Abysssec Research

1) Advisory information

Title	**: ndCMS Sql Injection Vulnerability**
Affected	**: ndCMS(Nickel and Dime CMS) v0.4rc1**
Discovery	**: www.abysssec.com**
Vendor	**: http://souurceforge.net/projects/ndcms-net**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- SQL Injection

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying application.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- SQL Injection:

This version of ndCMS has SQL Injection Vulnerability that its Database is Access with Table of Users tblUSERS Columns: userid , passwd.

Vulnerable Code:

```
.../express_edit/editor.aspx
Ln 65:
dbr = db.ExecuteReader("Select * from tblPAGES WHERE indx=" + Request.Params["indx"]);
```

And so on.