent requests.**
* **Example: Submitting two payment requests simultaneously → double credit.**
* **Mitigation: Lock user actions server-side, atomic operations.**

**2. Parameter Manipulation**

* **Definition: Altering client-side input to change business flow.**
* **Example: Changing item price in intercepted request.**
* **Mitigation: Validate server-side values; never trust client input.**

**3. Replay Attacks**

* **Definition: Resending a legitimate request to re-trigger an action.**
* **Example: Reuse password reset token multiple times.**
* **Mitigation: Use one-time tokens, timestamps, and session validation.**

**4. Workflow Bypass**

* **Definition: Skipping mandatory steps in a process.**
* **Example: Accessing confirmation page directly before payment step.**
* **Mitigation: Use server-side step-tracking and session state validation.**

**5. Abuse of Business Rules**

* **Definition: Using features against their intended business purpose.**
* **Example: Combining referral coupons in ways not allowed.**
* **Mitigation: Model abuse scenarios during design phase; implement abuse detection systems.**

# How Attackers Exploit BLVs

| Method | Tool | Description |
| --- | --- | --- |
| Modify API calls | Burp Suite / Postman | Tamper parameters or flow |
| Trigger race conditions | Turbo Intruder (Burp Plugin), curl script | Send concurrent requests |
| Replay requests | Repeater / Proxy | Re-use old tokens |
| Bypass UI controls | Manual inspection | Direct access to hidden routes |
| Use business logic fuzzing | Custom scripts | Try all coupon combos, cart scenarios |

# Mitigation:

| Area | Control |
| --- | --- |
| Server-Side Validation | Don’t trust frontend or APIs for pricing, workflow, etc. |
| Secure State Management | Enforce user step progression (e.g., can’t go to step 3 before 2) |
| Rate Limiting + Locking | Prevent race abuse and bulk actions |
| Transaction Integrity | Use atomic transactions (DB-level) |
| Monitoring for Abuse | Alert on unusual patterns (e.g., too many discounts) |
| Secure Business Rule Modeling | Perform abuse-case testing like threat modeling for logic |

# Tools for Business Logic Testing

| Tool | Use |
| --- | --- |
| Burp Suite (Manual) | Intercept and tamper requests |
| Turbo Intruder | Simulate race conditions and logic abuse |
| Postman | Replay and sequence API calls |
| Custom Python Scripts | Test discount logic, cart abuse, API testing |
| Manual Testing | Crucial for discovering logic flaws |

# Points

“Business Logic Vulnerabilities require **manual analysis, attacker mindset**, and deep understanding of the app's workflows.”

“They’re **missed by automated scanners** like Burp or ZAP — human review is essential.”

“Enforce **business abuse testing** in VAPT methodology for e-commerce, banking, and SaaS platforms.”

# Real-World Examples

| Company | Issue |
| --- | --- |
| Shopify | Coupon stacking via API replay |
| Uber (Bug Bounty) | Trip price manipulation by switching destinations |
| Apple Pay (2017) | Reuse of transaction tokens led to free purchases |