A5 Security Misconfiguration Lab

Mounting an attack

Put on your black hat and pretend we're going to try to break in. You got a hot tip that there was a list of users in clear text inadvertently saved in our web site.

1. Open a browser window and point it to the root of our legitimate website.
2. Now alter the url and add some filenames where this file might be. Try users.out, users.list, users.txt, users.db, etc. (Hint: if you can't find it, go ahead and look in Visual Studio at the root of our website).
3. Once you find it, look through it for some usernames to try.
4. Grab each of those names and try logging in to our site with them. Guess at some passwords. Try "password". Try the username with "123" added to it. Try the username itself and a few more.

Once you're logged in as a user you can move to the next step.

5. Again, take a look around the website in Server Explorer. Do you see any pages that you might be able use to mount other attacks? Write them down here:

_____
_____

6. Navigate to AddUserTemp.aspx. What does it do?

_____
_____

7. Add an administrative user or two. Try logging in as that user. Can you? ____ If he/she is an administrative user, can't you use that account to create more? ____

You might be shocked at how many sites out there have existing holes like this.

Hardening the site

All we would have needed to do to stop this attack is break any part of the chain. If the old users were removed, if the configuration file were gone, or if the old page were removed, the attacker could have been thwarted. Let's do all three.

8. Look through the entire website. Do you see any suspicious or unneeded files? Write them down below. They'll be candidates for deletion after you check with your team members to make sure nobody has need of them anymore.

_____
_____

9. Now look for old, unused pages. What are some of these?

_____
_____

10. Now open the users table. Look through the users, especially administrative users. Wait, wasn't John Effortson fired a couple of months ago? And kmitnick had to leave us for, umm, other reasons. Shouldn't their website credentials be either disabled or completely deleted? Write down these guys and any others you discover that can be deleted.

_____
_____

11. Now that you have some lists, gather your team members and make sure they're alright with you deleting these resources. (Hint: Include your instructor in your team if you're unsure of which resources can be removed.)

Once you have a clean site, you can be finished with this lab.