Continuous Dynamic Business Logic Assessment Methodology

Business logic assessments (BLAs) are manual assessments for web application security vulnerabilities that cannot be tested effectively in an automated fashion. BLAs are intended to complement the automated testing of our Continuous Dynamic services. BLA coverage extends beyond the base application URL to incorporate any associated host names (URLs) provided by the client. This proprietary BLA methodology is established from a variety of internal policies and procedures. All tests are performed using a combination of browser add-ons, industry-standard HTTP proxy tools, and custom tools developed in house.

Business logic is the intended behavior and functionality that governs the core of what an application does. Hackers exploit business logic vulnerabilities in many ways to gain unauthorized access to websites. Session handling, credit card transactions, and password recovery are some of the web-enabled business logic processes that malicious hackers have abused to compromise major websites.

Automated scanners cannot detect business logic flaws in applications because they cannot be programmed to understand the context. These flaws can only be detected via manual testing, so it is imperative to complement automated testing process with manual assessments by security experts. To find the unconventional ways a vulnerability can be exploited, we need to approach security as a hacker would.

Black Duck® Continuous Dynamic offers business logic assessments (BLAs) conducted by experienced security engineers to find business logic vulnerabilities.

Scope

BLAs are performed on web applications that utilize the hypertext transfer protocol (HTTP) on the application layer with an underlying transmission control protocol (TCP) transport layer. Coverage is provided for the base application URL supplied by the customer as well any associated host name URLs that have been approved.

Production Safety

Production safety is a top priority. Any kind of testing that can result in denial of service or have a potentially negative impact on an application is avoided. Forms that result in the types of actions shown here are carefully covered during the BLA.

Changes data	Deletes data	Spams (contact, email, etc.)
Adds data	Saves data	Manages sessions (login/logout)

General Methodology

All BLAs are conducted according to a standard set of policies, procedures, and tools. Compliance with all these standards is strictly enforced to ensure consistency in results. The BLA engineer conducts extensive vulnerability testing focusing on OWASP Top 10, WASC 2.0, and CWE Top 25 issues that are unlikely to be found by automated scanners. The overall methodology is similar to the approach that can be found in the OWASP Testing Guide v4. Our methodology and tests are kept up-to-date as new information becomes available via OWASP, other standards, and our own research.

Content Discovery

The BLA engineer manually navigates through the application and explores visible content. The engineer also uses a variety of techniques and tools to discover hidden content. This helps establish all known entry points for the application.

Steps include

- Explore visible content
- Discover hidden content

Application Analysis

The BLA engineer analyzes the business model of the application to determine its intended design and purpose. They record dynamic application functionality and workflows in a site map, and review and define user roles and permissions. They also identify the underlying technologies for the application.

Steps include

- Analyze application business model
- Identify technologies used
- Analyze client-side controls
- Map application functionality
- Review browser extension components

Configuration Testing

The BLA engineer reviews the application's environment for any type of issue that is associated with configuration settings.

Steps include

- Test for fingerprinting
- Test for information leakage
- Test for autocomplete attribute
- Test for directory indexing
- Test HTTP methods
- Test HTTP headers
- Test for exposed admin interfaces
- Test for predictable resources
- Test for server misconfiguration
- Test for transport layer protection

Authentication Testing

The BLA engineer reviews all authentication components for vulnerabilities.

Steps include

- Test authentication mechanism
- Test for unsafe transmission of credentials
- Test for default credentials
- Test password policy
- Test remember me functionality
- Test for insecure direct object references
- Test for account lockout mechanism
- Test multifactor authentication mechanism
- Test account recovery process

Authorization Testing

The BLA engineer reviews all access controls for vulnerabilities.

Steps include

- Test for horizontal privilege escalation
- Test for vertical privilege escalation
- Test general access controls

Session Management Testing

The BLA engineer reviews all session components for vulnerabilities.

Steps include

- Review session mechanism
- Test for unsafe transmission of session
- Test session strength
- Test session prediction
- Test for session fixation
- Test session cookie attributes
- Test session termination

Identity Management Testing

The BLA engineer reviews all user management components for vulnerabilities.

Steps include

- Analyze user role definitions
- Test account enumeration
- Test user registration process
- Test account suspension process
- Test weak security questions
- Test user administration/provisioning

Input Handling and Data Validation Testing

The BLA engineer tests the application for common injection flaws.

Steps include

- Test for cross-site scripting (XSS)
- Test for SQL injection
- Test for OS command injection
- Test for XML injection
- Test for query language injection
- Test for file inclusion
- Test for server-side include (SSI) injection
- Test for response header injection
- Test for URL redirector abuse
- Test for content spoofing
- Test for HTTP parameter pollution
- Test for information leakage
- Test for improper input handling
- Test for path traversal

Application Logic Testing

The BLA engineer reviews application workflows and identifies specific vulnerabilities.

Steps include

- Test for cross-site request forgery (CSRF)
- Test multistep process and workflow circumvention
- Test abuse of functionality
- Test file upload
- Test financial transactions
- Test contact functionality
- Test for denial of service

Client-Side Testing

The BLA engineer reviews client side components for vulnerabilities.

Steps include

- Test cross-origin resource sharing
- Test web sockets
- Test web storage
- Test for UI redressing

Tester Qualifications

Engineers who perform BLAs are hand-selected and promoted from other teams within the Continuous Dynamic Threat Research Center. Each engineer must complete extensive manual testing training and successfully pass a multiweek evaluation period. Most engineers on the team have completed hundreds of manual assessments.

Findings

BLA findings are reported via the Continuous Dynamic interface with a custom description and steps to reproduce. These findings will appear at the end of the BLA and will be indicated with a manual retest icon. The same vulnerability rating system that is used for automated findings is also used for BLA findings.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.