Referring URL authentication

Heading

When a user clicks on a link in a web page, the user's browser moves to the specified link. When the browser requests the new page, it sends along the URL of the previous page. This "sent along" URL is called a referring URL. When users click on EZproxy starting point URLs, EZproxy can check the referring URLs and choose to automatically authenticate them without presenting the login screen. From the users' perspective, they simply click on links that lead to databases.

You can enable referring URL authentication by editing user.txt and adding one or more lines similar to these:

::referer=http://www.yourlib.org/*
::referer=http://www.yourlib.org/login/*
::referer=http://www.yourlib.org/login/password.cgi

These lines proceed from most liberal to most specific. The first line would match any URL from the specified web server, the second would match any URL from the login directory (or any directory below it), and the third would match only the exact URL specified. In some instances, the URL may end up with the default port of 80 included, so you should make two entries in user.txt, one as above, and one with the explicit port. For example, if you were using the general form from above, you would also want to make the entry:

::referer=http://www.yourlib.org:80/*

Your user.txt file may have as many referring URL entries as desired to match all the possible web servers that may be referring users. However, you should only list referring URLs that come from authenticated sources.

When it works, and when it doesn’t

When referring URL works, it is very convenient and handy. It can be used in conjunction with systems like WebCT, it can provide a seamless, transparent authentication environment. However, you must plan to deal with instances where it will not work.

If you use only referring URL login, these problems can occur.

1. If users create bookmarks and try to use them after their EZproxy session has expired, they will not be authenticated and will end up seeing the login.htm page.
2. Some users run security software that suppresses the sending of the referring URL. In these instances, no referring URL is sent, so the user will not be authenticated and will again see the login.htm page.
3. If users know you are using referring URL authentication and know or can guess the URL you use to check authentication, then they could choose to fool EZproxy into believing it was receiving a referring URL from one of your servers without actually connecting to that server at all. This is an inherent security risk in using referring URLs.
In your login.htm page, it is important to provide information for users in these scenarios, and either provide them with an alternative way to login, or at least tell them that they must connect to databases from your referring URLs.