HTTPS/HTTP

Replacing HTTPS with HTTP resulted in a significant loss of security due to the absence of encryption and related security mechanisms. This exposes sensitive data to interception and manipulation, making HTTP traffic considerably riskier compared to HTTPS. Here are the main dissimilarities:

1. Encryption Absence: The most significant difference is the absences of encryption in HTTP traffic. Unlike HTTPS, where data is encrypted using SSL/TLS protocols during transmission, HTTP sends data in plain text. This means that anyone intercepting the traffic can easily read the information being exchanged between the client and the server.
2. Security Risks: Due to the lack of encryption, HTTP traffic is vulnerable to various security risks such as eavesdropping, man-in-the-middle attacks, and data tampering. Without the protection provided by encryption in HTTPS, sensitive information such as login credentials, personal details, and session tokens are exposed and can be easily captured by attackers.
3. No Certificate Exchange: HTTPS involves the exchange of SSL/TLS certificates between the client and the server to verify their identities and establish a secure connection. This step is completely absent in HTTP since there are no certificates involved. Therefore, there are no certificate-related messages exchanged between the client and the server in HTTP traffic.