RAPIFUZZ

DEMYSTIFYING API SECURITY

EXECUTIVE OVERVIEW

The year 2021 is not over, yet it is already the year of the API security incident. API flaws impact the entire business, not just dev or security or the business groups. Web APIs are the backbone of web, cloud, mobile applications, and even many open data initiatives.

REST is the predominant architectural style for building such Web APIs. Application programming interface (API) attacks could become the most-frequent attack vector that can cause data breaches by 2022.

Behind data breaches, there are usually broken, exposed, or hacked APIs involved in exposing sensitive medical, financial, and personal data for public consumption. That said, not all data is the same, and should not be protected in the same way either. Your approach to API security will most likely depend on what kind of data is getting transferred.

IMVISION[1] Industry survey on enterprise API security in early 2021, and their key findings include:

92%

of enterprises were using more than 10 APIs

1/3

of the security leaders think that their APIs get the protection they need

91%

of security leaders make API security a priority

80%

of them would like to gain more control over their APIs.

API's, consumed across domains and industries and, through every modern application like Mobile, IoT, B2B, Serverless, Cloud, Single Page Application uses API. Client devices are becoming varied and vigorous whereas, the logic moved from backend to frontend. This change has also increased the Cyber Threat Landscape. The move to innovate/deliver faster has also increased the usage of API.

"Without APIs, most software can not exist" as shared in the App Developer magazine. APIs are replacing traditional technologies in their ability to deliver safe & secure ways to connect in a faster way and providing organizations the competitive advantage. They have a very crucial role to play in virtually every industry today, and their importance is increasing steadily, as they move to the forefront of business strategies.
API's help organizations with methods to access data and software thereby letting engineering teams do their jobs in less time, with fewer resources.

This helps a company streamline its existing IT infrastructure, with quicker collaboration between internal and external teams.

> The study by IMVISION highlights that 50% or more of security leaders commented that General-purpose application security solutions such as WAF and SAST/DAST were not on their roadmap as tools for API Security

Reported API Breaches Instance

- ✓ CVE-2021-3036, which impacted PAN-OS XML API in April 2021[2]
- ✓ CVE-2021-29715 impacting IBM API Connect in August 2021[3]
- ✓ Panera Bread breach of 2018 revealed 37 Million customers with reports attributing it to a breach, due to an unauthenticated API Endpoint[4]
- ✓ The T-Mobile breach of 2018, where attackers exploited a 'leaky' API and exposed 2.3 million customer data[5]
- ✓ Capitol One breach of 2019, using a server-side request forgery, an attacker compromised an application gaining access to their AWS-based infrastructure configuration API. A case study by MIT "A Case Study of the Capital One Data Breach" describes the same in detail[6]

These are the more publicly used products than the ones reported and, there would be many more.

With the growing utilization of APIs, API Security is becoming important than ever before for organizations.API Security is complicated, slow and manual and dependant on the skill sets of the tester, and much more expensive to fix as compared to any standard bug on a website.

Leading to a limited scope of testing as testers focus on the inputs provided and the short period to test the application. The solution is to automate the process of API testing, enabling us to cover a large testing scope with accurate results.

API and API Types

Application Programming Interface, "is a set of clearly defined methods of communication between various software components". Applications like Twitter, Facebook, your internet or mobile banking application, etc. use API. For example, when you use a mobile banking application on your mobile phone, the application connects to the Internet and sends data to a server. The data retrieved by the server is then interpreted. It then performs the necessary actions needed to send it back to your phone. The information is presented in a readable way by the application after interpreting the data. All of this happens via API.

APIs have been there for a long time. A web service provides access to its service via an address on the World Wide Web, also known as a URI or URL. It is a piece of software or a system. The objective is to get information in a format that other applications can understand or parse. A web service uses HTTP to exchange information or HTTPS, which is encrypted. When an application, the "client", wants to communicate with the web service, the application sends an HTTP request and gets an HTTP response through the web service. In the request, much of the required information passes in the URL itself, as paths in the URL and/or as URL parameters.

Most often-used types of web service

- ✓ SOAP (Simple Object Access Protocol) is a protocol that defines the communication method and the structure of the messages with data transfer format as XML.

- ✓ XML-RPC is an older protocol than SOAP. For data transfer, it uses a specific XML, whereas SOAP allows a proprietary XML format. An XML-RPC call tends to be much simpler and uses less bandwidth than a SOAP call.

- ✓ JSON-RPC is similar to XML-RPC but uses JSON instead of XML for data transfer.

- ✓ REST (Representational state transfer) is not a protocol but rather a set of architectural principles. Architecture is what differentiates a REST service from other web services. Some of its characteristics include the simplicity of interfaces, identification of resources within the request, and the ability to manipulate the resources via the interface

- ✓ GraphQL is a query language for APIs. GraphQL provides a thorough description of the data in your API and is a runtime for fulfilling queries with the existing data. It gives clients the power to ask for exactly what they need making it easier to evolve and enabling powerful developer tools.

	RPC	SOAP	REST	GRAPHQL
ORGANIZED IN TERMS OF	Local procedure calling	Enveloped message structure	Compliance with 6 architectural constraints	Scheme and type system
LEARNING CURVE	Easy	Difficult	Easy	Medium
USE CASES	Command and action oriented APIs; Internal high perfomance communication in massive micro-services system	Payement gateways, identity management, CRM solutions, financial and telecommunication services, legacy system support	Public APIs, simple resource driven apps	Mobile APIs, complex systems, micro-services

API Security Testing and its Importance

The process of checking for security vulnerabilities in APIs is API security testing. The process involves testing endpoints of an API for security, correctness, and reliability and to ensure it complies with an organization's best practices. There is a crucial need to ensure that an API is secure considering, a vulnerable API could lead to Unauthorized Access, Data leakage, Sanctioning Fuzzy input, Injection Vulnerabilities, Parameter Tampering, and more.

API Security testing is to craft inputs to coax bugs or issues or any undefined behavior outof an API that may get compromised by a hacker.

The process begins by defining the API that needs testing while obtaining valid test cases that testers provide with the information on inputs and required outputs of the API. This helps API security testing to construct fuzzed input tailored to the input the API expects.

The output would be a security testing report consisting of vulnerabilities or bugs discovered while fuzzing the API. APIs allow data exchange between applications, and if a hacker breaches API security, then they can access sensitive data stored.

It is important to do a thorough security testing of APIs to:

- ✓ Prevent Data leaks of customers
- ✓ Protect your brand's reputation in the market post a breach resulting in revenue loss
- ✓ Protect against lawsuits (if there is negligence on your behalf)
- ✓ Test the APIs functionality, reliability, usability
- ✓ Help identify where the API diverges from published specifications.

Challenges and Gaps in API Security Testing

We discussed earlier that API Security is complicated, slow and manual, and dependant on the skill sets of the tester, along with being much more expensive to fix as compared to a standard bug on a website. Finding the right skill set along with having an adequate set of tests to ensure proper coverage of the API is a must.

According to the OWASP API Top 10, it is not uncommon for legitimate, authenticated users to exploit the API by utilizing calls that appear legitimate but intend to manipulate the API. These kinds of attacks, aiming to manipulate the business logic and exploit design flaws, are attractive to attackers.

Some of the key challenges in API security are:

- ✓ API Discovery- identifying the list of APIs consumed by any application?
- ✓ Segregation of API types, like REST, SOAP. If multiple formats are in use?
- ✓ Identifying the APIs consumed that needs testing
- ✓ Modeling the API- to understand what verbs, authentication methods, etc. they support
- ✓ Test cases to cover the entire application
- ✓ Manual testing is tester knowledge-dependent and time-consuming.
- ✓ Managing vulnerabilities discovered and tagging them as the project progresses.
- ✓ It is common for companies to test web, app, and mobile separately - but not the API itself since they don't have any UI.
- ✓ With legacy APIs, you might not know about the APIs already implemented or the documentation, so you don't know the next steps
- ✓ Some APIs require authentication to be properly tested, so one would need to follow the flow

Apart from testing the APIs, the tester needs to understand API functionalities and then test them for business logic vulnerabilities and traditional vulnerabilities.

Presently the most common approach towards application security testing which includes testing the APIs is to use SAST and DAST.

These may not be sufficient. For API security it is important to have a comprehensive which covers the business and traditional vulnerability approach. APIs are the backbone for applications and it is necessary to do a complete comprehensive security testing of APIs before deployment.

Application security testing does not focus on API security directly but uses SAST or DAST tools. Using SAST or DAST tools does not completely address the needs for API security. OWASP API SECURITY TOP 10 2019 focuses on API security whereas OWASP Top 10 Web Security 2017 & 2021 focus on the 'Ten Most Critical Web Application Security Risks".
APIs has a highly complex architecture and exposure to sensitive data, and enabling and maintaining the security of APIs becomes very critical.

Some of the challenges one could face while testing the APIs consumed in their web applications are:

- ✓ Discovering the list of APIs consumed within their application viz-a-viz getting a Bill of material of APIs.
- ✓ Classifying and segregating Commercial APIs from their Custom APIs
- ✓ Segregation of the different APIs like SOAP, JSON-RPC, XML-RPC, REST and GraphQL
- ✓ Validating of Business logic of APIs
- ✓ Testing the APIs as per OWASP API Security 2019
- ✓ Validating the API vulnerabilities discovered
- ✓ Integrating into the DevOps or DevSecOps process

Conclusion

API adoption has been on the rise and this has also increased the level of underlying security risks. Even large companies like Google and Facebook are sometimes caught off-guard, and it's time for organizations to enhance their security methods to safeguard their core systems and databases. API security testing is niche and needs to give due importance as it plays a very vital role in mitigating attacks against a product. It is important to ensure that during testing all accounted vulnerabilities thoroughly with proper verification along with validation that all APIs are covered during security testing.

It is important to ensure that the person testing should have a thorough understanding of API functionalities based on the business logic.

To be able to ensure that the APIs are secured it is important to have a deeper and detailed understanding of the nuances of API security testing, matched with the right API security testing tool. Some of these challenges that organizations may face during the process can be optimized and mitigated by implementing certain best practices that will help in easing the testing efforts. Organizations need to adopt a mindset of "security-first" while moving forward. The organization can leverage the benefits of the highly suggested API security testing tools while filling the gaps before it's too late.

Cited References

1. Imvison Enterprise API Security Servey. Retrieved from https://www.imvision.ai/2021-api-security-survey/
2. CVE-2021-3036 Detail; National Vulnerability Database. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2021-3036
3. CVE-2021-29715 Detail; National Vulnerability Database. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2021-29715
4. NEWS:Panera Bread blew off breach report for 8 months, leaked millions of customer records. Retrieved from https://www.csoonline.com/
5. T-Mobile was hit by a data breach affecting around 2 million customers. Retrieved from https://www.theverge.com
6. Capitol One fined. Retrieved from https://marketrealist.com/
7. Table. Retrieved from https://www.altexsoft.com/blog/soap-vs-rest-vs-graphql-vs-rpc/