Abysssec Research

1) Advisory information

Title	**: FreeDiscussionForums Multiple Remote Vulnerabilities**
Affected	**: Free Discussion Forum 1.0**
Discovery	**: www.abysssec.com**
Vendor	**: http://www.freediscussionforums.net**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- **Access to Admin's Section**

2- **Persistent XSS**

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

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Access to Admin's Section:

With this path you can easily access to Admin's section:

```
http://Example.com/ManageSubject.aspx
```

Vulnerable Code:

```
DLL  : App_Web_wngcbiby.dll
Class :  Class adminlogin

    protected void Button1_Click(object sender, EventArgs e)
        {
      ...
      if ((this.txtUserName.Text.Trim() == str) && (this.txtPassword.Text.Trim() == str2))
      {
        this.Session["User"] = "admin";
        base.Response.Redirect("ManageSubject.aspx");
      }
          }
```

2-Persistent XSS:

In this application also there is a Persistent XSS exist in title field.

```
Valnerable Code :
  DLL  : App_Web_wngcbiby.dll
  Class :  Class AddPost

      protected void Page_Load(object sender, EventArgs e)
        {
            if (base.Request.QueryString["forumId"] != null)
            {
               this.forumId = Convert.ToInt32(base.Request.QueryString["forumId"]);
            }
            if (base.Request.QueryString["title"] != null)
            {
               this.title =
Common.ReplaceString(base.Request.QueryString["title"].ToString().Trim());
             }
            ...
        }
```