Web Application Report

This report includes important security information about your Web Application.

Security Report

This report was created by IBM Rational AppScan 8.0.0.3
4/10/2012 10:15:48 AM

© Copyright IBM Corp. 2000, 2011. All Rights Reserved.

Report Information

Web Application Report

Scan Name: csm-uptlogin_040512-2

Scanned Host(s)

Host	Operating System	Web Server	Application Server
ncias-d704-v.nci.nih.gov:29543		Apache	Apache AXIS

Content

This report contains the following sections:

- Executive Summary
- Detailed Security Issues
- Remediation Tasks
- Application Data
- Application URLs
- Advisories & Fix Recommendations

Executive Summary

Test Policy

- Default

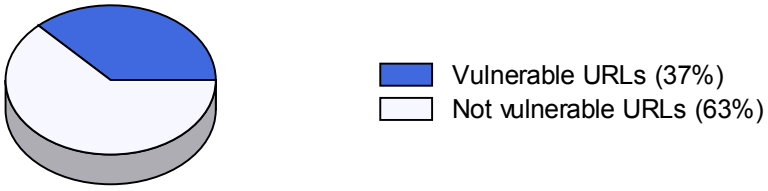
Security Risks

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 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 may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
- It is possible to prevent the web application from serving other users (denial of service)

Vulnerable URLs

37% of the URLs had test results that included security issues.



Scanned URLs

38 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
- Insecure web application programming or configuration
- 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

- Query parameters were passed over SSL, and may contain sensitive information

URLs with the Most Security Issues (number issues)

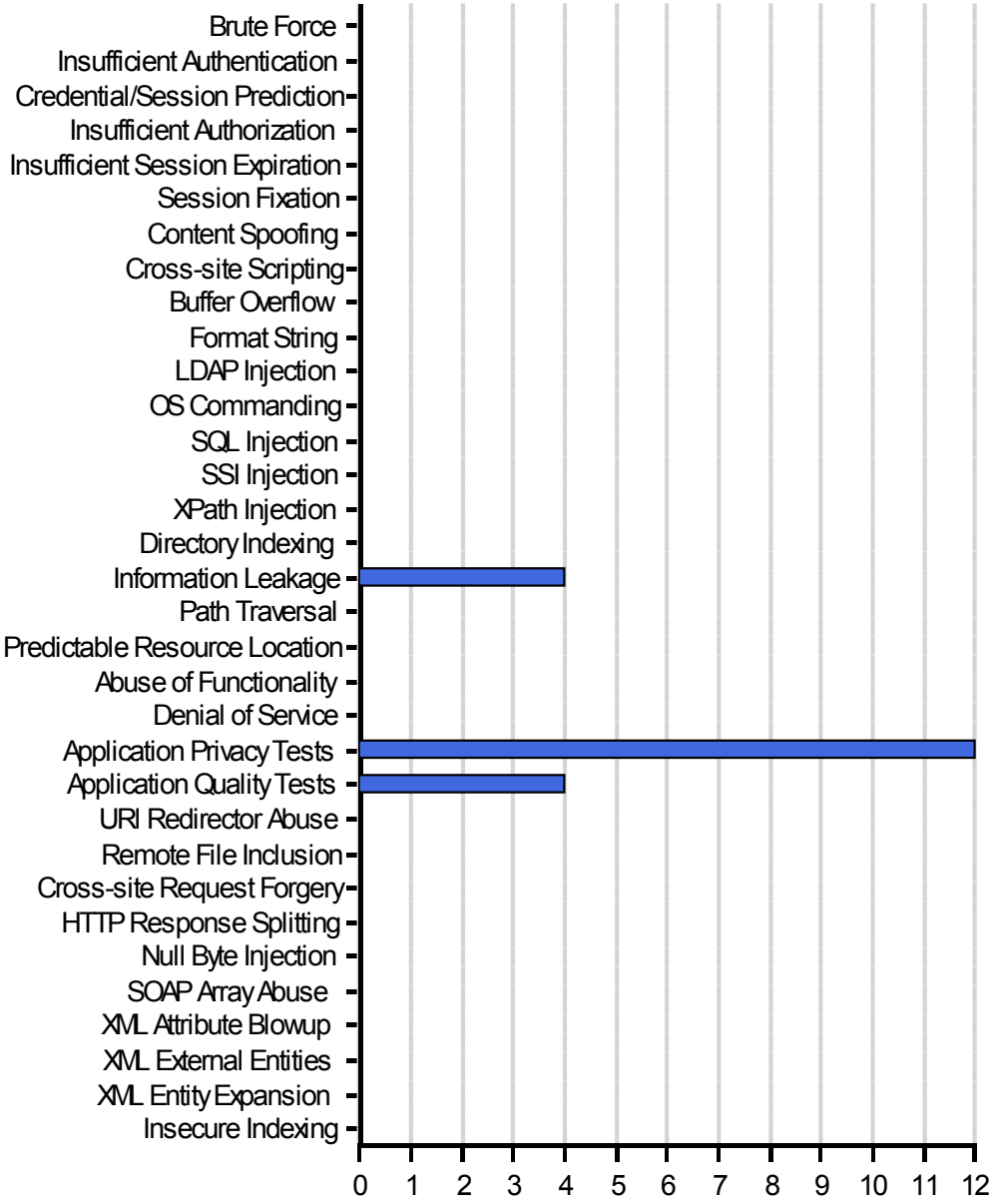
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do (3)
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/ (2)
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterApplicationSupport.do (2)
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterContactUs.do (2)
- https://ncias-d704-v.nci.nih.gov:29543/upt423/images/appLogo.gif;jsessionid=C785E2BDBEB2EA995525BE2A53106E58 (2)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
https://ncias-d704-v.nci.nih.gov:29543/	0	0	12	8	20
Total	**0**	**0**	**12**	**8**	**20**

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 (20 out of a total of 20 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 20 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

N/A

Remediation Tasks

N/A

Application Data

Script Parameters

URL	Name	Type	Value
https://ncias-d704-v.nci.nih.gov:29543/upt423/AdminHome.do;jsessionid=C785E2BDBEB2EA995525BE2A53106E58			
	__patternParameter__JSESSIONID____0	Simple Link	A43374260461538B9BEDE7B2B40B67DB
https://ncias-d704-v.nci.nih.gov:29543/upt423/ApplicationDBOperation.do			
	operation	Hidden	error
	OWASP_CSM_CSRFTOKEN	Hidden	0ITG-N31H-UWRE-ASO1-3QM1-9O1F-VNGZ-ZRDU
https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do			
	loginId	Hidden	SuperAdmin
	password	Hidden	changeme
	applicationContextName	Hidden	csmupt
	loginId	Hidden	SuperAdmin
	password	Hidden	changeme
	applicationContextName	Hidden	csmupt
https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do			
	tableId	Hidden	Logout
	OWASP_CSM_CSRFTOKEN	Hidden	0ITG-N31H-UWRE-ASO1-3QM1-9O1F-VNGZ-ZRDU
	tableId	Hidden	error
	OWASP_CSM_CSRFTOKEN	Hidden	0ITG-N31H-UWRE-ASO1-3QM1-9O1F-VNGZ-ZRDU
https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do;jsessionid=C785E2BDBEB2EA995525BE2A53106E58			
	tableId	Hidden	Application

URL	Name	Type	Value
	OWASP_CSM_CSRFTOKEN	Hidden	0ITG-N31H-UWRE-ASO1-3QM1-9O1F-VNGZ-ZRDU
	__patternParameter__JSESSIONID____0	Simple Link	C785E2BDBEB2EA995525BE2A53106E58
	tableId	Hidden	error
	OWASP_CSM_CSRFTOKEN	Hidden	0ITG-N31H-UWRE-ASO1-3QM1-9O1F-VNGZ-ZRDU
	__patternParameter__JSESSIONID____0	Simple Link	A43374260461538B9BEDE7B2B40B67DB
https://ncias-d704-v.nci.nih.gov:29543/upt423/PrivilegeDBOperation.do			
	operation	Hidden	error
	OWASP_CSM_CSRFTOKEN	Hidden	0ITG-N31H-UWRE-ASO1-3QM1-9O1F-VNGZ-ZRDU
https://ncias-d704-v.nci.nih.gov:29543/upt423/UserDBOperation.do			
	operation	Hidden	error
	OWASP_CSM_CSRFTOKEN	Hidden	0ITG-N31H-UWRE-ASO1-3QM1-9O1F-VNGZ-ZRDU
https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do			
	loginId	Text	SuperAdmin
	password	Password	changeme
	applicationContextName	Text	csmupt
https://ncias-d704-v.nci.nih.gov:29543/upt423/images/appLogo.gif;jsessionid=C785E2BDBEB2EA995525BE2A53106E58			
	__patternParameter__JSESSIONID____0	Simple Link	C785E2BDBEB2EA995525BE2A53106E58

Broken Links

Reason	URL
Response Status 500 - Internal Server Error	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/MenuSelection.do

JavaScripts

Script	URL
`skipNavigation()`	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do

Script	URL

<!--
function set(id)
{
document.MenuForm.tableId.value=id;
document.MenuForm.submit();
}
// -->
	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do

function skipNavigation()
{
document.getElementById ("saHomeHeader").focus();
window.location.hash="saHomeHeader";
document.getElementById ("ncilink").tabIndex = -1;
document.getElementById ("nihlink").tabIndex = -1;
document.getElementById ("skipmenu").tabIndex = -1;
 	
if(document.getElementById("homeLink"))
document.getElementById ("homeLink").tabIndex = -1;
if(document.getElementById ("adminhomeLink"))
document.getElementById ("adminhomeLink").tabIndex = -1;
 	
document.getElementById("saHome").tabIndex = -1;
document.getElementById("saApp").tabIndex = -1;
document.getElementById("saUser").tabIndex = -1;
document.getElementById("saPriv").tabIndex = -1;
document.getElementById ("saLogout").tabIndex = -1;
}
	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do

Script	URL

<!--
function setAndSubmit(target)
{
 	
document.UserForm.operation.value=target;
document.UserForm.submit();
}
// -->
 	
function skipNavigation()
{
document.getElementById("userHome").focus
();
window.location.hash="userHome";
document.getElementById
("ncilink").tabIndex = -1;
document.getElementById
("nihlink").tabIndex = -1;
document.getElementById
("skipmenu").tabIndex = -1;
 	
if(document.getElementById("homeLink"))
document.getElementById
("homeLink").tabIndex = -1;
if(document.getElementById
("adminhomeLink"))
document.getElementById
("adminhomeLink").tabIndex = -1;
if(document.getElementById("menuHome"))
document.getElementById
("menuHome").tabIndex = -1;
if(document.getElementById("menuUser"))
document.getElementById
("menuUser").tabIndex = -1;
if(document.getElementById("menuPE"))
document.getElementById
("menuPE").tabIndex = -1;
if(document.getElementById
("menuPrivilege"))
document.getElementById
("menuPrivilege").tabIndex = -1;
if(document.getElementById("menuGroup"))
...
	https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do

Script	URL

<!--
function setAndSubmit(target)
{
 	
document.PrivilegeForm.operation.value=target;
document.PrivilegeForm.submit();
}
 	
function skipNavigation()
{
document.getElementById("privHome").focus();
window.location.hash="privHome";
document.getElementById("ncilink").tabIndex = -1;
document.getElementById("nihlink").tabIndex = -1;
document.getElementById("skipmenu").tabIndex = -1;
 	
if(document.getElementById("homeLink"))
document.getElementById("homeLink").tabIndex = -1;
if(document.getElementById("adminhomeLink"))
document.getElementById("adminhomeLink").tabIndex = -1;
if(document.getElementById("menuHome"))
document.getElementById("menuHome").tabIndex = -1;
if(document.getElementById("menuUser"))
document.getElementById("menuUser").tabIndex = -1;
if(document.getElementById("menuPE"))
document.getElementById("menuPE").tabIndex = -1;
if(document.getElementById("menuPrivilege"))
document.getElementById("menuPrivilege").tabIndex = -1;
if(document.getElementById("menuGroup"))
document.getElementById("menuGroup").tabIndex = -1;
...
	https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do

Script	URL

<!--
function setAndSubmit(target)
{
document.ApplicationForm.operation.value=target;
document.ApplicationForm.submit();
}
 	
function skipNavigation()
{
document.getElementById("appHome").focus();
window.location.hash="appHome";
document.getElementById("ncilink").tabIndex = -1;
document.getElementById("nihlink").tabIndex = -1;
document.getElementById("skipmenu").tabIndex = -1;
 	
if(document.getElementById("homeLink"))
document.getElementById("homeLink").tabIndex = -1;
if(document.getElementById("adminhomeLink"))
document.getElementById("adminhomeLink").tabIndex = -1;
 	
document.getElementById("saHome").tabIndex = -1;
document.getElementById("saApp").tabIndex = -1;
document.getElementById("saUser").tabIndex = -1;
document.getElementById("saPriv").tabIndex = -1;
document.getElementById("saLogout").tabIndex = -1;
}
 	
// -->
	https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do;jsessionid=C785E2BDBEB2EA995525BE2A53106E58

setAndSubmit('loadAdd')	https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do;jsessionid=C785E2BDBEB2EA995525BE2A53106E58
setAndSubmit('loadSearch')	https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do;jsessionid=C785E2BDBEB2EA995525BE2A53106E58

Script	URL

<!--
function set(tableId)
{
document.MenuForm.tableId.value=tableId;
document.MenuForm.submit();
}
 	
function MM_swapImgRestore() { //v3.0
var i,x,a=document.MM_sr; for
(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++)
x.src=x.oSrc;
}
 	
function MM_preloadImages() { //v3.0
var d=document; if(d.images){ if(!d.MM_p)
d.MM_p=new Array();
var
i,j=d.MM_p.length,a=MM_preloadImages.argument
s; for(i=0; i<a.length; i++)
if (a[i].indexOf("#")!=0){ d.MM_p[j]=new
Image; d.MM_p[j++].src=a[i];}}
}
 	
function MM_findObj(n, d) { //v4.0
var p,i,x; if(!d) d=document; if
((p=n.indexOf("?"))>0&&parent.frames.length)
{
d=parent.frames[n.substring
(p+1)].document; n=n.substring(0,p);}
if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!
x&&i<d.forms.length;i++) x=d.forms[i][n];
for(i=0;!
x&&d.layers&&i<d.layers.length;i++)
x=MM_findObj(n,d.layers[i].document);
if(!x && document.getElementById)
x=document.getElementById(n); return x;
}
 	
function MM_swapImage() { //v3.0
var i,j=0,x,a=MM_swapImage.arguments;
document.MM_sr=new Array; for(i=0;i<(a.length
-2);i+=3)
if ((x=MM_findObj(a[i]))!=null)
{document.MM_sr[j++]=x; if(!x.oSrc)
x.oSrc=x.src; x.src=a[i+2];}
...
	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/

<!--
var focusControl = document.forms
["LoginForm"].elements["loginId"];
 	
if (focusControl.type != "hidden") {
focusControl.focus();
}
// -->
	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/

changeMenuStyle (this,'footerMenuItemOver'),showCursor()	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/

<!--
function set(id)
{
document.MenuForm.tableId.value=id;
document.MenuForm.submit();
}
// -->
	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do

Script	URL
`javascript: set('AdminHome')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`changeMenuStyle (this,'mainMenuItemOver'),showCursor()`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`set('AdminHome')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`javascript: set('Application')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`set('Application')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`javascript: set('User')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`set('User')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`javascript: set('Privilege')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`set('Privilege')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`set('Logout')`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`document.LoginForm.submit();`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
`function changeMenuStyle(obj, new_style) { obj.className = new_style; } function showCursor(){ document.body.style.cursor='hand' } function hideCursor(){ document.body.style.cursor='default' } function confirmDelete(){ if (confirm('Are you sure you want to delete?')){ return true; }else{ return false; } }`	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/scripts/script.js

Comments

Comment	URL
<tr><td class="appMenu" width="200" align="right"> </td><td class="appMenu" width="50" align="center"> </td></tr>	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do

Comment	URL
<tr><td class="appMenu" width="200" align="right"> </td><td class="appMenu" width="50" align="center"> </td></tr>	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do
new box for menu items	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do
end new box for menu items	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do
old links <tr><td colspan="2"> </td></tr> <tr> <td> </td> <td width="60%"> Application Applications that use CSM for security. User Users can serve as UPT Administrators. Privilege Standard privileges made available to applications. </td> <td width="30%"> </td> </tr>	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do
Page Title begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
Page Title ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
NCI hdr begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
NCI hdr ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
application hdr begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
new separate links depending on admin or super admin	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
end home links	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
application hdr ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
main content begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
target of anchor to skip menus	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
banner begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/

Comment	URL
welcome begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
welcome ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
sidebar begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
login begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
login ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
what's new begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
what's new ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
did you know? begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
did you know? ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
spacer cell begins (keep for dynamic expanding)	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
spacer cell ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
sidebar ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
main content ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
application ftr begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
application ftr ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
NCI footer begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
NCI footer ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
link 1 begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link 1 ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link 2 begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link 2 ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link 3 begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link 3 ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link priv 3.0.1 begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link priv 3.0.1 ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link 4 begins	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
link 4 ends	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do

Comment	URL
<tr><td class="appMenu" width="200" align="right"> </td><td class="appMenu" width="50" align="center"> </td></tr>	https://ncias-d704-v.nci.nih.gov:29543/upt423/pages/content/main/ErrorCSRF.html

Cookies

Name	Value	URL
JSESSIONID	7952F626CCFFB4B8020B6784BA54F930	
JSESSIONID	A43374260461538B9BEDE7B2B40B67DB	
ncbi_sid	9DFC783CE1F26D61_0009SID	
newuser	ncicbiitappscan	
JSESSIONID	C785E2BDBEB2EA995525BE2A53106E58	https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do
JSESSIONID	82A7691CEF2E93D40D56608BF2B53E26	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
JSESSIONID	45C211D67E5CCB0282CD240F65055390	https://ncias-d704-v.nci.nih.gov:29543/uptlogin/

Application URLs

- https://ncias-d704-v.nci.nih.gov:29543/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/AdminHome.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/AdminHome.do;jsessionid=C785E2BDBEB2EA995525BE2A53106E58
- https://ncias-d704-v.nci.nih.gov:29543/upt423/ApplicationDBOperation.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/FooterAccessibility.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/FooterApplicationSupport.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/FooterContactUs.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/FooterDisclaimer.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/FooterPrivacy.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/Login.dosaHomeHeader
- https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/MenuSelection.do;jsessionid=C785E2BDBEB2EA995525BE2A53106E58
- https://ncias-d704-v.nci.nih.gov:29543/upt423/PrivilegeDBOperation.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/UserDBOperation.do
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/AdminHome.do

- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterAccessibility.do
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterApplicationSupport.do
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterContactUs.do
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterDisclaimer.do
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/FooterPrivacy.do
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/LHome.do
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/Login.do
- https://ncias-d704-v.nci.nih.gov:29543/upt423/images/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/images/appLogo.gif;jsessionid=C785E2BDBEB2EA995525BE2A53106E58
- https://ncias-d704-v.nci.nih.gov:29543/upt423/pages/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/scripts/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/scripts/script.js
- https://ncias-d704-v.nci.nih.gov:29543/upt423/styles/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/pages/content/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/pages/content/main/
- https://ncias-d704-v.nci.nih.gov:29543/upt423/pages/content/main/ErrorCSRF.html
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/images/
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/scripts/
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/scripts/script.js
- https://ncias-d704-v.nci.nih.gov:29543/uptlogin/styles/

Advisories & Fix Recommendations

Session Identifier Not Updated

Application

WASC Threat Classification

Session Fixation

http://projects.webappsec.org/Session-Fixation

CVE ID(s)

N/A

CWE ID(s)

613

Security Risks

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

Possible Causes

Insecure web application programming or configuration

Technical Description

According to WASC:
"Session Fixation is an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to "fix" the session ID value. These techniques range from Cross-site Scripting exploits to peppering the web site with previously made HTTP requests. After a user's session ID has been fixed, the attacker waits for the user to login, and then uses the predefined session ID value to assume the user's online identity.
In general, there are two types of session management systems for ID values. The first type is "permissive" systems, that allow web browsers to specify any ID. The second type is "strict" systems, that only accept server-side generated values. With permissive systems, arbitrary session IDs are maintained without contact with the web site. Strict systems require that the attacker maintain the "trap -session", with periodic web site contact, preventing inactivity timeouts.
Without active protection against session fixation, the attack can be mounted against any web site using sessions to identify authenticated users. Web sites using session IDs are normally cookie-based, but URLs and hidden form-fields are used as well. Unfortunately, cookie-based sessions are the easiest to attack. Most of the currently identified attack methods are aimed toward the fixation of cookies.
In contrast to stealing a user's session ID after they have logged into a web site, session fixation provides a much wider window of opportunity. The active part of the attack takes place before the user logs in.
The session fixation attack is normally a three step process:
1) Session Set-Up
The attacker sets up a "trap-session" for the target web site and obtains that session's ID, or the attacker may select an arbitrary session ID used in the attack. In some cases, the established trap session value must be maintained with repeated web site contact.

2) Session Fixation
The attacker introduces the trap session value into the user's browser and fixes the user's session ID.
3) Session Entrance
The attacker waits until the user logs into the target web site, and then, when the fixed session ID value is used, the attacker may take over."

If a session management system accepts session IDs in the form of a URL parameter, the following request may force the session ID to the value of the URL parameter.
Code Snippet:
http://example/login.php?PHPSESSID=1234
According to WASC:
"Issuing a new session ID cookie value using a client-side script
---
A Cross-Site Scripting vulnerability on any web site in the domain can be used to modify the current cookie value.
Code Snippet:
http://example/<script>document.cookie="sessionid=1234;%20domain=.example.dom";</script>
Another similar example (using META tag injection):
http://example/<meta%20http-equiv=Set-Cookie%20content="sessionid=1234;%20domain=.example.dom">
Issuing a cookie using an HTTP response header

The attacker forces the target web site, or any other site in the domain, to issue a session ID cookie. This can be achieved in many ways:
- Breaking into a web server in the domain (e.g., a poorly maintained WAP server)
- Poisoning a user's DNS server, effectively adding the attacker's web server to the domain
- Setting up a malicious web server in the domain (e.g., on a workstation in Windows 2000 domain, all workstations are also in the DNS domain)
- Exploiting an HTTP response splitting attack"

Comparison of the session identifiers before and after the login process revealed they were not updated, which means that user impersonation may be possible. Preliminary knowledge of the session identifier value may enable a remote attacker to pose as a logged-in legitimate user.
The flow of attack:
An attacker uses the victim's browser to open the login form of the vulnerable site.
Once the form is open, the attacker writes down the session identifier value, and waits.
When the victim logs into the vulnerable site, his session identifier is not updated.
The attacker can then use the session identifier value to impersonate the victim user, and operate on his behalf.
The session identifier value can be obtained by utilizing a Cross-Site Scripting vulnerability, causing the victim's browser to use a predefined session identifier when contacting the vulnerable site, or by launching a Session Fixation attack that will cause the site to present a predefined session identifier to the victim's browser.

General Fix Recommendations

Always generate a new session to which the user will log in if successfully authenticated.
Prevent user ability to manipulate session ID.
Do not accept session IDs provided by the user's browser at login

References and Relevant Links

"Session Fixation Vulnerability in Web-based Applications", By Mitja Kolsek - Acros Security
PHP Manual, Session Handling Functions, Sessions and security

Cross-Site Request Forgery

Application

WASC Threat Classification

Cross-site Request Forgery

http://projects.webappsec.org/Cross-Site-Request-Forgery

CVE ID(s)

N/A

CWE ID(s)

352

Security Risks

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

Possible Causes

Insufficient authentication method was used by the application

Technical Description

Cross-Site Request Forgery (CSRF) is an attack that allows a hacker to perform an action on the vulnerable site on behalf of the victim. The attack is possible when the vulnerable site does not properly validate the origin of the request.
The severity of this vulnerability depends on the functionality of the affected application, for example, a CSRF attack on a search page is less severe than a CSRF attack on a money-transfer or profile-update pages.
The attack is performed by forcing the victim's browser to issue an HTTP request to the vulnerable site. If the user is currently logged-in to the victim site, the request will automatically use the user's credentials (like session cookies, user's IP address, and other browser authentication methods). Using this method, the attacker forges the victim's identity and submits actions on his or her behalf. In other words, the vulnerable site does not take the proper measures to validate that the user indeed wanted to perform the specific action.
Forcing the victim to send the unintended request can be done in numerous ways:
- Sending the victim a malicious link to the vulnerable application via e-mail.
- Putting a hot-link (like an image or frame) to the vulnerable site on the hacker's web page.
- Posting a link to the vulnerable site in a public forum.
- Using Cross-Site Scripting or Link Injection vulnerabilities in the site (or another site) and automatically redirecting the browser to the vulnerable site.
If the attacker uses a Link Injection vulnerability on the vulnerable site itself he or she increases the likelihood of the user being authenticated to the site, and by that increases the likelihood of the attack to succeed.
For example, using any of the above described options, an attacker can lure the victim to view a page containing:
<img src="http://bank/transfer?destination=John&money=1000" style='visibility:hidden'>
This will cause the victim's browser to automatically request the URL together with the current credentials of the browser.

If this banking site is vulnerable to CSRF, it will transfer 1000 dollars from the victim's account to John's bank account according to the application logic.
The Cross-Site Request Forgery attack is also known as CSRF (pronounced C-Serf), XSRF, Cross-Site Reference Forgery, One-Click Attack and Session Riding.
You can verify that your application is vulnerable to CSRF by:
[1] Checking that the vulnerable link/request does not include a parameter that is hard for an attacker to guess
[2] Checking that the vulnerable link/request performs an operation that should only be performed willingly
An application that contains a sensitive action, which can be accessed directly by a request that the user submitted unknowingly, is considered vulnerable to CSRF.
CSRF is also possible on login and logout pages. On logout pages CSRF can cause denial of service, since an attacker can forge consecutive logout requests from the victim. On login pages CSRF can allow an attacker to log the client into the attacker's account using a forged request containing the attacker's username and password. Login CSRF attacks can have serious consequences, depending on other site behavior. For example, if a site keeps a history of user actions (search history, for example) the attacker will be able to see the actions previously performed by the victim on the vulnerable site.

General Fix Recommendations

In order to avoid CSRF attacks, every request should contain a unique identifier, which is a parameter that an attacker cannot guess.
One suggested option is to add the session id taken from the session cookie and adding it as a parameter. The server must check that
this parameter matches the session cookie, and if not discard the request. The reason an attacker cannot guess this parameter is the "same origin policy"
that applies to cookies, so the attacker cannot forge a fake request that will seem real to the server.
Any secret that is hard to guess and is not accessible to an attacker (i.e. not accessible from a different domain) can be used instead of the session id.
This will prevent an attacker from crafting a seemingly valid request.

References and Relevant Links

Cross-site request forgery wiki page
"JavaScript Hijacking" by Fortify
Cross-Site Request Forgery Training Module