

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
2/6/2013 10:34:11 AM

Report Information

Web Application Report

Scan Name: caintegrator-qa.nci.nih.gov_rembbrandt_010813

Scanned Host(s)

Host	Operating System	Web Server	Application Server
caintegrator-qa.nci.nih.gov:443		Apache	
cabig.nci.nih.gov:443	Unix		
ssl.google-analytics.com:443			

Content

This report contains the following sections:

- Executive Summary
- Detailed Security Issues
- Advisories & Fix Recommendations

Executive Summary

Test Policy

- Default

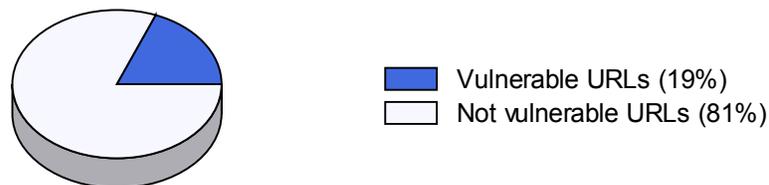
Security Risks

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 debugging information
- 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 sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
- It may be possible to bypass the web application's authentication mechanism
- 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

19% of the URLs had test results that included security issues.



Scanned URLs

1500 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.

- 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
- Insecure web application programming or configuration
- Query parameters were passed over SSL, and may contain sensitive information

- Debugging information was left by the programmer in web pages

URLs with the Most Security Issues (number issues)

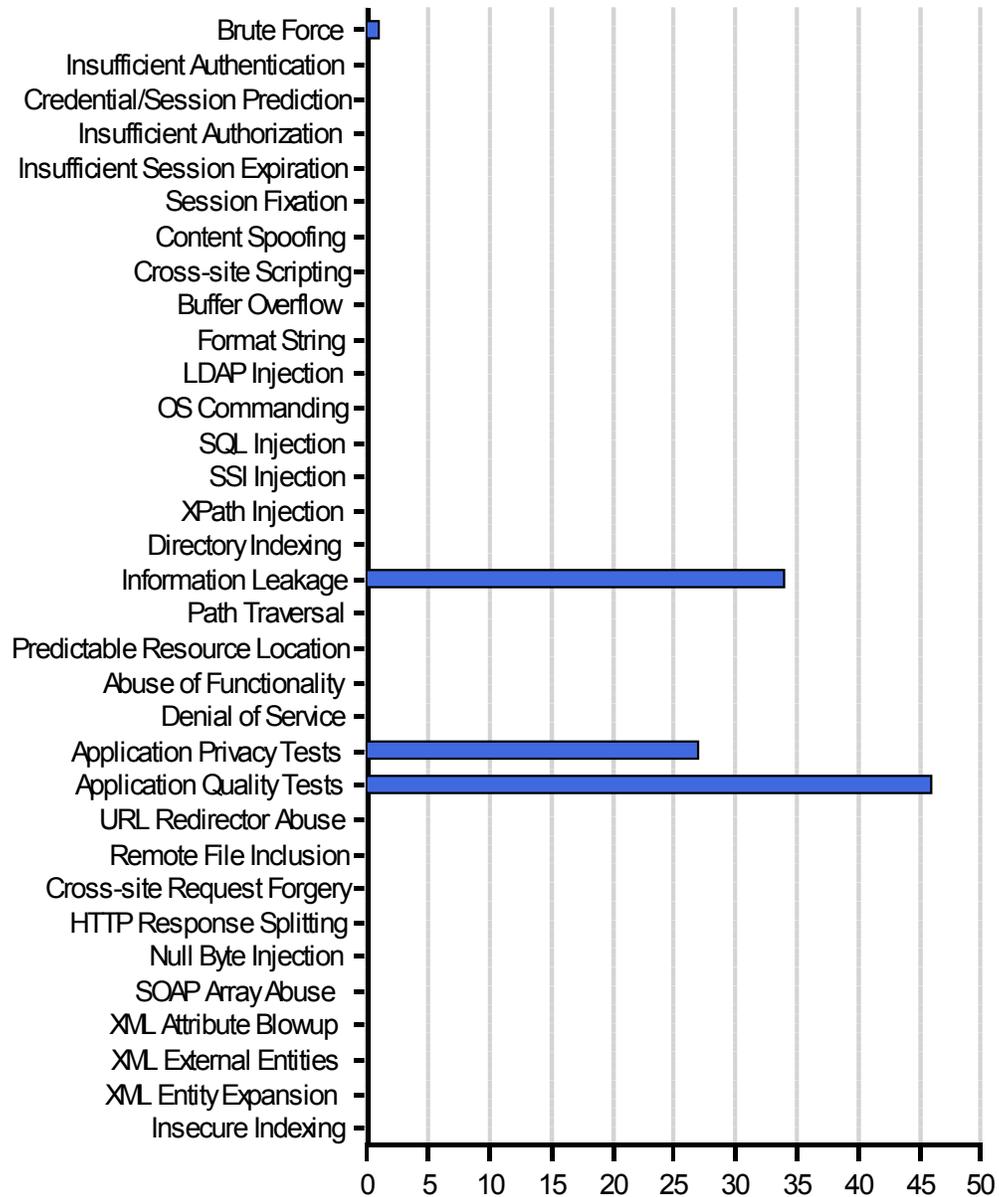
- <https://caintegrator-qa.nci.nih.gov/rembrandt/geneexpression.do> (11)
- <https://caintegrator-qa.nci.nih.gov/rembrandt/quickSearch.do> (11)
- <https://caintegrator-qa.nci.nih.gov/rembrandt/comparitivegenomic.do> (9)
- <https://caintegrator-qa.nci.nih.gov/rembrandt/alogin.do> (7)
- <https://caintegrator-qa.nci.nih.gov/rembrandt/classcomparison.do> (6)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
https://cabig.nci.nih.gov/	0	0	0	1	1
https://caintegrator-qa.nci.nih.gov/	0	1	29	76	106
https://ssl.google-analytics.com/	0	0	0	1	1
Total	0	1	29	78	108

Security Issue Distribution per Threat Class

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



Security Issue Cause Distribution

100% Application-related Security Issues (108 out of a total of 108 issues).

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

0% Infrastructure and Platform Security Issues (0 out of a total 108 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://caintegrator-qa.nci.nih.gov/rembrandt/alogin.do>

Total of 1 security issues in this URL

[1 of 1] Inadequate Account Lockout

Severity: Medium
Test Type: Application
Vulnerable URL: <https://caintegrator-qa.nci.nih.gov/rembrandt/alogin.do> (Parameter: password)
CVE ID(s): N/A
CWE ID(s): 307
Remediation Tasks: Enforce account lockout after several failed login attempts

Variant 1 of 2 [ID=25963]

The following changes were applied to the original request:

- Removed cookie 'JSESSIONID'
- Removed HTTP header 'Cookie'

Request/Response:

```
POST /rembrandt/alogin.do HTTP/1.1
Content-Length: 102
Accept: */*
Accept-Language: en-us
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: caintegrator-qa.nci.nih.gov
Content-Type: application/x-www-form-urlencoded
Referer: https://caintegrator-qa.nci.nih.gov/rembrandt/registration.do
```

```
org.apache.struts.taglib.html.TOKEN=6268029762760328c31d1acbdb961a9e&userName=RBTuser&password=RBTpass
HTTP/1.0 200 OK
Set-Cookie: JSESSIONID=8721659FC2C3EB1E85A35334C05B9225; path=/rembrandt; secure
Set-Cookie: JSESSIONID=AE03CBF740FDA5484E3EC4E43EC4279C; path=/rembrandt; secure
Content-Length: 8204
Date: Thu, 10 Jan 2013 18:34:12 GMT
Server: Apache
X-Powered-By: Servlet 2.5; JBoss-5.0/JBossWeb-2.1
Content-Type: text/html;charset=ISO-8859-1
Connection: close
```

```
<html>
<head><title>REMBRANDT - Repository for Molecular Brain Neoplasia Data (User Guidelines)</title>

  <META HTTP-EQUIV="Pragma" CONTENT="no-cache">
  <META HTTP-EQUIV="Expires" CONTENT="-1">

  <link rel="shortcut icon" href="/rembrandt/images/favicon.ico" />

  <LINK href="/rembrandt/css/bigStyle.css" rel="stylesheet" type="text/css">
  <script language="javascript" src="/rembrandt/js/caIntScript.js"></script>
  <script language="javascript" src="/rembrandt/js/rembrandtScript.js"></script>
  <!-- JB Begin: GF#19875 Gene Alias validation - without clicking the 'check alias' -->
```

```

    <script language="JavaScript" src="/rembrandt/js/geneexpression.js"></script>
    <!-- JB End: GF#19875 Gene Alias validation - without clicking the 'check alias'
-->

    <script language="javascript" src="/rembrandt/js/box/browsersniff.js"></script>
    <script language="javascript" src="/rembrandt/js/lib/prototype-
1.6.0.2.js"></script>
    <script language="javascript" src="/rembrandt/js/lib/Help.js"></script>

    <script language="javascript"
src="/rembrandt/js/lib/common/JSLoader.js"></script>
    <script language="javascript" src="/rembrandt/js/lib/window.js"></script>
    <script language="javascript" src="/rembrandt/js/lib/common/fat.js"></script>

    <script language="javascript"
src="/rembrandt/js/lib/scriptaculous/scriptaculous.js"></script>

    <script type="text/javascript" src="/rembrandt/js/overlib.js"></script>
    <script type="text/javascript" src="/rembrandt/js/overlib_hideform.js"></script>
    <script type="text/javascript" src="/rembrandt/js/menuSwapper.js"></script>
    <script type="text/javascript" src="/rembrandt/js/moveUpDown.js"></script>

    <script type='text/javascript'
src='/rembrandt/dwr/interface/DynamicListHelper.js'></script>
    <script type='text/javascript' src='/rembrandt/dwr/interface/Inbox.js'></script>
    <script type='text/javascript'
src='/rembrandt/js/lib/common/SidebarHelper.js'></script>
    <script type='text/javascript'
src='/rembrandt/js/lib/common/QueryDetailHelper.js'></script>

    <style type="text/css" media="screen">@import "/rembrandt/css/tabs.css";</style>

<script language="javascript" src="js/caIntScript.js"></script>
</head>
<body>
<!--header NCI-->
<table align="center" width="765" border="0" cellspacing="0" cellpadding="0"
bgcolor="#A90101" summary="This table is used to format page content">
<tr>
    <th></th><th></th><th></th><th></th>
</tr>
<tr bgcolor="#A90101">
    <td width="283" height="37" align="left"><a
href="http://www.cancer.gov"></a></td>
    <td align="right"><a
href="http://www.cancer.gov"></a></td>
</tr>
</table>
<!--header REMBRANDT image map-->
<div align="center" width="765px">
<div style="width:765px; border-bottom: 1px solid #000000; margin:0px;">
<map name="headerMap">
<area alt="REMBRANDT application logo" coords="7,8,272,50" href="login.do">
</map>

</div>
<!--end all headers-->
<div style="width:765px;" align="right">
<script type="text/javascript">Help.insertHelp("Rules_of_the_road", '',
"padding:2px;");</script>
</div>
<fieldset style="border: 1px solid #000066;width:765px">
<legend style="text-align:center;background-color:#ffffff">LEGAL RULES OF THE
ROAD</legend>
<p style="text-align:left">The Repository of Molecular
Brain Neoplasia DaTa (REMBRANDT) Database is provided

```

samples used to produce the data presented here were provided by the Neuro-Oncology Branch of the National Cancer Institute and other institutions that are collaborat...

Validation In Response:

N/A

Reasoning:

Two legitimate login attempts were sent, with several false login attempts in between. The last response was identical to the first. This suggests that there is inadequate account lockout enforcement, allowing brute-force attacks on the login page. (This is true even if the first response was not a successful login page.)

CWE ID:

307

Advisories & Fix Recommendations

Inadequate Account Lockout

Application

WASC Threat Classification

Brute Force

<http://projects.webappsec.org/Brute-Force>

CVE ID(s)

N/A

CWE ID(s)

307

Security Risks

It might be possible to escalate user privileges and gain administrative permissions over the web application

Possible Causes

Insecure web application programming or configuration

Technical Description

AppScan Detected that the application does not limit the number of false login attempts. It did so by sending 10 requests with a bad password, and then successfully logged in using the correct credentials.

Not limiting the number of false login attempts exposes the application to a brute force attack. A brute force attack is an attempt by a malicious user to gain access to the application by sending a large number of possible passwords and/or usernames.

Since this technique involves a large amount of login attempts, an application that does not limit the number of false login requests allowed is vulnerable to these attacks.

It is therefore highly recommended to restrict the number of false login attempts allowed on an account before it is locked.

Sample Exploit:

The following request illustrates a password-guessing request:

`http://site/login.asp?username=EXISTING_USERNAME&password=GUESSED_PASSWORD`

If the site does not lock the tested account after several false attempts, the attacker may eventually discover the account password and use it to impersonate the account's legitimate user.

General Fix Recommendations

Decide upon the number of login attempts to be allowed (usually from 3 to 5), and make sure that the account will be locked once the permitted number of attempts is exceeded.

To avoid unnecessary support calls from genuine users who were locked out of their account and require enabling, it is possible to suspend account activity only temporarily, and enable it after a specific period of time. Locking the account for a period of ten minutes or so is usually sufficient to block brute force attacks.

References and Relevant Links

["Blocking Brute-Force Attacks" by Mark Burnett](#)