API Headless Pentesting Requirements

About Synack's headless API Pentesting

Synack's headless API pentesting utilizes the diverse skills of the Synack Red Team (SRT) to provide thorough testing coverage and reporting on your APIs, all delivered through the Synack Platform.

Reports will detail the testing performed, including screenshots and vulnerability findings across the API requests. The reports are ideal for executive audiences and compliance auditors.

What do I need to start a test?

The Synack Customer Assessment Creation Wizard (with help from customer support and customer operations) will help guide you through the test preparation process. There are a few required items for API penetration testing, and a few other items that will improve your testing experience.

The more complete and thorough the documentation, the better the pentest and results.

Postman, OpenAPI Specification 3.0+ (formerly Swagger) or JSON documentation of the API is needed. All parameters and variables should be documented within the API documentation as Synack validates these during the test preparation process. Postman documentation is the preferred option and may expedite your scoping process. This documentation is usually created as part of the development cycle. QA, reliability or load testing can produce useful documentation for our security testing. Please note that we do not support scripting in the postman collections, including pre-request scripts to fetch auth tokens.

Necessary documentation

Postman documentation is the preferred option and may expedite your scoping process. This documentation is usually created as part of the development cycle. QA, reliability or load testing can produce useful documentation for our security testing.

Because the API does not have a user interface, you will need to provide a basic role description. This should include what access the account has, the rights to modify or view information and other critical details. Without knowing what access is intended, the SRT cannot test access control & privacy violations (ACPV) effectively.

If the test involves authentication, bearer tokens or similar authorizations, the SRT will need information on how to generate those credentials. The generation area does not need to be in scope for testing but can simply be used to get access and responses from the target. Ideally, many users can use the same authentication, or they can generate user specific authorizations if needed.

Optional

Although Synack needs at least a document showing our user rights, showing what other users can do is helpful. For example, if an SRT member is a normal user, knowing what the admin can do provides valuable additional information. If there is documentation for those admin calls, it can also allow the SRT to test more effectively. For example, if a researcher knows the API call and variables an admin uses, testing for authorization violations is much simpler.

External API documentation outside of the testing scope can help provide additional context for the SRT to test more effectively. External documentation may include API user guides or similar documents that help users or developers work with the API.

The more information provided to the SRT, the more they will understand your API in depth, and the better your testing results will be.