

# Sphider 1.3.4 Cross Site Scripting

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-05/msg00075.html>

---

- *From:* [decoder-bugtraq@xxxxxxxxxxxxx](mailto:decoder-bugtraq@xxxxxxxxxxxxx)
  - *Date:* 6 May 2008 20:09:03 -0000
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Sphider Cross Site Scripting Vulnerability

Original release date: 2008-04-29

Last revised: 2008-05-06

Latest version: <http://users.own-hero.net/~decoder/advisories/sphider134-xss.txt>

Source: Christian Holler <<http://users.own-hero.net/~decoder/>>

Systems Affected:

Sphider 1.3.4 (<http://www.sphider.eu/>) – A PHP Search Engine

Severity: Moderate

Overview:

Sphider is a search engine that has several features; one is a search suggestion feature as in "Did you mean xyz?" that corrects possible typos in your search, without however sanitizing this output. This feature is off by default, but turned on by many sites for convenience.

## I. Description

The output of the suggestion feature in Sphider does output the complete query if there is at least one word in this query that has the script has found a possible correction for. This word is highlighted and the rest of the search query is returned as it is. However, this output is completely unsanitized, allowing HTML/Javascript to be included.

## II. Impact

Depending on the site where this search script is deployed, this attack can be used to steal cookies from other users by tricking them into visiting a given URL.

## Sphider 1.3.4 Cross Site Scripting

### III. Proof of concept

search.php?query=xsss%20%3Cscript%3Ealert('HELLO');%3C/script%3E&search=1

where the first word in the query, "xsss" is a word that can be corrected by the search script. This generally depends on the indexed site(s) but such a word is very easy to find.

### IV. Solution

Currently none, author has been informed.

Timeline:

2008-04-29: Author informed

2008-05-06: Vulnerability notice published

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v2.0.6 (GNU/Linux)

iD8DBQFIIMGYJQIKXnJyDxURAm44AJ9JbT+63Krp95BZatccKal29DhkwCgoAE9  
eNhj/JgskwQVKgmdnFBEVG0=  
=DZrL

-----END PGP SIGNATURE-----