Business Logic Vulnerabilities Testing Checklist & Methodology

Eyad Islam El-Taher

February 8, 2026

Testing Methodology Overview

Phase 1: Application Mapping & Business Rule Analysis

Understanding Application Logic

1. **Identify Core Business Functions**
   - User registration and authentication workflows
   - Payment and transaction processing
   - Order management and shopping carts
   - Administrative functions and access controls
   - File upload and data processing
2. **Map User Workflows**
   - Document multi-step processes
   - Identify state transitions
   - Map parameter dependencies
   - Note validation points
3. **Analyze Business Rules**
   - Domain restrictions and validations
   - Pricing and discount logic
   - Access control requirements
   - Workflow constraints

Phase 2: Input Validation & Parameter Testing

Parameter Manipulation Checklist

1. **Numeric Parameter Testing**
   - Test negative values (e.g., -1, -1000)
   - Test zero values (0)
   - Test extremely large values (999999999)
   - Test decimal values (0.01, 100.99)
   - Test boundary conditions (min-1, max+1)
2. **String Parameter Testing**
   - Test empty strings
   - Test very long strings (10,000+ characters)
   - Test special characters (@, #, $, %, etc.)
   - Test Unicode and encoded characters
   - Test control characters
3. **Parameter Removal Testing**
   - Remove required parameters one at a time
   - Delete parameter names (not just values)
   - Test both URL and POST parameters
   - Include cookie parameter testing
4. **Type Confusion Testing**
   - Strings where numbers expected
   - Arrays where strings expected
   - Boolean values in non-boolean fields
   - Null values in required fields

Phase 3: Workflow & Sequence Testing

Workflow Bypass Testing

1. **Step Skipping**
   - Access step N+1 without completing step N
   - Bypass authentication steps
   - Skip payment steps
   - Circumvent verification steps
2. **Step Repetition**
   - Repeat the same step multiple times
   - Test for duplicate processing
   - Check for idempotency violations
3. **Step Reversal**
   - Return to earlier steps after completion
   - Test state consistency
   - Check parameter persistence
4. **Direct Endpoint Access**
   - Access protected endpoints directly via URL
   - Test authentication bypass via direct URLs
   - Check if workflow state is validated
5. **Parallel Process Testing**
   - Run multiple workflows simultaneously
   - Test race conditions
   - Check for concurrency issues

Phase 4: Business Rule Exploitation

Business Logic Testing

1. **Pricing & Discount Testing**
   - Manipulate price parameters
   - Test discount stacking
   - Apply discounts after item removal
   - Test coupon code reuse
2. **Inventory & Quantity Testing**
   - Test negative quantities
   - Test zero quantities
   - Test extremely large quantities
   - Test backorder/pre-order manipulation
3. **Access Control Testing**
   - Test role parameter manipulation
   - Try privilege escalation via workflow
   - Test admin function access from user accounts
   - Check email domain restrictions
4. **Transaction Testing**
   - Test transaction reversal
   - Check duplicate transaction processing
   - Test partial transaction completion
   - Verify transaction state consistency
5. **Time-Based Testing**
   - Test time-limited offers after expiration
   - Manipulate timestamps
   - Test session timeout handling
   - Check for race conditions in time-sensitive operations

Phase 5: Domain-Specific Testing

Domain-Specific Logic Testing

1. **E-commerce Specific Tests**
   - Gift card balance manipulation
   - Reward point exploitation
   - Referral program abuse
   - Shipping cost manipulation
2. **Banking/Financial Tests**
   - Transfer amount manipulation
   - Balance check bypass
   - Fee calculation exploitation
   - Transaction limit bypass
3. **Authentication/Authorization Tests**
   - 2FA bypass via workflow manipulation
   - Session fixation attacks
   - Remember-me token exploitation
   - Password reset logic flaws
4. **Email/Domain Validation Tests**
   - Email encoding discrepancies (UTF-7, encoded-word)
   - Domain parsing inconsistencies
   - Unicode overflow attacks
   - Punycode manipulation

Burp Macros	Automating multi-step workflows