Globant

S.H.I.E.L.D

Secure your HTTP, Internet, Emails, Logs & Data

UI NXT

SSL Pinning

Even though the SSL/TLS communications are secure as well as unbreakable, the MITM (Man-in-the-Middle) attack can still cause a threat to secure communication.

In MITM attacks, hackers discovered a loophole in the network communication and sought to be in the middle of communication between the client and the backend server with malicious intentions.

Certificate pinning is an added layer of communication protection between clients and servers.

Please refer to the Medium article to know more about SSL Pinning and its implementation on various platforms.

Security audit tools

Security audit tools measure the information and vulnerability of applications over multiple platforms, using these tools users can scan the applications and get the list of vulnerabilities that can be threaded later to the applications.

Security audit tools provide two types of scan options SAST(Static Application Security Testing) and DAST(Dynamic Application Security Testing)

Importance of Security audit tools:

- Identify security problems and gaps, as well as application weaknesses
- Comply with internal/External organization security policies

Best Security practices

Application security is something that gets neglected in the rush of delivering features on time. But considering different attacks we should allocate some time while developing any application to retrospect how our application will survive such attacks.

We studied various best practices that any developer can follow to make the app more secure. These practices can be easily implemented such as integrating SSL Pinning, disabling screen capture, using secure storage methods to avoid data theft, implementing cross-site scripting and proper session management, etc.

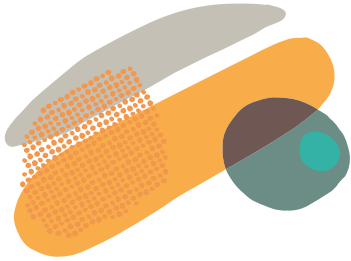
To know the best practices for Android developer, you can refer to the article.

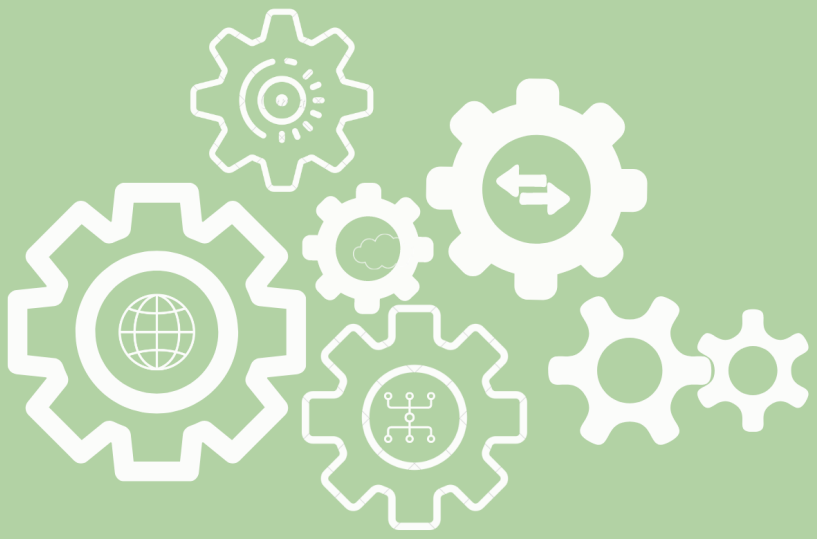
Are you struggling to understand what Cross Site Scripting really is? How does an XSS attack occur? And most importantly, how to combat such an attack? Don't worry! This amazing **article** will help you understand Cross-site scripting in detail.

The X-XSS-Protection header is designed to enable the cross-site scripting (XSS) filter built into modern web browsers. To know more about X-XSS protection and its usage please refer to the **article**

We use multiple external packages to reuse the functionalities, but have you ever wondered if these packages in turn install any other packages and if they are safe to use? You can refer to the **article** which explains in detail Traverse Dependency Vulnerabilities.

It is always recommended to use encryption to securely store your data, but what about encryption keys? Don't you think we should also secure them? This Medium **article** will definitely help you understand how you can secure and manage such keys.





Networking Protocols

For networking-related tasks, we have different protocols such as HTTP, HTTPS, gRPC, etc. However, do we know how they work, and what kind of security mechanism they have?

Consider the HTTP protocols, since its first version, it got evolved and included different features. To know more about different HTTP versions, their feature, advantages, and disadvantages please refer to the Medium **article**.

gRPC stands for Google Remote Procedure Call. It's a free and open-source framework developed by Google. You can refer to the Medium **article**, to know more about the working, features, and security aspects of this protocol.