
An Oldie but Goodie: The Cross-Site Scripting Vulnerability

Posted by Dave Wreski
31 December 2001

The vulnerability itself, CERT Advisory 2000-02, sometimes called cross-site scripting or malicious tagging, takes advantage of dynamically generated Web pages. Basically, a malicious script, which could be written in a number of different languages, can be inserted as input into dynamically . . .

The vulnerability itself, CERT Advisory 2000-02, sometimes called cross-site scripting or malicious tagging, takes advantage of dynamically generated Web pages. Basically, a malicious script, which could be written in a number of different languages, can be inserted as input into dynamically generated Web pages. Unless the pages are specifically built to protect against the insertions of these scripts, they allow an attacker to insert code that can poison cookies, expose SSL connections, access restricted sites, or pull off a number of other attacks.

Most commonly exploited avenues are search boxes or online forums. All an attacker has to do is insert malicious code in between scripting tags that the Web page will accept, by using <FORM> or <APPLET> tags, for instance. What makes this vulnerability especially prevalent is the number of different languages and technologies a Web designer needs to understand in order to protect against it. The exploit is possible using CGI, Perl, JavaScript, Java, .ASP, C++, and simple HTML.