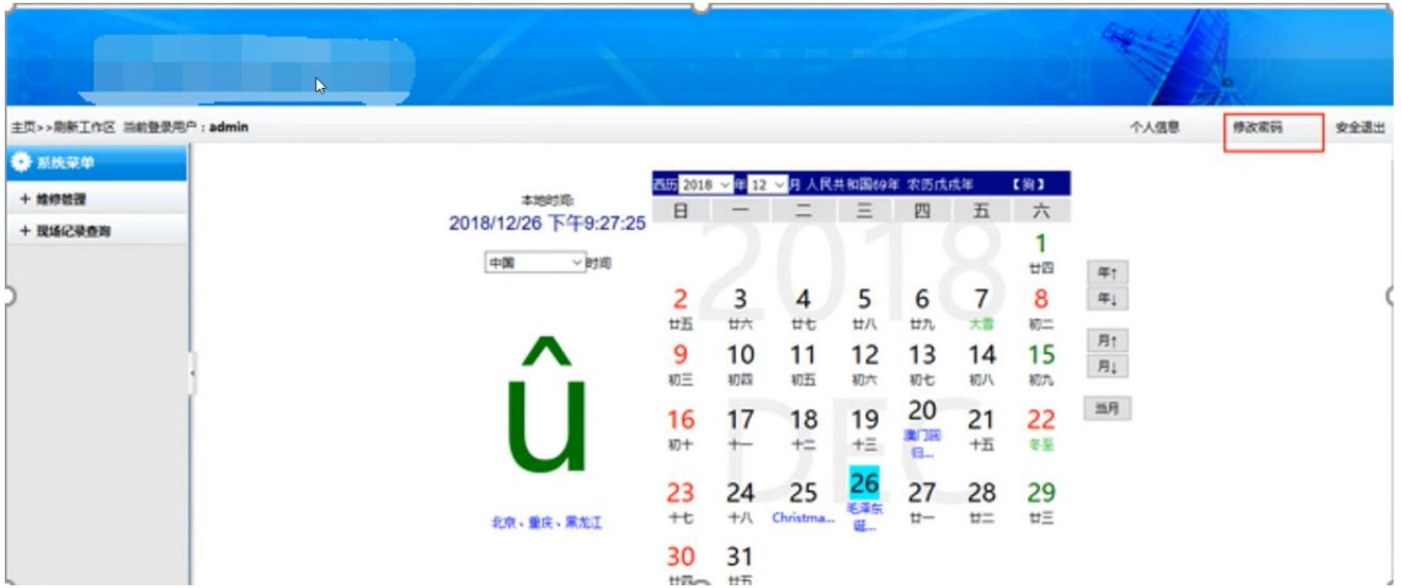
java代码审计深度解析

第一课　暴力破解

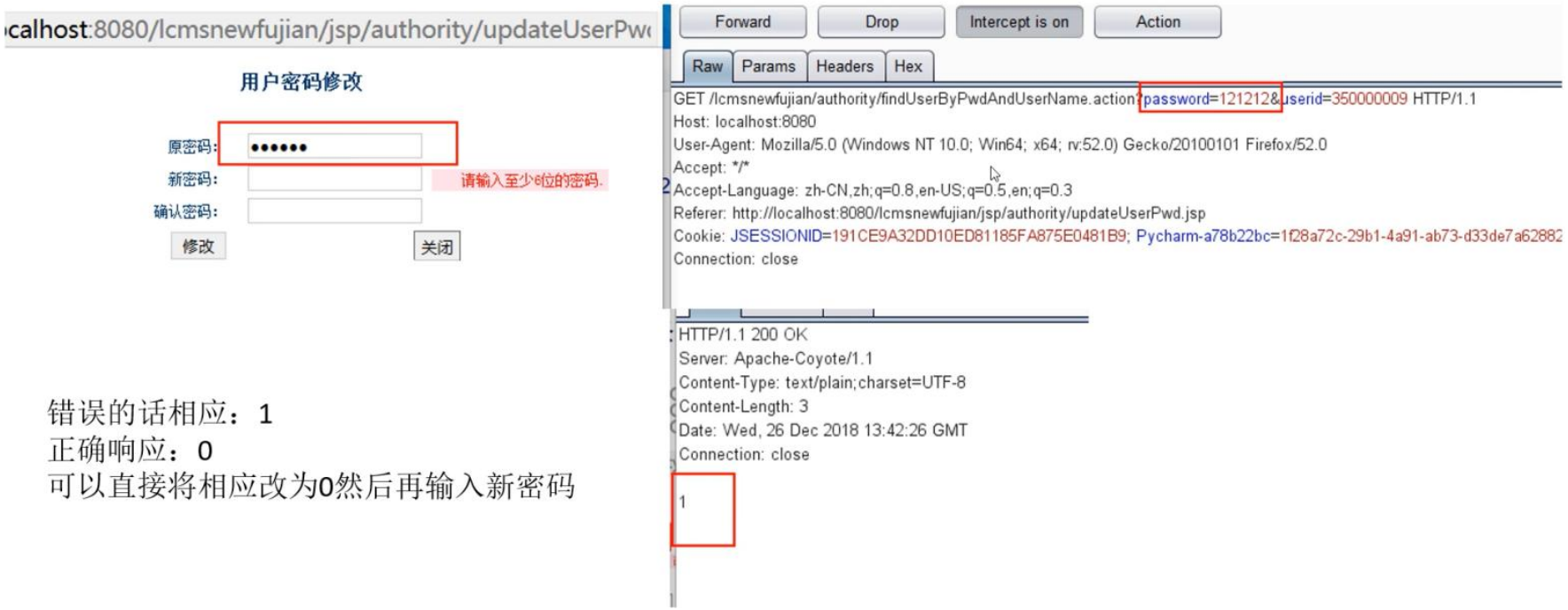
逻辑漏洞-任意修改密码

自动站设备保障系统



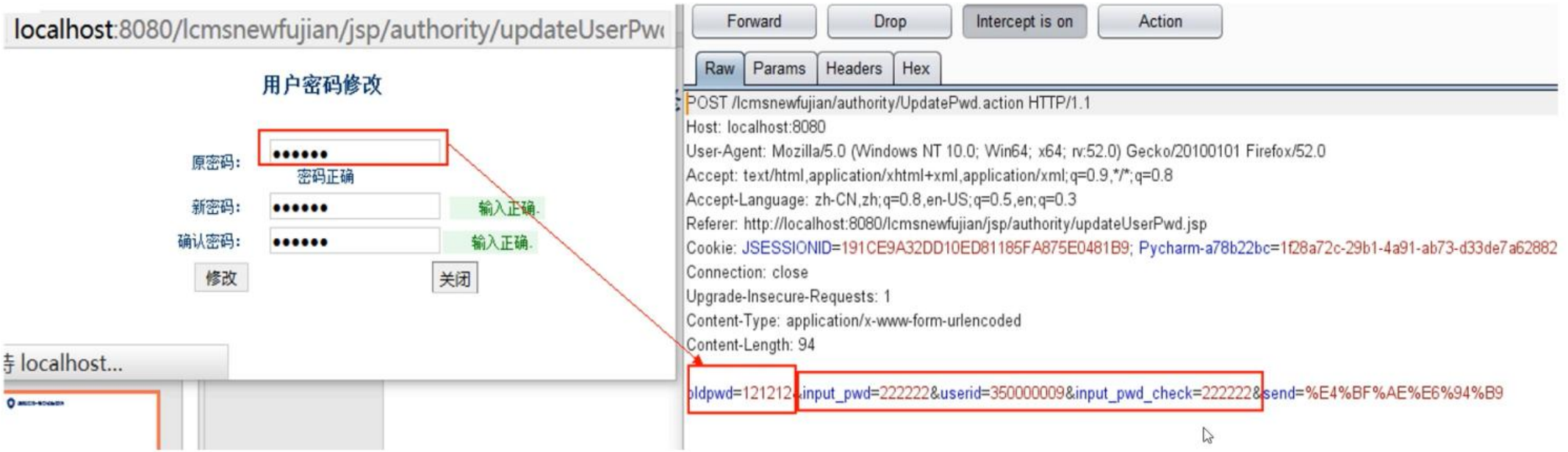
逻辑漏洞-任意修改密码

异步请求了原始密码：

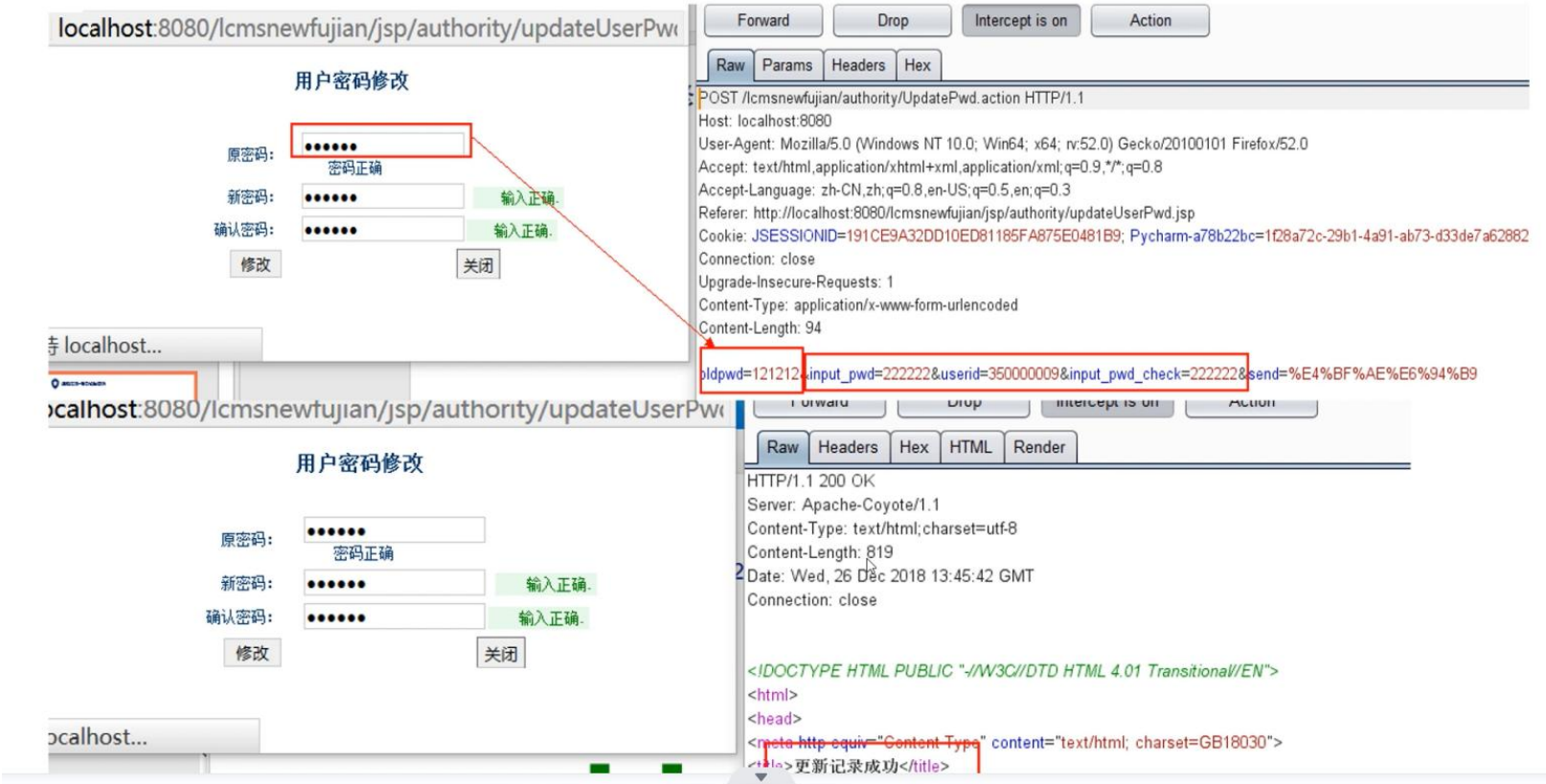


错误的话相应：1
正确响应：0
可以直接将相应改为0然后再输入新密码

逻辑漏洞-任意修改密码


localhost:8080/lcmsnewfujian/jsp/authority/updateUserPw
用户密码修改
原密码:
密码正确
新密码:
输入正确.
确认密码:
输入正确.
修改
关闭
localhost...
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /lcmsnewfujian/authority/UpdatePwd.action HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://localhost:8080/lcmsnewfujian/jsp/authority/updateUserPwd.jsp
Cookie: JSESSIONID=191CE9A32DD10ED81185FA875E0481B9; Pycharm-a78b22bc=1f28a72c-29b1-4a91-ab73-d33de7a62882
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
oldpwd=121212&input_pwd=222222&userid=350000009&input_pwd_check=222222&send=%E4%BF%AE%E6%94%B9

逻辑漏洞-任意修改密码


localhost:8080/lcmsnewfujian/jsp/authority/updateUserPw
用户密码修改
原密码:
密码正确
新密码:
输入正确.
确认密码:
输入正确.
修改
关闭
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /lcmsnewfujian/authority/UpdatePwd.action HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://localhost:8080/lcmsnewfujian/jsp/authority/updateUserPwd.jsp
Cookie: JSESSIONID=191CE9A32DD10ED81185FA875E0481B9; Pycharm-a78b22bc=1f28a72c-29b1-4a91-ab73-d33de7a62882
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
oldpwd=121212&input_pwd=222222&userid=350000009&input_pwd_check=222222&send=%E4%BF%AE%E6%94%B9
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 819
Date: Wed, 26 Dec 2018 13:45:42 GMT
Connection: close
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=GB18030">
更新记录成功</title>

逻辑漏洞-无验证码登陆

JSP页面：

```
<tr height="10">
    <td width="40%"></td>
    <td width="10%">用户名：</td>
    <td><input type="text" value="${userName }" name="userName" id="userName"/></td>
    <td width="30%"></td>
</tr>
<tr height="10">
    <td width="40%"></td>
    <td width="10%">密 码：</td>
    <td><input type="password" value="${password }" name="password" id="password"/></td>
    <td width="30%"></td>
</tr>
<tr height="10">
    <td width="40%"></td>
    <td width="10%"><input type="submit" value="登录"/></td>
    <td><input type="button" value="重置" onclick="resetValue()"/></td>
    <td width="30%"></td>
</tr>
<tr height="10">
```

逻辑漏洞-无验证码登陆-后台代码

```
protected void doPost(HttpServletRequest request, HttpServletResponse response)
        throws ServletException, IOException {
    String userName=request.getParameter("userName");
    String password=request.getParameter("password");
    request.setAttribute("userName", userName);
    request.setAttribute("password", password);
    if(StringUtil.isEmpty(userName)||StringUtil.isEmpty(password)){
        request.setAttribute("error", "用户名或密码为空！");
        request.getRequestDispatcher("index.jsp").forward(request, response);
        return;
    }
    User user=new User(userName,password);
    Connection con=null;
    try {
        con=dbUtil.getCon();
        User currentUser=userDao.login(con, user);
        if(currentUser==null){
            request.setAttribute("error", "用户名或密码错误！");
            // 服务器跳转
            request.getRequestDispatcher("index.jsp").forward(request, response);
        }else{
            // 获取Session
            HttpSession session=request.getSession();
            session.setAttribute("currentUser", currentUser);
```

谢谢观赏