



## Web Security School Lesson 1 Quiz

By Michael Cobb

- 1.) Which of the following is not considered a strong password?
  - a. WfgHLM94SED
  - b. xD\$8sf!H
  - c. 9Q-^g4FP7
  - d. P3t3rWh!t3
  - e. They are all strong passwords.
  
- 2.) Which is the correct physical boot sequence for a Web server?
  - a. Floppy Drive, Hard Drive, CD-ROM
  - b. CD-ROM, Hard Drive, Floppy Drive
  - c. Floppy Drive, CD-ROM, Hard Drive
  - d. Hard Drive, Floppy Drive, CD-ROM
  - e. CD-ROM, Floppy Drive, Hard Drive
  
- 3.) A Windows-hosted Web site displays dynamic pages using server-side scripting such as Active Server Pages or PHP. It also displays static pages with the .htm file extension. What are the correct IIS settings for the Web site?
  - a.
    - Script source access: enabled
    - Read: enabled
    - Write: enabled
    - Log visits: enabled
    - Execute Permissions: Scripts only
  
  - b.
    - Script source access: disabled
    - Read: enabled
    - Write: disabled
    - Log visits: enabled
    - Execute Permissions: None

- c.
  - Script source access: disabled
  - Read: enabled
  - Write: disabled
  - Log visits: enabled
  - Execute Permissions: Scripts only
  
- d.
  - Script source access: disabled
  - Read: enabled
  - Write: disabled
  - Log visits: enabled
  - Execute Permissions: Scripts and Executables
  
- e.
  - Script source access: disabled
  - Read: disabled
  - Write: disabled
  - Log visits: enabled
  - Execute Permissions: Scripts only

4.) An administrator needs to provide FTP services so that clients can download product documentation and sales people can upload their expense and meeting reports. Which is the correct FTP directory configuration?

- a.
  - Local Path: c:\inetpub\ftproot\files\
  - Read: enabled
  - Write: enabled
  - Log visits: enabled
  
- b.
  - Local Path: e:\inetpub\ftproot\files\
  - Read: enabled
  - Write: disabled
  - Log visits: enabled
  
- c.
  - Local Path: e:\inetpub\ftproot\clients\
  - Read: enabled
  - Write: enabled
  - Log visits: enabled
  - Local Path: e:\inetpub\ftproot\sales\
  - Read: enabled
  - Write: enabled
  - Log visits: enabled

- d. Local Path: e:\inetpub\ftproot\clients\  
Read: enabled  
Write: disabled  
Log visits: enabled  
Local Path: e:\inetpub\ftproot\sales\  
Read: enabled  
Write: enabled  
Log visits: enabled
  
- e. Local Path: e:\inetpub\ftproot\clients\  
Read: enabled  
Write: disabled  
Log visits: enabled  
Local Path: e:\inetpub\ftproot\sales\  
Read: disabled  
Write: enabled  
Log visits: enabled

5.) John Doe is responsible for the content of your Web site and its back up. Which are the correct group accounts to which John should belong?

- a. Power Users, Backup Operators and Administrators
- b. Content Managers, Backup Operators and Administrators
- c. Content Managers and Backup Operators
- d. Content Managers and Administrators
- e. Power Users, Content Managers and Backup Operators

-----  
ANSWERS

1.) **The correct answer is: a. WfgHLm94SED**

This password does not include any punctuation marks. A strong password is at least eight characters long, and is a combination of alphanumeric characters and punctuation marks.

2.) **The correct answer is: d. Hard Drive, Floppy Drive, CD-ROM**

The other boot sequences would allow someone who gained physical access to the Web server to try to bring the system up into a different OS than the one installed on the server. Only option d. prevents booting from removable media. Remember that you need to protect access to your BIOS settings with a password.

3.) **The correct answer is:**

c. **Script source access: disabled**

**Read: enabled**

**Write: disabled**

**Log visits: enabled**

**Execute Permissions: Scripts only**

Visitors to your site need to be logged, so Log visits needs to be enabled. They also need Read permission to view static .htm pages, and they need to be able to execute scripts so that the dynamic pages can be created. Visitors to your site should never be granted permission to execute programs or executables. Script source access should never be enabled on a live Web server because it allows users to access your pages' source code.

4.) **The correct answer is:**

e. **Local Path: e:\inetpub\ftproot\clients\**

**Read: enabled**

**Write: disabled**

**Log visits: enabled**

**Local Path: e:\inetpub\ftproot\sales\**

**Read: disabled**

**Write: enabled**

**Log visits: enabled**

This configuration means that clients can only access files in the clients directory and that sales people can only upload files to the sales directory. All FTP activity is being logged. The other configurations either don't provide separate sites directories for each type of account, or they give read and write permission on the same directory.

**5.) The correct answer is c. Content Managers and Backup Operators**

If John belongs to any of the other sets of group accounts, he has more permissions than he actually requires to perform his job. An even better application of this rule of least privileges is for John to have two accounts, one as a member of the Content Managers group and one as a member of the Backup Operators group. He can log on using the Content Managers account to manage the site's content and log on using the Backup Operators account to perform backup operations.