

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



An Toàn Ứng Dụng Web Và CSDL
Final Project

Nhóm 28:

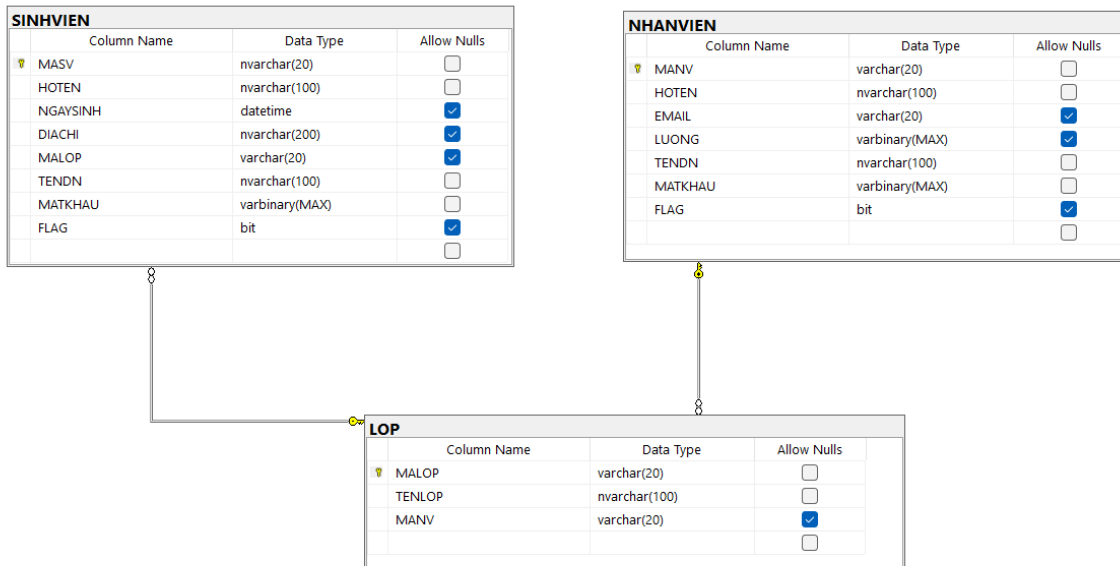
N18DCAT058: Hồ Minh Phong

N18DCAT100: Trần Quốc Trọng (c)

N18DCAT102: Huỳnh Tiến Vĩ

TP.HCM - 2021

1. Xây dựng Database QLSV



- Column FLAG trong 2 bảng NHANVIEN, SINHVIEN có nghĩa:
 - 1: dữ liệu được mã hóa phía DB
 - 0: dữ liệu được mã hóa phía Sever

2. Xây dựng web application

- Công nghệ sử dụng: Java web Spring MVC, JDBC, Tomcat 9, Eclipse
- Tạo trang login:

```
web.xml login.jsp
<div class="card-body px-lg-5 py-lg-5">
<div class="text-center text-muted mb-4">
<small>Sign in</small>
</div>
<form id="my_captcha_form" role="form" action="authentication.htm" method="post" autocomplete="off">
<div class="form-group mb-3">
<div class="input-group input-group-merge input-group-alternative">
<div class="input-group-prepend">
<span class="input-group-text"><i class="ni ni-circle-08"></i></span>
</div>
<input class="form-control" name="username" placeholder="Username" type="text" required autocomplete="off">
</div>
</div>
<div class="form-group">
<div class="input-group input-group-merge input-group-alternative">
<div class="input-group-prepend">
<span class="input-group-text"><i class="ni ni-lock-circle-open"></i></span>
</div>
<input class="form-control" name="password" placeholder="Password" type="password" required>
</div>
</div>
<div class="custom-control custom-control-alternative custom-checkbox">
<input class="custom-control-input" id=" customCheckLogin" type="checkbox" autocomplete="off">
</div>
</div>
<br>
<div class="text-center">
<div class="g-recaptcha" data-sitekey="6Lc3eEudAAAAJY_9P0Dun3qFaLCvrkWiQuSQrhh"></div>
<h6><:out value="{xm}"></h6>
<br>
<h5><:out value="{message}"> </h5>
<button id="nut" type="submit" class="btn btn-primary my-4" ${khoa} >Log in</button>
</div>
</form>
</div>
</div>
<div class="row mt-3">
```

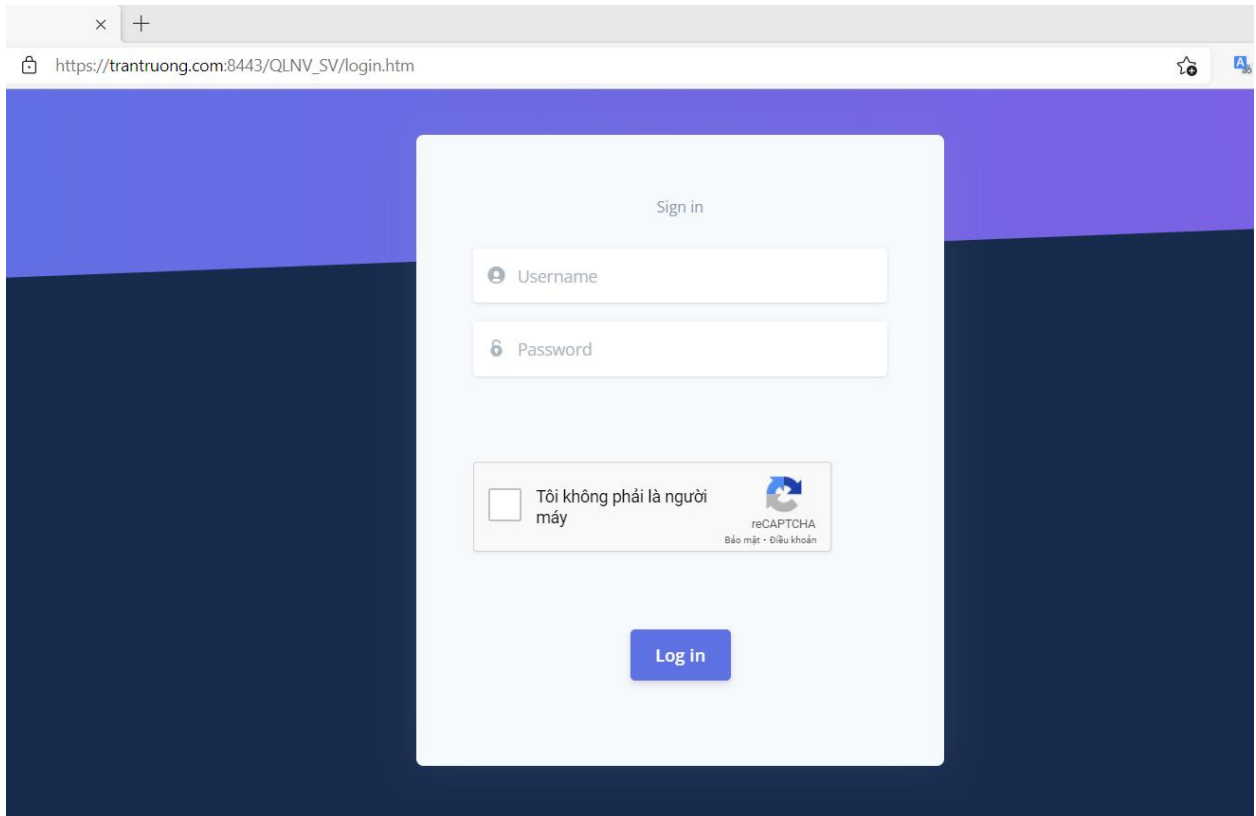


Figure 1. Login page

- Tạo trang quản lý nhân viên gồm các chức năng: thêm, xóa, sửa

```

web.xml web.xml QuanlyNhanVien.jsp
130 <!-- Light table -->
131 <div class="table-responsive">
132 <table class="table align-items-center table-flush">
133 <thead class="thead-light">
134 <tr>
135 <th scope="col" class="sort" data-sort="name">Mã Nhân Viên</th>
136 <th scope="col" class="sort" data-sort="budget">Họ Tên</th>
137 <th scope="col" class="sort" data-sort="status">Email</th>
138 <th scope="col">Luong</th>
139 <th scope="col" class="sort" data-sort="completion">User Name</th>
140 <th scope="col"></th>
141 </tr>
142 </thead>
143 <tbody class="list">
144 <c:forEach var="x" items="${staffs}">
145 <tr>
146 <th scope="row">
147 <div class="media align-items-center">
148 <div class="media-body">
149 <span class="name mb-0 text-sm"><c:out value="${x.manv}"/> </span>
150 </div>
151 </div>
152 </th>
153 <td>
154 <span class="badge badge-dot mr-4">
155 <span class="status"><c:out value="${x.hoten}"/> </span>
156 </span>
157 </td>
158 <td>
159 <div class="d-flex align-items-center">
160 <span class="completion mr-2"><c:out value="${x.email}"/> </span>
161 </div>
162 </td>
163 <td class="budget">
164 $ <c:out value="${x.luong}"/> USD
165 </td>
166 <td>
167 <div class="d-flex align-items-center">

```

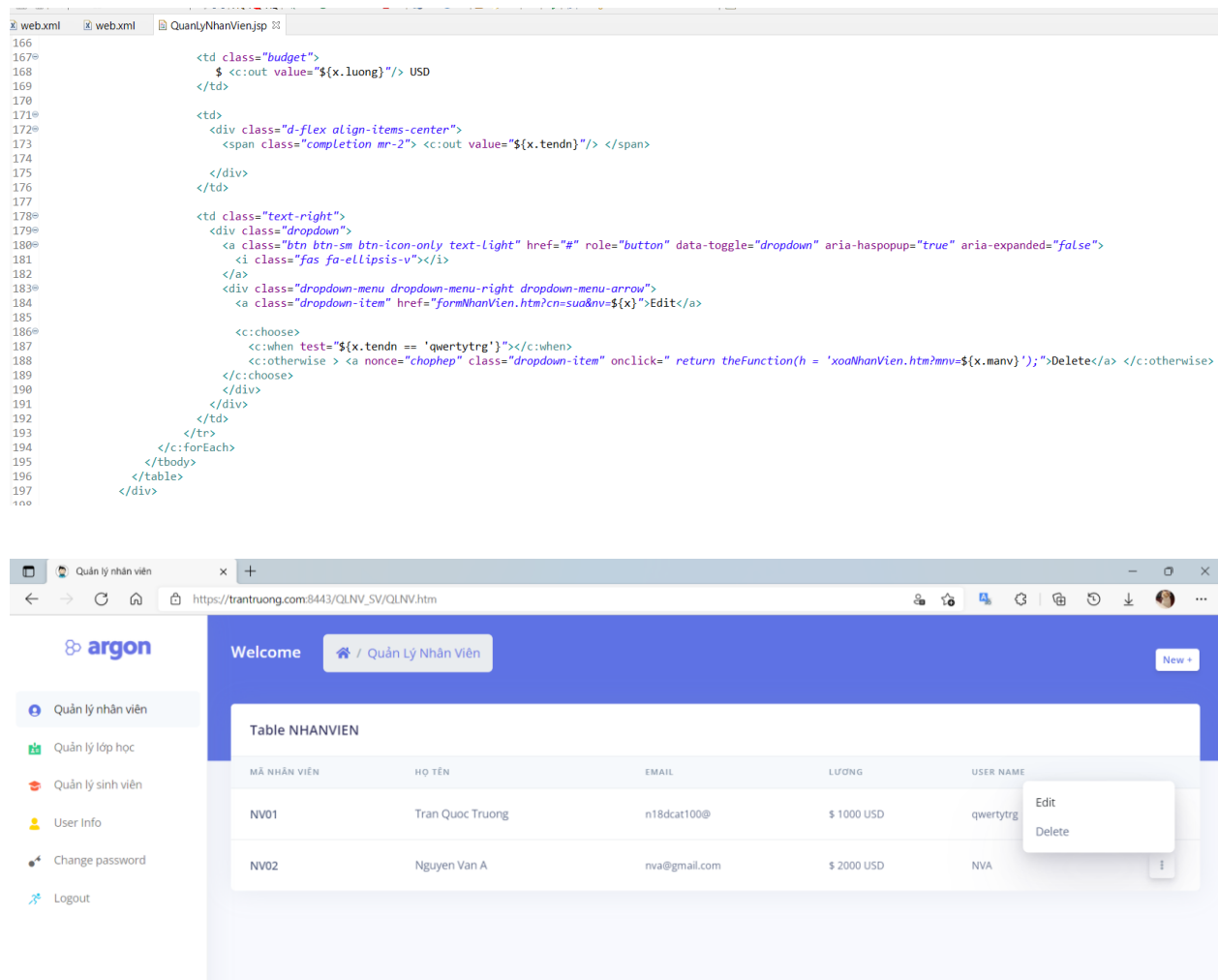


Figure 2. trang quản lý nhân viên

• Tạo form nhân viên



Form sinh viên

https://trantuan.com:8443/QLNV_SV/formNhanVien.htm?cn=them

argon

Welcome / Quản Lý Nhân Viên / Form

Quản lý nhân viên

Quản lý lớp học

Quản lý sinh viên

User Info

Change password

Logout

Edit Nhân Viên:

STAFF INFORMATION

Mã nhân viên

Email address

Họ tên

Lương

Tên đăng nhập

Mật khẩu

Submit

Figure 3. nhân viên form

- Tạo trang quản lý lớp học gồm các chức năng thêm, xóa, sửa

```

web.xml web.xml QuanLyNhanVien.jsp nhanvienForm.jsp *QuanLyLopHoc.jsp
139<tbody class="list">
140<c:forEach var="x" items="${classes}" varStatus="i">
141<tr>
142<th scope="row">
143<div class="media align-items-center">
144<div class="media-body">
145<span class="name mb-0 text-sm"> <c:out value="${i.index+1}"/> </span>
146</div>
147</div>
148</th>
149<th scope="row">
150<div class="media align-items-center">
151<div class="media-body">
152<span class="name mb-0 text-sm"> <c:out value="${x.malop}"/> </span>
153</div>
154</div>
155</th>
156<td>
157<span class="badge badge-dot mr-4">
158<span class="status"> <c:out value="${x.tenlop}"/> </span>
159</span>
160</td>
161<td>
162<div class="d-flex align-items-center">
163<span class="completion mr-2"> <c:out value="${x.manv}"/> </span>
164</div>
165</td>
166</td>
167</td>
168</td>
169</td>
170</td>
171<td class="text-right">
172<div class="dropdown">
173<a class="btn btn-sm btn-icon-only text-light" href="#" role="button" data-toggle="dropdown" aria-haspopup="true" aria-expanded="false">
174<i class="fas fa-ellipsis-v"></i>
175</a>
176<div class="dropdown-menu dropdown-menu-right dropdown-menu-arrow">
177<a class="dropdown-item" href="QLLH.htm?cn=sua&lp=${x}">Edit</a>
178<a class="dropdown-item" onclick="return theFunction(h = 'xoaLop.htm?ml=${x.malop}');">Delete</a>
179</div>
180</td>
181</td>

```

```

web.xml web.xml QuanLyNhanVien.jsp nhanvienForm.jsp *QuanLyLopHoc.jsp
244 </div>
245 <div class="card-body">
246 <form:form action="themSuaLop${kt}${MALOP}.htm" method="post" modelAttribute="lop" autocomplete="off">
247 <h6 class="heading-small text-muted mb-4">Class information</h6>
248 <div class="pl-lg-4">
249 <div class="row">
250 <div class="col-lg-11">
251 <div class="form-group">
252 <label class="form-control-label" for="input-username">Mã lớp</label>
253 <form:input autocomplete="off" type="text" id="input-username" class="form-control" placeholder="MALOP" required="required" pattern="LOP[0-9]{2}" title="LOP?? example LOP01" />
254 </div>
255 </div>
256 </div>
257 </div>
258 <div class="row">
259 <div class="col-lg-11">
260 <div class="form-group">
261 <label class="form-control-label" for="input-first-name">Tên lớp</label>
262 <form:input autocomplete="off" type="text" id="input-first-name" class="form-control" placeholder="TENLOP" required="required" pattern="[A-Za-z]{1,99}" maxlength="99" title="TENLOP?? example TENLOP01" />
263 </div>
264 </div>
265 </div>
266 </div>
267 </div>
268 <div class="row">
269 <div class="col-lg-11">
270 <div class="form-group">
271 <label class="form-control-label" for="input-first-name">Mã nhân viên</label>
272 <form:select autocomplete="off" class="form-control" required="required" path="manv">
273 <:forEach var="x1" items="{ids}">
274 <option <:if test="{lop2.manv == x1}">selected</c:if> value="{x1}"> {x1}</option>
275 </c:forEach>
276 </form:select>
277 </div>
278 </div>
279 </div>
280 </div>
281 </div>
282 </div>
283 </div>
284 </div>
285 <hr class="my-4" />
286

```

```

web.xml web.xml QuanLyNhanVien.jsp nhanvienForm.jsp *QuanLyLopHoc.jsp
268 <div class="row">
269 <div class="col-lg-11">
270 <div class="form-group">
271 <label class="form-control-label" for="input-first-name">Mã nhân viên</label>
272 <form:select autocomplete="off" class="form-control" required="required" path="manv">
273 <:forEach var="x1" items="{ids}">
274 <option <:if test="{lop2.manv == x1}">selected</c:if> value="{x1}"> {x1}</option>
275 </c:forEach>
276 </form:select>
277 </div>
278 </div>
279 </div>
280 </div>
281 </div>
282 </div>
283 </div>
284 </div>
285 <hr class="my-4" />
286
287 <div class="row">
288 <div class="col-lg-11">
289 <div class="form-group">
290 <label class="form-control-label" for="input-first-name">Chức năng: </label>
291 <div class="custom-control custom-radio custom-control-inline">
292 <input autocomplete="off" type="radio" id="customRadioInline1" name="customRadioInline1" class="custom-control-input" value="them" ${insertChecked}>
293 <label class="custom-control-label" for="customRadioInline1">Insert</label>
294 </div>
295 <div class="custom-control custom-radio custom-control-inline">
296 <input autocomplete="off" type="radio" id="customRadioInline2" name="customRadioInline1" class="custom-control-input" value="sua" ${updateChecked}>
297 <label class="custom-control-label" for="customRadioInline2">Update</label>
298 </div>
299 </div>
300 </div>
301 </div>
302 <div>
303 <button class="btn btn-primary" name="{chucnang}" type="submit">Submit</button>
304
305 </div>
306

```

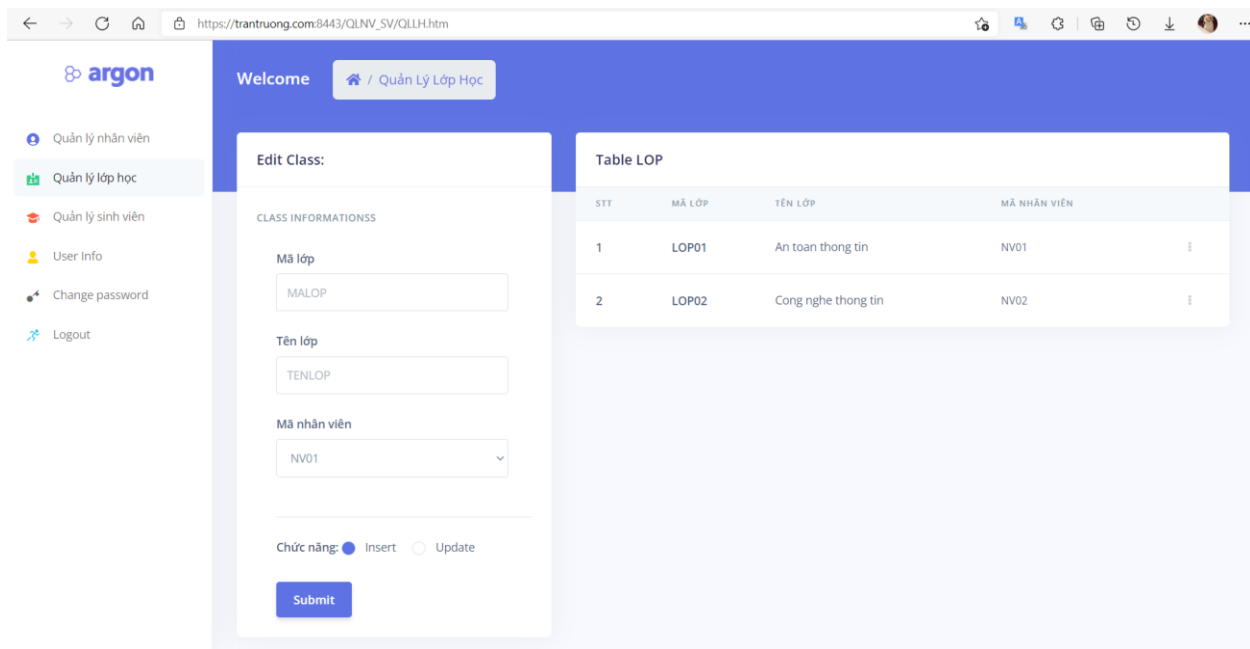


Figure 4. trang quản lý lớp học

- **Tạo trang quản lý sinh viên gồm các chức năng thêm, xóa, sửa, tìm kiếm:**

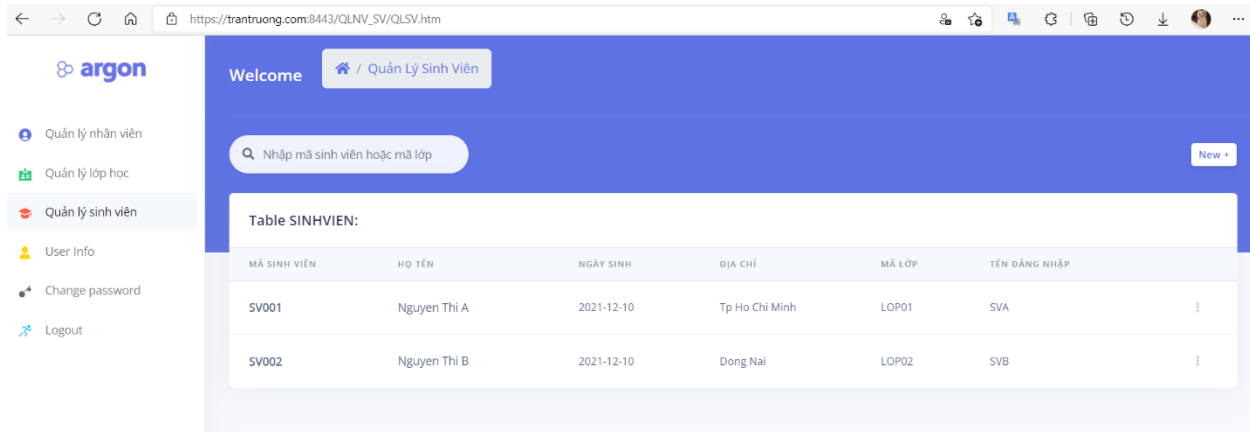


Figure 5. trang quản lý sinh viên

```

115<div class="header-body">
116<div class="row align-items-center py-4">
117
118<div class="col-lg-6 col-7">
119<form action="timkiem.htm" method="post" class="navbar-search navbar-search-light form-inline mr-sm-3" id="navbar-search-main" autocomplete="off">
120<div class="form-group mb-0">
121<div class="input-group input-group-alternative input-group-merge">
122<div class="input-group-prepend">
123<span class="input-group-text"><i class="fas fa-search"></i></span>
124<div>
125<input autocomplete="off" class="form-control" title="nhập ALL để hiển thị tất cả sinh viên" placeholder="Nhập mã sinh viên hoặc mã lớp" type="text" name="ma">
126</div>
127</div>
128<button type="button" class="close" data-action="search-close" data-target="#navbar-search-main" aria-label="Close">
129<span aria-hidden="true"></span>
130</button>
131</form>
132</div>
133

```

```
web.xml web.xml QuanLyNhanVien.jsp nhanvienForm.jsp *QuanLyLopHoc.jsp QuanLySinhVien.jsp
163<div class="table-responsive">
164<table class="table align-items-center table-flush">
165<thead class="thead-light">
166<tr>
167<th scope="col" class="sort" data-sort="name">Mã Sinh Viên</th>
168<th scope="col" class="sort" data-sort="budget">Họ Tên</th>
169<th scope="col" class="sort" data-sort="status">Ngày Sinh</th>
170<th scope="col">Địa Chỉ</th>
171<th scope="col" class="sort" data-sort="completion">Mã Lớp</th>
172<th scope="col" class="sort" data-sort="completion">Tên Đăng Nhập</th>
173<th scope="col"></th>
174</tr>
175</thead>
176<tbody class="list">
177<c:forEach var="x" items="${students}">
178<tr>
179<th scope="row">
180<div class="media align-items-center">
181<div class="media-body">
182<span class="name mb-0 text-sm"><c:out value="${x.masv}"/> </span>
183</div>
184</div>
185</th>
186
187<td>
188<span class="badge badge-dot mr-4">
189<span class="status"><c:out value="${x.hoten}"/> </span>
190</span>
191</td>
192
193<td>
194<div class="d-flex align-items-center">
195<span class="completion mr-2"><c:out value="${x.ngaysinh}"/> </span>
196
197</div>
198</td>
199
200<td class="budget">
201<c:out value="${x.diachi}"/>
202</td>
203
204<td>
205<div class="d-flex align-items-center">
```

```
.xml QuanLyNhanVien.jsp nhanvienForm.jsp *QuanLyLopHoc.jsp QuanLySinhVien.jsp
</td>
<td>
<div class="d-flex align-items-center">
<span class="completion mr-2"><c:out value="${x.malop}"/> </span>
</div>
</td>
<td>
<div class="d-flex align-items-center">
<span class="completion mr-2"><c:out value="${x.tendn}"/> </span>
</div>
</td>
<td class="text-right">
<div class="dropdown">
<a class="btn btn-sm btn-icon-only text-light" href="#" role="button" data-toggle="dropdown" aria-haspopup="true" aria-expanded="false">
<i class="fas fa-ellipsis-v"></i>
</a>
<div class="dropdown-menu dropdown-menu-right dropdown-menu-arrow">
<a class="dropdown-item" href="goformsv.htm?cn=sua&sv=${x}">Edit</a>
<a class="dropdown-item" onclick="return theFunction(h = 'xoaSinhVien.htm?msv=${x.masv}');">Delete</a>
</div>
```


• Tạo form sinh viên:

```
web.xml  web.xml  QuanLyNhanVien.jsp  nhanvienForm.jsp  *QuanLyLopHoc.jsp  QuanLySinhVien.jsp  sinhVienForm.jsp  ❏
130<div class="card-body">
131<!-- form -->
132<h6 class="heading-sm-ll text-muted mb-4">Student information</h6>
133<div class="pl-lg-4">
134<div class="row">
135<div class="col-lg-6">
136<div class="form-group">
137<label class="form-control-label" for="input-username">Mã sinh viên</label>
138<form:input autocomplete="off" type="text" id="input-username" class="form-control" placeholder="MASV" required="required" pattern="SV[0-9]{3}" title="SV??? example SV001, SV002" value="" />
139</div>
140</div>
141
142<div class="col-lg-6">
143
144<div class="form-group">
145<label class="form-control-label" for="input-first-name">Mã lớp</label>
146
147<form:select class="form-control" required="required" path="maLop" autocomplete="off">
148<:forEach var="x1" items="${ids}">
149<option <:if test="${sinhvien2.maLop == x1}">selected</if> value="${x1}">${x1}</option>
150</:forEach>
151
152</form:select>
153</div>
154</div>
155</div>
156
157<div class="row">
158
159<div class="col-lg-6">
160<div class="form-group">
161<label class="form-control-label" for="input-username">Họ tên</label>
162<form:input autocomplete="off" type="text" id="input-username" class="form-control" placeholder="HOTEN" pattern="[A-Za-z]{1,99}" maxlength="99" title="no special characters, numbers" value="" />
163</div>
164</div>
165
166<div class="col-lg-6">
167<div class="form-group">
168<label for="example-date-input" class="form-control-label">Ngày sinh</label>
169<form:input class="form-control" type="date" placeholder="year/month/day" required="required" value="${sinhvien2.ngaysinh}" id="example-date-input" path="ngaysinh"/>
170</div>
171</div>
172</div>
173
174<div class="row">
175
176<div class="col-lg-12">
177<div class="form-group">
178<label class="form-control-label" for="input-username">Địa chỉ</label>
179<form:input autocomplete="off" type="text" id="input-username" class="form-control" placeholder="DIACHI" required="required" pattern="[-.,A-Za-z0-9\s]{1,199}" maxlength="199" value="${sinhvien2.diaChi}" />
180</div>
181</div>
182</div>
183
184<div class="row">
185<div class="col-lg-6">
186<div class="form-group">
187<label class="form-control-label" for="input-first-name">Tên đăng nhập</label>
188<form:input autocomplete="off" type="text" id="input-first-name" class="form-control" placeholder="TENDN" required="required" pattern="[A-Za-z0-9]{1,99}" maxlength="99" title="no special characters, numbers" value="" />
189</div>
190</div>
191<div class="col-lg-6">
192<div class="form-group">
193<label class="form-control-label" for="input-last-name">Mật khẩu</label>
194<form:input autocomplete="off" type="text" id="input-last-name" class="form-control" placeholder="MATHAU" required="required" pattern="^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]{8,}$" />
195</div>
196</div>
197</div>
198
199<div class="row">
200
201<div class="col-lg-12">
202<button class="btn btn-primary" type="submit" name="${chucnang}">Submit</button>
203</div>
204</div>
205</form>
206</div>
207</div>
208</div>
```

Form sinh viên

https://trantruong.com:8443/QLNV_SV/goformsv.htm?cn=them

argon

Welcome / Quản Lý Sinh Viên / Form

Quản lý nhân viên

Quản lý lớp học

Quản lý sinh viên

User Info

Change password

Logout

Edit Sinh Viên:

STUDENT INFORMATION

Mã sinh viên

Mã lớp

Họ tên

Ngày sinh

Địa chỉ

Tên đăng nhập

Mật khẩu

Submit

Figure 6. Form sinh vien

- **Tạo trang đổi mật khẩu**

ssword

https://trantruong.com:8443/QLNV_SV/changepass.htm

Change Password

qwertytrg

Current Password

New Password

Confirm Password

Change pass

Figure 7. change pasword page

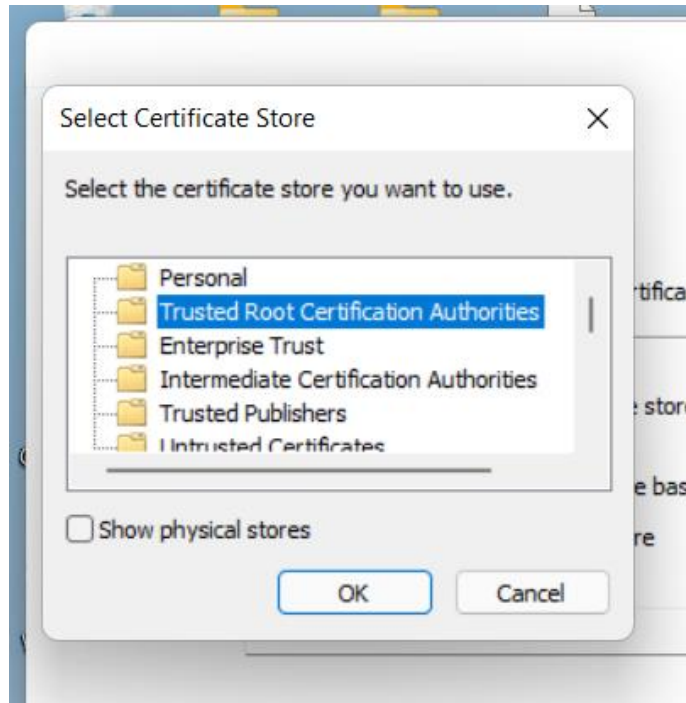


Figure 9. Thêm chứng chỉ vào Trusted Root CA





 mycert3.p12	12/7/2021 3:54 PM	Personal Informati...
 mycertificate3.jks	12/7/2021 3:56 PM	JKS File
 server.crt	12/7/2021 3:52 PM	Security Certificate
 server.key	12/7/2021 3:52 PM	KEY File

Figure 10. Tạo mycertificate3.jks từ 2 file .crt và .key

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" sslEnabledProtocols="TLSv1.2" schema="https" secure="true"
keystoreFile="C:\xampp\tomcat\conf\cert\mycertificate3.jks" keystorePass="Qwertytrg2"/>
```

Figure 11. cấu hình SSL cho tomcat trong file server.xml

- Chức năng thêm dữ liệu cột lương và mật khẩu được mã hóa phía server trước khi thêm vào DB

```

94 public static String encryptAES(String input) throws NoSuchPaddingException, NoSuchAlgorithmException,
95     InvalidAlgorithmParameterException, InvalidKeyException,
96     BadPaddingException, IllegalBlockSizeException, InvalidKeySpecException {
97     IvParameterSpec iv = generateIv();
98     SecretKey key = getKeyFromPassword(password);
99     Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
100     cipher.init(Cipher.ENCRYPT_MODE, key, iv);
101     byte[] cipherText = cipher.doFinal(input.getBytes());
102     String result = byte2hex(cipherText);
103     return result;
104 }
105
106
107 public static String decryptAES(byte[] cipherText) throws NoSuchPaddingException, NoSuchAlgorithmException,
108     InvalidAlgorithmParameterException, InvalidKeyException,
109     BadPaddingException, IllegalBlockSizeException, InvalidKeySpecException {
110
111     IvParameterSpec iv = generateIv();
112     SecretKey key = getKeyFromPassword(password);
113
114     Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
115     cipher.init(Cipher.DECRYPT_MODE, key, iv);

```

Figure 12. Mã hóa lương sử dụng AES

```

1 package Security;
2
3 import java.io.UnsupportedEncodingException;
4
21
22 public class Ciphers {
23     private static String password = "N18DCAT100";
24
25 public static String sha1(String input) throws NoSuchAlgorithmException {
26     String sha1 = null;
27     try {
28         MessageDigest msdDigest = MessageDigest.getInstance("SHA-1");
29         msdDigest.update(input.getBytes("UTF-8"), 0, input.length());
30         byte[] array = msdDigest.digest();
31         sha1 = byte2hex(array);
32     } catch (UnsupportedEncodingException | NoSuchAlgorithmException e) {
33         //Logger.getLogger(Encriptacion.class.getName()).log(Level.SEVERE, null, e);
34     }
35     return sha1;
36 }
37
38 public static SecretKey generateKey(int n) throws NoSuchAlgorithmException {
39     KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
40     keyGenerator.init(n);
41     SecretKey key = keyGenerator.generateKey();
42     return key;
43 }
44
45 public static SecretKey getKeyFromPassword(String password)
46     throws NoSuchAlgorithmException, InvalidKeySpecException {
47
48     SecretKeyFactory factory = SecretKeyFactory.getInstance("PBKDF2WithHmacSHA256");
49     KeySpec spec = new PBEKeySpec(password.toCharArray(), password.getBytes(), 65536, 256);
50     SecretKey secret = new SecretKeySpec(factory.generateSecret(spec).getEncoded(), "AES");
51     return secret;
52 }
53
54 public static IvParameterSpec generateIv() {
55     byte[] iv = new byte[16];
56     //new SecureRandom().nextBytes(iv);
57     //iv = "Example String".getBytes();
58     return new IvParameterSpec(iv);
59 }
60

```

Figure 13. Mật khẩu được hash SHA1

- Chức năng sửa dữ liệu cột lương và mật khẩu được mã hóa phía DB

```
-- sửa nhân viên
create proc update_nhanvien
    @MANVCu varchar(20),
    @MANVmoi varchar(20),
    @HOTEN nvarchar(100),
    @EMAIL varchar(20),
    @LUONG int,
    @TENDN nvarchar(100),
    @MATKHAU varchar(max),
    @FLAG bit
as
    declare @luongMahoa varbinary(max)
    open symmetric key myKey_AES_256 decryption by password = '123456'
    set @luongMahoa = ENCRYPTBYKEY(KEY_GUID('myKey_AES_256'), CONVERT(nvarchar, @LUONG))
    close symmetric key myKey_AES_256

    declare @matkhauHashed varbinary(max)
    set @matkhauHashed = HASHBYTES('SHA1', @MATKHAU)

update NHANVIEN
set MANV = @MANVmoi, HOTEN = @HOTEN, EMAIL = @EMAIL, LUONG = @luongMahoa, TENDN = @TENDN, MATKHAU = @matkhauHashed, FLAG = @FLAG
where MANV = @MANVCu
go

-- sửa sinh viên
create proc update_sinhvien
    @MASVCu nvarchar(20),
    @MASV nvarchar(20),
    @HOTEN nvarchar(100),
    @NGAYSINH datetime,
    @DIACHI nvarchar(200),
    @MALOP varchar(20),
    @TENDN nvarchar(100),
    @MATKHAU varchar(max),
    @FLAG bit
as
    declare @matkhauHashed varbinary(max)
    set @matkhauHashed = HASHBYTES('SHA1', @MATKHAU)

update SINHVIEN
set MASV = @MASV, HOTEN = @HOTEN, NGAYSINH = @NGAYSINH, DIACHI = @DIACHI, MALOP = @MALOP, TENDN = @TENDN, MATKHAU = @matkhauHashed, FLAG = 1
where MASV = @MASVCu
go
```

- Phòng chống SQL Injection

```
//thêm nhân viên
public static void insertNhanVien(NhanVien nv) {
    Connection kn = ConnectionMSSQL.LayKetNoi();
    //String sql = "exec insert_nhanvien '" + nv.getManv() + "', '" + nv.getHot
    String sql = "exec insert_nhanvien ?, ?, ?, ?, ?, ?, 0";
    try {
        PreparedStatement ps = kn.prepareStatement(sql);
        ps.setString(1, nv.getManv());
        ps.setString(2, nv.getHoten());
        ps.setString(3, nv.getEmail());
        ps.setBytes(4, Ciphers.hex2Byte(nv.getLuong().substring(2)));
        ps.setString(5, nv.getTendn());
        ps.setBytes(6, Ciphers.hex2Byte(nv.getMatkhau().substring(2)));
        ps.executeUpdate();
        ps.close();
        kn.close();
    } catch (SQLException e) {
        // TODO Auto-generated catch block
        //e.printStackTrace();
    }
}
```

Figure 14. Sử dụng tham số cho tất cả các lệnh truy vấn DB

```
holder="MANV" required="required" pattern="NV[0-9]{2}" title="NV?? example NV01, NV02" value="{nhanvien2.manv}" path=
```

```
.red="required" pattern="[a-z0-9._%+-]+@[a-z0-9.-]+\.[a-z]{2,}$" title="email@example.com, length no more than 20" maxl
```

```
ceholder="HOTEN" pattern="[A-Za-z\s]{1,99}" maxlength="99" title=" no special characters, numbers" required="required"
```

Figure 15. Sử dụng thuộc tính pattern kiểm soát input trong code phía client

```
44
45 public static boolean valLophoc(Lop lp) {
46     int error = 0;
47
48     if(lp.getMalop().trim().equals("") || !lp.getMalop().matches("LOP[0-9]{2}")) {
49         error++;
50     }
51
52     if(lp.getTenlop().trim().equals("") || !lp.getTenlop().matches("[A-Za-z\\s]{1,99}")) {
53         error++;
54     }
55
56     if(error != 0) {
57
58         return false;
59     }
60     return true;
61
62
63 public static boolean valSinhVien(SinhVien sv) {
64     int error = 0;
65
66     if(sv.getMasv().trim().equals("") || !sv.getMasv().matches("SV[0-9]{3}")) {
67         error++;
68     }
69 }
```

Figure 16. Sử dụng các hàm kiểm tra dữ liệu phía server

- Phòng chống XSS

- Kiểm soát input phía client và server bằng cách sử dụng thuộc tính pattern, các hàm kiểm tra, lọc dữ liệu input, parameter:

```

nhanvienForm... Ciphers.java accessNhanVi... *Filter.java NhanVienCon... LopHocContro... SinhVienCon... LoginControl... *validation...
1 package Security;
2
3 public class Filter {
4     public static String cleanSQLI(String input) {
5         int count = input.length();
6         while(count > 0){
7             input = input.replaceAll("[';-]", ".");
8             count--;
9         }
10        return input;
11    }
12
13    public static String cleanXSS(String input) {
14        int count = input.length();
15        while(count > 0){
16            input = input.replaceAll("<script>", ".").replaceAll("</script>", ".").replaceAll("<script", ".").replaceAll("javascript:", ".")
17                .replaceAll("=", ".").replaceAll("<", ".").replaceAll(">", ".");
18            count--;
19        }
20        return input;
21    }
22
23 }
24
25

```

```

172 @RequestMapping(value = "timkiem", method = RequestMethod.POST)
173 public String search(HttpServletRequest rq, ModelMap model) {
174     String keySearch = rq.getParameter("ma");
175     keySearch = Filter.cleanXSS(keySearch);
176     if(keySearch.toUpperCase().equals("ALL")) {
177         return "redirect:QLSV.htm";
178     }
179
180     //load kết quả
181     List<SinhVien> ds = accessSinhVien.search(keySearch.toUpperCase());
182     if(ds.isEmpty()) {
183         model.addAttribute("students", ds);
184     } else {
185         rq.setAttribute("result", "Sorry! No result for " + keySearch);
186     }
187
188     try {
189         //NhanVien x = accessNhanVien.UserInfo(accessNhanVien.MANV);
190         NhanVien x = new NhanVien(accessNhanVien.MANV, accessNhanVien.HOTEN, accessNhanVien.EMAIL, accessNhanVien.TENDN);
191         model.addAttribute("NV", x);
192     } catch (Exception e) {
193         // TODO: handle exception
194     }
195     return "QuanLySinhVien";
196 }
197
198 }
199

```

- Sử dụng thẻ <c:out> cho các attribute

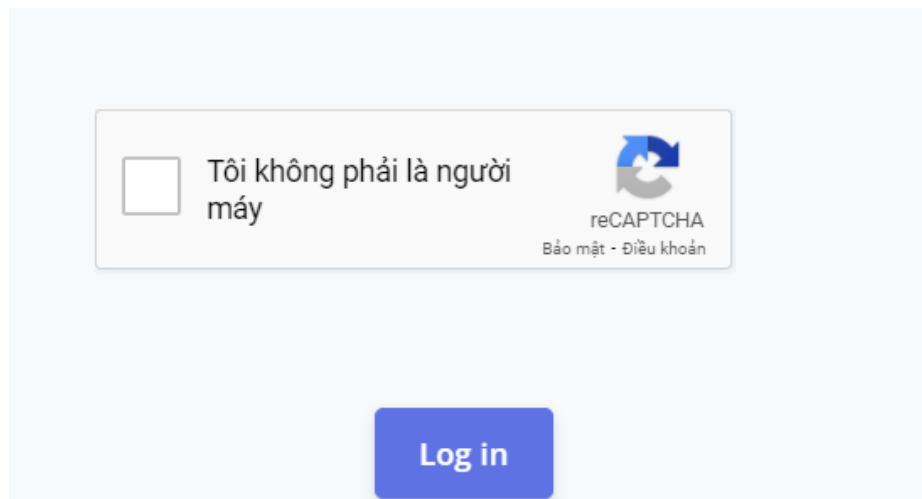
```

<tbody class="list">
    <c:forEach var="x" items="${staffs}">
        <tr>
            <th scope="row">
                <div class="media align-items-center">
                    <div class="media-body">
                        <span class="name mb-0 text-sm"> <c:out value="${x.manv}"/> </span>
                    </div>
                </div>
            </th>

            <td>
                <span class="badge badge-dot mr-4">
                    <span class="status"> <c:out value="${x.hoten}"/> </span>
                </span>
            </td>
        </tr>
    </c:forEach>
</tbody>

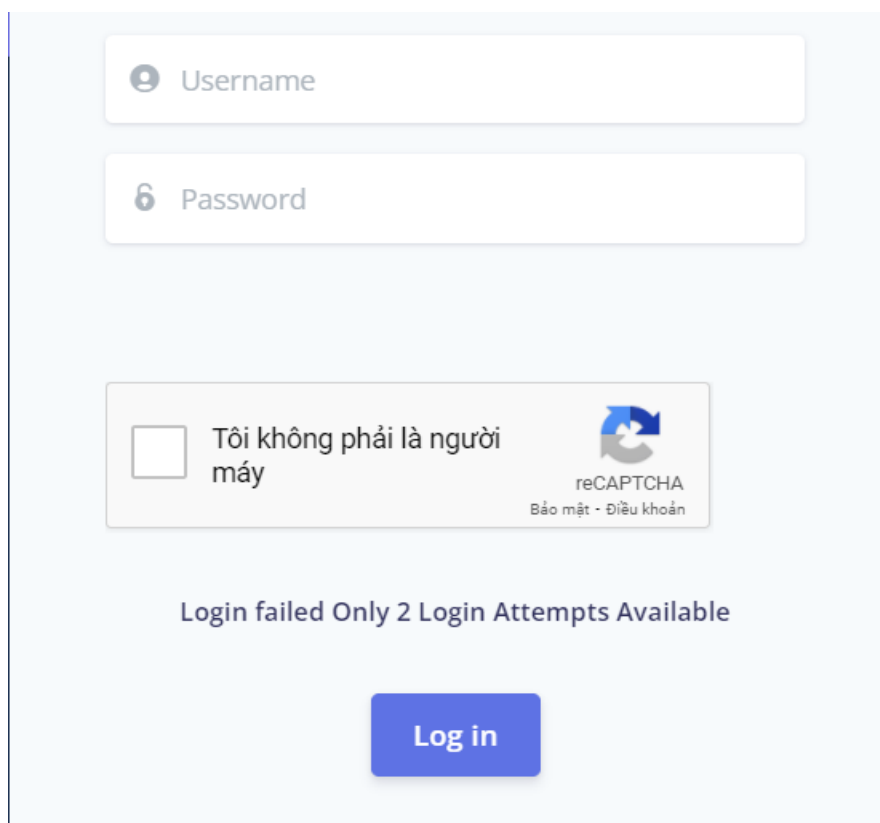
```


- Phòng chống brute-force attack



A login form on a light blue background. It features a reCAPTCHA v2 widget with the text "Tôi không phải là người máy" (I am not a robot) and the reCAPTCHA logo. Below the widget is a blue "Log in" button.

Figure 17. Sử dụng recaptcha v2 google



A login form on a light blue background, showing a failed login attempt. It includes input fields for "Username" and "Password". Below these fields is a reCAPTCHA v2 widget. A message "Login failed Only 2 Login Attempts Available" is displayed above the blue "Log in" button.

Figure 18. Khóa tài khoản nếu đăng nhập sai nhiều lần

```

web.xml web.xml LoginController.java
29 private static int turn = 3;
30 private HashMap<String, Integer> blacklist = new HashMap<String, Integer>();
31
32 @RequestMapping("login")
33 public String index(HttpServletRequest request) {
34
35     String wrongAuthen = "";
36     try {
37         wrongAuthen = request.getParameter("hl");
38
39         if(wrongAuthen.equals("again")) {
40             String recap;
41             String uname;
42             try {
43                 uname = request.getParameter("uname");
44                 uname = Filter.cleanXSS(uname);
45                 if(blacklist.containsKey(uname)) {
46                     Integer luot = blacklist.get(uname) - 1;
47                     if(luot <= 0) {
48                         blacklist.replace(uname, 0);
49                         return "loginFailed";
50                     } else {
51                         blacklist.replace(uname, luot);
52                         request.setAttribute("message", "Login failed Only " + blacklist.get(uname) + " Login Attempts Available");
53                     }
54                 } else {
55                     blacklist.put(uname, turn-1);
56                     request.setAttribute("message", "Login failed Only " + blacklist.get(uname) + " Login Attempts Available");
57                 }
58             }
59
60             recap = request.getParameter("recap");
61             if(recap.equals("nul")) {

```

- Cài đặt Modsecurity cho web application (Modsec được cài đặt trên apache; apache đóng vai trò là 1 reverse proxy tiếp nhận các request từ client và chuyển tiếp cho tomcat)

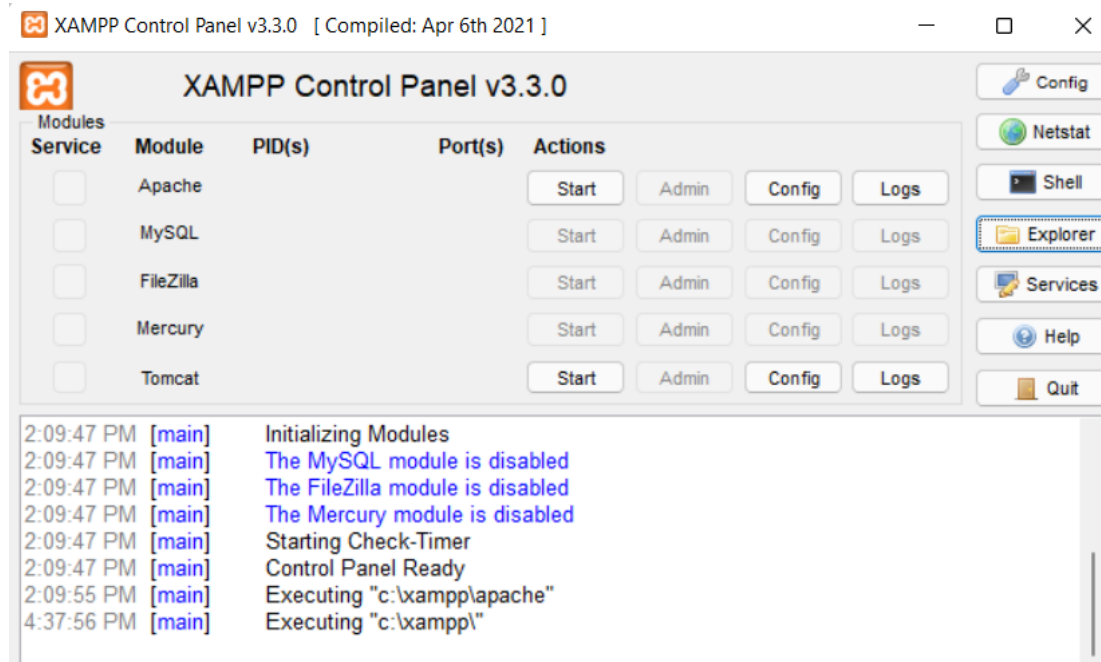


Figure 19. Cài đặt XAMPP

Name	Date modified	Type	S
mlogc-2.9.3	6/17/2019 7:00 PM	File folder	
mod_security-2.9.3	6/17/2019 7:00 PM	File folder	
-- Win64 VS16 --	6/17/2019 6:46 PM	File	
mod_security-2.9.3-win64-VS16.zip	12/3/2021 7:08 PM	WinRAR ZIP archive	
yajl.dll	6/16/2019 4:50 PM	Application extens...	

Figure 20. Tài Modsec từ <https://www.apachelounge.com/download/>

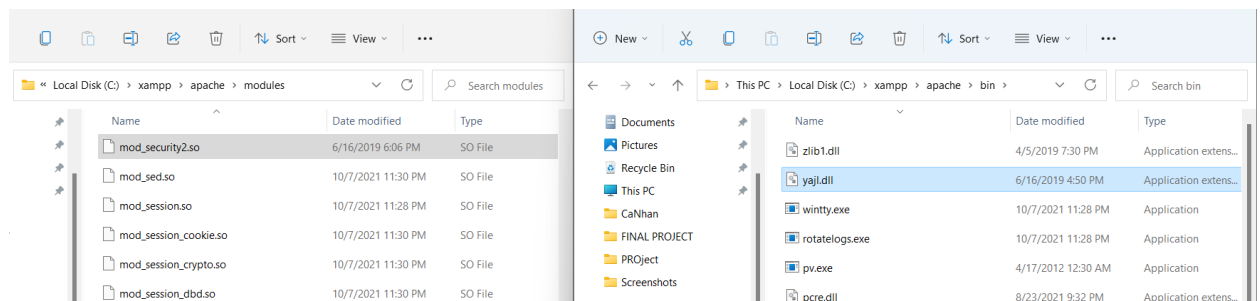


Figure 21. Thêm mod_security2.so và yajl.dll vào apache

Name	Date modified	Type	Size
REQUEST-900-EXCLUSION-RULES-DENY-EXAMPLE.conf	7/1/2020 11:38 PM	CONF File	14 KB
REQUEST-901-INITIALIZATION.conf	7/1/2020 11:38 PM	CONF File	13 KB
REQUEST-903-9001-DRUPAL-EXCLUSION-RULES.conf	7/1/2020 11:38 PM	CONF File	26 KB
REQUEST-903-9002-WORDPRESS-EXCLUSION-RULES.conf	7/1/2020 11:38 PM	CONF File	11 KB
REQUEST-903-9003-NEXTCLOUD-EXCLUSION-RULES.conf	7/1/2020 11:38 PM	CONF File	8 KB
REQUEST-903-9004-DOKUWIKI-EXCLUSION-RULES.conf	7/1/2020 11:38 PM	CONF File	2 KB
REQUEST-903-9005-CPANEL-EXCLUSION-RULES.conf	7/1/2020 11:38 PM	CONF File	18 KB
REQUEST-903-9006-XENFORO-EXCLUSION-RULES.conf	7/1/2020 11:38 PM	CONF File	2 KB
REQUEST-905-COMMON-EXCEPTIONS.conf	7/1/2020 11:38 PM	CONF File	11 KB
REQUEST-910-IP-REPUTATION.conf	7/1/2020 11:38 PM	CONF File	3 KB
REQUEST-911-METHOD-ENFORCEMENT.conf	7/1/2020 11:38 PM	CONF File	11 KB
REQUEST-912-DOS-PROTECTION.conf	7/1/2020 11:38 PM	CONF File	7 KB
REQUEST-913-SCANNER-DETECTION.conf	7/1/2020 11:38 PM	CONF File	50 KB
REQUEST-920-PROTOCOL-ENFORCEMENT.conf	7/1/2020 11:38 PM	CONF File	13 KB
REQUEST-921-PROTOCOL-ATTACK.conf	7/1/2020 11:38 PM	CONF File	6 KB
REQUEST-930-APPLICATION-ATTACK-LFI.conf	7/1/2020 11:38 PM	CONF File	6 KB
REQUEST-931-APPLICATION-ATTACK-RFI.conf	7/1/2020 11:38 PM	CONF File	54 KB
REQUEST-932-APPLICATION-ATTACK-RCE.conf	7/1/2020 11:38 PM	CONF File	

Figure 22. Tài xuống rule được xây dựng sẵn và thêm vào apache

```

#LoadModule speling_module modules/mod_speling.so
LoadModule ssl_module modules/mod_ssl.so
LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
LoadModule unique_id_module modules/mod_unique_id.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule watchdog_module modules/mod_watchdog.so
#LoadModule xml2enc_module modules/mod_xml2enc.so

LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
Include conf/ajp.conf
LoadModule security2_module modules/mod_security2.so

<IfModule security2_module>
    Include conf/modsecurity.conf
    Include conf/crs-setup.conf
    Include conf/rules/*.conf

    Include conf/sqlinjection.conf
    Include conf/xss.conf
    Include conf/modsecurity_crs.conf
</IfModule>

```

Figure 23. Cấu hình file httpd.conf

```

<!-- Define an AJP 1.3 Connector on port 8009 -->

<Connector protocol="AJP/1.3"
    address="::"
    port="8009"
    secretRequired="false"
    enableLookups="false"
    URIEncoding="UTF-8"
    redirectPort="8443" />

```

Figure 24. cấu hình tomcat server.xml

- **Backup restore Database (mời thầy xem qua video)**

4. Dùng tool đánh giá điểm yếu

- Acunetix (scan không sử dụng modsecurity)

Windows 10

Acunetix - Scans

https://localhost:3443/#/scans/fd644e0a-8698-4d16-afd2-09c95d7f89f5/info

Administrator

Scan

Full Scan - https://trantuong.com:8443/QLNV_SV/QLNV.htm

Stop Scan Pause Scan Generate Report WAF Export

Scan Information Vulnerabilities Site Structure Events

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Activity

Completed

Overall Progress 100%

Scanning of trantuong.com:8443 started Dec 10, 2021, 11:56:50 PM

Windows Defender used in this scan Dec 10, 2021, 11:56:52 PM

Login forms were detected but no LSR or Autologin are configured. Dec 11, 2021, 12:17:47 AM

Scanning of trantuong.com:8443 completed Dec 11, 2021, 12:29:14 AM

Scan Duration 32m 23s

Requests 18,773

Average Response Time 1ms

Paths Identified 55

Target Information

Address https://trantuong.com:8443/QLNV_SV/QLNV.htm

Server Unknown

Operating System Java/J2EE

Identified Technologies Yes

Responsive

Latest Alerts

Subresource Integrity (SRI) not implemented Dec 11, 2021, 12:21:35 AM

Login page password-guessing attack Dec 11, 2021, 12:21:29 AM

Insecure Referrer Policy Dec 11, 2021, 12:07:37 AM

Content Security Policy (CSP) not implemented Dec 10, 2021, 11:58:27 PM

Email addresses Dec 10, 2021, 11:57:18 PM

Windows 10

Acunetix - Vulnerabilities

https://localhost:3443/#/scans/fd644e0a-8698-4d16-afd2-09c95d7f89f5/vulnerabilities

Administrator

Scan

Full Scan - https://trantuong.com:8443/QLNV_SV/QLNV.htm

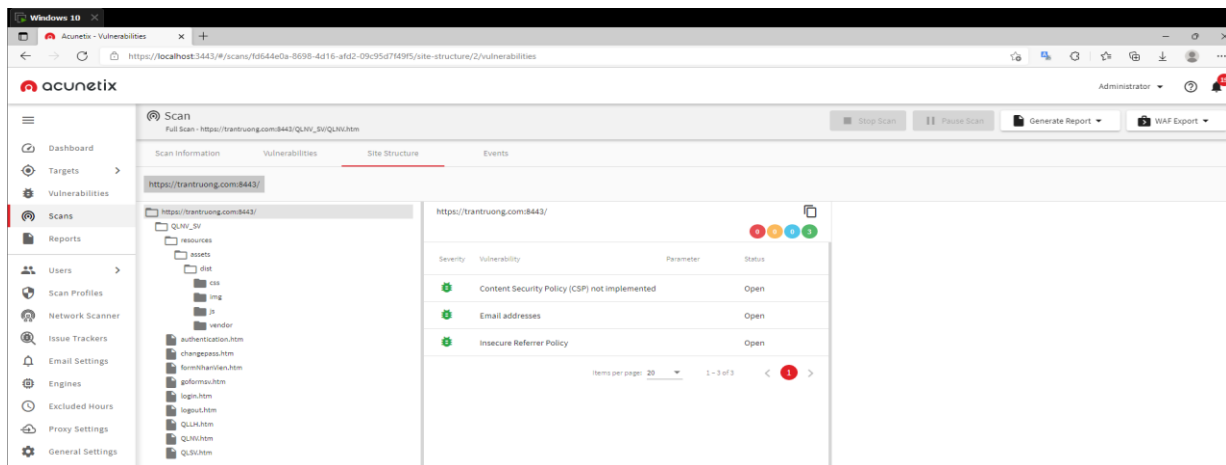
Stop Scan Pause Scan Generate Report WAF Export

Scan Information Vulnerabilities Site Structure Events

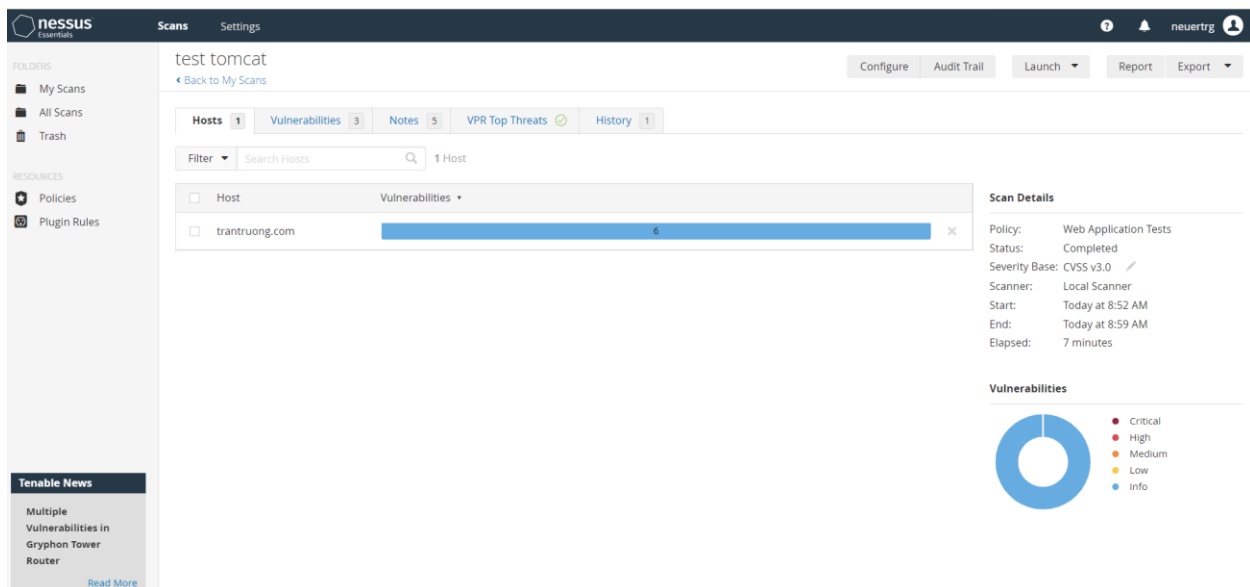
Filter

Severity	Vulnerability	URL	Parameter	Status	Confidence %
Open	Content Security Policy (CSP) not implemented	https://trantuong.com:8443/		Open	95
Open	Email addresses	https://trantuong.com:8443/		Open	95
Open	Insecure Referrer Policy	https://trantuong.com:8443/		Open	95
Open	Subresource Integrity (SRI) not implemented	https://trantuong.com:8443/QLNV_SV/login.htm		Open	95
Open	Login page password-guessing attack	https://trantuong.com:8443/QLNV_SV/login.htm		Open	80

Items per page: 20 1 - 5 of 5



- **Nessus (scan tomcat ko dùng modsec)**



 Trash

Plugin Rules

[Read More](#)[◀ Back to Hosts](#)

Export ▼

3

Q

3 Vulnerabilities

Host Details

IP: 127.0.0.1
DNS: trantruong.com
OS: Windows 11
Start: Today at 8:52 AM
End: Today at 8:59 AM
Elapsed: 7 minutes
KB: [Download](#)

A donut chart with a single blue segment representing 100%.

- Critical
- High
- Medium
- Low
- Info