RAPIFUZZ

APIs help to bridge the communication gap between an application and third-party applications. APIs are the front door to your data. Modern applications use commercial and custom APIs. While making custom APIs, it is important to ensure that the APIs built are secure, as vulnerabilities can lead to the compromise of the application. Application testing now involves testing of APIs for vulnerabilities. RAPIFUZZ is an automated security testing solution that allows organizations to test their Web APIs against the OWASP Top-10.

CHALLENGES

API testing is complicated, more expensive to fix, traditionally slow and manual and dependent on the skills of the tester. Some of the major challenges application security testers face are:

- ✓ What to test as they don't have a detailed list of the APIs being consumed by the application
- ✓ Identifying the different API types
- ✓ Writing unique and large number of test cases to ensure complete application coverage
- ✓ Managing vulnerabilities discovered and tagging them as the project progresses

COVERAGE

OWASP 2019 API Security Coverage

- ✓ **A2**- Broken Authentication
- ✓ **A3**- Excessive Data Exposure
- ✓ **A4**- Lack of Resources & Rate Limiting
- ✓ **A7**- Security Misconfiguration
- ✓ **A8**- Injection

CYBERMOKSH

ALERTNESS | KNOWLEDGE | WISDOM

FEATURES

- ✓ Clientless-does not require the user to install any client.
- ✓ Generates a detailed bill of material of APIs consumed by the Web Applications
- ✓ Segregates APIs from URLs & commercial APIs from custom APIs
- ✓ Tests individual APIs or APIs embedded in a Web Application
- ✓ Models the custom API for security testing and identifies bad practices
- ✓ Tests web APIs against API OWASP 2019
- ✓ Provides detailed reporting of Vulnerabilities with payload used, CWE number mapping, mitigation methods & bad practices

HOW IT WORKS

RAPIFUZZ performs a series of security checks against your web APIs based on requirements laid out in the OWASP Top-10. By leveraging the automated testing that your development team already performs (i.e. unit tests), RAPI intelligently executes a series of fuzz and passive security tests. Once configured, interactions will primarily occur through your existing build-system interfaces.

RAPI can test a web application or Individual APIs and acts as a man-in-the-middle proxy, capturing traffic created by your existing automated testing. The captured data is fuzzed by RAPI and sent to the test target.

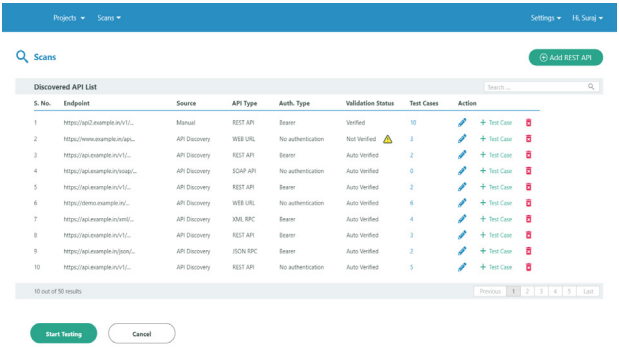
Enable automated API testing in easy steps:

- ✓ Identify the Application or Individual API
- ✓ Enter the details of your project and then the URL details of the Application or the API
- ✓ Start the process and enable proxy on your browser.
- ✓ More you click on your web application, the better the coverage.
- ✓ Segregates Web URL's and APIs and Identifies REST APIs

DISCOVERY

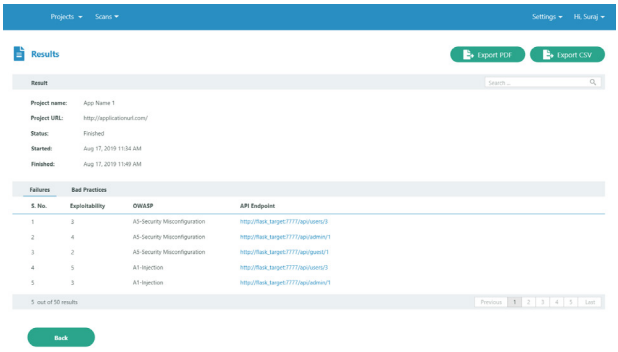
- ✓ Discovers custom and commercial APIs being consumed in the web application
- ✓ Provide a detailed Bill of Material (BOM), of the API's being consumed

- ✓ Identifies 3rd party most used commercial APIs like Google etc.
- ✓ Segregates API's from WEB URL's and buckets them as URL, REST API and Other APIs



TEST

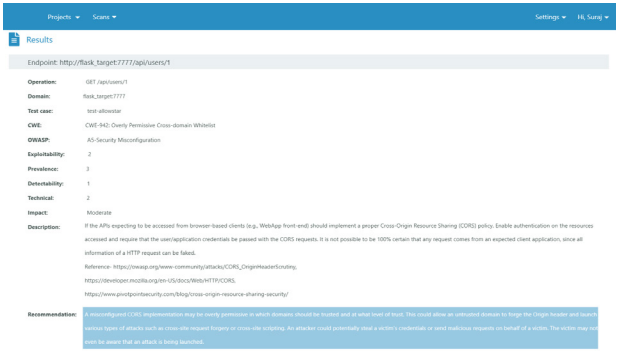
- ✓ Acts like the man-in-the-middle proxy and captures traffic
- ✓ Data captured is fuzzed by RAPIFUZZ
- ✓ Tests each API individually against our exhaustive test cases to discover vulnerabilities
- ✓ Performs testing based on requirements laid out by OWASP 2019 API Security
- ✓ Test and retest, as it creates unique tags every time you test your Application/API



MITIGATION

- ✓ Identifies the vulnerability and provides detailed information about them.
- ✓ Provides details about the vulnerable end point and the payload used for exploitation

- ✓ Provides mitigations methods as per the methods that is mentioned in OWASP 2019 API Security
- ✓ Provides custom researched mitigation methods and references, done by our research team



REPORTING

- ✓ Provides a detailed PDF report detailing scanned application, vulnerable end points, mitigation methods and recommendations.
- ✓ Maps Vulnerability discovered to OWASP 2019 API Security
- and mapping it to the CWE Number
- ✓ Generate reports as per individual test wise, project wise and organization wise
- ✓ Detailed reporting with recommendations

CYBERMOKSH

ALERTNESS | KNOWLEDGE | WISDOM