

# Web Application Report

**This report includes important security information about your Web Application.**

## Security Report

This report was created by IBM Rational AppScan 8.0.0.1  
3/23/2011 10:48:24 AM

# Report Information

## Web Application Report

Scan Name: ncias-d614-v.nci.nih.gov\_032211\_admin

### Scanned Host(s)

Host	Operating System	Web Server	Application Server
ncias-d614-v.nci.nih.gov:443			

### Content

This report contains the following sections:

- Executive Summary
- Detailed Security Issues
- Remediation Tasks

# Executive Summary

## Test Policy

- Default

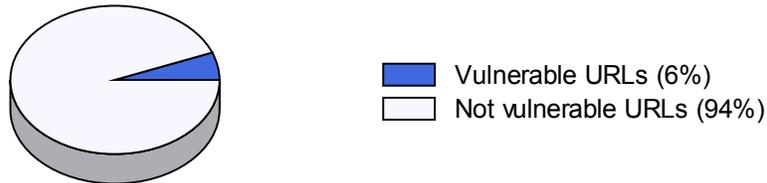
## Security Risks

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 gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It may be possible to steal user and session information (cookies) that was sent during an encrypted session
- It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
- It might be possible to escalate user privileges and gain administrative permissions over the web application
- It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

## Vulnerable URLs

6% of the URLs had test results that included security issues.



## Scanned URLs

**8395 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.

- Sensitive information might have been cached by your browser
- The web application sends non-secure cookies over SSL
- The web server or application server are configured in an insecure way

- Temporary files were left in production environment
- Query parameters were passed over SSL, and may contain sensitive information

**URLs with the Most Security Issues (number issues)**

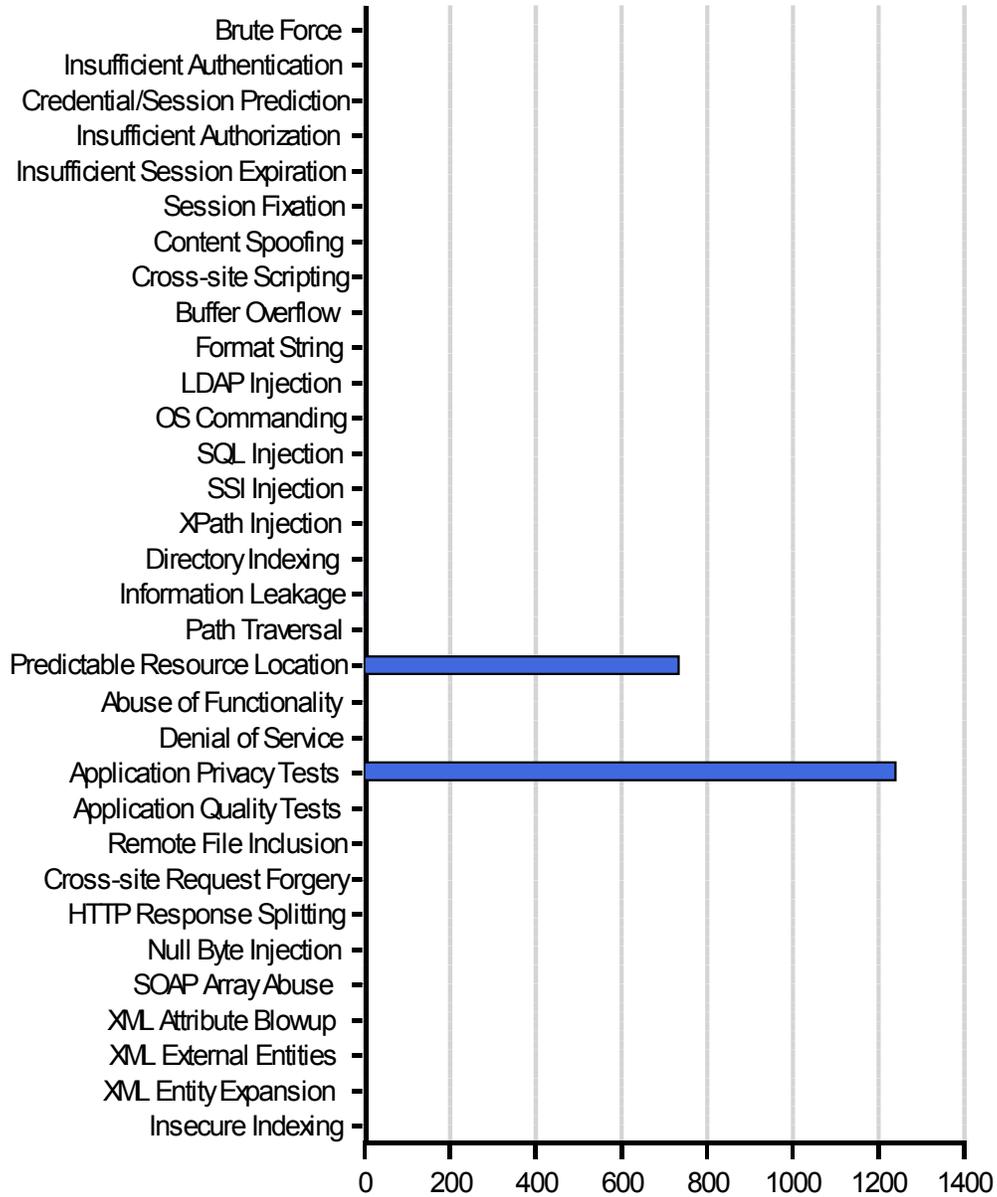
- <https://ncias-d614-v.nci.nih.gov/admin/core/collectionprotocol/> (9)
- <https://ncias-d614-v.nci.nih.gov/admin/core/specimencollectionssummary/> (7)
- <https://ncias-d614-v.nci.nih.gov/admin/core/contact/> (6)
- <https://ncias-d614-v.nci.nih.gov/admin/lookups/anatomicsource/> (6)
- <https://ncias-d614-v.nci.nih.gov/admin/lookups/diagnosis/> (6)

**Security Issues per Host**

Hosts	High	Medium	Low	Informational	Total
<a href="https://ncias-d614-v.nci.nih.gov/">https://ncias-d614-v.nci.nih.gov/</a>	1	1	1973	8	1983
<b>Total</b>	<b>1</b>	<b>1</b>	<b>1973</b>	<b>8</b>	<b>1983</b>

### 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 (1982 out of a total of 1983 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 1983 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://ncias-d614-v.nci.nih.gov/admin/>

Total of 1 security issues in this URL

## [1 of 1] Session Identifier Not Updated

Severity: High  
Test Type: Application  
Vulnerable URL: <https://ncias-d614-v.nci.nih.gov/admin/>  
CVE ID(s): N/A  
CWE ID(s): 613  
Remediation Tasks: Do not accept externally created session identifiers

### **Variant 1 of 1 [ID=5]**

The following may require user attention:

```
POST /admin/ HTTP/1.1
Cookie: sessionid=be457e6a5b092e58bb9a1edd4efba67b;
csrftoken=e7c861c5fa58110eda5b40ec4b8de1f6
Content-Length: 112
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://ncias-d614-v.nci.nih.gov/admin/
Content-Type: application/x-www-form-urlencoded
Host: ncias-d614-v.nci.nih.gov
Connection: Keep-Alive
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Accept-Language: en-US

csrftoken=e7c861c5fa58110eda5b40ec4b8de1f6&username=admin&password
=%24r!pr0to&this_is_the_login_form=1
HTTP/1.1 200 OK
Set-Cookie: sessionid=be457e6a5b092e58bb9a1edd4efba67b; path=/; secure
Content-Length: 6630
Date: Tue, 22 Mar 2011 14:47:56 GMT
Server: Apache
Expires: Tue, 22 Mar 2011 14:47:59 GMT
Vary: Cookie
Last-Modified: Tue, 22 Mar 2011 14:47:59 GMT
ETag: "b35a1179e08a79fa94aa0baf6944ac1e"
Cache-Control: max-age=0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
```

```

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en-us" xml:lang="en-us" >
<head>
<title>Site administration | Django site admin</title>
<link rel="stylesheet" type="text/css" href="/static/admin_media/css/base.css" />
<link rel="stylesheet" type="text/css" href="/static/admin_media/css/dashboard.css" />
<!--[if lte IE 7]><link rel="stylesheet" type="text/css"
href="/static/admin_media/css/ie.css" /><![endif-->

<script type="text/javascript">window.__admin_media_prefix__ =
"/static/admin_media/";</script>

<meta name="robots" content="NONE,NOARCHIVE" />
</head>

<body class="dashboard">

<!-- Container -->
<div id="container">

    <!-- Header -->
    <div id="header">
        <div id="branding">

<h1 id="site-name">Django administration</h1>

        </div>

        <div id="user-tools">
            Welcome,
            <strong>SRL</strong>.

            <a href="/admin/password_change/">
                Change password</a> /

            <a href="/admin/logout/">
                Log out</a>

        </div>

    </div>
<!-- END Header -->

```

```

<!-- Content -->
<div id="content" class="colMS">

    <h1>Site administration</h1>

<div id="content-main">

    <div class="module">
    <table summary="Models available in the Core application.">
    <caption><a href="core/" class="section">Core</a></caption>

    <tr>

        <th scope="row"><a href="core/address/">Addresses</a></th>

        <td><a href="core/address/add/" class="addlink">Add</a></td>

        <td><a href="core/address/" class="changelink">Change</a></td>
    </tr>

    <tr>

        <th scope="row"><a href="core/collectionprotocol/">Collection protocols</a></th>

        <td><a href="core/collectionprotocol/add/" class="addlink">Add</a></td>

        <td><a href="core/collectionprotocol/" class="changelink">Change</a></td>
    </tr>

    <tr>

        <th scope="row"><a href="core/contact/">Contacts</a></th>

        <td><a href="core/contact/add/" class="addlink">Add</a></td>

```

```
<td><a href="core/contact/" class="changelink">Change</a></td>
</tr>
<tr>
<th scope="row"><a href="core/institution/">Institutions</a></th>

<td><a href="core/institution/add/" class="addlink">Add</a></td>

<td><a href="core/institution/" class="changelink">Change</a></td>
</tr>
<tr>
<th scope="row"><a href="core/participantcollectionssummary/">Participant
collection summaries</a></th>

<td><a href="core/participantcollectionssummary/add/"
class="addlink">Add</a></td>

<td><a href="core/participantcollectionssummary/"
class="changelink">Change</a></td>
</tr>
<tr>
<th scope="row"><a href="core/specimenscollectionssummary/">Specimen
collection summaries</a></th>

<td><a href="core/specimenscollectionssummary/add/" class=...
```

**Validation In Response:**

N/A

**Reasoning:**

One or more session identifiers were not updated in the response.

CWE ID:  
613

## Remediation Tasks

URL	Remediation Tasks	Addressed Security Issues
<a href="https://ncias-d614-v.nci.nih.gov/admin/">https://ncias-d614-v.nci.nih.gov/admin/</a> (1)	Do not accept externally created session identifiers (High)	Session Identifier Not Updated