Top 15+ Ways How To Prevent API Attacks You Never Knew

API [Application Programming Interface] attacks can significantly impact and cause threats to the security, performance, usability and functionality of any web application.

APIs act as a bridge or intermediate between different applications, these applications help and assist in easily communicating and allow to exchange of data and information seamlessly.

As the technology in the web development area increased the threats to web applications have increased dramatically, due to the majority of larger applications heavily relying on APIs for data and information exchange.

Some malicious programs or codes try to manipulate and compromise the data utilized in software applications and be misused if hacked.

Therefore, in this post, I will guide you with **15+ Way on How To Prevent API Attacks and How to Avoid these types of attacks and threats.**

15+ Ways How To Prevent API Attacks in Tabular Form

1. Use SSL Certificate for Web Applications.
2. Take appropriate measures to stop unauthorized access.
3. Use proper validation client side and server side.
4. Encrypt sensitive and important data.

5 Use Token-Based Security:
6 Use parameterized queries to avoid SQL injections.
7 Deploy Web Application Firewall (WAF) for an additional layer of security.
8 Check and validate third-party dependencies.
9 Implement proper IP Whitelisting/Blacklisting.
10 Customize Secure File Uploads according to your needs.
11 Cross-Origin Resource Sharing (CORS) allows valid domains to access APIs.
12 API gateway for centralized management and security of web applications.
13 Validate request and response of data [content-type].
14 Periodic Security Audits.
15 Use proper Security Headers.

How To Prevent Against API Attacks In Points

1. Use SSL Certificate for Web Applications.
2. Take appropriate measures to stop unauthorized access.
3. Use proper validation client side and server side.
4. Encrypt sensitive and important data.
5. Use Token-Based Security:
6. Use parameterized queries to avoid SQL injections.
7. Deploy a Web Application Firewall (WAF) for an additional layer of security.
8. Check and validate third-party dependencies.
9. Implement proper IP Whitelisting/Blacklisting.
10. Customize Secure File Uploads according to your needs.
11. Cross-Origin Resource Sharing (CORS) allows valid domains to access APIs.
12. API gateway for centralized management and security of web applications.
13. Validate request and response of data [content-type].
14. Periodic Security Audits.
15. Use proper Security Headers.

1. Use SSL.

SSL [Secured Socket Layer] is mandatory to secure web application and online project as it encrypt sensitive data and information.

The website and online project that displays Https before their domain are ranked well on search engines and are more trusted by users.

2. Proper Authorization.

Valid and proper authorization should be practiced and the control should be given to user with required and necessary resources.

Software developers or system administrators must provide authorization to clients and users so that unauthorized access should be restricted.

3. Validations.

Use proper validation client side and server side so that the application can be protected from vulnerabilities and SQL injections.

Validations can significantly make applications more potent against hackers and crackers.

4. Encrypt Sensitive and Important Data.

Hackers and crackers are always on the look for any back door entries so that they can steal your sensitive data and information and later misuse them for their own benefits.

To avoid such incidence programmer or developer must encrypt their important data and information.

5. Parameterized Query.

There are various types of hacking and cracking but some of the common practice is to expose the vulnerabilities present in any software or any application.

SQL injection is one of such method where hackers try to access your database using wrong practices and exposing poor SQL query pattern.

Using parameterized queries is a good practice to prevent SQL injection attacks

6. Deploy Web Application Firewall (WAF).

Deploying Web Application Firewall (WAF) is a good practice for providing additional layer of security for your web applications and mobile applications.

These WAF is specifically designed and developed to prevent applications from hacking attacks and online vulnerabilities.

These WAF block malicious code, hacking code and helps | assists traffic for better performance and functioning.

7. Third Party Dependencies.

Third-party dependencies are external code or libraries or components that are used and utilized for better and faster development process.

These libraries often provides variety of benefits for applications such as speed, accuracy, design, community support, faster development and debugging process.

There are significant advantages of third parties' libraries still there are certain disadvantages that are important to pay attention while development.

`Such vulnerabilities are mentioned below.`

1. Regular Updates.
2. License Compatibility.
3. Check for Compatibility.
4. Dependency Bloat.
5. Version Pinning.
6. Lack of Control.

8. Customize Secure File Uploads.

File uploads should be secure and customized so that they can be protected from uploading malicious code to our applications and make them vulnerable.

Some precautionary and preventive measures must be taken into consideration to customize file upload such are file type validation, filenames, and use of captcha code.

The above steps can make your application more potent against malicious code and hackers. This customization can add an additional layer of security to our application.

9. IP Whitelisting/Blacklisting.

Implementing proper IP Whitelisting/Blacklisting can filter unwanted traffic coming to the application. These can significantly improve the overall security and proper functioning of websites and applications.

Prevention Against API Attacks Using Infographics

What Is API

`API stands for Application Programming Interface.`

API is a software program that connects two software applications and helps in data | information exchange.

In other words, API is a bridge and can communicate between applications easily.

These applications are developed by programmers and software engineers for more productive and enhanced performance.

APIs can make the process of software development speedier and in an innovative manner. APIs are important in complex, feature and function-rich projects.

The advanced library functions can make the tasks and operations easy compared to older days when APIs were not used.

APIs are more prominently used in the development of web and mobile applications, cloud services, and other software solutions.

`Some of the major characteristics of APIs are included below.`

1. Standardization.
2. Abstraction.
3. Modularity.
4. Reuse.
5. Interoperability.

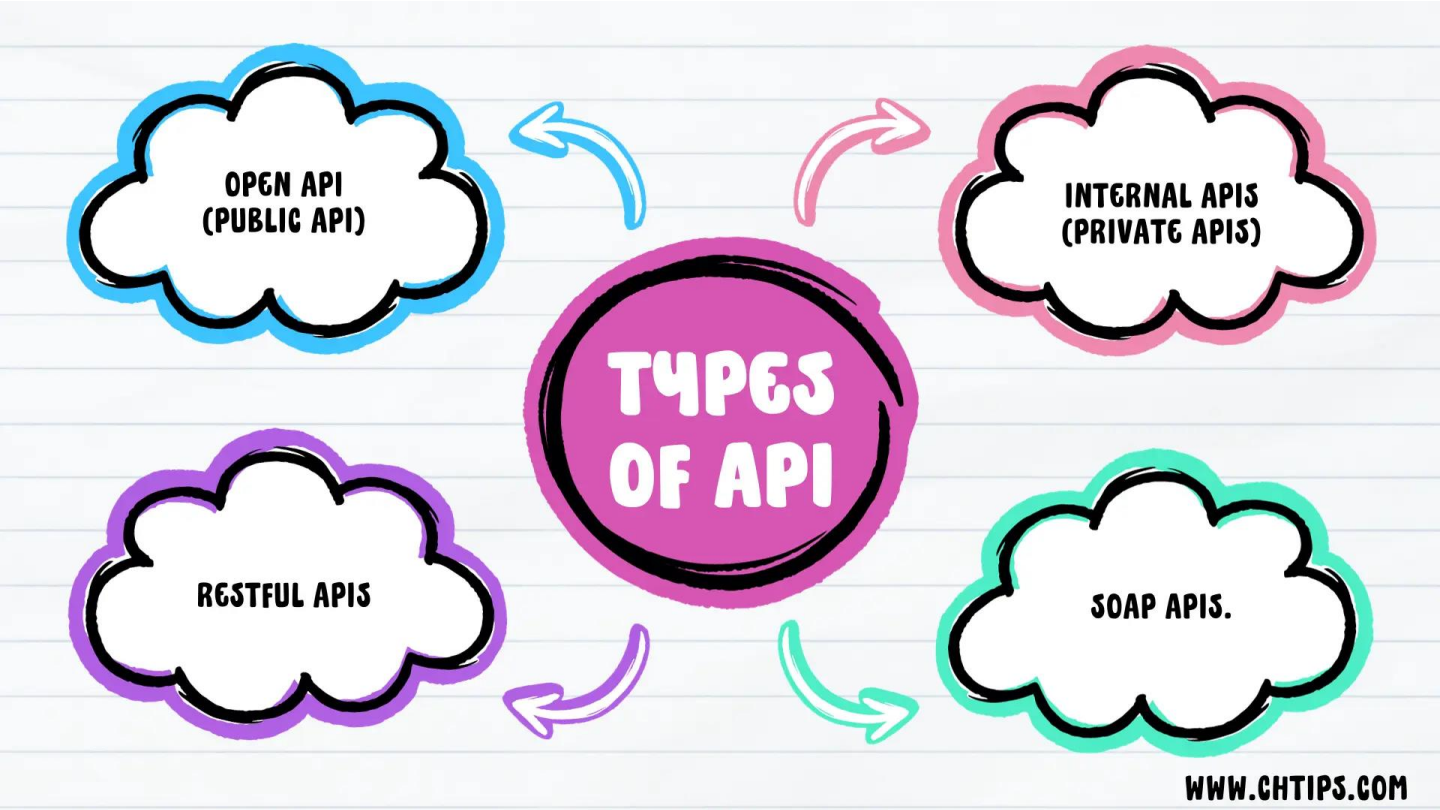
What Are The Types Of API Security?

1. Authentication Attacks.
2. Authorization Attacks.
3. Injection Attacks.
4. Denial-of-Service (DoS).
5. Cross-Site Scripting (XSS).
6. Data Exfiltration.
7. Cross-Site Request Forgery (CSRF).

`Related Articles`

- Learn Cybersecurity
- Computer Basic Tutorials

What Are The 4 Types Of API?



1. Open APIs (Public APIs):
2. Internal APIs (Private APIs):
3. RESTful APIs.
4. SOAP APIs.

How Can I Improve My API Security?

There are certain measures that can be taken to avoid future issues related to API security some of them are mentioned below.

1. Regular and Periodic Updates.
2. Dependency Management Tools.
3. Version Pinning.
4. Security Audit.
5. Valid Documentations.
6. Input validations and Sanitization.
7. License Compliance.

Popular Programming Languages

1 Python
2 PHP
3 Java
4 C
5 C++

Frequently Asked Questions [FAQs]

How do I protect my API?

The best practices on how to protect API.
1. Use HTTPS.
2. Filters results using validations.
3. Encrypt data and information.
4. Validating authorized access.

What is the legal protection of API?

API can be protected under intellectual property rights.

How do I encrypt an API request?

To encrypt an API request developer must use SSL to add security to the application.

Can APIs be breached?

Yes.

What is API full form?

Application Programming Interface.

Who created API?

C. J. Date in 1974.

What language is API written in?

API can be written in any programming language that suits your requirements.

Who built REST API?

Roy Fielding.

For More Information Please Do Visit :

https://www.chtips.com/cybersecurity/how-to-prevent-api-attacks/