

A common researcher diagnosis error: misreading error messages

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-10/0040.html>

From: Steven M. Christey (*coley_at_mitre.org*)

Date: 10/04/05

Date: Tue, 4 Oct 2005 17:11:51 -0400 (EDT)

To: bugtraq@securityfocus.com

In "Re: BID #14752 update", Josh Zlatin-Amishav pointed out a vulnerability diagnosis error that seems to be happening more frequently:

```
>BID 14752 is not only an XSS vulnerability, the real problem is a
>directory transversal flaw and affects Guppy versions less than
>4.5.6a.
>
>[snip]
>
>The code in printfaq.php <4.5.4 reads:
>
>if ($pg!="") {
>include(DBBASE.$pg.INCEXT);
>
>If you set $pg to "<script>alert(XSS)</script>" you receive an error
>that PHP can't include the file and the javascript gets executed. This
>assumes register_globals and display_errors are enabled. You can also
>set $pg to: "../../../../../../../../etc/passwd%00" and read the
>password file
```

I am seeing increasing numbers of reports by researchers who make the same diagnostic error that you just highlighted. They throw some input for one vuln type at an application (say, XSS manipulations), get an error that shows "XSS," and completely miss the fact that the error message shows a more serious problem at play, such as SQL injection or directory traversal. The XSS is "resultant" from these other "primary" errors.

Similarly, just because you throw a long input at a program and the program fails, it doesn't necessarily mean that you found a buffer overflow. You could have triggered a memory allocation error; or the program didn't recognize the argument as a valid argument; or it spotted the long input and returned a null pointer, but forgot to check and led to a null dereference; or multiple other reasons.

SecurityFocus Bugtraq: A common researcher diagnosis error: misreading error messages

For those researchers who care about quality of information, make sure that you interpret error messages correctly, especially if you're using some generic attack program that throws a lot of junk at an application. Error messages are important clues, but not the whole story.

Vulnerability information analysts – e.g. for vulnerability databases and scanning tools – should be vigilant for these common diagnostic errors.

In this particular instance, it doesn't help that PHP's error message generators don't seem to quote the error messages that are generated, so a lot of "XSS-as-symptom-but-not-cause" problems are reported for PHP apps. Whether this is a problem with PHP itself or not is a separate question.

– Steve