HTTPAuth Working Group
Internet-Draft
Updates: 2617 (if approved)
Intended status: Experimental
Expires: January 8, 2014

R. Shekh-Yusef
Avaya

July 7, 2013

An Encoding Mechanism for HTTP Digest Authentication draft-ietf-httpauth-digest-encoding-02

Abstract

RFC2617 does not define how to treat Unicode characters [UNICODE] outside the ASCII range [RFC20] with the "Digest" scheme. This document defines an extension to the "Digest" scheme, and a mechanism that enables the client and server to negotiate their support for the UTF-8 [RFC3629] character encoding scheme.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1 Introduction

RFC2617 does not define how to treat Unicode characters [UNICODE] outside the ASCII range [RFC20] with the "Digest" scheme. This document defines an extension to the "Digest" scheme, and a mechanism that enables the client and server to negotiate their support for the UTF-8 [RFC3629] character encoding scheme.

The encoding impacts the way the server and the user agent concatenate the username-value, realm-value, and password when they calculate A1, as defined in section 3.2.2.2 of RFC2617.

1.1 Terminology

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 RFC 2119 [RFC2119].

Several terms used in this document are defined in [RFC6365] and [UNICODE].

2 The "charset" auth-param

The "Digest" mechanism allows for new parameters to be defined and used with Authenticate and Authorization headers. This document defines a new optional "charset" auth-param that could be used by the client and the server to indicate the encoding scheme they support.

The only allowed value is "UTF-8", to be matched case-insensitively.

3 Mechanism

When a user agent attempts to access a resource and get challenged by the server, the server will indicate it supported encoding scheme, and in response the user agent will indicate whether it supports that encoding scheme or not in the subsequent request it sends to the server.

3.1 Server Behavior

In challenges, servers MAY use the "charset" authentication parameter (case-insensitive) to express the character encoding they expect the user agent to use.

When the server receives the subsequent request with the Proxy-Authenticate or WWW-Authenticate header fields, it looks for the "charset" parameter. If the "charset" parameter is present, and its value matches the encoding the server sent to the client, the server will continue with its normal operation using the encoding it sent to the client. If, on the other hand, the "charset" parameter value is preceded by an exclamation point (!), the server can immediately decline the request.

If the new request with the Proxy-Authenticate or WWW-Authenticate header fields does not have the "charset" parameter, the server will know that it is dealing with a client that does not support this specification and should continue to perform its current operation.

3.2 Client Behavior

A user agent that follows this specifications MUST NOT include the "charset" parameter in any subsequent request if it did not receive it from the server in a challenge.

If the user agent supports the encoding indicated by the server, it SHOULD add the "charset" parameter, with the value it received from the server, to the Proxy-Authenticate or WWW-Authenticate header fields it sends back to the server.

If the user agent does not support the encoding indicated by the server, it SHOULD add the "charset" parameter to the Proxy-Authenticate or WWW-Authenticate header fields it sends back to the server, but the value in the parameter should be preceded by an exclamation point (!).

A user agent that does not follow this specification will ignore the parameter and will not include it in any subsequent request.

4 Security Considerations

<Security considerations text>

5 IANA Considerations

<IANA considerations text>

6 Acknowledgments

The author would like to thank Julian Reschke for his help and comments on and off the list, and for the idea of using the "auth-param" to indicate the supported encoding, as described in his document that deals with the encoding for the Basic scheme.

The author would also like to thank Bjoern Hoehrmann, Paul Hoffman, and Martin Durst for their comments on the mailing list, and Peter Saint-Andre for his comments and text that clarified the scope of the document.

7 References

7.1 Normative References

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

[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.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC6365] Hoffman, P., Klensin, J., "Terminology Used in Internationalization in the IETF", BCP: 166, RFC 6365, September 2011.

[UNICODE] The Unicode Consortium, "The Unicode Standard, Version 6.0". <http://www.unicode.org/versions/Unicode6.0.0/>.

[RFC20] Cerf, V., "ASCII format for Network Interchange", RFC 20, October 1969.

Authors' Addresses

Rifaat Shekh-Yusef
Avaya
250 Sydney Street
Belleville, Ontario
Canada

Phone: +1-613-967-5267
Email: rifaat.ietf@gmail.com