Synack

DATASHEET

API Pentesting with Synack

Provide Guaranteed Coverage and Find Exploitable Vulnerabilities with Headless API Testing

In addition to our continuous web application pentesting, Synack offers API offensive security testing for headless APIs—that is, APIs without an accompanying web application/GUI.

Our offensive API testing 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 comprehensive testing performed, including screenshots and vulnerability findings across scoped API requests. These reports are ideal for showcasing work and communicating results to executive audiences and compliance auditors.

How it works

STEP 1

SCOPING

Understand how many API requests are to be tested

STEP 2

ACTIVATE

Submit API documentation through the Synack Platform

STEP 3

TESTING

Researchers with proven API testing skills are activated on scoped API requests

STEP 4

REPORTS

Receive reports in the Synack Platform detailing coverage and any vulnerability findings

Benefits of testing APIs with Synack

- Test headless APIs in addition to web applications, allowing for more comprehensive coverage of your attack surface
- Receive reports showcasing the testing methodologies performed on each API call
- Testing APIs earlier in the software development life cycle catches vulnerabilities sooner rather than later, shifting left and influencing the development of more secure web applications

Compliance-ready results and reporting show coverage

Reports can be generated on-demand within the Synack Platform for audiences like executives and compliance auditors. SRT researchers will document their API testing efforts for submitted endpoints, including screenshots and proof of concept for exploitable vulnerabilities found.

This documentation is vetted by Synack Vulnerability Operations to make sure that reported vulnerabilities are exploitable and to minimize noise and false positives.

API security testing methodologies

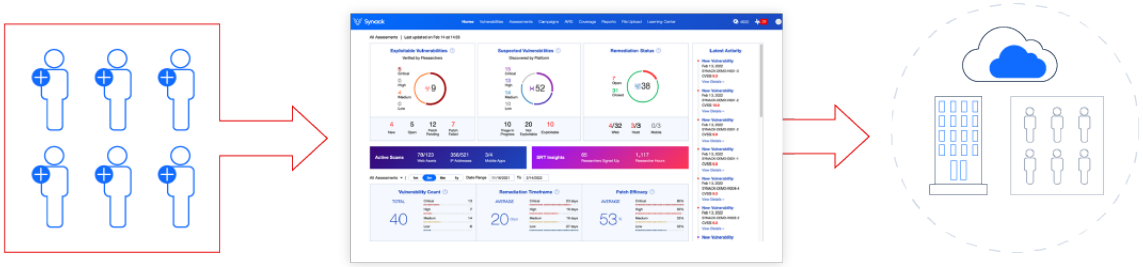
SRT researchers will check for common and critical vulnerabilities on each API endpoint, emulating a true outside adversary. Their work is influenced by frameworks such as the OWASP API Top 10. Vulnerabilities sought include:

- Broken object level authorization
- Broken user authentication
- Excessive data exposure
- Broken function level authorization
- Injection vulnerabilities
- Lack of resource & rate limiting
- Security misconfiguration

Diverse human skills provide a true adversarial perspective

SRT researchers have a diversity of job titles, reconnaissance skills, certifications and educational backgrounds. Representing over 80 countries, the human element brought by the SRT takes API security testing beyond the capabilities of automated solutions like API scanners, firewall solutions and traffic monitoring.

When performing API testing with Synack, researchers with demonstrated API testing skill sets will be activated for your attack surface.



Synack Red Team

Activated on-demand

To test your attack surface and augment your team