

# Re: Security controls in a web application

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-07/msg00179.html>

---

- *From:* "Roger Abell [MVP]" <[mvpNoSpam@xxxxxxx](mailto:mvpNoSpam@xxxxxxx)>
  - *Date:* Mon, 23 Jul 2007 23:46:33 -0700
- 

You do not state what accounts are being used.

In general, one may be better off passing account management tasks to the operating system or database server (SQL 2k5 at least; Oracle ??) rather than attempting to reinvent the whole as a one man show.

"Big Charles" <[cherediatech@xxxxxxxx](mailto:cherediatech@xxxxxxxx)> wrote in message  
[news:1185154492.526010.247340@xx](mailto:news:1185154492.526010.247340@xx)

Hello,

I have developed a web application in .NET that interacts with Oracle database. Now this app is been audited according to security issues of ISO 17799.

I'm afraid that my web app is lacking of many security controls.

I have implemented some security controls like a login page that asks for userid and password in order to access the web app. Also, every web page calls a stored procedure when is loaded. That SP consults if the userid is allowed to access that web page.

However, there are many other security controls that I didn't know. For example, a guy asked me if the login page controls how many times can somebody try to login. If somebody tries to login more than three times with no success, then the user account has to be blocked for some time. That is in order to avoid hacking, because somebody can use some program to generate random passwords and trying to login over and over until it succeeds.

My question is: Is there any practical guide to follow about what security controls must be implemented in a web application that interacts with database? I think it should exists, like:

- Passwords have to have 6 alphanumeric characters at least.
- If the user logs in for the first time, the application has to force him to change his password.
- If the user tries to login more than three times unsuccessfully, then the account has to be blocked
- etc, etc

Re: Security controls in a web application

Thank you very much!