

Basic Authorization Security Issue?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-10/2682.html>

From: Hector Santos (*nospam_at_nospam.com*)

Date: 10/28/03

Date: Mon, 27 Oct 2003 23:37:09 -0500

I find the following to be an unbelievable claim by a IE user, but is the following possible?

I have a customer using our intranet who is saying he is having a Basic Authentication security issue with his setup. He says (paraphrased):

"Even if I close the browser, when I restart it, I can immediate log into the web server again without any basic authorization IE POPUP Dialog login box. It seems like closing the browser is not releasing the credentials as you say it should when the browser is closed."

What gives? Is this possible? I gave even reason to indicate that this claim with be a major issue with IE and thus since no one else is reporting it, I find it hard to believe.

Today, he confirmed it again saying he has not been to our support web site in days and today he restarted the browser, went to our web site and he was immediately logged in again with any login dialog problem.

I checked our web logs and sure seems to confirm his claim.

When an non-authorized URL request in our intranet web server is attempted, an 401 Authorization Error is sent for the response. This forces the browser to popup the Basic Authentication login dialog box. The request is resent with the basic authorization credentials and the user is logged in. The only possible way the web server can get the user account name and password is with the HTTP standard Authorization: Basic line.

Based on the web logs, I am seeing the first URL from this specific guy as a successful authorized request thus somewhat validating his claim. The reference URL does not any login information (i.e, <http://user:pwd@domain.com>). Even if it was, you can only pass the username/password on the url using a special URL alias that redirections them. I don't have my detail socket trace enabled so I can't see/validate the GET request block having the authorization header line, but it has to be there if he is logged in with this request which is verified with his user

microsoft.public.security: Basic Authorization Security Issue?

name logged.

```
X.Y.Z.W - MARK XXXXX - [27/Oct/2003:22:44:06 -0500] "GET / HTTP/1.1" 302 141
"http://www.santronics.com/" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; .NET CLR 1.0.3705; .NET CLR 1.1.4322)" XXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Based on the WEB log entry, he is using the IE browser:

(compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705; .NET CLR 1.1.4322)

Is this possible with IE? It is a known issue?

```
--
Hector Santos
WINSERVER "Wildcat! Interactive Net Server"
support: http://www.winserver.com
sales: http://www.santronics.com
```