

[UNIX] Jaws Cross Site Scripting (GlossaryModel.php)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0115.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/21/05

To: list@securiteam.com

Date: 21 Apr 2005 15:07:41 +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>

Jaws Cross Site Scripting (GlossaryModel.php)

SUMMARY

" <<http://www.jaws-project.com/index.php>> Jaws is a Framework and Content Management System for building dynamic web sites. It aims to be User Friendly giving ease of use and lots of ways to customize web sites, but at the same time is Developer Friendly, it offers a simple and powerful framework to hack your own modules."

Jaws is vulnerable to cross site scripting attacks, allowing malicious users to steal identity cookies.

DETAILS

Vulnerable Systems:

- * Jaws version 0.4

Immune Systems:

- * Jaws version 0.5

The Glossary gadget doesn't filter out dangerous characters in the process of adding a new word to the glossary, allowing the insertion of items from

Securiteam: [UNIX] Jaws Cross Site Scripting (GlossaryModel.php)

<script>alert(document.cookie)</script> to more complex JavaScript code.

Workaround:

Replace the NewTerm function in GlossaryModel.php for this new one.

```
/**
 * Adds a new term
 *
 * @access public
 * @param string $term Term
 * @param string $desc Term's description
 * @return boolean Returns true if term was added
 */
function NewTerm ($term, $desc)
{
    //xss fix
    if(strpos($term, "<") || strpos($term, ">"))
        $term = strip_tags($term);
    if(strpos($desc, "<") || strpos($desc, ">"))
        $desc = strip_tags($desc);

    $sql = "INSERT INTO [[term]] (term, description,
createtime, updatetime)
VALUES ({term},{desc},NOW(),NOW())";
    $rs = $GLOBALS["app"]->DB->Execute ($sql, array ("term" =>
$term, "desc" => $desc));

    if ($rs) {
        $GLOBALS["session"]->PushLastResponse
(_t("GLOSSARY_TERM_ADDED"),RESPONSE_NOTICE);
        return true;
    } else {
        $GLOBALS["session"]->PushLastResponse
(_t("GLOSSARY_ERROR_TERM_NOT_CREATED"), RESPONSE_ERROR);
        return new JawsError
(_t("GLOSSARY_ERROR_TERM_NOT_CREATED"), _t("GLOSSARY_NAME"));
    }
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:nah@suckea.com> Paulino Calderon.

=====

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.