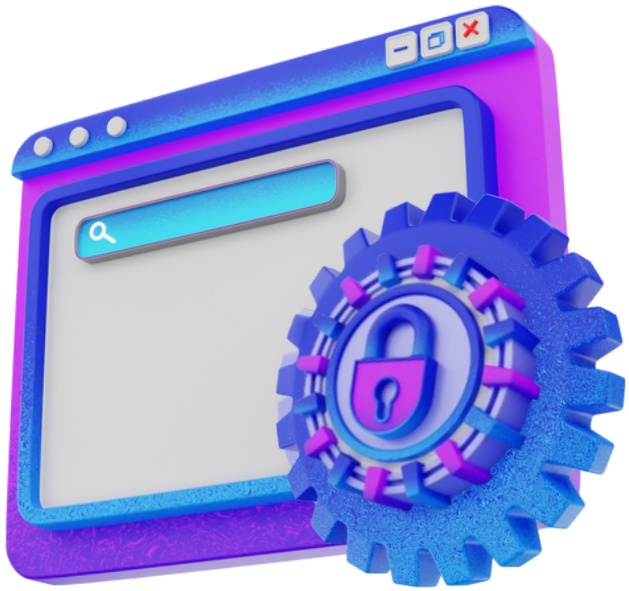
QUALYSEC
BEYOND CYBERSECURITY

METHODOLOGY

WEB APPLICATION PENETRATION TESTING



APPLICATION

PENETRATION TESTING

Qualysec uses a combination of automated and manual testing methods to uncover security vulnerabilities in applications. The process starts with crawling and gathering information about the application. Then, the team uses automated tools to scan for vulnerabilities and manually confirms the findings. Lastly, they manually exploit any errors or weaknesses in the application's logic and infrastructure to gain access to sensitive information and privileged functionality.

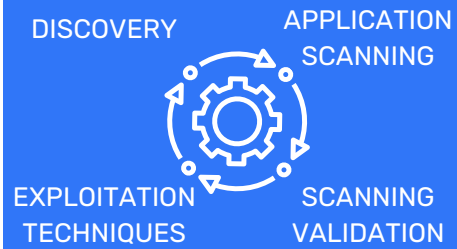
PROCESS OVERVIEW

Phase 1

PRE-ASSESSMENT

Phase 2 &3

DISCOVERY & PRODUCT TESTING



Phase 4

ANALYSIS & REPORTING

PHASE 1 : PRE-ASSESSMENT

Before beginning fieldwork, it is essential to fulfilling the necessary assessment criteria to guarantee the timely and successful completion of the project.

PRE-ASSESSMENT REQUIREMENTS	
APPLICATION INFORMATION	The assessment team needs comprehensive information about the application, such as: • Any related documentation for the application • A finished Application Assessment Scoping Survey.
ENVIRONMENT ACCESS	The assessment team may require access to resources related to the application's deployment environment, including: • VPN access to access an internal testing environment • Whitelisting of IP addresses to allow Qualysec's testing infrastructure to bypass security appliances.
APPLICATION ACCESS	The assessment team may require access to resources related to the application, including: • Two sets of credentials for each application role • Accounts that belong to different tenants or have access to distinct data sets.
DUE CARE	During the assessment, Qualysec endeavors to minimize network availability disruptions, especially when conducting automated scanning, manual validation, or penetration testing. Before testing, the assessment team will discuss the risks to the environmental stability with the client and identify the process to follow in case of any disruptions are observed.
AUTHORITY	If any part of the target network is hosted on third-party systems, written consent for testing must be obtained from the third party before the assessment begins.

PHASE 2 :

DISCOVERY AND VULNERABILITY SCANNING

During this phase, automated tools and manual techniques are employed together to create an application footprint and detect any potential vulnerabilities.

DISCOVERY AND VULNERABILITY SCANNING	
AUTOMATED DISCOVERY WITH MANUAL CRAWL	Both manual and automated techniques are employed to construct an application footprint.
APPLICATION SCANNING	The team employs commercial and open-source application security scanners to identify vulnerabilities in the web application. Automated tools allow the team to expand the scope and perform a variety of attacks rapidly during a limited-time assessment.

PHASE 3 : MANUAL TESTING

Automated scanning tools can significantly decrease the time needed for basic application checks, but they cannot substitute for a manual assessment.

MANUAL TESTING	
AUTOMATED SCANNING VALIDATION	Automated vulnerability scanning tools can decrease the time needed to evaluate a target network, but they tend to generate a large number of false positives. The assessment team manually reviews all findings to eliminate false positives and uncover additional findings.
MANUAL EXPLOITATION TECHNIQUES	A manual assessment is essential to inspect the application logic and discover complex and critical vulnerabilities. These findings can then be used to gain unauthorized access to the application, sensitive data, and the underlying operating system. Manual testing may include: • Identifying gaps in authentication and authorization controls • Examining session management • Discovering data security and encryption weaknesses • Exploiting injection vulnerabilities and weak input validation • Using file transfer capability • Circumventing application logic

PHASE 4 : ANALYSIS AND REPORTING

After identifying the threats and vulnerabilities, the assessment team carries out the following activities:

TECHNICAL ANALYSIS ACTIVITIES	
LIKELIHOOD DETERMINATION	For each vulnerability, the assessment team determines the probability of it being exploited based on the following factors: • The motivation and capability of the threat source • The nature of the vulnerability • The existence and effectiveness of controls.
IMPACT ANALYSIS	For every vulnerability, the assessment team evaluates and calculates the impact of exploitation on the confidentiality, integrity, and availability of systems and data.
SEVERITY DETERMINATION	The assessment team evaluates the probability and impact of exploitation for each vulnerability to determine its severity, by taking into account the likelihood and impact of exploitation and classifying it as critical, high, medium, or low.

PHASE 5 : REMEDIATION REVIEW (OPTIONAL)

The assessment team may repeat the scanning and testing of identified vulnerabilities after the client confirms that the vulnerabilities have been addressed (if desired).