

## What is an Application Assessment?

An application assessment is an evaluation of the security controls implemented within a web or mobile application. The purpose of this assessment is to identify security vulnerabilities and provide professional recommendations on remediating threats. Unlike a traditional vulnerability scan that simply identifies vulnerabilities, an application assessment includes exploitation and a full demonstration of how exploiting one or more security vulnerabilities could impact the application, its data, and potentially the infrastructure that the application resides on.

By performing an application assessment, your organization can understand the mindset of an attacker and how to prepare for application-based attacks, which usually occur on a very frequent basis. Once completed, your organization can use the results of the assessment as a baseline for deploying other applications to your environment or mobile platform, providing reassurance while adhering to industry security best practices.

**An application assessment will benefit your organization with:**

- Defining security best practices for web and mobile applications
- Preparing against malicious threats, targeting your web or mobile application
- Identifying potential threats that could result in a successful attack
- Reducing the overall attack surface within the application environment or mobile application

Our consultants perform several assessment activities to identify potential threats that may result in a successful attack against data, services, and systems within your web and mobile application environments.



### IDENTIFYING SECURITY THREATS

Identify security vulnerabilities within your web or mobile application that pose a threat to your sensitive information. Our activities involve both manual and automated processes to deliver quality application testing services and results.



### DEMONSTRATION OF IMPACT

If possible, our consultants will also demonstrate the impact of successfully exploiting any identified security vulnerabilities. This will allow your organization to understand additional resources and data that may be accessible beyond normal application functionality once access is granted.



### MISCONFIGURATION CHECKS

In addition to identifying security vulnerabilities, our consultants will also note any configuration threats that could eventually lead to a successful attack when combined with other information and attack vectors.



## Our Application Testing Methodology

Based on our professional experience, research, and the activities performed by modern-day attackers, Vonahi Security consultants follow an application testing methodology that combines both traditional and new attack techniques to provide quality application testing services.

### INTELLIGENCE GATHERING

An understanding of the application is gathered during this process. With knowledge of functionality, purpose, and its features, our consultants can build out an attack plan to leverage potential weaknesses within the application.

### THREAT MODELING

An analysis of the identified vulnerabilities is performed, which includes performing additional research about the identified vulnerabilities and how it could affect the application. From this analysis, the consultant identifies the best approach to formulating an attack against the exposed security flaws.

### POST-EXPLOITATION

During post-exploitation, our consultants will attempt to gain further access into the environment, system, and/or data exposed during post-compromise. Lateral movement within the environment may also be performed.

### VULNERABILITY ANALYSIS

Both manual and automated application testing is performed during this phase to identify security vulnerabilities that may exist within the application.

### PERFORM EXPLOITATION

If an attack can be performed, such as SQL injection or remote code execution, our consultants will perform exploitation to enumerate information and/or access application and system resources.

### TIMELY REPORTING

Documentation is collected, reviewed, and presented to your organization in a clear, concise, and effective manner. In addition to supporting data, strategic and technical recommendations are provided to help your organization with successful remediation.

## What You Get

At Vonahi Security, we understand the demands and expectations for quality information security services. As part of our application testing services, your organization can expect the following:



Project Management & Planning



Daily Status / Progress Reports



Quality Deliverables & Presentations



Experienced & Certified Security Experts



## ABOUT US

Vonahi Security is a cybersecurity consulting firm that offers comprehensive information security services. Our team is comprised of security experts experienced in offensive and defensive operations, allowing us to provide quality information security services. We ensure your organization is successful with achieving its security goals and remaining one step ahead of malicious adversaries.

HELLO WORLD. MEET MODERN SECURITY.

 [www.vonahi.io](http://www.vonahi.io)

 [info@vonahi.io](mailto:info@vonahi.io)

 1.844.VONASEC (866-2732)

   @vonahisec