BISHOPFOX

METHODOLOGY

Hybrid Application Assessment

Bishop Fox’s Hybrid Application Assessment methodology identifies application security vulnerabilities by combining automated and manual testing techniques across the applications architecture and its codebase.

Assessments begin by crawling and footprinting the application. Next, the assessment team conducts vulnerability scans with automated tools and then manually validates the results. Finally, the team manually identifies and exploits implementation errors and business logic to gain access to privileged application functionality, sensitive information, and the underlying application infrastructure. The methodology outlined in this document provides a detailed look at the step-by-step process and delineation of responsibilities that are critical to accomplishing predetermined objectives.

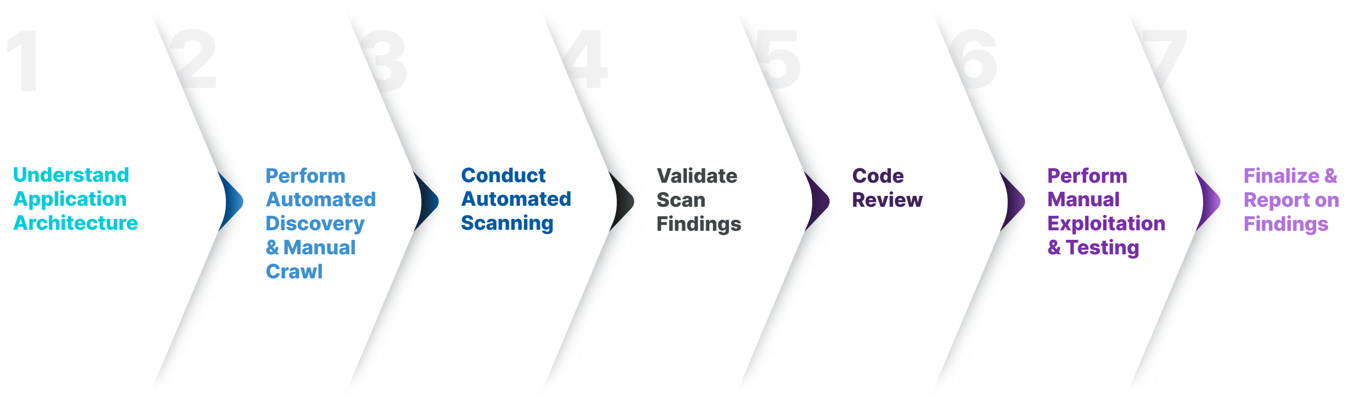
Summary of Engagement

Before the engagement can begin, Bishop Fox consultants require access to the application itself as well as source code and a completed Application Assessment Scoping Survey.

Once access has been provided, Bishop Fox consultants perform a fully automated and manual crawl of the applications footprint across commercial and open-source tools to detect vulnerabilities within the web application. Bishop Fox's assessment experts then sift through the results to understand the high-impact findings that carry a sizable portion of the risk. From these high-impact automated and manual findings, Bishop Fox Application experts then simulate an adversary targeting your application. In the process, Bishop Fox assessment experts: find gaps in authentication and authorization controls, review session management, identify data security and encryption weaknesses, exploit injection and weak input validation vulnerabilities, all while testing file transfer capability and the circumvention of application logic. The assessments are timeboxed and focus on demonstrating the real-world impact of misconfigurations in your applications. Additionally, Bishop Fox Application experts frequently find mistakes made by individual operators or teams that impact the larger environment. For instance, a team may deploy an application with default credentials or known vulnerabilities. If that application is compromised by an attacker, the attacker can often gain access to privileged credentials that can then be used to compromise additional components that an application interacts with. Further by conducting a review of the application's source code, the assessment team can rapidly discover specific types of application security issues and logic flaws. The team attempts to identify application vulnerabilities across architecture and application logic flaws, inadequate input validation, improper implementation of cryptographic modules, use of insecure functions and improper error handling.

Once weaknesses have been discovered, consultants document initial discovery and enumeration findings including successful exploitation. Remediation steps applicable to each threat are outlined in detail and reviewed with stakeholders for feedback and clarification. Once feedback has been applied, reports are finalized and communicated to all parties. It is important to note that the primary outcome of this engagement is ensuring your security teams understand all application-based exposures and prioritization of remediation against the likelihood of attack, business impact, and required resource allocation.

High-level Process



1 Understand Application Architecture

2 Perform Automated Discovery & Manual Crawl

3 Conduct Automated Scanning

4 Validate Scan Findings

5 Code Review

6 Perform Manual Exploitation & Testing

7 Finalize & Report on Findings

Methodology Details

Phase 1: Pre-assessment

The following assessment requirements must be met before the start of fieldwork activities 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: • Any available documentation related to the application • A completed Application Assessment Scoping Survey
ENVIRONMENT ACCESS	The assessment team may need access to the following resources related to the application deployment environment, including but not limited to: • VPN access to reach an internal test environment • Allow-listing of IP addresses (Bishop Fox's testing infrastructure must be permitted to bypass security appliances)
APPLICATION ACCESS	The assessment team may need access to the following resources, including but not limited to: • Two sets of credentials for each application role • Accounts belonging to different tenants or with access to unique data sets
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 • Environment access
DUE CARE	Throughout the assessment, Bishop Fox makes an effort to minimize disruptions to network availability, particularly when performing any automated scanning, manual validation, or penetration testing. Prior to testing, the assessment team will discuss risks to environmental stability with the client and identify the escalation path in the event that any disruptions are observed.
AUTHORITY	If any portion of the product or related resources is hosted on a third-party system, testing consent from the third party must be obtained in writing prior to the start of the assessment.

	Bishop Fox	Client
Understand application architecture	✓	✓
Provide application information		✓
Provision environment access		✓
Provision application access		✓
Provide source code		✓

Phase 2: 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.

AUTOMATED DISCOVERY WITH MANUAL CRAWL	A combination of manual and automated techniques is 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 timeboxed assessment.

	Bishop Fox	Client
Perform automated techniques to build a footprint of the application	✓	
Perform manual techniques to uncover additional application weaknesses	✓	
Use commercial application security scanners to detect vulnerabilities	✓	
Use open-source tools to scan the application for vulnerabilities	✓	

Phase 3: Manual Testing

While automated scanning tools can significantly reduce the amount of time needed to perform basic application checks, they are not an adequate replacement for a manual assessment.

AUTOMATED SCANNING VALIDATION	Although automated vulnerability scanning tools reduce the amount of time required to assess a target network, these engines are by nature designed to err on the side of caution and subsequently produce an elevated level of false positives. The assessment team manually reviews all findings to eliminate false positives and uncover any additional findings.
MANUAL EXPLOITATION TECHNIQUES	A manual assessment is necessary to examine the application logic and identify complex and critical vulnerabilities. These findings can then be leveraged to gain unauthorized access to the application, sensitive data, and the underlying operating system. Manual testing may include but is not limited to: • Finding gaps in authentication and authorization controls • Reviewing session management • Identifying data security and encryption weaknesses • Exploiting injection vulnerabilities and weak input validation • Leveraging file transfer capability • Circumventing application logic
SOURCE CODE ANALYSIS	By conducting a review of the application's source code, the assessment team can rapidly discover specific types of application security issues and logic flaws. The team attempts to identify application vulnerabilities in the following areas: • Architecture and application logic flaws • Inadequate input validation • Improper implementation of cryptographic modules • Use of insecure functions • Improper error handling

	Bishop Fox	Client
Manually validate all automated scan findings	✓	
Eliminate false positives	✓	
Apply manual exploitation and testing techniques	✓	
Find gaps in authentication and authorization controls	✓	
Review session management	✓	
Identify data security and encryption weaknesses	✓	
Exploit injection vulnerabilities and weak input validation	✓	
Test file transfer capability	✓	
Circumvent application logic	✓	
Architecture and application logic flaws	✓	
Identify inadequate input validation	✓	
Uncover improper implementation of cryptographic modules	✓	
Expose the use of insecure functions	✓	
Identify improper error handling	✓	

Phase 4: Analysis & Reporting

Bishop Fox reports contain an Executive-level summary of the engagement, which includes the assessment goals, a synthesis of the highest-impact findings, and high-level recommendations. Within each finding, a vulnerability definition is given along with detailed replication steps and tailored recommendations. For each finding, the assessment team builds a holistic view of the business risk it represents by performing the following technical analysis activities.

LIKELIHOOD DETERMINATION	For each vulnerability, the assessment team determines the likelihood that it will be exploited based on the following factors: • Threat-source motivation and capability • Nature of the vulnerability • Existence and effectiveness of controls
IMPACT ANALYSIS	For each vulnerability, the assessment team analyzes and determines the impact of successful exploitation as it affects the organization and its customers in the areas of confidentiality, integrity, and availability of systems and data.
SEVERITY DETERMINATION	Bishop Fox determines severity ratings using in-house expertise and industry-standard rating methodologies such as the Open Web Application Security Project (OWASP) and the Common Vulnerability Scoring System (CVSS) to evaluate the likelihood and impact of exploitation. The team weighs those factors to classify the overall severity as critical, high, medium, or low. The severity of each finding is determined independently of the severity of other findings.

	Bishop Fox	Client
Likelihood determination	✓	
Impact analysis	✓	✓
Severity determination	✓	

Phase 5: Remediation Review (Optional)

Optionally, the assessment team re-performs scanning and testing of the identified vulnerabilities after the client indicates that the vulnerabilities have been addressed.

Appendix

Delineation of Responsibilities	Bishop Fox	Client
Phase 1: Pre-assessment Requirements		
Understand application architecture	✓	✓
Provide application information		✓
Provision environment access		✓
Provision application access		✓
Provide source code		✓
Phase 2: Discovery and Vulnerability Scanning		
Perform automated techniques to build a footprint of the application	✓	
Perform manual techniques to uncover additional application weaknesses	✓	
Use commercial application security scanners to detect vulnerabilities	✓	
Use open-source tools to scan the application for vulnerabilities	✓	
Phase 3: Manual Testing		
Manually validate all automated scan findings	✓	
Eliminate false positives	✓	
Apply manual exploitation and testing techniques	✓	
Find gaps in authentication and authorization controls	✓	
Review session management	✓	
Identify data security and encryption weaknesses	✓	
Exploit injection vulnerabilities and weak input validation	✓	
Test file transfer capability	✓	
Circumvent application logic	✓	
Architecture and application logic flaws	✓	
Identify inadequate input validation	✓	
Uncover improper implementation of cryptographic modules	✓	
Expose the use of insecure functions	✓	
Identify improper error handling	✓	
Phase 4: Analysis & Reporting		
Likelihood determination	✓	
Impact analysis	✓	✓
Severity determination	✓	