HTTPAuth Working Group
Internet-Draft
Updates: 2617 (if approved)
Intended status: Standards Track
Expires: March 17, 2014

J. Reschke
greenbytes

September 13, 2013

The 'Basic' HTTP Authentication Scheme
draft-ietf-httpauth-basicauth-update-00

Abstract

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

Editorial Note (To be removed by RFC Editor before publication)

Discussion of this draft takes place on the HTTPAuth working group mailing list (http-auth@ietf.org), which is archived at <http://www.ietf.org/mail-archive/web/http-auth/current/maillist.html>.

XML versions, latest edits and the issues list for this document are available from <http://greenbytes.de/tech/webdav/#draft-ietf-httpauth-basicauth-update>.

The changes in this draft are summarized in Appendix A.1.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 17, 2014.

Copyright Notice

Table of Contents

1. Introduction 3
2. Notational Conventions 3
3. The 'Basic' Authentication Scheme 3
4. Security Considerations 4
5. IANA Considerations 5
6. Acknowledgements 5
7. References 6
7.1. Normative References 6
7.2. Informative References 6
Appendix A. Change Log (to be removed by RFC Editor before publication) 7
A.1. Since RFC 2617 7
Appendix B. Open issues (to be removed by RFC Editor prior to publication) 7
B.1. edit 7
B.2. upd 7
B.3. enc 7
Index 8

1. Introduction

This document defines the "Basic" Hypertext Transfer Protocol (HTTP) Authentication Scheme ([draft-ietf-httpbis-p7-auth]). 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]), as the user name and password are passed over the network as cleartext.

The "Basic" scheme previously was defined in Section 2 of [RFC2617]. This document updates the definition, and also addresses internationalization issues.

Other documents updating RFC 2617 are "Hypertext Transfer Protocol (HTTP/1.1): Authentication" ([draft-ietf-httpbis-p7-auth], defining the authentication framework) and "HTTP Digest Update" ([draft-ietf-httpauth-digest-update], updating the definition of the '"Digest" authentication scheme).

2. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. The 'Basic' Authentication Scheme

The "basic" authentication scheme is based on the model that the client must authenticate itself with a user-ID and a password for each realm. The realm value should be considered an opaque string which can only be compared for equality with other realms on that server. The server will service the request only if it can validate the user-ID and password for the protection space of the Request-URI. There are no optional authentication parameters.

For Basic, the framework above is utilized as follows:

```
challenge   = "Basic" realm
credentials = "Basic" basic-credentials
```

Upon receipt of an unauthorized request for a URI within the protection space, the origin server MAY respond with a challenge like the following:

```
WWW-Authenticate: Basic realm="WallyWorld"
```

where "WallyWorld" is the string assigned by the server to identify the protection space of the Request-URI. A proxy may respond with

the same challenge using the Proxy-Authenticate header field.

To receive authorization, the client sends the userid and password, separated by a single colon (":") character, within a base64 [RFC2396] encoded string in the credentials.

```
basic-credentials = base64-user-pass
base64-user-pass  = <base64 [RFC2045] encoding of user-pass,
                    except not limited to 76 char/line>
user-pass   = userid ":" password
userid      = *<TEXT excluding ":">
password    = *TEXT
```

Userids might be case sensitive.

If the user agent wishes to send the userid "Aladdin" and password "open sesame", it would use the following header field:

```
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

A client SHOULD assume that all paths at or deeper than the depth of the last symbolic element in the path field of the Request-URI also are within the protection space specified by the Basic realm value of the current challenge. A client MAY preemptively send the corresponding Authorization header with requests for resources in that space without receipt of another challenge from the server. Similarly, when a client sends a request to a proxy, it may reuse a userid and password in the Proxy-Authorization header field without receiving another challenge from the proxy server. See Section 4 for security considerations associated with Basic authentication.

4. Security Considerations

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. HTTP does not prevent the addition of enhancements (such as schemes to use one-time passwords) to Basic authentication.

The most serious flaw in Basic authentication is that it results in the essentially 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) to protect sensitive or valuable information.

A common use of Basic authentication is for identification purposes -- requiring the user to provide a user name and password as a means of identification, for example, for purposes of gathering accurate usage statistics on a server. When used in this way it is tempting to think that there is no danger in its use if illicit access to the protected documents is not a major concern. This is only correct if the server issues both user name and password to the users and in particular does not allow the user to choose his or her own password. The danger arises because naive users frequently reuse a single password to avoid the task of maintaining multiple passwords.

If a server permits users to select their own passwords, then the threat is not only unauthorized access to documents on the server but also unauthorized access to any other resources on other systems that the user protects with the same password. Furthermore, in the server's password database, many of the passwords may also be users' passwords for other sites. The owner or administrator of such a system could therefore expose all users of the system to the risk of unauthorized access to all those sites if this information is not maintained in a secure fashion.

Basic Authentication is also vulnerable to spoofing by counterfeit servers. If a user can be led to believe that he is connecting to a host containing information protected by Basic authentication when, in fact, he is connecting to a hostile server or gateway, then the attacker can request a password, store it for later use, and feign an error. This type of attack is not possible with Digest Authentication. Server implementers SHOULD guard against the possibility of this sort of counterfeiting by gateways or CGI scripts. In particular it is very dangerous for a server to simply turn over a connection to a gateway. That gateway can then use the persistent connection mechanism to engage in multiple transactions with the client while impersonating the original server in a way that is not detectable by the client.

5. IANA Considerations

IANA maintains the registry of HTTP Authentication Schemes ([draft-ietf-httpbis-p7-auth]) at <http://www.iana.org/assignments/http-authschemes>.

The entry for the "Basic" Authentication Scheme shall be updated with a pointer to this specification.

6. Acknowledgements

This specification takes over the definition of the "Basic" HTTP Authentication Scheme, previously defined in RFC 2617. We thank John

Franks, Phillip M. Hallam-Baker, Jeffery L. Hostetler, Scott D. Lawrence, Paul J. Leach, Ari Luotonen, and Lawrence C. Stewart for their work on that specification, from which significant amounts of text was borrowed. See Section 6 of [RFC2617] for further acknowledgements.

7. References

7.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[draft-ietf-httpbis-p7-auth] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Authentication", draft-ietf-httpbis-p7-auth-23 (work in progress), July 2013.

7.2. Informative References

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246,

August 2008.

[draft-ietf-httpauth-digest-update] Shekh-Yusef, R. and D. Ahrens, "HTTP Digest Update", draft-ietf-httpauth-digest-update-05 (work in progress), September 2013.

Appendix A. Change Log (to be removed by RFC Editor before publication)

A.1. Since RFC 2617

This draft acts as a baseline for tracking subsequent changes to the specification. As such, it extracts the definition of "Basic", plus the related Security Considerations, and also adds the IANA registration of the scheme. Changes to the actual definition will be made in subsequent drafts.

Appendix B. Open issues (to be removed by RFC Editor prior to publication)

B.1. edit

Type: edit

julian.reschke@greenbytes.de (2013-09-11): Umbrella issue for editorial fixes/enhancements.

B.2. upd

In Section 3:

Type: change

julian.reschke@greenbytes.de (2013-09-12): Update the definition to reflect underlying changes (RFC2616->httpbis, RFC2396->2616, other references).

B.3. enc

In Section 3:

Type: change

julian.reschke@greenbytes.de (2013-09-12): Fix the encoding issue, by pulling in draft-ietf-httpauth-basicauth-enc.

Index

B
base64-user-pass 4
basic-credentials 4

C
challenge 3
credentials 3

P
password 4

U
user-pass 4
userid 4

Author's Address

Julian F. Reschke
greenbytes GmbH
Hafenweg 16
Muenster, NW 48155
Germany

EMail: julian.reschke@greenbytes.de
URI: http://greenbytes.de/tech/webdav/