Report on Various Methodologies of API Authentication Testing: Lifecycle, Application use and Challenges

Satish Kumar Alaria
Assistant Professor, Department of Computer Science & Engineering,
Arya Institute of Engineering & Technology,
Jaipur, Rajasthan (India)

Abstract: - API testing is the process of testing the application programming interface to make sure that it is secure, correct, reliable and is in alignment with the best practices of the business or organisation. The popularity of API began when internet as a service came into the market. The benefits of using API have been introduced in organisations and developers are encouraged to report and use API as much as possible. This is since API have specifications and elements which helps the organisations to manage their API efficiently bases upon the integration, important documentation, and testing tools. Over the period, most of the organisations are moving their applications and processes online due to which all the crucial data is available online. This gave rise to security and privacy issue of the data and information of the clients of the organisation. It is important that proper API authentication protocols and methods are followed to provide best secure and safe APIs to the end user.

Keywords: - Introduction to API, Importance of API authentication testing, API authentication techniques, API testing process, Advantages, Challenges of API authentication testing.

*****

Introduction – [1]

API which is application programming interface is the interface which helps to facilitate communication between two software systems. It allows to exchange data between the two systems. API helps to identify what type of requests can be made, how a request can be made, what will be the format of the data etc. Most of the organisation have moved to online APIs in their business models. This means that all the data and information related to one user will be present online. Therefore, it is very important that the data and information is safe and secure and have less risk of data being hacked as it is crucial information about the users. Here comes the concept of API authentication testing which is used to test whether the API are secure or not. It is necessary that API which are present online should have authentication security protocols, and proper authentication methods should be followed before the data exchange between two systems starts. This is to make sure that the two systems which are about to exchange data are authorised to do so and make sure that there is secure exchange of the data. The objective of API testing is to make sure that the programming interfaces functions properly, are reliable, have efficient performances, and secure enough to keep the data safe with them. The difference between in GUI testing and API testing is that the input to API test is given in the form of software which will send calls to other software and the output which the system will give will be observed and notes as compared to input and output in traditional way of testing. To test the authentication of the systems, whenever a call is made by one software to the other, the receiver will first test whether the client is the authorised client or not. Authentication protocol is used to identify the validation of the client who is trying to make connection. The credentials of the client who is requesting the connection is sent to the server which is at remote location in text or encrypted form. It will be tested by the server whether the client should be given access or not. Therefore, the main objective of the API authentication testing is to make sure that each client who is requesting to gain access is a valid client and only then access should be provided. The testing should also test whether the user is trying to access and not by mistake and make sure that the system is secure enough to not let the hacker hack the systems and get all the crucial credentials of the users.

Importance of API Security testing: - [2]

API security testing means to make sure that the interface which are present in the network which allows to exchange data between two software is safe and secure and cannot be easily hacked by the hackers. Since a lot of information about client is available in internet and can be hacked easily it is important that efficient security protocols must be used to check the authorisation of users making request in an API system. Conducting API security testing is important due to following reasons: -

- The objective of API security testing is to make sure that the basic security need of the system is met. This includes to make sure that the data is encrypted, the conditions of authorisation and user access have been met etc.

- API security testing will act like hacker and try to hack the system and find out the bugs and try to fix them and make them secure enough so that it could not be attacked by the hacker.
- Almost all the organisations are using API interfaces as it provides efficient interfaces to the developers for the services offered by the organisations.
- API make sure that the security compliance of organisations are met during its implementation process.
- With the help of proper API security testing techniques, the risks related to various domains of the organisations reduces.

API Security best practices: - [3]

In order to make sure that the security of API interfaces is done, proper policies and protocols should be followed for the authentication and authorisation of the users. Some of the best practices to be followed are as following: -

1. Data encryption: -
   The first best practice to be followed is to make sure that the data is encrypted efficiently. This can be done by using TLS which helps to reduce the risk of cyber-attacks. To modify the data, the users should have digital signature to decrypt the data.
2. Quotas for APIs: -
   The risk of being attacked can be reduced if there is quota for API to identify the number of times it is called and hence by tracking the usage the risk associated with the hacker's attack can be reduced.
3. API gateway: -
   For API security testing, API gateways can be used which helps to identify the number of times an API is called and helps to monitor the utilization of an API.
4. Access control: -
   In this method, specific access control rules will be implemented which helps to check the authorised use of the API interfaces.

API authentication methodologies: - [4]

In order to test the security of the API it is important to follow and implement authentication protocols and algorithms so that hackers cannot attack it easily. There are many methodologies used for API authentication testing which are discussed below: -

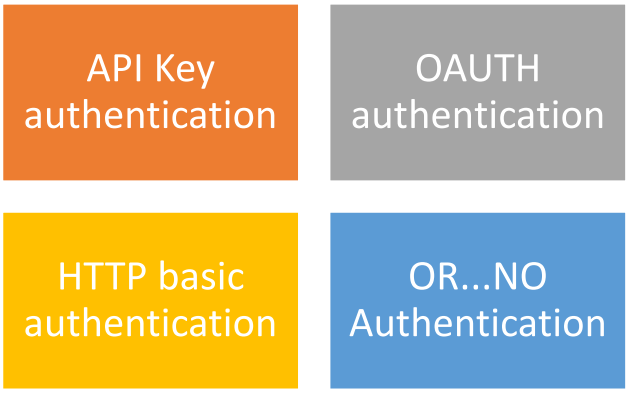

Figure 1 Types of API authentication methods.

1. API key authentication: -
   - In this method, a unique key is generated to be used by the developers and whenever developers make request this key is given to them.
   - The key generated by API is a combination of different numbers and letters which is very long string, and it is difficult to guess.
   - The minimum length is as long as 30 characters, but it can be longer than this. The longer the key, the harder it is to guess.
   - It will be present it the header of the API authorisation and is unique and specific to the developers.
   - The developers who have this key can only access and work on the APIs.

2. OAUTH authentication: -
   - This method uses OAuth 2.0 authorization framework to give access to third party developers for HTTP services.
   - This framework is efficient to provide approvals itself between the API owner and the service.
   - Using this method, the developers can obtain access on their own. OAUTH is about authorization which means that user is seeking permission to access.
   - It is carried out in three steps: -
     a. The user first generates request to access the API interface after which the consumer will seek permission to do so.
     b. After this, the user is directed to the service provider and gets permission.
     c. The consumer will get a access token and access the secured resource.
   - This way in this method, an authorised token is given to the user to use the resources.

3. HTTP basic authentication technique: -
   - This is the simplest form of API authentication where username and password are used whenever API call is made.
   - The request will consist of a header where the username and password are present in encrypted form.
   - So, whenever a developer makes API call, the authorization is tested by providing username and password to the developer.
   - The HTTP uses client side and server-side protocols.
   - At the server-side, it must test the authorisation by checking the header to its corresponding header field. It server-side finds out that the header consists of unauthorised header than it must send error message saying the same.
   - At client side, when client want to send request to the server-side, then it must contain the authorised header having correct username and password, only then it will be provided access.

4. OR….NO Authentication: -
   - There's generally the choice of applying no verification by any stretch of the imagination.
   - Engineers can simply make a solicitation to a particular URL and get a reaction without requiring any certifications or an API key.
   - This approach is usually utilized in inner APIs facilitated on-premises however is certainly not a suggested practice.
   - This method is used for testing purpose, where user can create account without the need for authorisation from other systems.
   - This type of method provides facility only to lock fields, to disable or enable user access, to provide other login page, etc.

Advantages of API Security testing: - [5]
There are many advantages of API security testing which are discussed below: -

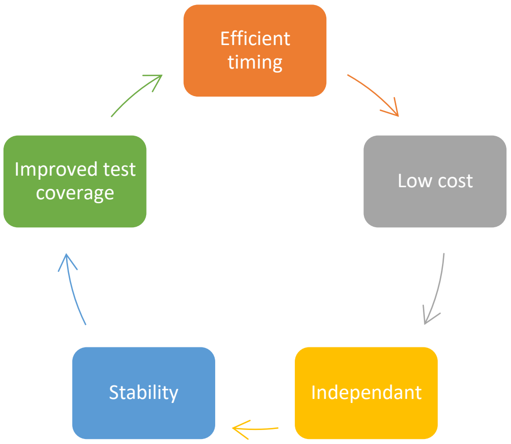

Figure 2 Advantages of API testing.

1. Efficient timing: -
   API testing helps to save time as it gives faster test results as compared to other testing techniques. As a result of this the speed of development process also increases.
2. Low cost involved: -
   Since API testing tales less time to give results, it has proved to be cost effective. The speed of conducting API test helps to make effective and efficient use of resources which results in less testing expenses.
3. Independent feature: -
   API testing does not depend upon any language like java, dotnet, c etc. This gives choice to the developer to use language of their own interest and in which they are comfortable.
4. Test Coverage: -
   Unit tests won't get these bugs; however, API tests are exceptionally intended to guarantee that all framework parts fill in as planned before they are utilized. Programming interface testing supports the revelation of connection point, server, and data set blemishes, bringing about superior in general programming quality and a superior client experience for end-clients.
5. Stability: -
   API interface testing is stable and gives reliable results. Test engineers will have access to updated test suites, and API interfaces are well documented. Due to their stable behaviour these are easy to maintain.

Challenges of API security testing: - [6]
Besides benefits of API, following are few challenges of API testing: -

1. Lack of resources and timing: - API does not have the feature to prevent the number of calls made by the user. If the pattern of requesting and making call to the API is observed, then it will become very easy for the attackers to hack the system.
2. Authentication and authorisation: -

This is the main challenge of the API security testing. If it does not implement efficient security testing protocols, then it will be very easy for the attackers to hack the system.

3. API monitoring: -
   APIs are not logged properly and also not monitored due to which it is complex to identify the patterns.

Conclusion: - Programming interface testing is the most common way of testing the application programming connection point to ensure that it is secure, right, dependable and is in arrangement with the prescribed procedures of the business or association. The ubiquity of API started when web as a help came into the market. The advantages of utilizing API have been presented in associations and designers are urged to report and involve API however much as could reasonably be expected. This is since API have particulars and components which assists the associations with dealing with their API productively bases upon the combination, significant documentation, and testing apparatuses. Over the period, a large portion of the associations are moving their applications and cycles online because of which every one of the urgent information is accessible on the web. This led to security and protection issue of the information and data of the clients of the association.

References: -

[1]. https://www.guru99.com/api-testing.html
[2]. https://www.synopsys.com/glossary/what-is-api-security-testing.html
[3]. https://beaglesecurity.com/blog/article/api-security-testing.html
[4]. https://www.3pillarglobal.com/insights/most-popular-api-authentication-methods/#:~:text
[5]. https://www.studytonight.com/post/what-is-api-testing-what-are-the-advantages-and-drawbacks