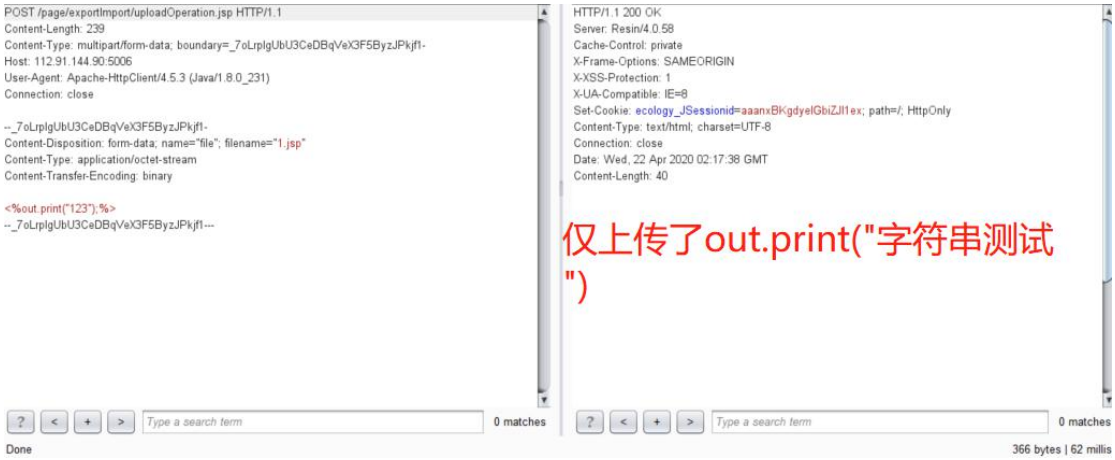
漏洞位于: /page/exportImport/uploadOperation.jsp 文件中

Jsp 流程大概是:判断请求是否是 multipart 请求,然就没有了,直接上传了,啊哈哈哈哈哈
重点关注 File file=new File(savepath+filename),
Filename 参数,是前台可控的,并且没有做任何过滤限制

```jsp
<%
    String filePath ="";
    File tmpDir = null;
    File saveDir = null;
    String tmpPath = GCONST.getRootPath() + "page\\exportImport\\fileTransferTemp\\";
    String savePath = GCONST.getRootPath() + "page\\exportImport\\fileTransfer";
    tmpDir = new File(tmpPath);
    saveDir = new File(savePath);
    if (!tmpDir.isDirectory())
        tmpDir.mkdir();
    if (!saveDir.isDirectory())
        saveDir.mkdir();
    try {
        if (ServletFileUpload.isMultipartContent(request)) {
            DiskFileItemFactory dff = new DiskFileItemFactory();
            dff.setRepository(tmpDir);
            dff.setSizeThreshold(1024000);
            ServletFileUpload sfu = new ServletFileUpload(dff);
            sfu.setSizeMax(5000000);
            sfu.setSizeMax(10000000);
            FileItemIterator fii = sfu.getItemIterator(request);
            while (fii.hasNext()) {
                FileItemStream fis = fii.next();
                if (!fis.isFormField() && fis.getName().length() > 0) {
                    String fileName = fis.getName();
                    if(fis.getName().lastIndexOf("//")>0){
                        fileName = fis.getName().substring(fis.getName().lastIndexOf("//"));
                    }
                    BufferedInputStream in = new BufferedInputStream(fis.openStream());
                    File file = new File(savePath+"//" + fileName);
                    FileOutputStream fos = new FileOutputStream(file);
                    BufferedOutputStream outS = new BufferedOutputStream(fos);
                    Streams.copy(in, outS, true);
                    filePath = savePath+"//" + fileName;
                    if(outS!=null){
                        outS.close();
                    }
                    if(fos!=null){
                        fos.close();
                    }
                    if(in!=null){
                        in.close();
                    }
                }
            }
        }
    } catch (Exception e) {
```

利用非常简单,只要对着
127.0.0.1/page/exportImport/uploadOperation.jsp
来一个 multipartRequest 就可以,利用简单,自评高危!!



然后请求路径:
view-source:http://112.91.144.90:5006/page/exportImport/fileTransfer/1.jsp


不安全 | view-source:112.91.144.90:5006/page/exportImport/fileTransfer/1.jsp
应用
中移(动)信息技术有...
技术专栏 | 深入理...
斐斐打码--专业的...
(2条消息)Tomcat...
Pay
1
123