

RE: passwords in asp pages

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-03/0323.html>

From: Miller, Joe (joe.miller_at_us.mizuho-sc.com)

Date: 03/10/04

Date: Wed, 10 Mar 2004 14:07:31 -0500
To: <SECURITY-BASICS@securityfocus.com>

You didn't specify the details about version, but here is a solution that might work well for you. You can create a COM class that handles all database related calls. For instance, the class can hand out ADO connections based off of some criteria. The asp pages will do nothing about the specifics of the connection other than the type (ie. by type I mean it knows to connect to DB XYZ on SQL Server). All the specifics about the connection (server, db, user, password) are managed by the COM DLL.

You can now do:

```
<% Set oDBCClassFactory = CreateObject("MyDBExpert.ClassFactory")
   Set oADODConn = oDBCClassFactory.getConnection(enumWhichDB) %>
```

The details about the connection are now abstracted behind the Class Factory interface. In general, sprinkling connection specific properties about your asp (or any client code), is not recommended. It is much better to delegate this responsibility to a connection expert class. This is not only better in terms of security, but improves the overall maintenance of the system (ie. only need to manage connections in one place).

Hope this helps.

-----Original Message-----

From: [mailto:ian@kingcon.com]
Sent: Tuesday, March 09, 2004 9:00 AM
To: SECURITY-BASICS@securityfocus.com
Subject: passwords in asp pages

I am new to security and I have no training in asp programming, so I am wondering if I am right in being scared of the following instance...

A IIS based website which has asp pages which contain plaintext passwords for credentials to an sql database on another machine. The passwords are in between <% %> so I assume that means they are only processed on the server and the user does not see them, and there do not

SecurityFocus BASICS: RE: passwords in asp pages

seem to be any .inc files calling these pages. The server is also up to date with patches as far as I know.

This situation really bothers me, but I'm not experienced enough to know how it could be exploited or whether it could be exploited at all. I just don't like the fact that passwords to a db user are scattered all over the website. I need something to make it easy to say to the people responsible... "Here look this is what can be done to the website to gather the passwords and destroy your data. I don't think it is wise you do this, it is in your best interests to change this pattern." The programmer seemed to just brush it off, when I said that they could be viewed if their source was viewed, by telling me that they would be only processed by the server itself, which still doesn't make me feel good at all.

Shouldn't the password be encrypted? Separated in their own file?

Is it correct to assume that an attacker who elevated their privileges on the web box could view these files and gain access to the database that way through some other method?

What else can be done by an attacker against asp pages that would allow this data to be discovered?

Also if I could actually just demonstrate it right before their eyes that would be a big help.

Thanks for any advice.

Ian
:)

Go to www.missingkids.com

Though the words, opinions, and/or policies expressed herein are probably right, and most likely right if you disagree with them, they are the personal words, opinions, and/or policies of the person using this account. They are not, and the author does not claim they are, the words, opinions, and/or policies of the company and officers of Merrill Information Systems Inc., any forum they are placed in, or any entity other than the author himself that they may appear to represent. That being said, the author probably thinks they should be the opinion of those bodies, unless he is playing the devil's advocate.

Send complaints or compliments to the author at:

ianian@333ki-ngc.on.com

Taking out all numbers and spaces and the first ian in the address, because spammers use bots, some mailing lists block this information from prying eyes, and people who pay attention can follow instructions.

RE: passwords in asp pages

SecurityFocus BASICS: RE: passwords in asp pages

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:
http://www.infosecinstitute.com/courses/ethical_hacking_training.html

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:
http://www.infosecinstitute.com/courses/ethical_hacking_training.html
