Course work on scripting and security

Law, Security

Scripting and Security

Scripting is a potential web vulnerability because its power also comes with the opportunity for abuse. The scripting language can be used to force some disallowed states on either the client or server machines. This can later result into system failure or crash within the system. There are some scripts which have the capabilities of exploiting vulnerabilities in the underlying operating systems. The scripts then become exploits and hence cause trouble or damages to the system. There are attempts to make the scripting languages in the web secure but at the same time there are individuals who are notorious individuals who discover new codes sequence that can enable them go round the controls and checks. (p. 126)

Scripting is also a potential web vulnerability because it can cause damage to the computers if not properly handled. For instance, if a java security manager is not properly implemented, then the java code can crawl out of the sandbox and do a lot of harm to the client computer in form of a malicious applet.

Scripting can also be regarded as a potential web vulnerability because it can cause a lot of trouble if malicious codes are include. ActiveX for instance is a powerful tool with several capabilities but can also cause a lot of trouble if not properly checked. (p. 128) Each of the programming languages usually has strong capabilities. However, some of these capabilities can be short lived as the scripting languages pose a problem of web vulnerability. If no precautionary measure is taken in order to ensure that the codes are well protected, then the scripting languages can cause a lot of harm. Some of the scripting languages which help in accomplishing tasks are the ones that

contain malicious codes that can affect the computers in the web. Scripting can also be potential web vulnerability due to the presence of poisoned cookies. Such cookies can trigger the download of malicious software which can in turn cause a lot of harm to the computer. Scripting languages can also be a potential source of web vulnerability since they can result into buffer overflows. This type of attack is usually common on the server side and the computer's performance can be greatly degraded.

The scripting languages can also cause; malicious HTML tags in web requests, malicious codes from other clients, clients sending malicious codes to themselves and abuse of tags. This eventually affects the whole network and the performance of the computers is greatly degraded. Some of the malicious codes sent can literally bring the computers affected to a halt.

References

Chapter 6: Computer Security basics