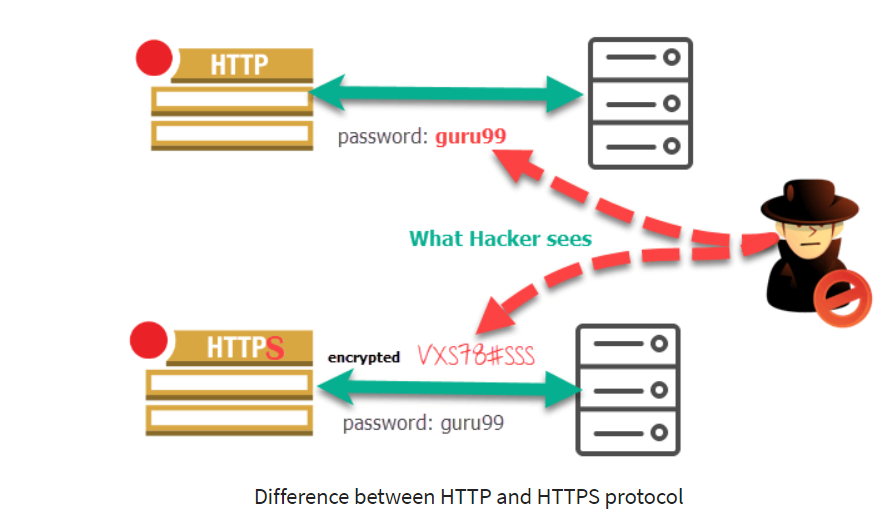
**HTTP and HTTPS protocols**



What is HTTP?

HTTP stands for **Hyper Text Transfer Protocol**. It is based on the TCP/IP protocol. The International Standard Organization has defined a model called Open System Interconnection or the OSI model that can be used in communication. This model helps to get an understanding of how communication occurs between the sender and the receiver. It is a layered model.  HTTP works in the application layer of the OSI model. It is used to deliver web pages. It is also possible to transfer text, audio, video, images using this protocol.

HTTP works according to the request and response cycle. For example, when the user or the client browses for pediaa.com, he is requesting a web page from the server. That request is sent to the server as an HTTP message. Then, the server responds back by providing the correct web page.



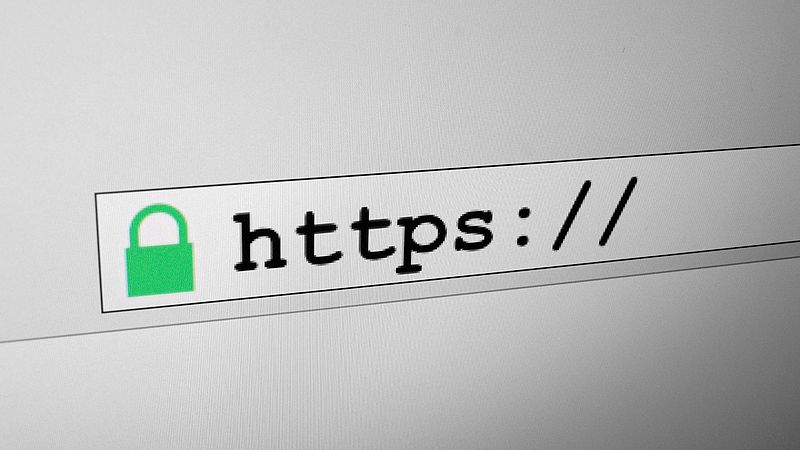
An **HTTP message** consists of three sections: start line, header, and body. The start line contains the method (GET, POST), URI (Uniform Resource Identifier), and HTTP version. The **URI** helps the server to find the location of the resource. The **header** contains the name, value pairs. There will be no content in the body section if it is a request.

The **HTTP response** also has the same three sections. There is no method or URI in the start line. The start line contains the HTTP version and the status code. The status code helps to inform the client whether the request is successful or not. The header contains the same information as in the request while the body section contains the requested file.

## What is HTTPS?

HTTPS stands for **Hyper Text Transfer Protocol Secure**. It transfers data securely via the network. HTTPS is also known as **HTTP over TLS, HTTP over SSL**and**HTTP secure**. The objective of designing this protocol is to improve privacy when communicating with websites. It is used in banking websites, online e-commerce websites, etc. It is also used in Google.com, Facebook, Twitter and many more.

To secure the website, the owner should purchase SSL (Secure Socket Layer) certificate. They are expensive and can be obtained by hosting companies. This SSL certificate is similar to an online identification card. This certificate also helps to encrypt the data to pass via HTTPS protocol.



When the user or the client requests a webpage, the server checks the SSL certificate. It verifies the identity of the website. Then the data is sent from the server to the client. The response message is encrypted at the server’s end and decrypted at the client’s end. An unauthorized party cannot read this message as it is encrypted. Therefore, HTTPS provides more security in communication.

## Types of SSL/TLS certificate used with HTTPS

Now in this HTTPS and HTTP difference tutorial, we will cover the types of SSL/TLS certificates used with HTTPS:

### Domain Validation:

Domain validation validates that the person who applies for a certificate is an owner of the domain name. This type of validation generally takes a few minutes up to a few hours.

### Organization Validation:

The Certification Authority not only validate the domain's ownership but also owners identify. It means that an owner might be asked to provide the personal ID proof document to prove their identity.

### Extended Validation:

Extended validation is a topmost level of validation. It includes validation of domain ownership, owner identity as well as registration proof of business.

## Difference Between HTTP and HTTPS

## 

## Advantages of HTTP:

* HTTP can be implemented with other protocol on the Internet, or on other networks
* HTTP pages are stored on computer and internet caches, so it is quickly accessible
* Platform independent which allows cross-platform porting
* Does not need any Runtime support
* Usable over Firewalls! Global applications are possible
* Not Connection Oriented; so no network overhead to create and maintain session state and information.

## Advantages of HTTPS

* In most cases, sites running over HTTPS will have a redirect in place. Therefore, even if you type in HTTP:// it will redirect to an https over a secured connection
* It allows users to perform secure e-commerce transaction, such as online banking.
* SSL technology protects any users and builds trust
* An independent authority verifies the identity of the certificate owner. So each SSL Certificate contains unique, authenticated information about the certificate owner.

## Limitations of HTTP

* There is no privacy as anyone can see content
* Data integrity is a big issue as someone can alter the content. That's why HTTP protocol is an insecure method as no encryption methods are used.
* Not clear who you are talking about. Anyone who intercepts the request can get the username and password.

## Limitations of HTTPS

* HTTPS protocol can't stop stealing confidential information from the pages cached on the browser.
* SSL data can be encrypted only during transmission on the network. So it can't clear the text in the browser memory
* HTTPS can increase computational overhead as well as network overhead of the organization.