

CodeReview 08/19/2020

August 19, 2020 1:11 PM

1. SQL Injection -

- strSQL.*=.*request.getParameter*
- Concatination of strings to a query. --> sql.*=*+"

The screenshot shows a code editor interface with a search bar at the top containing the query "strSQL.*=.*request.getParameter". Below the search bar, there are tabs for "In Project", "Module", "Directory", and "Scope". The search results are displayed in a list on the right side of the screen, showing 8 matches in 4 files. The files listed are:

- medicationSummary_rightpanel.jsp
- medicationSummary_rightpanel.jsp
- medicationSummary_rightpanel.jsp
- BiometricInterface.java
- GatewayEDISetup.java
- showRxAdministration.jsp
- showRxAdministration.jsp
- showRxAdministration.jsp

The code snippets from the search results show various SQL queries being constructed by concatenating strings. For example, in medicationSummary_rightpanel.jsp, there are multiple instances of:

```
String strSQLMedSummRxItemIds = "SELECT itemid, RxOrderNo FROM glrxmain WHERE encounterId=" + DataValidation.getIntegerValue(request.getParameter("pnencid")) + " AND PatientsFlag=-1";  
String strSQLLock = "SELECT encLock, dateFrom enc WHERE encounterId=" + request.getParameter("pnencid");  
strSQLLock = "SELECT DefaultMedSummaryGroupBy FROM userprofile WHERE UserId=" + request.getParameter("lnUserId");  
strSQL += " AND BinaryImage=" + iRequest.getParameter("binaryData") + "';"  
strSQLnsUpd.append(" FTPUserId = ")append(request.getParameter("logind"))append("');"  
strSQL = "INSERT INTO structorders (encounterid, detailid, valueid, rxitemid) values (" + strEncId + "," + strStructId + ",'" + request.getParameter("lnValueId") + "');"  
strSQL = "insert into structorders (encounterid, detailid, value, rxitemid) values (" + strEncId + "," + strStructId + ",'" + request.getParameter("lnValueId") + "');"  
strSQL = "insert into structorders (encounterid, detailid, value, rxitemid) values (" + strEncId + "," + strStructId + ",'" + request.getParameter("lnValueId") + "');"
```

In ccmr_admin_main_struct.jsp, there is an update statement:

```
String strSQLMedSummRxItemIds = "SELECT itemid, RxOrderNo FROM glrxmain WHERE encounterId=" + DataValidation.getIntegerValue(request.getParameter("pnencid")) + " AND PatientsFlag=-1";  
nMedsToBeDisplayed = Integer.parseInt(catalog.itemkey.getItemKeyValueFromName(oRoot, "NedSummary_Limit", "50"));  
} catch (Exception ex){  
    EewLog.AppendExceptionToLog(ex);  
}  
  
String strSQLMedSummRxItemIds = "SELECT itemid, RxOrderNo FROM glrxmain WHERE encounterId=" + DataValidation.getIntegerValue(request.getParameter("pnencid")) + " AND PatientsFlag=-1";  
//+ " AND AssessId=0 ";  
obf.DataSet dsMedSummRxItemIds = obf.DBHelper.executeSQL(oRoot, strSQLMedSummRxItemIds);  
if(dsMedSummRxItemIds.getRows() > 0){  
    for( int ab=1; ab<=dsMedSummRxItemIds.getRows(); ab++)
```

The screenshot shows a code editor interface with a code snippet from ccmr_admin_main_struct.jsp. The code contains a string replacement operation:

```
String itemName = request.getParameter("itemname");  
itemName = itemName.replaceAll("\\", "");  
strSQL = "update structdatadetail set name = '" + itemName + "' where id =" + strId ;  
DBHelper.executeUpdate(strSQL);
```

The screenshot shows a code editor interface with a code snippet from ccmr_nf_ncaa_backgroundController.jsp. The code contains an update query:

```
String itemId = request.getParameter("itemid");  
String itemName = request.getParameter("itemname");  
String[] options = request.getParameter("options").split(",");  
String defaultValue = request.getParameter("defaultValue");  
String trigger = request.getParameter("trigger");  
oRoot = Root.createDbConnection(null);  
strSQL = "update items set itemName = "+itemName+", itemDesc = "+itemName+", keyName = "+trigger+" where itemid = "+itemId;  
pStmt = oRoot.con.prepareStatement(strSQL);  
pStmt.execute();
```

2. XSS - CrossSite Scripting :

- <%=request.getParameter(
- <%=, "request.getParameter
- .InnterHtml
- .eval(

Find in Path

Match case Words Regex ? File mask:

100+ matches in 29+ files

In Project Module Directory Scope

```
<input type="text" name="uname" id="uname" value="<%>=request.getParameter("uname")>=>null?strEmail:request.getParameter("uname")%>" maxLength=50 autoComplete="off" style="width:250px" /> MUCapture.jsp 524
var TrUserId= <%>=request.getParameter("TrUserId")>%
serviceLevel = <%>=request.getParameter("ServiceLevel")>%
userId = <%>=request.getParameter("TrUserId")>%
<input type="hidden" name="hdEnclId" id="hdEnclId" value="<%>=request.getParameter("pnrcid")>%" />
<input type="hidden" name="hdPtlId" id="hdPtlId" value="<%>=request.getParameter("ptld")>%" />
<input type="hidden" name="hdViewType" id="hdViewType" value="<%>=request.getParameter("viewType")>%" />
<input type="hidden" name="hdAssessmentId" id="hdAssessmentId" value="<%>=request.getParameter("AssessmentId")>%" />
<input type="hidden" name="hdUserldVal" id="hdUserldVal" value="<%>=request.getParameter("TrUserId")>%" />
value=<%>=request.getParameter("FromDate")>=>null?CwMobile.CwUtils.getTodaysDate("MM/dd/yyyy"):request.getParameter("FromDate")%>">
value=<%>=request.getParameter("ToDate")>=>null?CwMobile.CwUtils.getTodaysDate("MM/dd/yyyy"):request.getParameter("ToDate")%>">
value=<%>=request.getParameter("PatientId")>=>null?request.getParameter("PatientId")%>">
value=<%>=request.getParameter("PatientName")>=>null?request.getParameter("PatientName")%>">

mobiledoc/src/main/webapp/jsp/EPCSAdminConsole.jsp
241     }
242     });
243     });
244     });
245
246     serviceLevel = '<%>=request.getParameter("ServiceLevel")>%'  

247     userId = '<%>=request.getParameter("TrUserId")>%'  

248
249     if(serviceLevel == null || serviceLevel.length<1 || serviceLevel!="MailOrder")serviceLevel ="Retail";
250   );
251 }
```

3. Path Traversal

- java.io.FileInputStream fileInputStream=new java.io.FileInputStream(strLogDirName + strFileName);
- File.delete()
- fileName
- path
- <http://localhost:8080/mobiledoc/jsp/webemr/visionplan/downloadRefundReport.jsp?filePath=C:\eClinicalWorks\tomcat\test.txt&fileName=test.txt>

```
<%
String filePath=request.getParameter("filePath");
String fileName=request.getParameter("fileName");
try{
//Download in browser.
response.setContentType("text/html");
java.io.PrintWriter out1 = response.getWriter();
response.setContentType("APPLICATION/OCTET-STREAM");
response.setHeader("Content-Disposition", "attachment; filename=\"" + fileName + "\"");
java.io.InputStream fileInputStream = new java.io.InputStream(filePath);
int i;
while ((i = fileInputStream.read()) != -1) {
    out1.write(i);
}
fileInputStream.close();
out1.close();
}
catch(Exception ex){
com.ecw.dao.EcwLog.AppendExceptionToLog(ex);
}
finally{
java.io.File objLogFile=new java.io.File(filePath);
if(objLogFile.exists()){
objLogFile.delete();
}
}
%>
```

4. Command injection

- Runtime.getRuntime().exec(command);

Find in Path

In Project Module Directory Scope

```
public Process exec(String[] cmdarray) throws IOException {
    Process proc = Runtime.getRuntime().exec(command);
    Process proc = Runtime.getRuntime().exec(command);
    Process proc = Runtime.getRuntime().exec(command1);
    Process proc = Runtime.getRuntime().exec(command);
    Process proc = Runtime.getRuntime().exec(command);
    Process runtimeProcess = Runtime.getRuntime().exec(executeCmd);
    runtimeProcess = Runtime.getRuntime().exec(executeCmd);

buildSrc/src/main/java/git/GitUtility.java

173
174     public String executeCommand(String [] command) throws Exception{
175         String result = "";
176         BufferedReader br = null;
177         BufferedReader br1 = null;
178         InputStreamReader isr = null;
179         InputStreamReader esr =null;
180
181         try {
182             Process proc = Runtime.getRuntime().exec(command);
183             isr = new InputStreamReader(proc.getInputStream());
184             esr = new InputStreamReader(proc.getErrorStream());
185             br = new BufferedReader(isr);
186             br1 = new BufferedReader(esr);
187
188             String line = "";
189             result = "";
190
191         } catch (IOException e) {
192             e.printStackTrace();
193         }
194     }
195 }
```

5. XXE:

pattern:
.parse(xml)

XML Parsers in Java:

- javax.xml.validation.Validator
- SchemaFactory
- SAXTransformerFactory
- XMLReader
- SAXReader
- JAXB Unmarshaller

Find in Path

Match case Words Regex ? File mask: *.java

14 matches in 6 files

In Project Module Directory Scope

```
DOMParser domParser = new DOMParser();

mobilePhyPortal/src/main/java/portal/PXHelper.java

159     public static Document getXmlDocument(String strData, boolean bParseFile) throws IOException, org.xml.sax.SAXException
160     {
161         String strXml = null;
162
163         DOMParser domParser = new DOMParser();
164         domParser.setFeature( s: "http://apache.org/xml/features/disallow-doctype-decl" , b: true);
165         domParser.setFeature( s: "http://xml.org/sax/features/external-parameter-entities" , b: false);
166         domParser.setFeature( s: "http://xml.org/sax/features/external-general-entities" , b: false);
167
168         strData = strData.trim();
169         strXml = "<?xml version='1.0' encoding='UTF-8'?>" + strData;
170         if (bParseFile)
171         {
172             domParser.parse(strData);
173         }
174         else
175         {
176             org.xml.sax.InputSource oIn = new org.xml.sax.InputSource(new StringReader(strXml));
177             domParser.parse(oIn);
178         }
179     }

OBFAdminHelper.java
mobilePhyPortal/PXHelper.java
mobilePhyPortal/PXHelper.java
mobilePhyPortal/PXHelper.java
mobilePhyPortal/PXHelper.java
mobilePhyPortal/PXHelper.java
CwXmlHelper.java
CwXmlHelper.java
CwXmlHelper.java
```

6. ReadLine Vulnerability :

- request.getReader
- readLine()
- while((jsonString = reader.readLine()) != null){
 - <http://10.211.35.77:8123/mobiledoc/jsp/allergy/ShotSchedule/ShotAjaxPage.jsp?opt=SaveBottle>

```
mobiledoc/src/main/webapp/jsp/allergy/ShotSchedule/ShotAjaxPage.jsp
58
59
60
61     e.printStackTrace();
62 }
63 }else if (request.getParameter("opt") != null && request.getParameter("opt").equals("UpdateBottle")) {
64     try{
65         Map inputMap = new HashMap();
66         List<Map> proLst = new ArrayList<Map>();
67         response.setContentType("application/json");
68         StringBuilder buffer = new StringBuilder();
69         BufferedReader reader = request.getReader();
70         String jsonString;
71         while((jsonString = reader.readLine()) != null){
72             buffer.append(jsonString);
73         }
74     }
75 }
```

8. Session test on the product.

- Collect all the project routes(URLs)
- Collect all the servlets
- Hit all the urls without authenticated session,Using intruder
- Observe the responses 200,500
- identify urls supposed to work w/o authenticated session. Audit them.

9. Header Injection

```
response.setHeader("Content-Disposition", "attachment; filename=\"" + request.getParameter("strZipFileName") + "\");
```

10. Insecure Deserialization

r00

Be aware of the following Java API uses for potential serialization vulnerability.

1. XMLdecoder with external user defined parameters
2. XStream with fromXML method
(xstream version <= v1.46 is vulnerable to the serialization issue)
3. ObjectInputStream with readObject
4. Uses of readObject, readObjectNodData, readResolve OR readExternal
5. ObjectInputStream.readUnshared
6. Serializable

Reference:

https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html

11. Out of band communication:

- HttpURLConnection conn = (HttpURLConnection) url.openConnection();
- https://
- http://
- ftp://
-

12. Sensitive information in queryString :

- +password+
- &password=
- &SSN
- Sessionid
- token
- PHI
- PII

13. Vulnerable Cryptography Algorithms used

- MD5
- MD4
- SHA-1

14. Sensitive information in logs:

```
username
password
token
Phi
Pii
Sessionid
```

The screenshot shows a search interface with the query 'appendtolog.*password'. It lists 42 matches across 24 files. Some of the highlighted log entries include:

- InterfaceLogger AppendToLog("Please set MQ Username and Password to start MQ due to interopUseCredentialForMQ is Enabled ");
- EcwLog AppendToLog("Please set MQ Username and Password to start MQ due to interopUseCredentialForMQ is Enabled ");
- InterfaceLogger AppendToLog("interopUseCredentialForMQ: "+ bSecureMQ + " MQUsername: " + strUsername + " MQPassword: " + strPassword, PM, nInterfaceld);
- InterfaceLogger AppendToLog("Please set MQ Username and Password to start MQ due to interopUseCredentialForMQ is Enabled ");
- EcwLog AppendToLog("Please set MQ Username and Password to start MQ due to interopUseCredentialForMQ is Enabled ");
- InterfaceLogger AppendToLog("In checkMD5Password: "+ strSqlIntType);
- EcwLog AppendToLog("debugging date "+ new Date().toString()); empi.objects.PatientMigration-> preparePatientList :: strPassword = "");
- EcwLog AppendToLog("debugging date "+ new Date().toString()); empi.objects.PatientMigration-> readExcelFile :: strPassword = "");
- EcwLog AppendToLog("Parameters are not properly configured strUrl: "+strUrl+ " strSId: "+strSId+ " strPwrd: "+strPwrd);
- EcwLog AppendToLog("Failed to decrypt Password or login with Kiosk Auth Type 1");
- EcwLog AppendToLog("Password changed successfully and message to user in not sent.");
- oRoot AppendToLog("invalid user username: "+uname+", password: "+password);
- AppendToLog("strFTPHostname "+strFTPHostname+ " strFTPUUsername "+strFTPUUsername+ " strFTPUsername "+strTPassword+ " strTPassword");
- AppendToLog("strFTPHostname "+ftp_Host+ " strFTPUUsername "+ftp_User+ " strTPassword "+ftp_Pwd);
- InterfaceLogger AppendToLog("dimock certPwd value: "+ certPassword, PMUtility.intfType, PM);

15. Trust Boundary Violation :

The screenshot shows a search interface with the query 'session.setAttribute.*request.getParameter'. It lists many matches across multiple files. Some of the highlighted code snippets include:

- session.setAttribute("clientname",request.getParameter("clientname"));
- session.setAttribute("followup",request.getParameter("followup"));
- session.setAttribute("activity",request.getParameter("activity"));
- session.setAttribute("activitySubtype",request.getParameter("activitySubtype"));
- session.setAttribute("voicoid",DataValidation.sanitizeInt(request.getParameter("Invid")));
- session.setAttribute("k",request.getParameter("k"));
- session.setAttribute("l",request.getParameter("l"));
- session.setAttribute("voicoid",request.getParameter("Invid"));
- session.setAttribute("voicoid",DataValidation.sanitizeInt(request.getParameter("Invid")));
- session.setAttribute("GUID",request.getParameter("GUID"));
- session.setAttribute("GUID",request.getParameter("GUID"));
- session.setAttribute("GUID",request.getParameter("GUID"));
- session.setAttribute("GUID",request.getParameter("GUID"));
- session.setAttribute("GUID",request.getParameter("GUID"));
- session.setAttribute("voicoid",DataValidation.escapeStringForHTML(request.getParameter("Invid")));

16. Sensitive Data Disclosure in Response:

```
- <%=.*password
- <%=.*session
```

```
try
{
    catalog.SafeMed oSM = new catalog.SafeMed();
    strXML = oSM.GetProblemList(strData);
}
catch( Exception ex )
{
    strXML = CwXmlHelper.getErrorXml(ex.getMessage());
}

<%><%=strXML%><%@page import="catalog.CwXmlHelper"%>
```

Find in Path

Match case Words Regex ? File mask: *.java

22 matches in 20 files

<TD class="Data"><INPUT type="password" width="" id=pass name=pass value= "<%&strPassword%>" align=left class="select"></TD>

setAvailabilityInfo.jsp 179

var strForgotPasswordEnabled = <%&strForgotPasswordEnabled%>

. You have until <%&strPwdGuideLineEnforceDt%> to update your password

var canSetPassword = <%&canSetPassword%>;

<option value="01"><%&x12cfg.getISA03().equalsIgnoreCase("01")?"selected":""%> title="01 - Password">01 - Password</option>

<option value="01"><%&x12cfg.getISA03().equalsIgnoreCase("01")?"selected":""%> title="01 - Password">01 - Password</option>

<option value="01"><%&x12cfg.getISA03().equalsIgnoreCase("01")?"selected":""%> title="01 - Password">01 - Password</option>

ftpPasswd = <%&strFtpPassword%> "/>

<option value="01"><%&objx270cfg.getISA03().equalsIgnoreCase("01")?"selected":""%> title="01 - Password">01 - Password</option>

messageForChangePassword: This password expires in + <%&nDiffDays%> + days. Do you want to change the password now?

<option value="01"><%&x12cfg.getISA03().equalsIgnoreCase("01")?"selected":""%> title="01 - Password">01 - Password</option>

<td class="Data"><input type="password" id="ftpwdid" name="ftppwd" value= "<%&strFtpPassword%>" align="left" style="WIDTH: 200px; HEIGHT: 20px">

<td><input type="password" value= <%&DataValidation.escapeStringForHTML(strPassword)%> name = pwd' id = pwd' value= ></td>

<input type="hidden" value= <%&DataValidation.escapeStringForHTML(strPassword)%> id="password" name="password">

<%&strHostName%>&hostport-&dbname=<%&strDbName%>&instanceName=<%&DataValidation.escapeStringForJavaScript(strDbInstance)%>&username=<%&DataValidat

PatientPaymentPostingLog.jsp 327

updateX12CfInfo.jsp 112

billingmenu/updateX12Info.jsp 112

emdeonPatientSetup.jsp 125

update270Cfg.jsp 330

changePasswordOnLogin.jsp 135

Endonstmt.jsp 188

getDatabase.jsp 133

updateX12CfInfo.jsp 327

ImportMedicareDataFromCloud.jsp 264

ShowConfigurationRealTimeClaimStatus.jsp 128

quoteIndex.jsp 63

SaveConfig.jsp 19

PdmSettings.jsp 131

accessEClInMobileAcctn.jsp 354

<input type="hidden" name="corpDhdId" id="corpDhdId" value= <%&DataValidation.escapeStringForHTML(strCorpPassword)%>">

var selpwd = <%&DataValidation.escapeStringForJavaScript(strClearingHousePassword)%>;

var pass = <%&mypassword%>;

<jsp:setProperty name="URLConfigbean" property="password" value= <%&strPassword%> />

Password&nbsp<input type="password" id="password_0" value= <%&DataValidation.escapeStringForHTML(strPassword)%>" style="width:200px;">

=<%&uid %>&TrUserId=<%&nTrUserId %><>Forgot eClinicalMobile Password

<tr height='20pt'><td class="tableCell" ><a href='/mobiledoc/jsp/mobilephyportal/accessEClInMobileAcctn.jsp?uid=<%&uid %>&TrUserId=<%&nTrUserId %>'><u>Password Settings</u>, MobileSettings.jsp 73

mobiledoc/src/main/webapp/jsp/admin/setAvailabilityInfo.jsp

173

174

175

<TD class="DataLabel" >Password: </TD>

<#if (&IsExist){ >

<TD class="Data"><INPUT type="password" width="" id=pass name=pass value="<%&strPassword%>" align=left

Ctrl+Enter Open in Find Window

```
sendRedirect(Request.getparam(url))  
Req.forward(Request.getparam(url))
```

```
Response.set-header(Request.getparam(url), 302)
```

