

## RE: passwords in asp pages

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-03/0309.html>

---

**From:** Mike (mike\_at\_superiorholidayadventures.ca)

**Date:** 03/10/04

Date: Wed, 10 Mar 2004 08:25:06 -0500  
To: <SECURITY-BASICS@securityfocus.com>

> *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...*

Welcome. I'm rather new myself, and am finding security to be an interesting "field". I put field in quotes, because I feel that it's something that should be incorporated by everybody and isn't just for specialists.

> *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 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.*

## SecurityFocus BASICS: RE: passwords in asp pages

Well, even if it's not exploitable today, it could be tomorrow by a vulnerability that's yet to be uncovered. Or worse yet, the vulnerability is 0day; unknown to vendors, but known to "hackers".

If this was done on a machine before Code Red, it may not have been "possible" to view the contents (or download) .asp files. CR and it's variants showed the weaknesses in IIS' unicode processing and it would have been very simple to download the .asp pages once that vulnerability was known.

You don't mention what version of IIS this is, what OS, and what the patch-level is. If it's NT4 or 2000 and unpatched, you may still be vulnerable.

As well, be aware that internal users may be able to gain access to this file. Do you have any wireless devices on this network?

I'm familiar with web-programming, and experience says to at least store the username/password combo in the database. Encrypting the username/password in the db would be a very good next step. A third step would be to encrypt the transmission using SSL.

Everyone: Am I missing anything else above?

> *Shouldn't the password be encrypted? Seperated in their own file?*

Yes, get them out of the .asp page and put them somewhere more secure.

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

Yes, be sure too that your db server is secured/patched/not accessible through the internet.

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

I'm sure there are all kinds of attacks. OWASP.org may be a good resource to look into.

Good Luck,

Mike Fetherston

---

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

RE: passwords in asp pages

## SecurityFocus BASICS: RE: passwords in asp pages

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](http://www.infosecinstitute.com/courses/ethical_hacking_training.html)

---