BISHOP FOX®

8240 S. Kyrene Road
Suite A-113
Tempe, AZ 85284

P 480 621 8967
F 480 383 6401
www.bishopfox.com

HYBRID APPLICATION ASSESSMENT METHODOLOGY

Bishop Fox's hybrid application assessment methodology leverages the real-world attack techniques of application penetration testing in combination with targeted source code review to thoroughly identify application security vulnerabilities. These full knowledge assessments begin with automated scans of the deployed application and application source code. Next, analyses of the scan results are combined with manual review to thoroughly identify potential application security vulnerabilities. In addition, the team performs a review of the application architecture and business logic to locate any design-level issues. Finally, the team performs manual exploitation and review of these issues to validate the findings.

Phase I: Pre-Assessment

The following assessment requirements must be met to ensure the timely and successful completion of the project.

Pre-Assessment Requirements	
Application Information	The assessment team requires detailed application information including, but not limited to: • A recursive directory listing from the web root • Any available documentation related to the application • A Completed Application Assessment Questionnaire
Environment Access	The assessment team may need access to the following resources related to the application deployment environment including, but not limited to: • Administrative access to the underlying servers • Database schemas, LDAP models • Server configuration information (i.e., web server)
Application Access	The assessment team may need access to the following application resources including, but not limited to: • Application logic diagrams • Two sets of credentials for each application role • Network access to the application if it is not directly accessible

Pre-Assessment Requirements

Source Code

The assessment team requires access to the application source code which may include, but is not limited to:

- Complete, build-quality application source code
- Pre-compiled, functional binaries
- Any related libraries used in the application
- Access to the application build environment

Due Care

The assessment team performs a review of all pre-assessment information and proposed testing activities to determine their potential for adverse impact against the networks and applications. These activities include:

- Identifying all primary and secondary targets in addition to potential collateral targets
- Listing all proposed testing and assessment activities
- Compiling a Target Affects Matrix to associate each testing activity with the targets it may potentially affect
- Detailing the potential impact between each testing and target interaction
- Severity ranking each potential impact
- Updating test plans in accordance with acceptable severity levels

Throughout the assessment, the Bishop Fox team makes a best effort to minimize disruptions to network availability, particularly when performing any automated scanning, manual validation, or penetration testing.

Authority

If any portion of the application or related resources is hosted on a third-party system, the testing consent form must be completed prior to the start of fieldwork.

Phase II: Discovery and Vulnerability Scanning

In this phase, automated tools in conjunction with manual techniques are used to build an application footprint and identify any potential vulnerabilities.

Discovery and Vulnerability Scanning	
Automated Discovery with Manual Crawl	Automated site spiders in combination with manual discovery techniques are used to build a footprint of the application.
Application Scanning	Commercial and open source application security scanners are used to detect vulnerabilities within the web application. Automated tools permit the team to increase coverage and quickly attempt a variety of attacks during a time-boxed assessment.

Phase III: Manual Testing and Code Analysis

While automated scanning tools can significantly reduce the amount of time to perform basic application checks, they are no replacement for a manual assessment.

Manual Testing and Code Analysis	
Scanning Validation	The assessment team manually validates all findings from automated scanners to eliminate any false positives.
Manual Exploitation Techniques	A properly performed manual assessment is necessary to deep-dive into the application logic to identify complex and critical vulnerabilities. Much of web application testing technique comes from assessor experience and the ability to correlate disparate information into useful findings. These findings can then be leveraged to gain unauthorized access to the application, any associated data, and the underlying operating system. Manual testing may include but is not limited to: • Authentication and authorization bypass • Session management • Identifying data security and encryption weaknesses • Bypassing client-side validation • Exploiting query injection and input validation • Leveraging file transfer capability • Circumventing application logic

Manual Testing and Code Analysis	
Source Code Analysis	Review of application source code permits the rapid discovery of certain types of application security issues and logic flaws. The assessment team attempts to identify application vulnerabilities in the following areas: • Architecture and application logic flaws • Inadequate input validation • Improper implementation of cryptographic modules • Usage of insecure functions • Improper error handling

Phase IV: Analysis

After threat and vulnerability identification, the assessment team performs the following activities.

Analysis Activities	
Likelihood Determination	For each vulnerability, the assessment team derives the likelihood that a potential vulnerability will be exercised, based on the following factors: • Threat-source motivation and capability • Nature of the vulnerability • Existence and effectiveness of existing controls
Impact Analysis	For each potentially successful exploitation of a vulnerability, the assessment team analyzes and determines the impact of such an exercise as it affects systems and data in the following areas: • Confidentiality, Integrity, and Availability
Severity Determination	The assessment team determines the severity of each threat and vulnerability pair by using severity scales and severity-level matrices. The team also develops descriptions of the various levels of severity — critical, high, medium, and low.

Phase V: Compliance Review

Optionally, the assessment team gathers information pertaining to specific industry regulations to determine compliance with relevant requirements.

Compliance Activities	
PCI Compliance Testing	When requested, the assessment team reviews the application in observance of the PCI DSS requirements. Specifically, the team performs an assessment that accomplishes the following: • Satisfies both automated and manual testing requirements in Section 6.6 • Identifies issues described in Sections 6.5.1 – 6.5.10 • Validates compliance with requirements described in Sections 6.3, 6.3.1.1 – 6.3.1.5, 6.3.4, 6.3.7