Abysssec Research

1) Advisory information

Title	**: VisualSite CMS Multiple Vulnerabilities**
Affected	**: VisualSite 1.3**
Discovery	**: www.abysssec.com**
Vendor	**: http://sourceforge.net/projects/visualsite/**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- **Logical Bug for Lock Admin's Login**
2- **Persistent XSS in admin section**
3-

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- Logical Bug for Lock Admin's Login:

If you enter this values in Login Page (http://Example.com/Admin/Default.aspx) three times during five minutes , the Admin's login will be locked:

```
Username : 1' or '1'='1
Password : foo
```

Vulnerable Code is in this file:

```
../App_Code/VisualSite/DAL.cs
Ln 378:
public static User GetUser(string username)
{
User result = null;
DataTable matches = ExecuteRowset(String.Format("SELECT [ID], [Username], [Password], [LockedDate] FROM
[User] WHERE [Username] = '{0}'", Sanitise(username)));
if (matches != null && matches.Rows.Count > 0)
{
...
}
return result;
}
```

2- Persistent XSS in admin section:

In Edit Section which is accessible to Admin, it is possible to enter a script in Description field that only executed in the following path and never executed in other situations:

```
http://Example.com/SearchResults.aspx?q={}
```