**'Basic' HTTP Authentication**

This document defines the "Basic" Hypertext Transfer Protocol (HTTP)

authentication scheme, which transmits credentials as **user-id/**

**password pairs**, **encoded using Base64**

This scheme is not considered to be a secure method of user

authentication unless used in conjunction with some external secure

system such as **TLS** (Transport Layer Security, [[RFC5246](https://tools.ietf.org/html/rfc5246)]), as the

user-id and password are passed over the network as cleartext.

To receive authorization, the client

1. obtains the user-id and password from the user,

2. constructs the user-pass by concatenating the user-id, a single

colon (":") character, and the password,

3. encodes the user-pass into an octet sequence (see below for a

discussion of character encoding schemes),

4. and obtains the basic-credentials by encoding this octet sequence

using Base64 ([[RFC4648], Section 4](https://tools.ietf.org/html/rfc4648#section-4)) into a sequence of US-ASCII

characters ([[RFC0020](https://tools.ietf.org/html/rfc0020)]).

If the user agent wishes to send the user-id "Aladdin" and password

"open sesame", it would use the following header field:

**Authorization: Basic** QWxhZGRpbjpvcGVuIHNlc2FtZQ==

The **user's name is "test"**,

and the **password** is the string **"123"**

**followed by the Unicode character U+00A3 (POUND SIGN)**. Using the

character encoding scheme UTF-8, the user-pass becomes:

**'t' 'e' 's' 't'** ':**' '1' '2' '3' #**

74 65 73 74 3A 31 32 33 C2 A3

Encoding this octet sequence in **Base64** ([[RFC4648], Section 4](https://tools.ietf.org/html/rfc4648#section-4)) yields:

**dGVzdDoxMjPCow==**

Thus, **the Authorization header** field would be:

**Authorization: Basic** **dGVzdDoxMjPCow==**

Or, for proxy authentication:

Proxy-Authorization: Basic dGVzdDoxMjPCow==

The Basic authentication scheme is not a secure method of user

authentication, nor does it in any way protect the entity, which is

transmitted in cleartext across the physical network used as the

carrier.

The most serious flaw of Basic authentication is that it results in

the cleartext transmission of the user's password over the physical

network. Many other authentication schemes address this problem.

Because Basic authentication involves the cleartext transmission of

passwords, it SHOULD NOT be used (without enhancements such as HTTPS

[[RFC2818](https://tools.ietf.org/html/rfc2818)]) to protect sensitive or valuable information.

In HTTP Basic Auth, the application expects a header that contains a username and a password.

If it doesn't receive it, it returns an HTTP 401 "Unauthorized" error.

And returns a header WWW-Authenticate with a value of Basic, and an optional realm parameter.

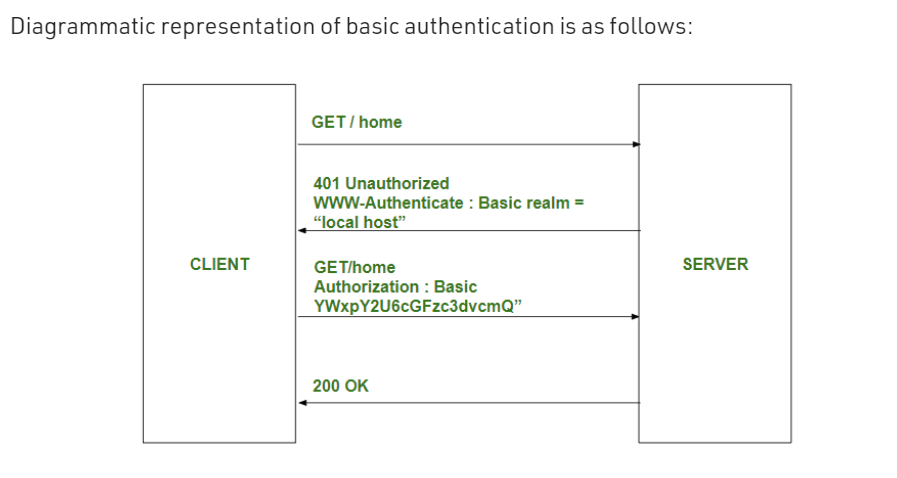
That tells the browser to show the integrated prompt for a username and password.

Then, when you type that username and password, the browser sends them in the header automatically.

As per section 4.1 of RFC-7235, when an HTTP server returns a 401 response, it must also return a WWW-Authenticate header :

1. A server generating a 401 (Unauthorized) response MUST send a
2. WWW-Authenticate header field containing at least one challenge.

The **HTTP WWW-Authenticate** response header defines the authentication method that ought to be wont to gain access to a resource. As discussed earlier, the **WWW-Authenticate header** is sent along with a 401 Unauthorized response



401 Response

You can also define the 401 “Unauthorized” response returned for requests with missing or incorrect credentials. This response includes the WWW-Authenticate header, which you may want to mention.