

2026 Q1 OneTrust Main Web App & API Penetration Test

OneTrust

May 2026

Revision History

Version	Revision Date	Revised By	Description
1.0	3/11/2026	Protiviti Attack & Penetration	Initial Draft
2.0	5/7/2026	Protiviti Attack & Penetration	Finalized

Disclaimer

This report is intended solely for the use of management of OneTrust ("Client" or "OT") and is not to be used or relied upon by others for any purpose whatsoever. This report and the related findings and recommendations detailed herein provide management with information about the condition or risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.

This report presents the results of a web application penetration test and API penetration test performed by Protiviti between January 5th, 2026 and February 20th, 2026 on the OneTrust Main application. The scope of the review was limited to specific target systems which were agreed upon during project scoping. This executive summary report is designed for the reader to understand the level of security assessed, to identify security deficiencies, to identify areas of strength and weakness, and to develop a course of action to correct vulnerabilities and mitigate associated risks.

Penetration testing is an uncertain process which is based upon past experiences, currently available information, and known threats. It should be understood that all information security systems, which by their nature are dependent on their human operators, are vulnerable to some degree. Therefore, while the team believes to have identified the major security vulnerabilities on the systems analyzed, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures. This report identifies known vulnerabilities that were detected during the test period; new devices, configuration changes and new/future vulnerabilities were not tested. While the matters presented herein are the result of the review, had additional procedures been performed, other matters may have been identified that would have been reported to OT.

Additionally, this report contains information concerning potential vulnerabilities of OT network(s)/system(s) and methods for exploiting them. The team recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein.

Executive Summary

Background

In Q1 of 2026, OneTrust ("Client" or "OT") engaged a third-party, Protiviti to perform a web application penetration test and API penetration test on the OT Main application. The project focused on evaluating controls that directly correlate to threats and risks that may compromise the confidentiality, integrity, and availability of sensitive information that resides on OT's technology environment.

Fieldwork was performed remotely from Protiviti security labs between January 5th, 2026, and February 20th, 2026.

Objectives and Scope

This engagement was executed with the intent of assessing controls that are in place within the applications and are designed to minimize the risks of the organization. Emphasis was placed on evaluating the application safeguards that restrict unauthorized access to the OT application, the data it transmits, and the critical data (e.g., credentials, personally identifiable data, credit card information, etc.) it stores.

The scope of the engagement included the following:

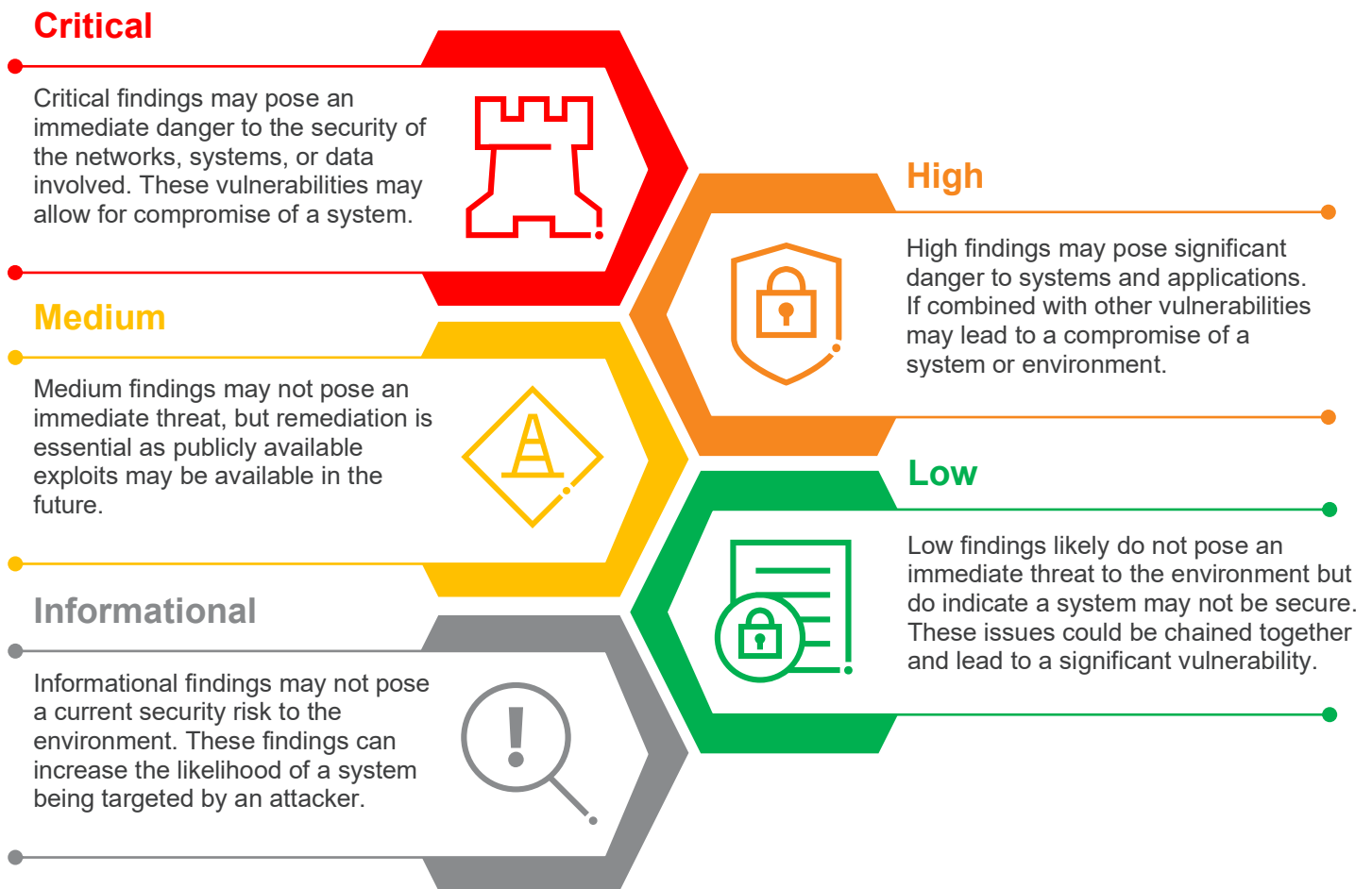
- **Web Application Penetration Test** – Performed a series of tests on the OT Main application using automated commercial application scanning tools and web proxies to crawl and map the target. Specifically, application entry points, programming languages, structure, and error codes were identified to complete the application mapping process. Protiviti leveraged the data collected from the crawling and mapping phase to perform a series of automated tests, manual tests, and validation activities to evaluate the security posture of the application.
- **API Penetration Test** – Protiviti performed series of tests using automated commercial API scanning tools and proxies to crawl and map the target APIs. The data collected from the crawling and mapping phase was then used to perform a series of automated tests, manual tests, and validation activities to evaluate the overall security posture of the API.

2026 Q1 OneTrust Main Web App & API Penetration Test

Protiviti's Approach to Evaluating Results

Observations and recommendations made during this review have received one of the following risk rankings. These rankings address the significance of the risk and likelihood the risk could occur in the business environment. The rankings should be reviewed by management and used as a tool to determine the level of attention and effort that should be given to each observation and recommendation.

Each vulnerability or risk identified has been labeled with a particular significance rating of critical, high, medium, low, or informational risk levels, defined as follows:



2026 Q1 OneTrust Main Web App & API Penetration Test

Summary of Observations

The following table summarizes the total number of findings in each ranking:

Phases	Critical	High	Medium	Low	Info
Web Application Penetration Test	0	0	1	1	1
API Penetration Test	0	0	0	1	0
Total	0	0	1	2	1

The table below summarizes the observations identified during the 2026 Q1 OT Main Web AppAPI Penetration Test:

Ref.	Observation	Criticality
Web Application Penetration Test		
W.1	Cloud Server-Side Request Forgery	Medium
W.2	HTML Injection via Email Notification	Low
W.3	Information Disclosure	Info
API Penetration Test		
A.1	Insecure Access Controls	Low

Appendix A - Testing Methodologies

Web Application Penetration Test Methodology

Overview: During web application penetration testing, Protiviti attempts to identify insecure configurations, failures in business logic, and exploitable vulnerabilities that a malicious actor could abuse. Protiviti leverages found vulnerabilities to gain unauthorized access to sensitive information being handled by the application, to gain elevated or privileged access to the application itself, and/or to gain access to the web application's underlying infrastructure (e.g., the server hosting the web application). Protiviti initially tests from an unauthenticated perspective to simulate an attacker who does not have valid credentials for the application. Additionally, Protiviti continues testing with valid credentials and attempts to identify privilege escalation vectors and other attacks that could be performed from an authenticated perspective.

Steps listed in this section detail the general flow of activities and the type of tasks performed during web application penetration tests.



Crawling and Spidering: Protiviti profiles or "footprints" the in-scope web applications. This includes "crawling" and "spidering" the applications to identify pages and resources available to end users. Protiviti also attempts to identify pages or resources not directly referenced by the application. In addition, Protiviti attempts to identify the underlying technology utilized by the application (e.g., programming languages, libraries, frameworks, etc.).

Purpose: The purpose of application mapping is to build an inventory of the application's static and dynamic pages and to identify the application's architecture. This information is leveraged in later phases to identify attack vectors and vulnerabilities.

Unauthenticated Testing: Protiviti leverages the data collected during the application mapping phase to perform a series of tests to evaluate the security posture of the application from an unauthenticated perspective. Protiviti attempts to identify application misconfigurations, coding errors, and other vulnerabilities, especially those outlined in the OWASP Top 10. Common web application vulnerabilities include Structured Query Language (SQL) injection, cross-site scripting (XSS), broken authentication/access controls, etc. Tests are also performed to better understand the functionality of the in-scope applications, which aids in identifying exploitable lapses in application logic.

Purpose: The purpose of unauthenticated testing is to evaluate the security posture of the application against an attacker who has not compromised valid credentials.

Authenticated Testing: Protiviti performs testing of the web application(s) from the perspective of an authenticated user. Protiviti specifically tests the authenticated areas of the application and focuses on identifying issues like session hijacking, privilege escalation, authentication bypass, access control deficiencies, or unauthorized account "hopping."

Purpose: Performing authenticated testing of the in-scope application(s) provides an understanding of what an attacker with compromised credentials or a malicious user could potentially exploit.

Vulnerability Scanning (Web Application Layer): Protiviti uses automated vulnerability scanners to identify exploitable web application vulnerabilities. Automated vulnerability scanners identify thousands of known vulnerabilities while also attempting common attack vectors. Protiviti then performs false-positive analysis to verify discovered vulnerabilities.

2026 Q1 OneTrust Main Web App & API Penetration Test

Purpose: The objective of automated vulnerability scanning is to identify as many potential vulnerabilities as possible and to augment manual testing to provide a comprehensive view of the security posture of the in-scope web application(s).

API Penetration Test Methodology

Overview: During API penetration testing, Protiviti attempts to identify insecure configurations, access control failures, and exploitable vulnerabilities that a malicious actor could abuse. Protiviti leverages found vulnerabilities to gain unauthorized access to sensitive information being handled by the API, to gain elevated or privileged access to the application itself, and/or to gain access to the API's underlying infrastructure (e.g., the server hosting the API). Protiviti initially tests from an unauthenticated perspective to simulate an attacker who does not have valid access for the API. Additionally, Protiviti continues testing with valid credentials and attempts to identify privilege escalation vectors and other attacks that could be performed from an authenticated perspective.

Steps listed in this section detail the general flow of activities and the type of tasks performed during API penetration tests.

Crawling and Spidering: Protiviti profiles or "footprints" the in-scope API. This includes perusing any API documentation (Swagger, Postman, etc.) and includes "crawling" and "spidering" the routes to identify active endpoints and resources available to end users. Protiviti also attempts to identify endpoints or resources not directly referenced by the in-scope API. In addition, Protiviti attempts to identify the underlying technology utilized by the API (e.g., programming languages, libraries, frameworks, etc.).

Purpose: The purpose of API mapping is to build an inventory of the API's endpoints and to identify the API's architecture. This information is leveraged in later phases to identify attack vectors and vulnerabilities.

Unauthenticated Testing: Protiviti leverages the data collected during the API Endpoint mapping phase to perform a series of tests to evaluate the security posture of the API from an unauthenticated perspective. Protiviti attempts to identify misconfigurations, coding errors, and other vulnerabilities, especially those outlined in the OWASP Top 10. Common API vulnerabilities include Structured Query Language (SQL) injection, Server-Side Request Forgery (SSRF), broken authentication/authorization controls, etc. Tests are also performed to better understand the functionality of the in-scope endpoints, which aids in identifying exploitable lapses in the consumption of the API.

Purpose: The purpose of unauthenticated testing is to evaluate the security posture of the API against an attacker who has not compromised valid credentials.

Authenticated Testing: Protiviti performs testing of the API from the perspective of an authenticated user. Protiviti specifically tests the authenticated areas of the application and focuses on identifying issues like session hijacking, privilege escalation, authentication bypass, access control deficiencies, or unauthorized account "hopping."

Purpose: Performing authenticated testing of the in-scope application provides an understanding of what an attacker with compromised credentials or a malicious user could potentially exploit.

Face the Future with Confidence