

[UNIX] Advanced Guestbook XSS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0121.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/29/04

To: list@securiteam.com

Date: 29 Dec 2004 14:23:23 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Advanced Guestbook XSS

SUMMARY

<<http://proxy2.de/scripts.php>> Advanced Guestbook is "a PHP-based guestbook script. It includes many useful features such as preview, templates, e-mail notification, picture upload, page spanning , html tags handling, smilies, advanced guestbook codes and language support".

By triggering an SQL error it is possible to cause Advanced Guestbook to display arbitrary HTML and/or JavaScript.

DETAILS

Vulnerable Systems:

* Advanced Guestbook 2.3.1 and prior

Exploit:

```
index.php?entry=<script>alert(document.cookie)</script>
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:emile.van.elen@gmail.com>>
Emile van Elen.

Securiteam: [UNIX] Advanced Guestbook XSS

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.