It rather involved being on the other side of this airtight hatchway: If they can inject code, then they can run code

devblogs.microsoft.com/oldnewthing/20100114-00

January 14, 2010

Raymond Chen

One category of the dubious security vulnerability is designing an insecure system, putting together an exploit, and then blaming one of the components of the exploit rather than the insecure system in the first place.

> I have found a critical security vulnerability in the XYZ scripting object which permits modifying files on the Web server itself.
>
> To effect this exploit, write a script which instantiates the control and use the `Save` method to tell it to save its contents. The `Save` method does not attempt to block directory traversal, so you can pass any path to the `Save` method and overwrite any file on the server.
>
> To deploy this exploit, find a Web server which has a writeable directory that also has execute permission and which executes scripts as SYSTEM. Upload the script to the server, and then from another machine, visit the Web server to view the page you just uploaded. The Web server will execute the script as a server-side script, and the target file will be overwritten.

Well, yes, this whole set-up is definitely vulnerable, but why are you blaming the XYZ scripting object? For one thing, you can do exactly the same thing with any other scripting object that can write files. For example, just use the `FileSystemObject` object. In fact, that object is even better than the XYZ object, because the file system object lets you control what is written!

But the real security vulnerability is that the person who set up the Web site did so insecurely. If you let untrusted users upload scripts to the server and configure the server to execute them as SYSTEM without restriction, then naturally those users can upload scripts that do dangerous things to the server. That's not the script's fault; it's the fault of the person who set up the Web server to execute those scripts in such an insecure manner in the first place! (You might have a case if the insecure configuration is the default, but I don't know of any modern servers that do.)

Raymond Chen

Follow