SearchSecurity.com
Security School

Web Security School Lesson 3 Quiz

By Michael Cobb

1.) Which is the best directory structure for a Web site that includes static and dynamic content?

a. E:\inetpub\wwwroot\mywebsite

b. C:\inetpub\wwwroot\mywebsite

c. E:\inetpub\wwwroot\myserver\scripts
E:\inetpub\wwwroot\myserver\static

d. C:\inetpub\wwwroot\myserver\scripts
C:\inetpub\wwwroot\myserver\static

e. E:\inetpub\wwwroot\myserver\executables
E:\inetpub\wwwroot\myserver\static

2.) Which option is not a reason for validating data received from a Web form before processing it?

a. The user might have misspelled their name
b. The user might have entered an invalid date
c. The data may contain malicious code
d. The data may be of the wrong type
e. None of the above

3.) True or False: Hidden form fields are a safe way to pass sensitive information from one form to another.

4.) Your Windows IIS Web server has been attacked and you think the hacker has gained access to your database server that contains customer details and orders received via the Internet. What is the first thing you should do?

a. Disconnect all compromised machines from your network
b. Reboot the server and log on as the local administrator
c. Consult your security policy
d. Determine if the Web server is running a network sniffer
e. Create a backup of your system

5.) Even if your Web server is initially set up in a perfectly secure and pristine state, it will degrade over time. Which factor can speed up this degradation?

a. Using Windows IIS instead of Linux
b. Having a very popular Web site
c. Having a lot of administrators with access to the server
d. Having regular vulnerability assessments
e. Regularly changing the contents of the home page

Answers

1.) **The correct answer is:**
c. E:\inetpub\wwwroot\myserver\scripts
E:\inetpub\wwwroot\myserver\static
You must put your Web content on a separate volume or drive from your operating system, so the answers with directories located on the C drive are incorrect. In order to follow the principle of least privilege, you must separate your scripts from your static content so that only files in the scripts directory are given permission to execute. Finally, you do not want to give executables permission to run on your Web server.

2.) **The correct answer is: a. The user might have misspelled their name**
All data received from a Web form needs to be checked to ensure that the required date has been entered, that it is the correct type of data (for example numerals and not characters) and that it does not contain malicious code. You may want to check that the user

has entered their name but unfortunately, you have no way of knowing whether they have misspelled it.

3.) **The correct answer is: False**
The value of a hidden form field can be easily read by anyone viewing the page source. An attacker can look through Web pages stored in a computer’s cache and use or change the value in order to try to fraudulently access other information. The correct way to handle sensitive information is by using session variables or a temporary database record.

4.) **The correct answer is: c. Consult your security policy**
The first thing you do if you suspect that your system has been compromised is consult your security policy. Your security policy will contain the procedures to follow to deal with the compromise. If you do not have a security policy you should immediately consult with management to ensure the recovery effort can be coordinated with other departments such as the media and legal teams. The next step is to regain control of your system, which involves the other options listed.

5.) **The correct answer is: c. Having a lot of administrators with access to the server**
The more people who have access to a system, the faster it will degrade. Therefore, the more administrators you have, the more often you should audit. Security scanning helps you audit the system to verify that your intended configuration is effective and up to date.