7SYSTEM
COMMITTED TO THE FUTURE

# RESTAPIFUZZ

RestAPIFuzz is an automated tool to enable organization to test their RESTAPIs for security vulnerabilities. RestAPIFuzz has unique test cases to cover major test cases to cover OWASP AP 2019 and has an easy user-friendly GUI which makes it easy for organizations to deploy and use RestAPIFuzz.

## API FRAMEWORKS ARE NECESSARY

APIs are the entry gate to any organizations, as web application are constantly exposing their APIs to external 3rd parties. Testing APIs is important so as to be able to identify security vulnerabilities, inconsistencies, or bugs which could result in the API being compromised.

## CHALLENGES

Some of the challenges organizations face during API testing are;

- ✓ APIs are complicated and requires the person testing to have a strong knowledge of the API and the application
- ✓ They are expensive to fix
- ✓ Traditionally process to test is manual and slow and dependent on the skills of the person testing it
- ✓ Defining the scope and having the right skill set to be able to model the API and more.

## FEATURES

RestAPIFuzz is clientless, which means one does not need to install any agents on the client machines. Having a user-friendly GUI makes it easy for anyone to use it without the need of being proficient or have a strong knowledge on APIs. With a few clicks allow, one is able to test any individual API or the APIs embedded in your web.

If one is testing a web application, RestAPIFuzz, uses interactive application testing technology to discover RestAPI consumed in the web application and then uses API modelling technology to test the RestAPI discovered for any security vulnerabilities. It then maps the vulnerabilities to OWASP 2019 API Security along with providing details on the vulnerabilities discovered, mapping vulnerabilities  to CWE numbers and providing remediations along with the payload used which triggered the vulnerability.

## HOW IT WORKS

RESTAPIFUZZ , uses interactive application testing technology & API modelling to discover APIs and then test the discovered APIs against a series of custom defined test cases and payloads to discover vulnerabilities based on requirements laid out in the OWASP Top-10. It leverages automated testing which the security team can use to intelligently executes a series of test cases and payloads to test the APIs. It’s user friendly GUI enables the user to easily in a few clicks configure execution of the testing. RESTAPIFUZZ can test a web application or Individual APIs & acts as a MITP and uses a proxy to capture the traffic between the application under test and the client machine and the RESTAPIFUZZ server. Once captured, it uses the data to test RESTAPIFUZZ and sent to the test target.  User can easily enable automated testing in Five (5) clicks

- ✓ Identify the Application or Individual API to be tested
- ✓ Create a project and enter its details like Web Application URL or API End point
- ✓ Initiate the Proxy on your web browser.
- ✓ Click on the web application / or interact with the API. More you interact, , better is the coverage
- ✓ Wait for some time and it will generate a detailed testing report

## RESTAPIFUZZ DISCOVERY

- ✓ Discovers custom and commercial APIs
- ✓ Provide you a detailed list of APIs being consumed by your web application

## RESTAPIFUZZ REPORTING

- ✓ Individual test wise, project wise and organization wise reporting also in PDF format
- ✓ Detailed reporting with recommendations for every project

## RESTAPIFUZZ MITIGATION

- ✓ Recommendation as per OWASP into possible recommendations
- ✓ Provides custom researched mitigation methods and also various references

## RESTAPIFUZZ TEST

- ✓ Test the APIs discovered using API modelling
- ✓ Extensive testing with custom test cases
- ✓ Performs testing based on requirements laid out by OWASP 2019 API Security testing.
- ✓ Identifies and maps the vulnerability to a CWE
- ✓ Uses fault message data to find vulnerabilities

7SYSTEM
COMMITTED TO THE FUTURE