

# [UNIX] paBox Cross Site Scripting

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0095.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 03/22/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 22 Mar 2005 18:00:25 +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>

-----

paBox Cross Site Scripting

---

## SUMMARY

" <<http://www.phparena.net/pabox.php>> paBox is a PHP/mysql shoutbox script (Also known as a tagboard.) You can add it to your site and visitors can post new messages, it is similar to a guestbook."

paBox is vulnerable to a cross site scripting vulnerability due lack of validation of user provided input.

## DETAILS

Vulnerable Systems:

\* paBox version 2.0

The parameter in the form that lets you select which 'smilie' to use as an icon for your post is prone to a script injection attack.

The specific parameter is:

```
<INPUT type=radio CHECKED value="wink.gif" name=posticon>
```

Where wink.gif become the value of the SRC attribute of the <img> tag when your post is submitted.

## Securiteam: [UNIX] paBox Cross Site Scripting

By altering the value of wink.gif, or adding another instance of this parameter, its possible to inject malicious code into the value of the parameter, for example:

```
<INPUT type=radio CHECKED  
value=""><script>document.write(document.cookie);</script>"  
name=posticon>click me
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:Sean@sage-web.com> Rift.

=====

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.