Basic Authentication Log Out

v1.0 June 2002

Maven Security Consulting, Inc.
PO Box 37635 PMB 50645
Philadelphia, PA 19101-0635
http://www.MavenSecurity.com

Introduction

This paper describes how you could clear HTTP Basic Authentication credentials from a browser without requiring the user to close their browser.

> *It should be noted that there are no official HTTP/HTML mechanisms for clearing user credentials from a user's browser when basic authentication has been used. Therefore, the method described in this document is offered as a technically feasible sign-off method. However, whether this technique is "user-friendly" and viable for large-scale production systems is not guaranteed. As with any design changes, performance and user acceptance testing will be required before deploying into production.*

Background

Web browsers store Basic Authentication credentials in memory. The credentials are associated with a specific web site and realm name. The **realm name** is an arbitrary name set by the web server to define a specific area of a web site. This is useful if partitioning a site into different areas. The realm name is shown to the user when they are prompted to enter their user name and password.

Figure 1 - Sample Prompt for Basic Authentication

.htaccess

For example, to restrict access for the directory `/~chris` to only the user **Chris**, you could use a `.htaccess` file (for Apache).

The `.htaccess` file would look something like this:

```
AuthType Basic

AuthName UserArea

AuthUserFile /usr/local/apache/conf/users

<Limit GET POST>

Require user Chris

</Limit>
```

Later, if you wanted to clear Chris' name and password from the browser, you will need to create two "Logout" links in series (i.e. the first link leads to a page that contains the second link). The first would lead to a page that instructed the user (e.g. Chris) to click on the link below (the second and last “Logout” link) and enter "EXIT" as the user name and password when prompted. Explain to the user how this will erase over the real credentials in the browser's memory, making it impossible for someone to steal them from the PC at a later time.

(Alternatively, this page can simply explain that the browser needs to be shutdown completely in order to clear the credentials. Therefore, the rest of this paper is moot.)

Now, when the user clicks on this second link it should point to a directory (let's call it `/LOGOUT`) that has the following `.htaccess` file:

```
AuthType Basic

AuthName UserArea

AuthUserFile /usr/local/apache/conf/users

<Limit GET POST>

Require user EXIT

</Limit>
```

The browser only tracks the credentials by site name and realm name (both of which are the same as before - "UserArea" is the realm name in this example). Therefore, this new "sign-on" attempt (for the user named EXIT) will write over the old credentials in the browser’s memory. Since only the user called "EXIT" (with a password of “EXIT”) is

acceptable to enter this directory (/LOGOUT), this prevents Chris (or any other user) from accidentally entering a valid account name and password. The web site would continue to prompt the user until they entered the correct user name and password (i.e. EXIT/EXIT).

This method requires the creation of a user with the name "EXIT" and the password as "EXIT". The `index.html` file for the `/LOGOUT` directory is the document that will be shown to the user after they enter "EXIT" in the Basic authentication dialog box. Therefore, the `index.html` file could contain some sort of "success" message, such as "You have successfully cleared your user name and password from memory – thanks for using Basic Authentication ;-)."

Unfortunately, this method requires the user to take several steps. If the site enforces a lockout mechanism to prevent brute-force attacks (and it should), this could cause problems if someone accidentally (or intentionally) locks the EXIT user. Therefore, the lockout mechanism for the EXIT user should not be enforced.

Unfortunately, if the user leaves their computer unattended, forgetting to logout, there does not appear to be any way to remotely clear the HTTP Basic authentication credentials from the browser. Java or JavaScript could be used to automatically request the logout URL, but it cannot enter the required user name and password (i.e., EXIT) into the dialog box in order to write over the cached credentials.