Security Questions for Web Apps

1. Are all client-server communications protected by a well-established cryptographic technology, such as SSL?
2. Is your input validation done on the client-side, the server-side, or a combination of both?
3. Do you perform the same input validation steps on both the client-side and server-side, or are additional validation methods applied on the server-side?
4. Do you expose any authentication scripts to the user? This includes scripts that are reachable by viewing the page source.
5. If you do expose authentication scripts, are these scripts obfuscated?
6. Do you remove developer comments from all code viewable by the client?
7. Do you lock accounts after a defined number of failed login attempts?
8. If you do lock accounts, what message do you present to the user notifying them that the account has been locked?
9. If you do lock accounts, how do you determine how many attempts a user can try before being locked out of their account? By storing a cookie with a count that's incremented? By incrementing a server-side variable based on an open session?
10. Do you expose usernames on your site?
11. Do you require unique usernames?
12. Do you provide an encrypted HTTP connection to transmit authorization credentials?
13. Do you transmit user credentials as query string parameters or in the POST request?
14. Do you store user credentials in cookies on the client?
15. Do you switch to HTTPS when the login page is loaded in the browser?
16. Do you require users to change their passwords periodically?
17. Do you allow users to recover forgotten passwords?
18. Do you limit the number of attempts a user can answer a password recovery challenge question?
19. Do you use any "remember me" functionality? If you do, do you store only nonsecret items, such as usernames?
20. Does your account registration page disallow an infinite number of registration attempts?
21. Do you support user impersonation for helpdesk staff?
22. Do you use a multi-stage login? If yes, do you store all information from earlier stages on the server while the login session is in progress?
23. Does your authentication process use any CAPTCHA controls?
24. Does the application log all authentication-related events, including login, logout, password change, password reset, account suspension, and account recovery?