

# [UNIX] Multiple Cross-Site Scripting Vulnerabilities in Nuked-Klan

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0076.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 01/29/03

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 29 Jan 2003 16:06:27 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Multiple Cross-Site Scripting Vulnerabilities in Nuked-Klan

---

## SUMMARY

<<http://www.nuked-klan.org/>> Nuked Klan is a PHP Gateway for "clans". Many Cross-Site Scripting vulnerabilities have been found in Nuked Klan that allows attackers to inject script codes into the page and use them on client's browser as if they were provided by the site.

These Cross-Site Scripting vulnerabilities are found in the following modules: Guestbook, Forum, and Shoutbox.

An attacker can input specially crafted links and/or other malicious scripts.

## DETAILS

Vulnerable systems:

- \* Nuked Klan version 1.2 beta and prior

Immune systems:

- \* Nuked Klan version 1.3 beta and prior

## Securiteam: [UNIX] Multiple Cross-Site Scripting Vulnerabilities in Nuked-Klan

### Guestbook:

A vulnerability was discovered in the page for posting messages, at this address:

[http://\[target\]/index.php?file=Guestbook&req=post\\_book](http://[target]/index.php?file=Guestbook&req=post_book)

The vulnerability is at the level of the interpretation of the "Author" field.

Indeed, the insertion of a hostile code script in this field makes it possible to a malicious user to carry out this script on the navigator of the visitors.

A hostile code could be:

```
[script>alert("Cookie="+document.cookie)/script]
```

(Open a window with the cookie of the visitor, replace [] by <>)

### Forum:

A vulnerability was discovered in the page for posting new messages in the forum, at this address:

[http://\[target\]/index.php?file=Forum&op=post\\_screen&forum\\_id=0](http://[target]/index.php?file=Forum&op=post_screen&forum_id=0)

The vulnerability is at the level of the interpretation of the "Titre" and "Pseudo" field.

Indeed, the insertion of a hostile code script in this field makes it possible to a malicious user to carry out this script on the navigator of the visitors.

A hostile code could be:

```
[script>alert("Cookie="+document.cookie)/script]
```

(Open a window with the cookie of the visitor, replace [] by <>)

### Shoutbox:

A vulnerability was discovered in the page for posting messages in "La Tribune Libre". Indeed, the insertion of a hostile code script in this field makes it possible to a malicious user to carry out this script on the navigator of the visitors.

A hostile code could be:

```
[script>alert("Cookie="+document.cookie)/script]
```

(Open a window with the cookie of the visitor, replace [] by <>)

Vulnerable line in submit.php:

```
$shout = str_replace("|", "", $SB_text);
```

Possible solutions:

Modify the code in order to analyze the whole of the text sent by the user and to replace the hostile elements.

-----Code example-----

```
<?
```

```
$SB_text = str_replace("<", "[", $SB_text);
```

## Securiteam: [UNIX] Multiple Cross-Site Scripting Vulnerabilities in Nuked-Klan

```
$SB_text = str_replace(">", "]", $SB_text);  
$SB_text = htmlentities($SB_text);  
$shout = str_replace("|", "", $SB_text);  
?>
```

---

### Solutions:

Upgrade your version to beta 1.3

Upgrade Guestbook with the appropriate patch:

<<http://tomysnockers.net/download/Guestbook.rar>>  
<http://tomysnockers.net/download/Guestbook.rar>

Upgrade Shoutbox with the appropriate patch:

<[http://www.nuked-klan.org/files/Shoutbox\\_13.zip](http://www.nuked-klan.org/files/Shoutbox_13.zip)>  
[http://www.nuked-klan.org/files/Shoutbox\\_13.zip](http://www.nuked-klan.org/files/Shoutbox_13.zip)

### Vendor status:

The vendor has been notified.

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:gregory.lebras@security-corp.org>> Grégory Le Bras | Security Corporation.

=====  
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](mailto:list-unsubscribe@securiteam.com)

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