

WebMCQ Security Issues

This document offers an easy-to-understand, non-technical overview of important security measures implemented in WebMCQ software. It will help you understand why security has the potential to create so many problems on the Internet, and how WebMCQ addresses those potential problems.

1. Introduction

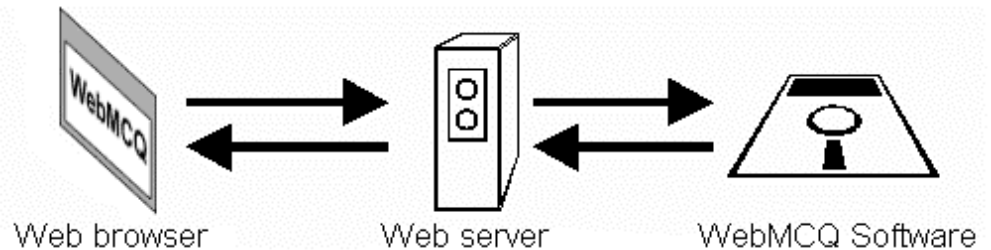
One of the primary concerns about any important data transactions made over the Web is **security**. While the Internet provides unprecedented possibilities for communication, it also brings with it the potential for individuals to attempt to gain unauthorised access to private information. One of the reasons that security is so problematic on the Internet is that it is often made the responsibility of individuals who do not have the time and resources to implement effective security policies. Good security management requires an up-to-the-minute specialist knowledge of the latest threats, software flaws and security holes in Internet protocols. As a teacher, academic or researcher who just wants to provide access to material over the Web, the task of effective security management is daunting and unreasonably difficult.

Fortunately, there is a solution - leave security management to Internet security experts so that you can get on with the job of creating and managing questions. With WebMCQ's service-based approach, we can advise on the best security policies to implement in your particular situation, and we will then implement those policies for you. It's all part of our service.

2. Types of Security

As an administrator of Web-based questions, you are really interested in two types of security - **Transaction Security**, and **Database Security**. The first term refers to the security of information as it is sent across the Internet, and the second refers to the safety of that information once it has been stored on an Internet computer. We will look at both types of security in detail below, and examine how WebMCQ works at all times to prevent unauthorised access to your material.

Before being able to properly appreciate the security measures implemented in WebMCQ, you will benefit from a basic understanding of how the WebMCQ system works. There are essentially three parties to every Web transaction involving WebMCQ - the Web browser, the Web server, and WebMCQ Software (actually, there are many more intervening parties that pose security problems, but these will be discussed later). As shown in the figure below, a web transaction starts with a request for information from the Web browser. This request for information is then passed via the Internet to a Web server (think of the Web server as a computer program whose job it is to listen out for information requests and respond to them). If the Web browser's request is a request for WebMCQ content, the Web server passes this request on to the WebMCQ Software. The WebMCQ Software examines the request, and if the request is deemed authentic and valid, will send appropriate information back to the Web server, which in turn passes that information to the original Web browser.



So, in summary, every WebMCQ transaction involves information being sent back and forth between a Web browser and WebMCQ Software. Since the Web browser and WebMCQ Software do not know how to talk to one another directly, the Web server acts as a 'mediator' to translate requests and responses between them.

3. Transaction Security

Transaction Security is the term used here to refer to the safety of information as it is being sent across the Internet, and the need to protect information from persons attempting to 'break into' the WebMCQ system and thereby access information that they should not have access to. Because it has been designed for use in several different situations, WebMCQ can operate at different levels of security. There are three levels of security in total, and depending on how much security you need, WebMCQ can implement security at one, two, or all three levels.

The levels of transaction security are:

(a) The Software Level - WebMCQ software has several security measures built-in, to prevent unauthorised access to information, and to allow you to restrict access to particular individuals if you so wish. This includes the ability to protect access to your questions by setting passwords, and limiting what is acceptable for valid User ID entries. Behind-the-scenes, WebMCQ also embeds several invisible encrypted letter strings in each transaction that store information about who is accessing a question, at what time, from which computer, and what information they are allowed to access. If anybody attempts to gain unauthorised access to the system, WebMCQ will know because the encrypted letter string will not match the unauthorised configuration.

(b) The Web server Level - Our Web servers make powerful additional security measures available to WebMCQ. These include a second (even more secure) level of password protection, and the ability to limit access only to particular computers.

(c) The Web Protocols Level - A special protocol called **Secure Sockets Layer** was developed several years ago to allow secure communication between Browsers and Web servers. This is the protocol used to protect financial transactions and other sensitive information on the Web. It is an extra layer of security whereby all requests are encrypted before being sent by the Web browser. Only the Web server being contacted knows how to decode the request, which it then does before passing the request on to WebMCQ Software. When WebMCQ Software sends its response to the Web server, the Server again encrypts the information in a way that only the original Web browser is able to decode.

It was mentioned above that in addition to the three major parties to every WebMCQ transaction, there are actually a large number of other parties involved. Those parties are any number of Internet computers that receive information as it travels along the Internet between the Browser and the Server. This creates potential problems because unknown persons could potentially 'eavesdrop' on information being sent between the Browser and the Server. Secure Sockets Layer encryption solves this problem very effectively, because anybody who attempts eavesdrop on information will only see random-looking encrypted data - only the intended recipient of data knows how to decode it.

4. Database Security

Database security is the term used to refer to the safety of information stored on our Internet computers once WebMCQ questions have been created and after data from those questions has been collected. WebMCQ works by storing all data on our central computers, so that question administrators have convenient and immediate access this data via the Web. As an administrator concerned with security, you not only need to know that information is protected while it is being sent across the Internet - you also need to be sure that once it is stored on a computer, it cannot be accessed from there by unauthorised persons. Again, WebMCQ works to prevent unauthorised access in several ways:

(a) Physically-Secure Machines - WebMCQ computers are always held in physically secure locations, so that direct access to them by intruders is prevented. In addition, the physical location of our computers always remains secret.

(b) No User Accounts - WebMCQ computers are always configured exclusively for use by WebMCQ. Nobody other than authorised administrators have accounts on our machines, which means we can implement much tighter security than the vast majority of machines connected to the Internet.

(c) Minimal Internet Services Running - After general user accounts, the biggest threat to Internet machines generally comes from programs that interface directly with the Internet. Some of these programs are necessary - the Web server, for example! However, many others are not necessary for WebMCQ computers because they are dedicated to a single specific purpose. This means that the potential security risks posed by non-essential Internet Service programs is eliminated on our machines.

5. Conclusion

WebMCQ has been designed from the ground up with security issues at the forefront. As part of our service model of distribution, we can take the burden of security management from you, leaving you free to concentrate on creating content. Furthermore, security can be tailored to your particular needs, and we can advise on appropriate policies for your particular situation. Whether you plan to present a demonstration quiz to thousands of students on the Internet, or want to gather highly-sensitive data from employees in a corporate setting, you can do so with confidence when you use WebMCQ.

This information is copyright © 1998, 1999 WebMCQ Pty Ltd.
<http://www.webmcq.com/>