Internal Mobile Application Security Audit Report

Level: 1

“Project Name: EZnetCRM Android Application”

Date: 9th Sept 2015

By:

Swati Bhardwaj

Information Security Analyst

1.

Vulnerability Name: **Debugger Mode is enabled**

Severity: **HIGH**

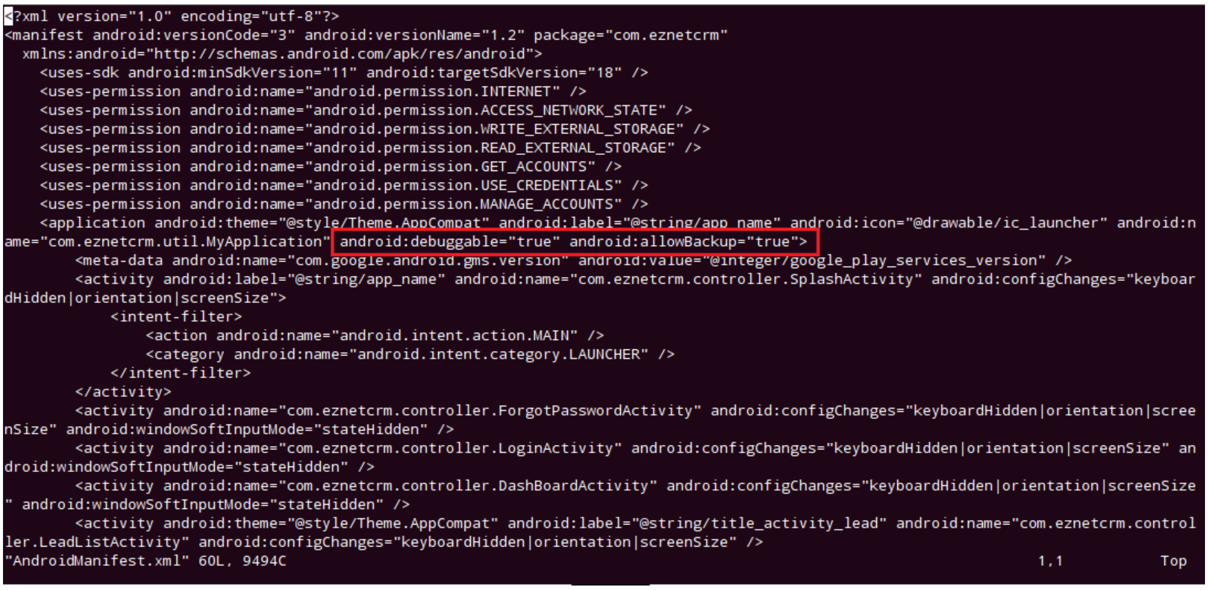
Description:

During the analysis, it was found that the android application has debugger mode ON. It allowed to successfully retrieve all the application methods by debugging the android application. An attacker may take advantage of that and use this information for further attacks.

Recommendation:

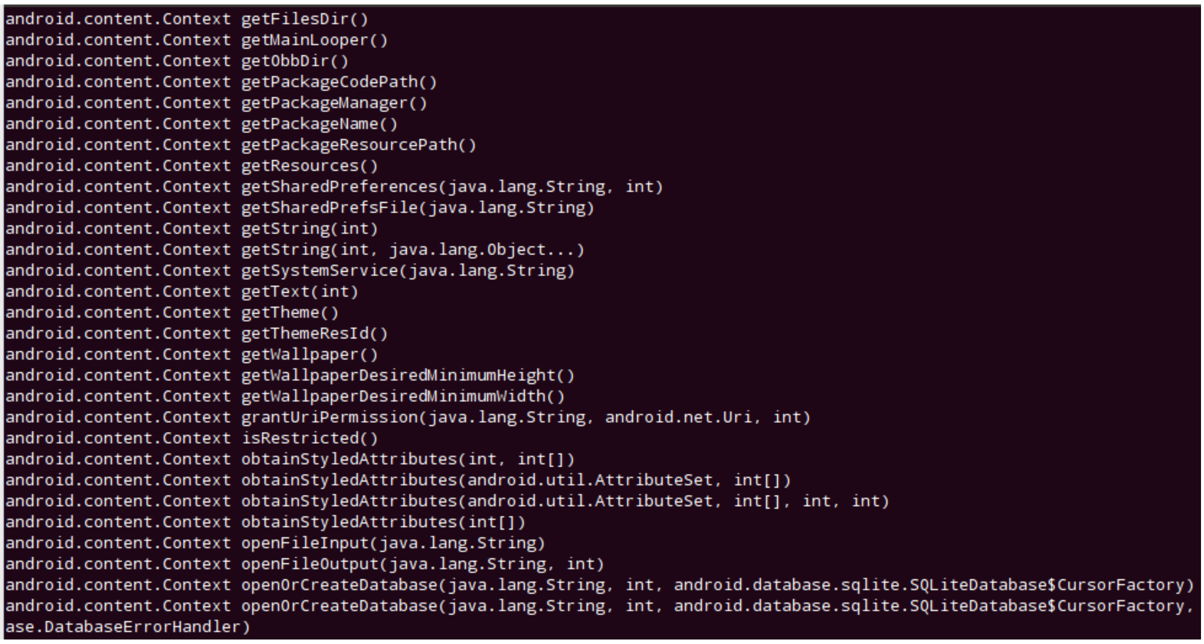
Debugger Mode should be disabled.

Screen Shot:



```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="3" android:versionName="1.2" package="com.eznetcrm"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="11" android:targetSdkVersion="18" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.GET_ACCOUNTS" />
    <uses-permission android:name="android.permission.USE_CREDENTIALS" />
    <uses-permission android:name="android.permission.MANAGE_ACCOUNTS" />
    <application android:theme="@style/Theme.AppCompat" android:label="@string/app_name" android:icon="@drawable/ic_launcher" android:n
ame="com.eznetcrm.util.MyApplication" android:debuggable="true" android:allowBackup="true">
        <meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version" />
        <activity android:label="@string/app_name" android:name="com.eznetcrm.controller.SplashActivity" android:configChanges="keyboar
dHidden|orientation|screenSize">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:name="com.eznetcrm.controller.ForgotPasswordActivity" android:configChanges="keyboardHidden|orientation|scree
nSize" android:windowSoftInputMode="stateHidden" />
        <activity android:name="com.eznetcrm.controller.LoginActivity" android:configChanges="keyboardHidden|orientation|screenSize" an
droid:windowSoftInputMode="stateHidden" />
        <activity android:name="com.eznetcrm.controller.DashBoardActivity" android:configChanges="keyboardHidden|orientation|screenSize
" android:windowSoftInputMode="stateHidden" />
        <activity android:theme="@style/Theme.AppCompat" android:label="@string/title_activity_lead" android:name="com.eznetcrm.control
ler.LeadListActivity" android:configChanges="keyboardHidden|orientation|screenSize" />
"AndroidManifest.xml" 60L, 9494C                                                                          1,1           Top
```

Extracted Methods



```
android.content.Context getFilesDir()
android.content.Context getMainLooper()
android.content.Context getObbDir()
android.content.Context getPackageCodePath()
android.content.Context getPackageManager()
android.content.Context getPackageName()
android.content.Context getPackageResourcePath()
android.content.Context getResources()
android.content.Context getSharedPreferences(java.lang.String, int)
android.content.Context getSharedPrefsFile(java.lang.String)
android.content.Context getString(int)
android.content.Context getString(int, java.lang.Object...)
android.content.Context getSystemService(java.lang.String)
android.content.Context getText(int)
android.content.Context getTheme()
android.content.Context getThemeResId()
android.content.Context getWallpaper()
android.content.Context getWallpaperDesiredMinimumHeight()
android.content.Context getWallpaperDesiredMinimumWidth()
android.content.Context grantUriPermission(java.lang.String, android.net.Uri, int)
android.content.Context isRestricted()
android.content.Context obtainStyledAttributes(int, int[])
android.content.Context obtainStyledAttributes(android.util.AttributeSet, int[])
android.content.Context obtainStyledAttributes(android.util.AttributeSet, int[], int, int)
android.content.Context obtainStyledAttributes(int[])
android.content.Context openFileInput(java.lang.String)
android.content.Context openFileOutput(java.lang.String, int)
android.content.Context openOrCreateDatabase(java.lang.String, int, android.database.sqlite.SQLiteDatabase$CursorFactory)
android.content.Context openOrCreateDatabase(java.lang.String, int, android.database.sqlite.SQLiteDatabase$CursorFactory,
ase.DatabaseErrorHandler)
```

Kindly Fix the Vulnerabilities throughout the Application

2.

Vulnerability Name: Clear Text Credentials Stored on User Device

Severity: HIGH

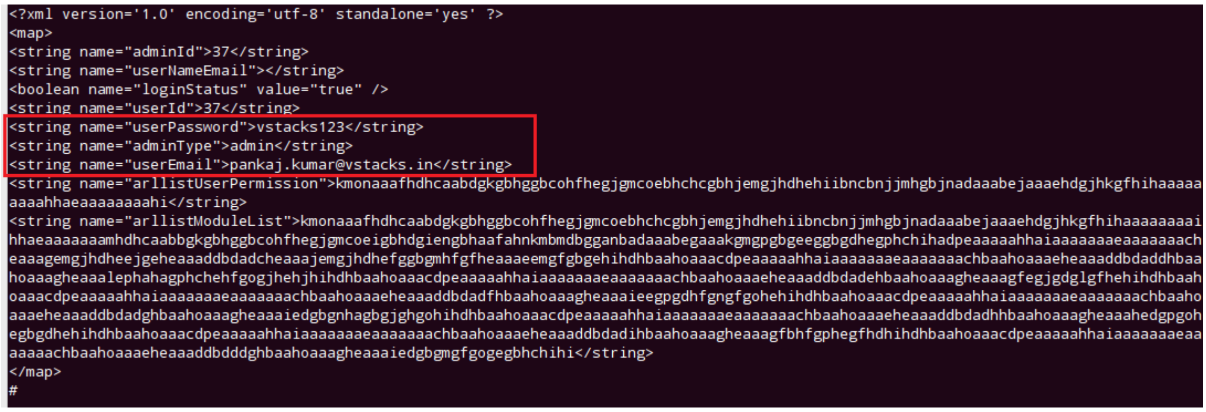
Description:

It is possible to retrieve the clear text credentials from the user device. Other malicious applications may access these credentials and use it for unauthorized access. An attacker might take the advantage of that and use this information for further attacks.

Recommendation:

Clear Text Credentials should not be stored in the user devices or it should be encrypted.

Screen Shot:



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="adminId">37</string>
<string name="userNameEmail"></string>
<boolean name="loginStatus" value="true" />
<string name="userId">37</string>
<string name="userPassword">vstacks123</string>
<string name="adminType">admin</string>
<string name="userEmail">pankaj.kumar@vstacks.in</string>
<string name="arllistUserPermission">kmonaaafhdhcaabdgkgbhggbcohfhegjgmcoebhchcgbhjemgjhdhehiibncbnjjmhgbjnadaaabejaaaehdgjhkgfhihaaaaa
aaaahhaeaaaaaaaaahi</string>
<string name="arllistModuleList">kmonaaafhdhcaabdgkgbhggbcohfhegjgmcoebhchcgbhjemgjhdhehiibncbnjjmhgbjnadaaabejaaaehdgjhkgfhihaaaaaaaai
hhaeaaaaaaamhdhcaabbgkgbhggbcohfhegjgmcoeigbhdgiengbhaafahnkmbmdbgganbadaaabegaaakgmgpgbgeeggbgdhegphchihadpeaaaaahhaiaaaaaaaeaaaaaaach
eaaagemgjhdheejgeheaaaddbdadcheaaajemgjhdhefggbgmhfgfheaaaeemgfgbgehihdhbaahoaaacdpeaaaaahhaiaaaaaaaeaaaaaaachbaahoaaaeheaaaddbdaddhbaa
hoaaagheaaalephahagphchehfgogjhehjhihdhbaahoaaacdpeaaaaahhaiaaaaaaaeaaaaaaachbaahoaaaeheaaaddbdadehbaahoaaagheaaagfegjgdglgfhehihdhbaah
oaaacdpeaaaaahhaiaaaaaaaeaaaaaaachbaahoaaaeheaaaddbdadfhbaahoaaagheaaaieegpgdhfgngfgohehihdhbaahoaaacdpeaaaaahhaiaaaaaaaeaaaaaaachbaaho
aaaeheaaaddbdadghbaahoaaagheaaaiedgbgnhagbgjghgohihdhbaahoaaacdpeaaaaahhaiaaaaaaaeaaaaaaachbaahoaaaeheaaaddbdadhhbaahoaaagheaaahedgpgoh
egbgdhehihdhbaahoaaacdpeaaaaahhaiaaaaaaaeaaaaaaachbaahoaaaeheaaaddbdadihbaahoaaagheaaagfbhfgphegfhdhihdhbaahoaaacdpeaaaaahhaiaaaaaaaeaa
aaaaachbaahoaaaeheaaaddbdddghbaahoaaagheaaaiedgbgmgfgogegbhchihi</string>
</map>
#
```

Kindly Fix the Throughout the Application

3.

Vulnerability Name: Application sends Username and Password in Clear Text

Severity: HIGH

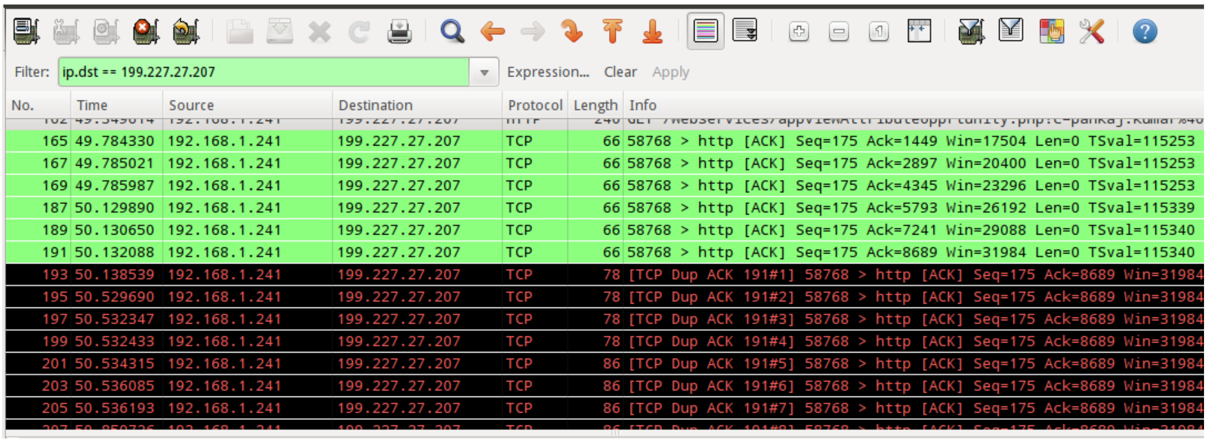
Description:

Application is sending clear text user name and password which might be captured in the network. An attacker might be able to take the advantage of that and use these credentials for unauthorized access in the application.

Recommendation:

HTTPS should be implement in the application.

Screen Shot:



Filter: ip.dst == 199.227.27.207

No.	Time	Source	Destination	Protocol	Length	Info
162	49.549014	192.168.1.241	199.227.27.207	HTTP	240	GET /webservices/appviewAttributeOpportunity.php?e=pankaj.kumar%40
165	49.784330	192.168.1.241	199.227.27.207	TCP	66	58768 > http [ACK] Seq=175 Ack=1449 Win=17504 Len=0 TSval=115253
167	49.785021	192.168.1.241	199.227.27.207	TCP	66	58768 > http [ACK] Seq=175 Ack=2897 Win=20400 Len=0 TSval=115253
169	49.785987	192.168.1.241	199.227.27.207	TCP	66	58768 > http [ACK] Seq=175 Ack=4345 Win=23296 Len=0 TSval=115253
187	50.129890	192.168.1.241	199.227.27.207	TCP	66	58768 > http [ACK] Seq=175 Ack=5793 Win=26192 Len=0 TSval=115339
189	50.130650	192.168.1.241	199.227.27.207	TCP	66	58768 > http [ACK] Seq=175 Ack=7241 Win=29088 Len=0 TSval=115340
191	50.132088	192.168.1.241	199.227.27.207	TCP	66	58768 > http [ACK] Seq=175 Ack=8689 Win=31984 Len=0 TSval=115340
193	50.138539	192.168.1.241	199.227.27.207	TCP	78	[TCP Dup ACK 191#1] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984
195	50.529690	192.168.1.241	199.227.27.207	TCP	78	[TCP Dup ACK 191#2] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984
197	50.532347	192.168.1.241	199.227.27.207	TCP	78	[TCP Dup ACK 191#3] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984
199	50.532433	192.168.1.241	199.227.27.207	TCP	78	[TCP Dup ACK 191#4] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984
201	50.534315	192.168.1.241	199.227.27.207	TCP	86	[TCP Dup ACK 191#5] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984
203	50.536085	192.168.1.241	199.227.27.207	TCP	86	[TCP Dup ACK 191#6] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984
205	50.536193	192.168.1.241	199.227.27.207	TCP	86	[TCP Dup ACK 191#7] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984
207	50.850736	192.168.1.241	199.227.27.207	TCP	86	[TCP Dup ACK 191#8] 58768 > http [ACK] Seq=175 Ack=8689 Win=31984

Kindly Fix the Vulnerabilities throughout the Application

4.

Vulnerability Name: **Directory Listing**

Severity: **MEDIUM**

Description:

The web service is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Recommendation:

You should make sure the directory does not contain any sensitive information or you should restrict directory listings from the web server configuration.

URL:

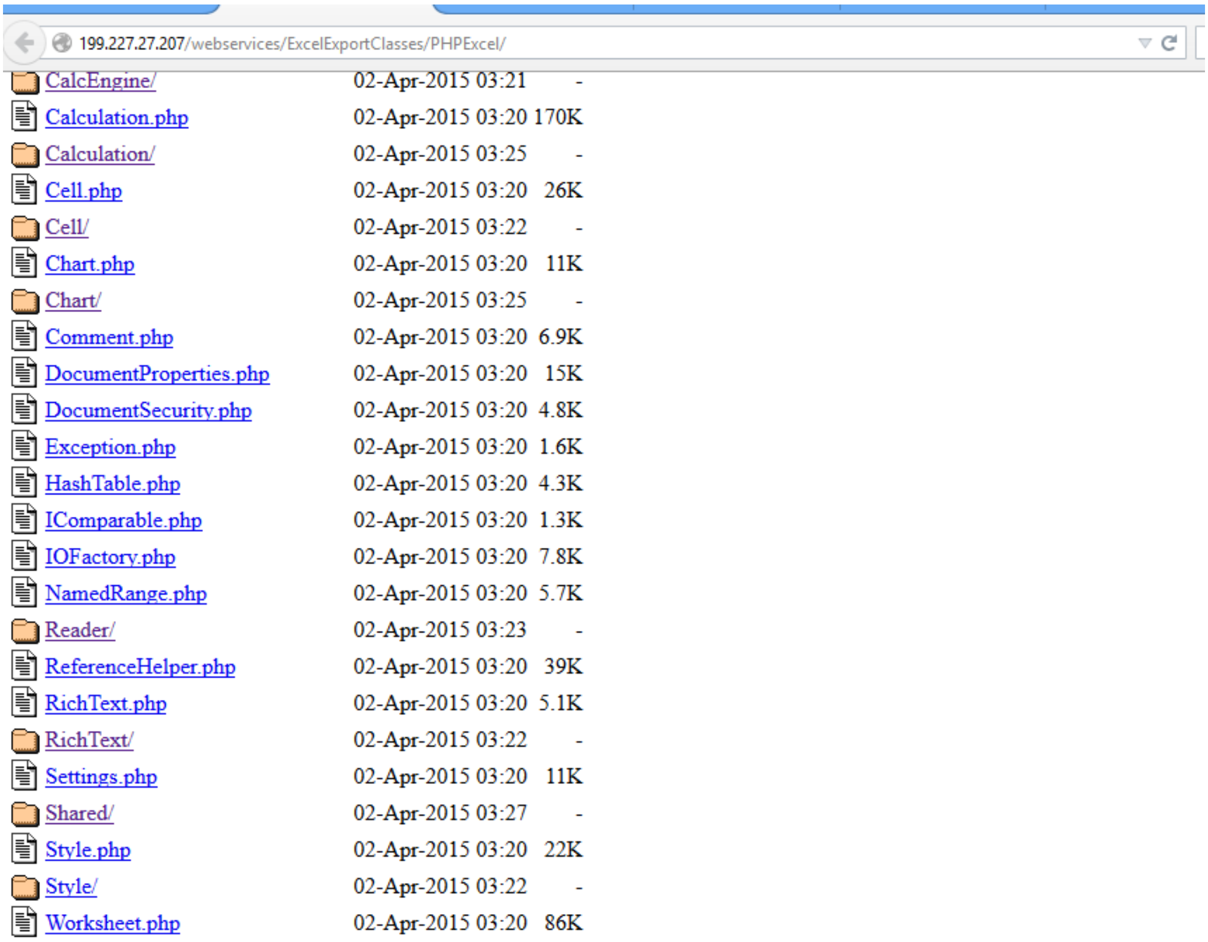
- http://199.227.27.207/webservices/
- http://199.227.27.207/webservices/ExcelExportClasses/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/CachedObjectStorage/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/CalcEngine/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Calculation/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Cell/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Chart/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Chart/Renderer/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Reader/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Reader/Excel5/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Reader/Excel2007/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/Escher/

- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/JAMA/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/OLE/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/PCLZip/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/OLE/PPS/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/JAMA/utils/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/Escher/DgContainer/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/Escher/DggContainer/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Worksheet/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Worksheet/AutoFilter/
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Worksheet/AutoFilter/Column/

Kindly Fix the Vulnerabilities throughout the Application

Screen Shot:

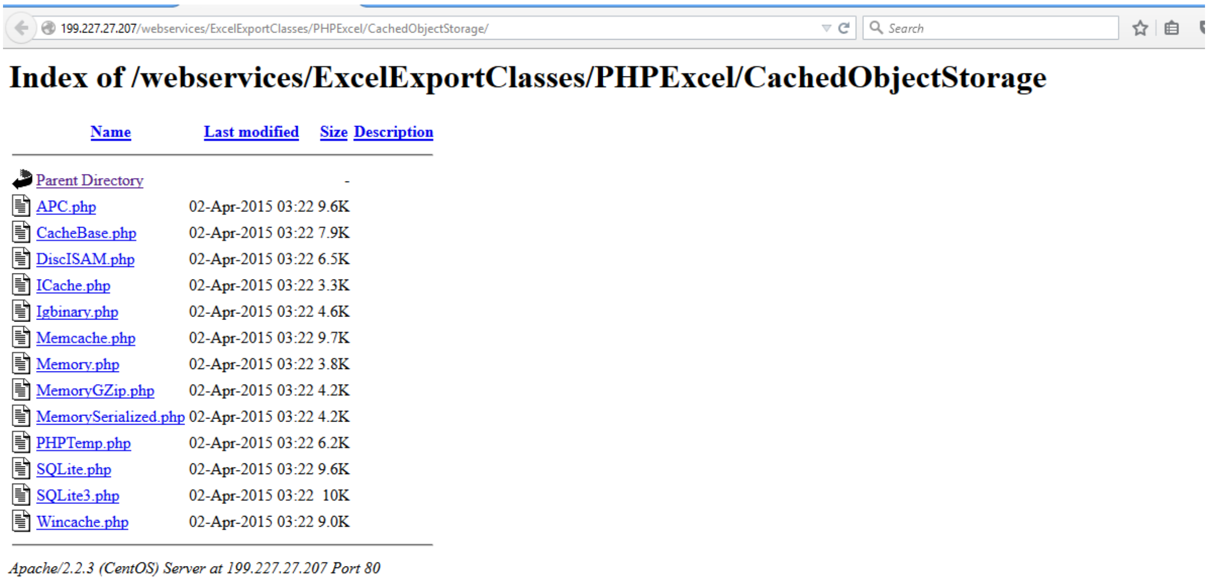
1



199.227.27.207/webservices/ExcelExportClasses/PHPExcel/

CalcEngine/	02-Apr-2015 03:21	-
Calculation.php	02-Apr-2015 03:20	170K
Calculation/	02-Apr-2015 03:25	-
Cell.php	02-Apr-2015 03:20	26K
Cell/	02-Apr-2015 03:22	-
Chart.php	02-Apr-2015 03:20	11K
Chart/	02-Apr-2015 03:25	-
Comment.php	02-Apr-2015 03:20	6.9K
DocumentProperties.php	02-Apr-2015 03:20	15K
DocumentSecurity.php	02-Apr-2015 03:20	4.8K
Exception.php	02-Apr-2015 03:20	1.6K
HashTable.php	02-Apr-2015 03:20	4.3K
IComparable.php	02-Apr-2015 03:20	1.3K
IOFactory.php	02-Apr-2015 03:20	7.8K
NamedRange.php	02-Apr-2015 03:20	5.7K
Reader/	02-Apr-2015 03:23	-
ReferenceHelper.php	02-Apr-2015 03:20	39K
RichText.php	02-Apr-2015 03:20	5.1K
RichText/	02-Apr-2015 03:22	-
Settings.php	02-Apr-2015 03:20	11K
Shared/	02-Apr-2015 03:27	-
Style.php	02-Apr-2015 03:20	22K
Style/	02-Apr-2015 03:22	-
Worksheet.php	02-Apr-2015 03:20	86K

2



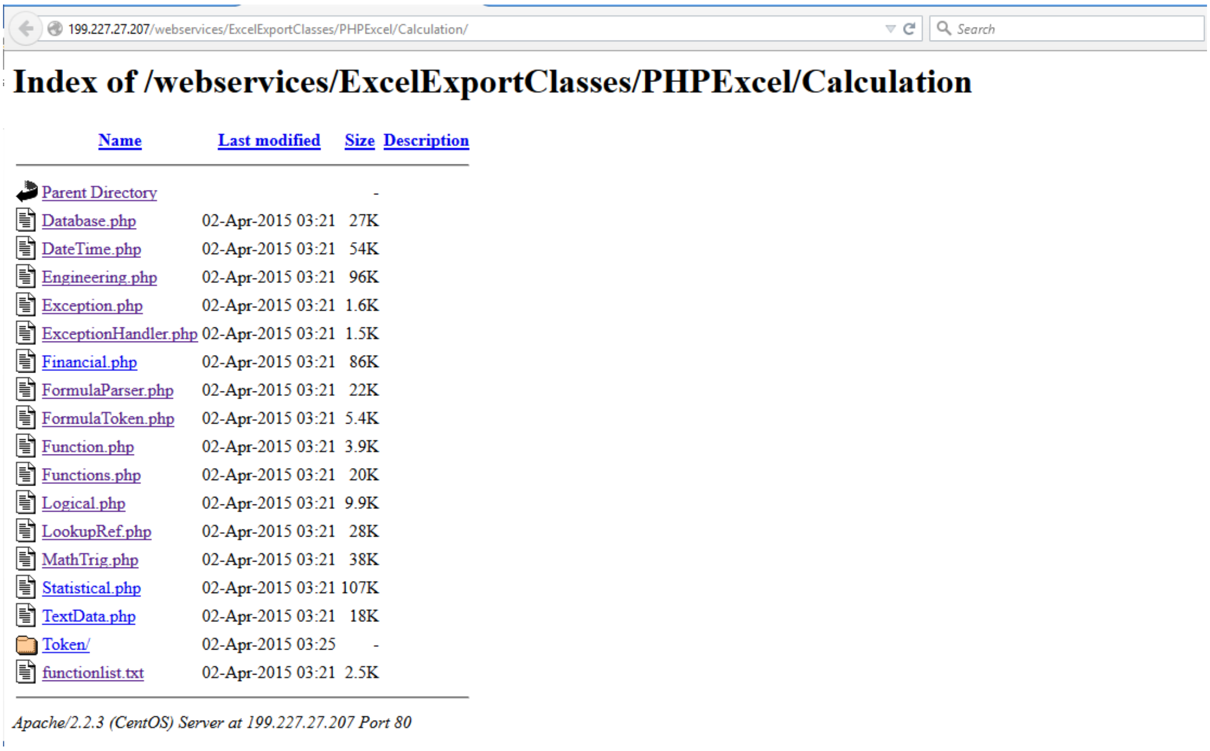
199.227.27.207/webservices/ExcelExportClasses/PHPExcel/CachedObjectStorage/

Index of /webservices/ExcelExportClasses/PHPExcel/CachedObjectStorage

Name	Last modified	Size	Description
Parent Directory		-	
APC.php	02-Apr-2015 03:22	9.6K	
CacheBase.php	02-Apr-2015 03:22	7.9K	
DiscISAM.php	02-Apr-2015 03:22	6.5K	
ICache.php	02-Apr-2015 03:22	3.3K	
Igbinary.php	02-Apr-2015 03:22	4.6K	
Memcache.php	02-Apr-2015 03:22	9.7K	
Memory.php	02-Apr-2015 03:22	3.8K	
MemoryGZip.php	02-Apr-2015 03:22	4.2K	
MemorySerialized.php	02-Apr-2015 03:22	4.2K	
PHPTemp.php	02-Apr-2015 03:22	6.2K	
SQLite.php	02-Apr-2015 03:22	9.6K	
SQLite3.php	02-Apr-2015 03:22	10K	
Wincache.php	02-Apr-2015 03:22	9.0K	

Apache/2.2.3 (CentOS) Server at 199.227.27.207 Port 80

3

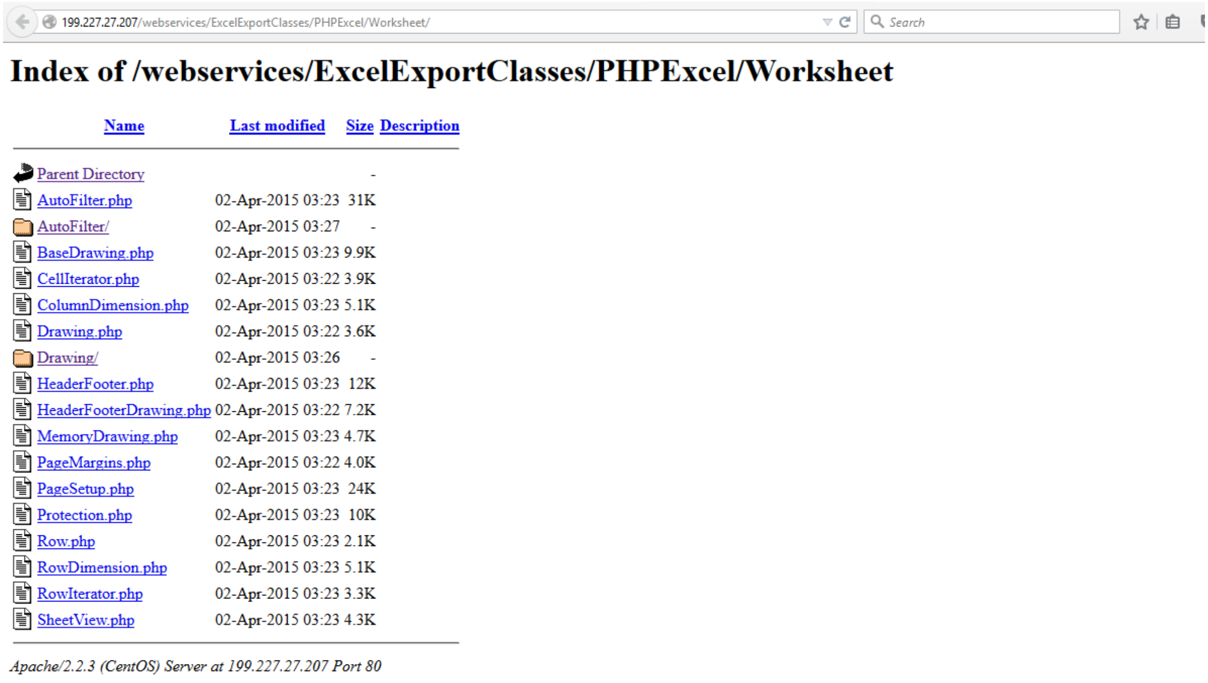

199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Calculation/
Search

Index of /webservices/ExcelExportClasses/PHPExcel/Calculation

Name	Last modified	Size	Description
Parent Directory		-	
Database.php	02-Apr-2015 03:21	27K	
DateTime.php	02-Apr-2015 03:21	54K	
Engineering.php	02-Apr-2015 03:21	96K	
Exception.php	02-Apr-2015 03:21	1.6K	
ExceptionHandler.php	02-Apr-2015 03:21	1.5K	
Financial.php	02-Apr-2015 03:21	86K	
FormulaParser.php	02-Apr-2015 03:21	22K	
FormulaToken.php	02-Apr-2015 03:21	5.4K	
Function.php	02-Apr-2015 03:21	3.9K	
Functions.php	02-Apr-2015 03:21	20K	
Logical.php	02-Apr-2015 03:21	9.9K	
LookupRef.php	02-Apr-2015 03:21	28K	
MathTrig.php	02-Apr-2015 03:21	38K	
Statistical.php	02-Apr-2015 03:21	107K	
TextData.php	02-Apr-2015 03:21	18K	
Token/	02-Apr-2015 03:25	-	
functionlist.txt	02-Apr-2015 03:21	2.5K	

Apache/2.2.3 (CentOS) Server at 199.227.27.207 Port 80

4


199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Worksheet/
Search

Index of /webservices/ExcelExportClasses/PHPExcel/Worksheet

Name	Last modified	Size	Description
Parent Directory		-	
AutoFilter.php	02-Apr-2015 03:23	31K	
AutoFilter/	02-Apr-2015 03:27	-	
BaseDrawing.php	02-Apr-2015 03:23	9.9K	
CellIterator.php	02-Apr-2015 03:22	3.9K	
ColumnDimension.php	02-Apr-2015 03:23	5.1K	
Drawing.php	02-Apr-2015 03:22	3.6K	
Drawing/	02-Apr-2015 03:26	-	
HeaderFooter.php	02-Apr-2015 03:23	12K	
HeaderFooterDrawing.php	02-Apr-2015 03:22	7.2K	
MemoryDrawing.php	02-Apr-2015 03:23	4.7K	
PageMargins.php	02-Apr-2015 03:22	4.0K	
PageSetup.php	02-Apr-2015 03:23	24K	
Protection.php	02-Apr-2015 03:23	10K	
Row.php	02-Apr-2015 03:23	2.1K	
RowDimension.php	02-Apr-2015 03:23	5.1K	
RowIterator.php	02-Apr-2015 03:23	3.3K	
SheetView.php	02-Apr-2015 03:23	4.3K	

Apache/2.2.3 (CentOS) Server at 199.227.27.207 Port 80

Kindly Fix the Vulnerabilities throughout the Application

5.

Vulnerability Name: **Source Code Disclosure**

Severity: **HIGH**

Description:

Server-side source code may contain sensitive information which can help an attacker formulate attacks against the application.

Recommendation:

Server-side source code is normally disclosed to clients as a result of typographical errors in scripts or because of misconfiguration, such as failing to grant executable permissions to a script or directory. You should review the cause of the code disclosure and prevent it from happening.

URL:

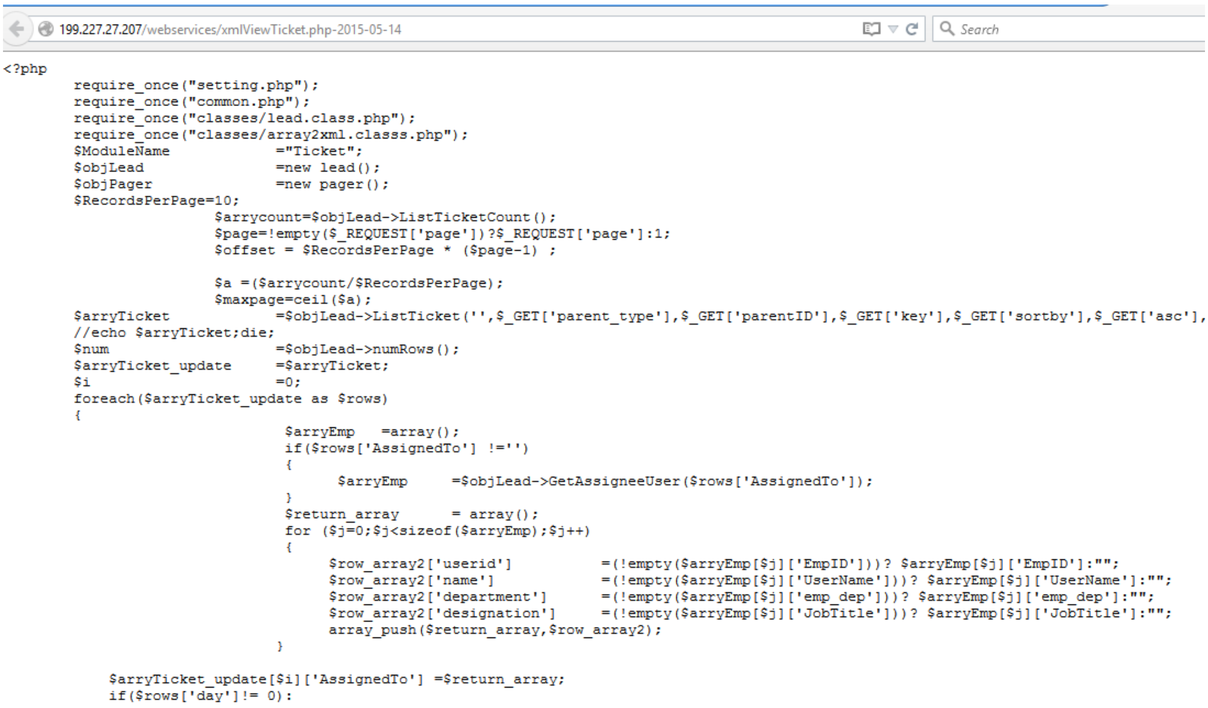
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Calculation/functionlist.txt
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Chart/Renderer/PHP%20Charting%20Libraries.txt
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/PCLZip/readme.txt
- http://199.227.27.207/webservices/ExcelExportClasses/PHPExcel/Shared/PCLZip/gnu-lgpl.txt
- http://199.227.27.207/webservices/appConvertLead.php-29-1-15
- http://199.227.27.207/webservices/appConvertLead.php123
- http://199.227.27.207/webservices/appLeadexportxls.php-30-03-2015-s
- http://199.227.27.207/webservices/appViewLead.php-3-2-15
- http://199.227.27.207/webservices/appViewLead.php-work-18
- http://199.227.27.207/webservices/appViewOpportunity.php-4-2-15
- http://199.227.27.207/webservices/appViewtask.php-3-2-15
- http://199.227.27.207/webservices/appViewtask.php-23-1-15
- http://199.227.27.207/webservices/appViewtask.php-25-03--2015

- http://199.227.27.207/webservices/appadddocument.php-28-1-15
- http://199.227.27.207/webservices/appadddocument.php19-1-15
- http://199.227.27.207/webservices/appaddeditdeletequote.php-23-1-15
- http://199.227.27.207/webservices/appaddlead.php-17-03-2015
- http://199.227.27.207/webservices/appcontactexport.php-30-03-2015-ss
- http://199.227.27.207/webservices/appleadexport.php-01-04-2015-s
- http://199.227.27.207/webservices/applogin.php-3-2-15
- http://199.227.27.207/webservices/appquoteexport.php--01-04-15-s
- http://199.227.27.207/webservices/appticketlist.php-4-2-15
- http://199.227.27.207/webservices/appticketlist.php-3103-2015-s
- http://199.227.27.207/webservices/appviewAttributetask.php-31-03-2015-s
- http://199.227.27.207/webservices/appviewTicket.php-4-2-15
- http://199.227.27.207/webservices/appviewTicket.php-23-1-15
- http://199.227.27.207/webservices/appviewcompaign.php-4-2-15
- http://199.227.27.207/webservices/appviewdocument.php-4-2-15
- http://199.227.27.207/webservices/appviewdocument.php-28-03-2015-s
- http://199.227.27.207/webservices/appviewquote.php-4-2-15
- http://199.227.27.207/webservices/setting.php_2_7
- http://199.227.27.207/webservices/webservice.txt
- http://66.55.11.23/webservices/getCustomerADDDoc.php?c=pankaj.kumar@vstacks.in
- http://199.227.27.207/webservices/xmlViewCompaign.php-2015-05-14
- http://199.227.27.207/webservices/xmlViewCustomer.php-2015-05-14
- http://199.227.27.207/webservices/xmlViewDocument.php-2015-05-14
- http://199.227.27.207/webservices/xmlViewLead.php-2015-05-14
- http://199.227.27.207/webservices/xmlViewOpportunity.php-2015-05-14
- http://199.227.27.207/webservices/xmlViewQuote.php-2015-05-14
- http://199.227.27.207/webservices/xmlViewTask.php-2015-05-14
- http://199.227.27.207/webservices/xmlViewTicket.php-2015-05-14

Kindly Fix the Vulnerabilities throughout the Application

Screen Shot:

1

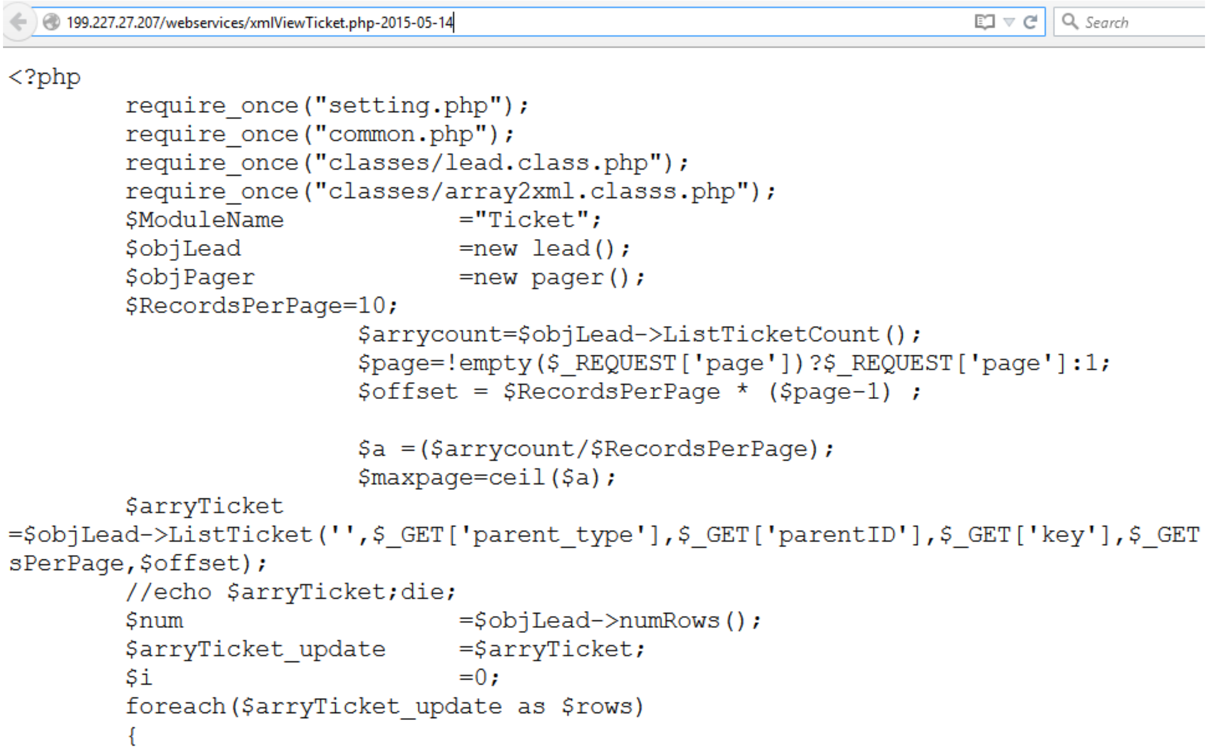


```
<?php
        require_once("setting.php");
        require_once("common.php");
        require_once("classes/lead.class.php");
        require_once("classes/array2xml.classs.php");
        $ModuleName             ="Ticket";
        $objLead                =new lead();
        $objPager               =new pager();
        $RecordsPerPage=10;
                        $arrycount=$objLead->ListTicketCount();
                        $page=!empty($_REQUEST['page'])?$_REQUEST['page']:1;
                        $offset = $RecordsPerPage * ($page-1) ;

                        $a =($arrycount/$RecordsPerPage);
                        $maxpage=ceil($a);
        $arryTicket             =$objLead->ListTicket('',$_GET['parent_type'],$_GET['parentID'],$_GET['key'],$_GET['sortby'],$_GET['asc'],
        //echo $arryTicket;die;
        $num                    =$objLead->numRows();
        $arryTicket_update      =$arryTicket;
        $i                      =0;
        foreach($arryTicket_update as $rows)
        {
                                $arryEmp   =array();
                                if($rows['AssignedTo'] !='')
                                {
                                      $arryEmp     =$objLead->GetAssigneeUser($rows['AssignedTo']);
                                }
                                $return_array      = array();
                                for ($j=0;$j<sizeof($arryEmp);$j++)
                                {
                                     $row_array2['userid']          =(!empty($arryEmp[$j]['EmpID']))? $arryEmp[$j]['EmpID']:"";
                                     $row_array2['name']            =(!empty($arryEmp[$j]['UserName']))? $arryEmp[$j]['UserName']:"";
                                     $row_array2['department']      =(!empty($arryEmp[$j]['emp_dep']))? $arryEmp[$j]['emp_dep']:"";
                                     $row_array2['designation']     =(!empty($arryEmp[$j]['JobTitle']))? $arryEmp[$j]['JobTitle']:"";
                                     array_push($return_array,$row_array2);
                               }

            $arryTicket_update[$i]['AssignedTo'] =$return_array;
            if($rows['day']!= 0):
```

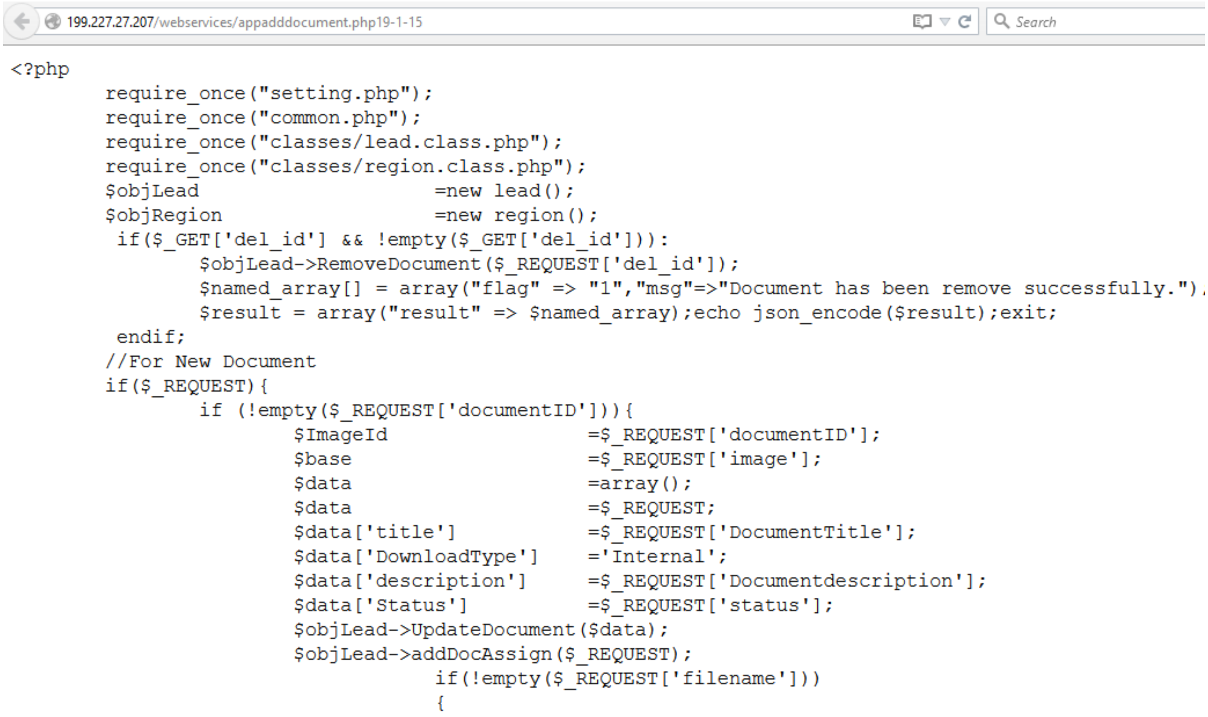
2.



```
<?php
        require_once("setting.php");
        require_once("common.php");
        require_once("classes/lead.class.php");
        require_once("classes/array2xml.classs.php");
        $ModuleName             ="Ticket";
        $objLead                =new lead();
        $objPager               =new pager();
        $RecordsPerPage=10;
                        $arrycount=$objLead->ListTicketCount();
                        $page=!empty($_REQUEST['page'])?$_REQUEST['page']:1;
                        $offset = $RecordsPerPage * ($page-1) ;

                        $a =($arrycount/$RecordsPerPage);
                        $maxpage=ceil($a);
        $arryTicket
=$objLead->ListTicket('',$_GET['parent_type'],$_GET['parentID'],$_GET['key'],$_GET
sPerPage,$offset);
        //echo $arryTicket;die;
        $num                    =$objLead->numRows();
        $arryTicket_update      =$arryTicket;
        $i                      =0;
        foreach($arryTicket_update as $rows)
        {
```

3.



```
<?php
        require_once("setting.php");
        require_once("common.php");
        require_once("classes/lead.class.php");
        require_once("classes/region.class.php");
        $objLead                    =new lead();
        $objRegion                  =new region();
         if($_GET['del_id'] && !empty($_GET['del_id'])):
                $objLead->RemoveDocument($_REQUEST['del_id']);
                $named_array[] = array("flag" => "1","msg"=>"Document has been remove successfully.");
                $result = array("result" => $named_array);echo json_encode($result);exit;
         endif;
        //For New Document
        if($_REQUEST){
                if (!empty($_REQUEST['documentID'])){
                        $ImageId                     =$_REQUEST['documentID'];
                        $base                        =$_REQUEST['image'];
                        $data                        =array();
                        $data                        =$_REQUEST;
                        $data['title']               =$_REQUEST['DocumentTitle'];
                        $data['DownloadType']        ='Internal';
                        $data['description']         =$_REQUEST['Documentdescription'];
                        $data['Status']              =$_REQUEST['status'];
                        $objLead->UpdateDocument($data);
                        $objLead->addDocAssign($_REQUEST);
                                    if(!empty($_REQUEST['filename']))
                                    {
```

Kindly Fix the Vulnerabilities throughout the Application

6.

Vulnerability Name: **Inter Path Disclosure**

Severity: **MEDIUM**

Description:

It is possible to view the inter path of the application. An attacker might take the advantage of that and use this information for further attacks.

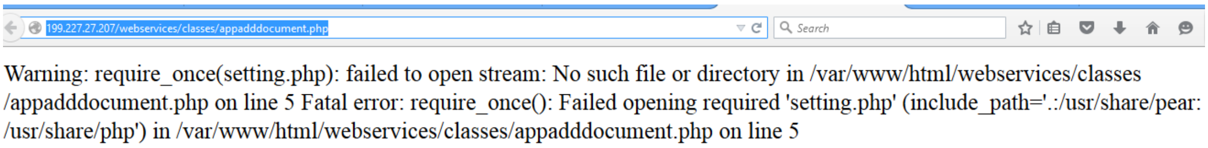
Recommendation:

It is recommended to review the cause of the path disclosure and prevent it from happening.

URL:

http://199.227.27.207/webservices/classes/appadddocument.php

Screen Shot:



```
Warning: require_once(setting.php): failed to open stream: No such file or directory in /var/www/html/webservices/classes
/appadddocument.php on line 5 Fatal error: require_once(): Failed opening required 'setting.php' (include_path='.:/usr/share/pear:
/usr/share/php') in /var/www/html/webservices/classes/appadddocument.php on line 5
```

Kindly Fix the Vulnerabilities throughout the Application

7.

Vulnerability Name: Internal Information might be downloaded by an anonymous users

Severity: HIGH

Description:

It is possible to view and download the internal campaign details information anonymously. An attacker might take the advantage of that and use this this information for own personal use or malicious activity.

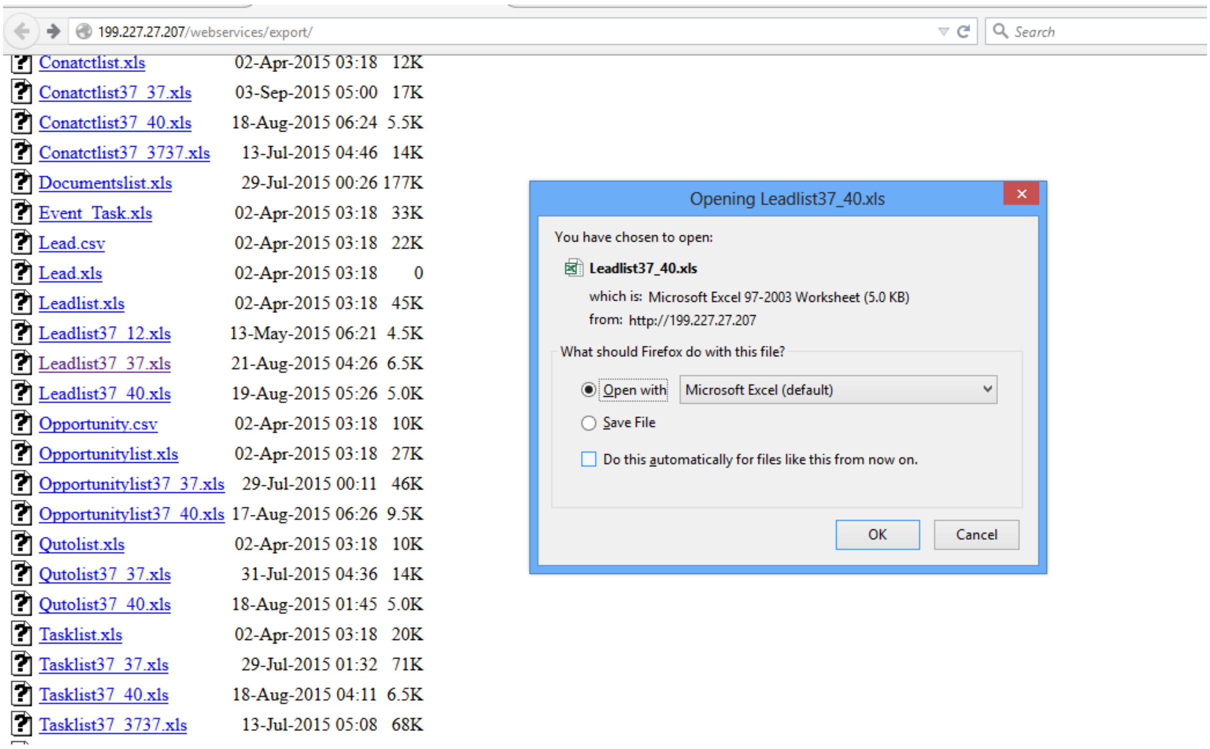
Recommendation:

All the type reports should be restricted by anonymous access and it should be stored outside the public folders.

URL:

- http://199.227.27.207/webservices/export/Campaignlist.xls
- http://199.227.27.207/webservices/export/Conatctlist37_40.xls
- http://199.227.27.207/webservices/export/Leadlist.xls
- http://199.227.27.207/webservices/export/Opportunitylist.xls
- http://199.227.27.207/webservices/export/Opportunitylist.xls
- http://199.227.27.207/webservices/export/Opportunitylist37_40.xls
- http://199.227.27.207/webservices/export/Qutolist.xls

Screen Shot:



199.227.27.207/webservices/export/

Conatctlist.xls	02-Apr-2015 03:18	12K
Conatctlist37_37.xls	03-Sep-2015 05:00	17K
Conatctlist37_40.xls	18-Aug-2015 06:24	5.5K
Conatctlist37_3737.xls	13-Jul-2015 04:46	14K
Documentslist.xls	29-Jul-2015 00:26	177K
Event_Task.xls	02-Apr-2015 03:18	33K
Lead.csv	02-Apr-2015 03:18	22K
Lead.xls	02-Apr-2015 03:18	0
Leadlist.xls	02-Apr-2015 03:18	45K
Leadlist37_12.xls	13-May-2015 06:21	4.5K
Leadlist37_37.xls	21-Aug-2015 04:26	6.5K
Leadlist37_40.xls	19-Aug-2015 05:26	5.0K
Opportunity.csv	02-Apr-2015 03:18	10K
Opportunitylist.xls	02-Apr-2015 03:18	27K
Opportunitylist37_37.xls	29-Jul-2015 00:11	46K
Opportunitylist37_40.xls	17-Aug-2015 06:26	9.5K
Qutolist.xls	02-Apr-2015 03:18	10K
Qutolist37_37.xls	31-Jul-2015 04:36	14K
Qutolist37_40.xls	18-Aug-2015 01:45	5.0K
Tasklist.xls	02-Apr-2015 03:18	20K
Tasklist37_37.xls	29-Jul-2015 01:32	71K
Tasklist37_40.xls	18-Aug-2015 04:11	6.5K
Tasklist37_3737.xls	13-Jul-2015 05:08	68K

Opening Leadlist37_40.xls

You have chosen to open:

Leadlist37_40.xls

which is: Microsoft Excel 97-2003 Worksheet (5.0 KB)

from: http://199.227.27.207

What should Firefox do with this file?

● Open with Microsoft Excel (default)

○ Save File

□ Do this automatically for files like this from now on.

Kindly Fix the Vulnerabilities throughout the Application

8

Vulnerability Name: Unauthorized Information Disclosure

Severity: HIGH

Description:

It is possible to view the internal information application information without the login. An attacker might take the advantage of that and use this information for further attacks.

URL:

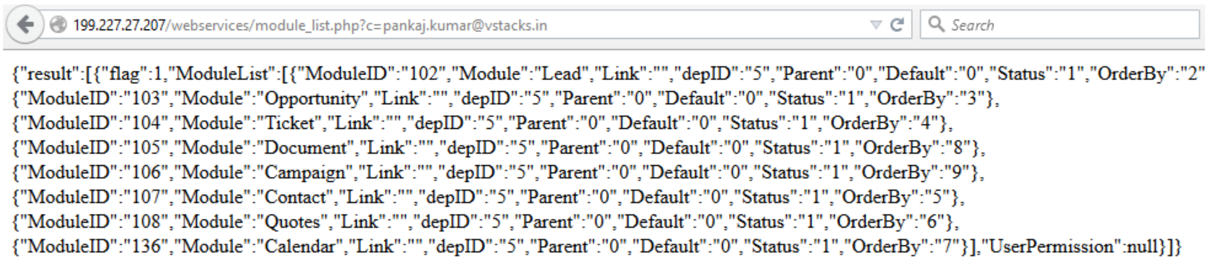
-
  http://199.227.27.207/webservices/module_list.php?c=pankaj.kumar@vstacks.in
- http://199.227.27.207/webservices/appviewAttributelead.php?c=pankaj.kumar%40vstacks.in&att_source=11&att_Status=12&att_Industry=51
- http://199.227.27.207//webservices/getAttribute.php?c=pankaj.kumar%40vstacks.in&attr=SalesStage
- http://199.227.27.207///webservices/getSateclistbycountry.php?c=pankaj.kumar%40vstacks.in&country_id=106
- http://199.227.27.207/webservices/appViewOpportunity.php?c=pankaj.kumar%40vstacks.in&page=0&UserID=37&moduleId=103

Recommendation:

It is commentated to implement proper session management in the URL.

Screen Shot:

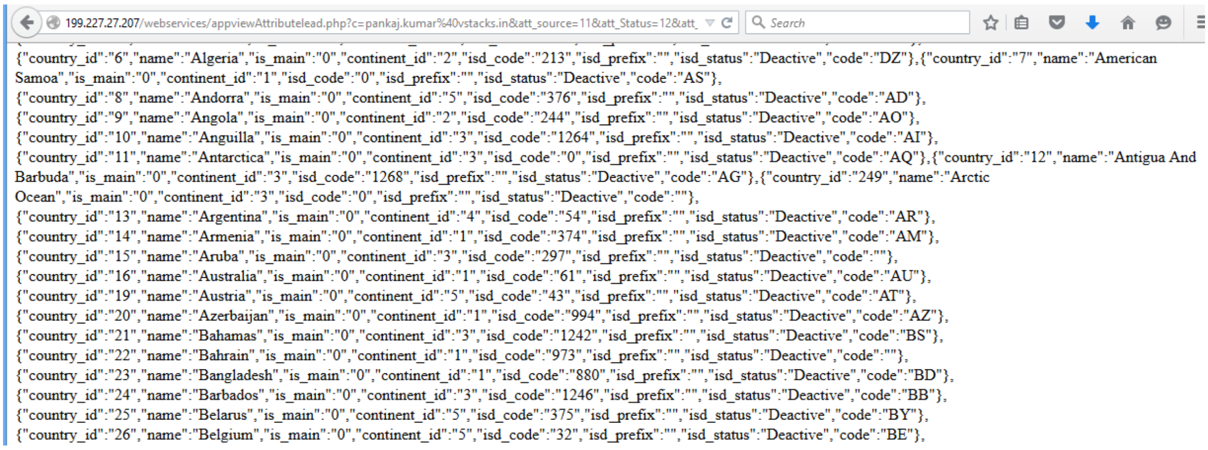
1



199.227.27.207/webservices/module_list.php?c=pankaj.kumar@vstacks.in
Search

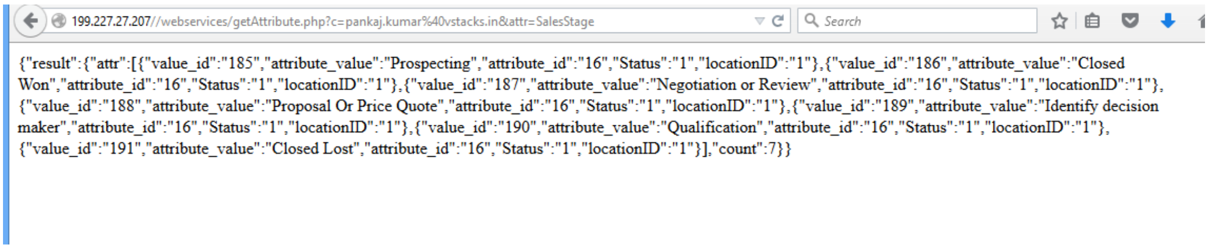
```
{"result":[{"flag":1,"ModuleList":[{"ModuleID":"102","Module":"Lead","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"2"
{"ModuleID":"103","Module":"Opportunity","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"3"},
{"ModuleID":"104","Module":"Ticket","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"4"},
{"ModuleID":"105","Module":"Document","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"8"},
{"ModuleID":"106","Module":"Campaign","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"9"},
{"ModuleID":"107","Module":"Contact","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"5"},
{"ModuleID":"108","Module":"Quotes","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"6"},
{"ModuleID":"136","Module":"Calendar","Link":"","depID":"5","Parent":"0","Default":"0","Status":"1","OrderBy":"7"}],"UserPermission":null}]}
```

2


199.227.27.207/webservices/appviewAttributelead.php?c=pankaj.kumar%40vstacks.in&att_source=11&att_Status=12&att_
Search

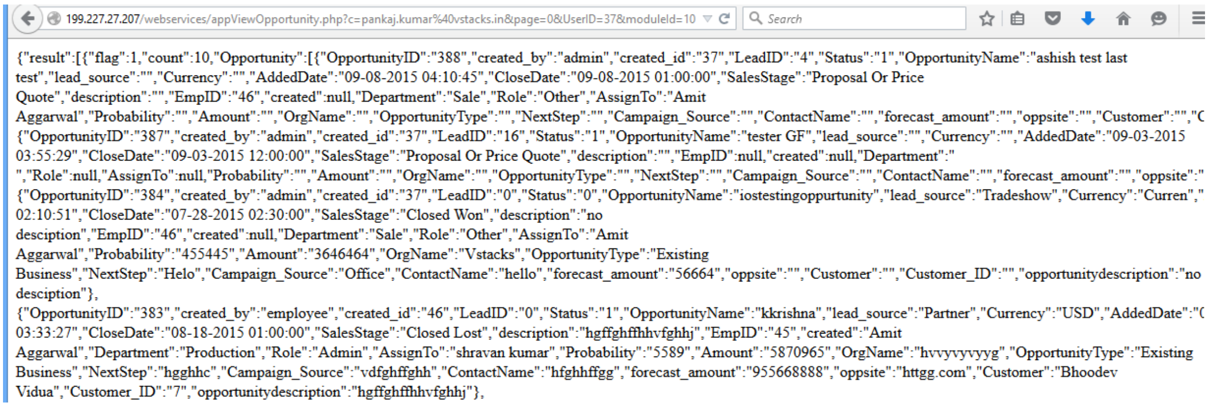
```
{"country_id":"6","name":"Algeria","is_main":"0","continent_id":"2","isd_code":"213","isd_prefix":"","isd_status":"Deactive","code":"DZ"},{"country_id":"7","name":"American
Samoa","is_main":"0","continent_id":"1","isd_code":"0","isd_prefix":"","isd_status":"Deactive","code":"AS"},
{"country_id":"8","name":"Andorra","is_main":"0","continent_id":"5","isd_code":"376","isd_prefix":"","isd_status":"Deactive","code":"AD"},
{"country_id":"9","name":"Angola","is_main":"0","continent_id":"2","isd_code":"244","isd_prefix":"","isd_status":"Deactive","code":"AO"},
{"country_id":"10","name":"Anguilla","is_main":"0","continent_id":"3","isd_code":"1264","isd_prefix":"","isd_status":"Deactive","code":"AI"},
{"country_id":"11","name":"Antarctica","is_main":"0","continent_id":"3","isd_code":"0","isd_prefix":"","isd_status":"Deactive","code":"AQ"},{"country_id":"12","name":"Antigua And
Barbuda","is_main":"0","continent_id":"3","isd_code":"1268","isd_prefix":"","isd_status":"Deactive","code":"AG"},{"country_id":"249","name":"Arctic
Ocean","is_main":"0","continent_id":"3","isd_code":"0","isd_prefix":"","isd_status":"Deactive","code":""},
{"country_id":"13","name":"Argentina","is_main":"0","continent_id":"4","isd_code":"54","isd_prefix":"","isd_status":"Deactive","code":"AR"},
{"country_id":"14","name":"Armenia","is_main":"0","continent_id":"1","isd_code":"374","isd_prefix":"","isd_status":"Deactive","code":"AM"},
{"country_id":"15","name":"Aruba","is_main":"0","continent_id":"3","isd_code":"297","isd_prefix":"","isd_status":"Deactive","code":""},
{"country_id":"16","name":"Australia","is_main":"0","continent_id":"1","isd_code":"61","isd_prefix":"","isd_status":"Deactive","code":"AU"},
{"country_id":"19","name":"Austria","is_main":"0","continent_id":"5","isd_code":"43","isd_prefix":"","isd_status":"Deactive","code":"AT"},
{"country_id":"20","name":"Azerbaijan","is_main":"0","continent_id":"1","isd_code":"994","isd_prefix":"","isd_status":"Deactive","code":"AZ"},
{"country_id":"21","name":"Bahamas","is_main":"0","continent_id":"3","isd_code":"1242","isd_prefix":"","isd_status":"Deactive","code":"BS"},
{"country_id":"22","name":"Bahrain","is_main":"0","continent_id":"1","isd_code":"973","isd_prefix":"","isd_status":"Deactive","code":""},
{"country_id":"23","name":"Bangladesh","is_main":"0","continent_id":"1","isd_code":"880","isd_prefix":"","isd_status":"Deactive","code":"BD"},
{"country_id":"24","name":"Barbados","is_main":"0","continent_id":"3","isd_code":"1246","isd_prefix":"","isd_status":"Deactive","code":"BB"},
{"country_id":"25","name":"Belarus","is_main":"0","continent_id":"5","isd_code":"375","isd_prefix":"","isd_status":"Deactive","code":"BY"},
{"country_id":"26","name":"Belgium","is_main":"0","continent_id":"5","isd_code":"32","isd_prefix":"","isd_status":"Deactive","code":"BE"},
```

3


199.227.27.207//webservices/getAttribute.php?c=pankaj.kumar%40vstacks.in&attr=SalesStage
Search

```
{"result":{"attr":[{"value_id":"185","attribute_value":"Prospecting","attribute_id":"16","Status":"1","locationID":"1"},{"value_id":"186","attribute_value":"Closed
Won","attribute_id":"16","Status":"1","locationID":"1"},{"value_id":"187","attribute_value":"Negotiation or Review","attribute_id":"16","Status":"1","locationID":"1"},
{"value_id":"188","attribute_value":"Proposal Or Price Quote","attribute_id":"16","Status":"1","locationID":"1"},{"value_id":"189","attribute_value":"Identify decision
maker","attribute_id":"16","Status":"1","locationID":"1"},{"value_id":"190","attribute_value":"Qualification","attribute_id":"16","Status":"1","locationID":"1"},
{"value_id":"191","attribute_value":"Closed Lost","attribute_id":"16","Status":"1","locationID":"1"}],"count":7}}
```

4


199.227.27.207/webservices/appViewOpportunity.php?c=pankaj.kumar%40vstacks.in&page=0&UserID=37&moduleId=10
Search

```
{"result":[{"flag":1,"count":10,"Opportunity":[{"OpportunityID":"388","created_by":"admin","created_id":"37","LeadID":"4","Status":"1","OpportunityName":"ashish test last
test","lead_source":"","Currency":"","AddedDate":"09-08-2015 04:10:45","CloseDate":"09-08-2015 01:00:00","SalesStage":"Proposal Or Price
Quote","description":"","EmpID":"46","created":null,"Department":"Sale","Role":"Other","AssignTo":"Amit
Aggarwal","Probability":"","Amount":"","OrgName":"","OpportunityType":"","NextStep":"","Campaign_Source":"","ContactName":"","forecast_amount":"","oppsite":"","Customer":"","C
{"OpportunityID":"387","created_by":"admin","created_id":"37","LeadID":"16","Status":"1","OpportunityName":"tester GF","lead_source":"","Currency":"","AddedDate":"09-03-2015
03:55:29","CloseDate":"09-03-2015 12:00:00","SalesStage":"Proposal Or Price Quote","description":"","EmpID":null,"created":null,"Department":"
","Role":null,"AssignTo":null,"Probability":"","Amount":"","OrgName":"","OpportunityType":"","NextStep":"","Campaign_Source":"","ContactName":"","forecast_amount":"","oppsite":"
{"OpportunityID":"384","created_by":"admin","created_id":"37","LeadID":"0","Status":"0","OpportunityName":"iostestingoppurtunity","lead_source":"Tradeshow","Currency":"Curren","
02:10:51","CloseDate":"07-28-2015 02:30:00","SalesStage":"Closed Won","description":"no
desciption","EmpID":"46","created":null,"Department":"Sale","Role":"Other","AssignTo":"Amit
Aggarwal","Probability":"455445","Amount":"3646464","OrgName":"Vstacks","OpportunityType":"Existing
Business","NextStep":"Helo","Campaign_Source":"Office","ContactName":"hello","forecast_amount":"56664","oppsite":"","Customer":"","Customer_ID":"","opportunitydescription":"no
desciption"},
{"OpportunityID":"383","created_by":"employee","created_id":"46","LeadID":"0","Status":"1","OpportunityName":"kkrishna","lead_source":"Partner","Currency":"USD","AddedDate":"(
03:33:27","CloseDate":"08-18-2015 01:00:00","SalesStage":"Closed Lost","description":"hgffghffhhvfghhj","EmpID":"45","created":"Amit
Aggarwal","Department":"Production","Role":"Admin","AssignTo":"shravan kumar","Probability":"5589","Amount":"5870965","OrgName":"hvyvyvyyyg","OpportunityType":"Existing
Business","NextStep":"hgghhc","Campaign_Source":"vdfghffghh","ContactName":"hfghhffgg","forecast_amount":"955668888","oppsite":"httgg.com","Customer":"Bhoodev
Vidua","Customer_ID":"7","opportunitydescription":"hgffghffhhvfghhj"},
```

Kindly Fix the Vulnerabilities throughout the Application

9.

Vulnerability Name:	**SQL Injection**
Severity:	**HIGH**

Description

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query. Various attacks can be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and executing operating system commands.

URL:

- http://199.227.27.207///webservices/getSateclistbycountry.php?c=pankaj.kumar%40vstacks.in&country_id=106
- http://199.227.27.207/webservices/appViewOpportunity.php?c=pankaj.kumar%40vstacks.in&page=0&UserID=37&moduleId=103

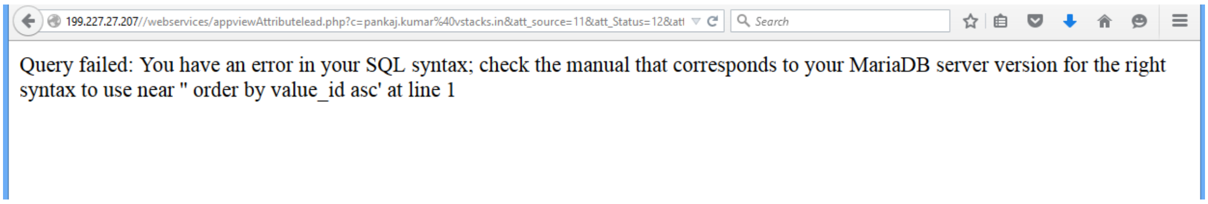
Recommendation:

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize every variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigation for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string in which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.
- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

Screen Shot:



199.227.27.207//webservices/appviewAttributelead.php?c=pankaj.kumar%40vstacks.in&att_source=11&att_Status=12&att
Search

```
Query failed: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right
syntax to use near '' order by value_id asc' at line 1
```

Kindly fix the vulnerabilities Throughout the Application