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
5/17/2012 10:57:53 AM

Report Information

Web Application Report

Scan Name: Abstractor.retest

Scanned Host(s)

Host	Operating System	Web Server	Application Server
registryplustest.dshs.state.tx.us:443	Win32	IIS	ASP.NET

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

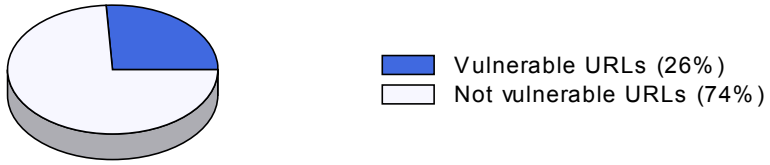
Security Risks

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 retrieve information about the site's file system structure, which may help the attacker to map the web site
- 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 gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- 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

Vulnerable URLs

26% of the URLs had test results that included security issues.



Scanned URLs

99 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
- Query parameters were passed over SSL, and may contain sensitive information
- Sensitive information might have been cached by your browser
- Insufficient authentication method was used by the application

URLs with the Most Security Issues (number issues)

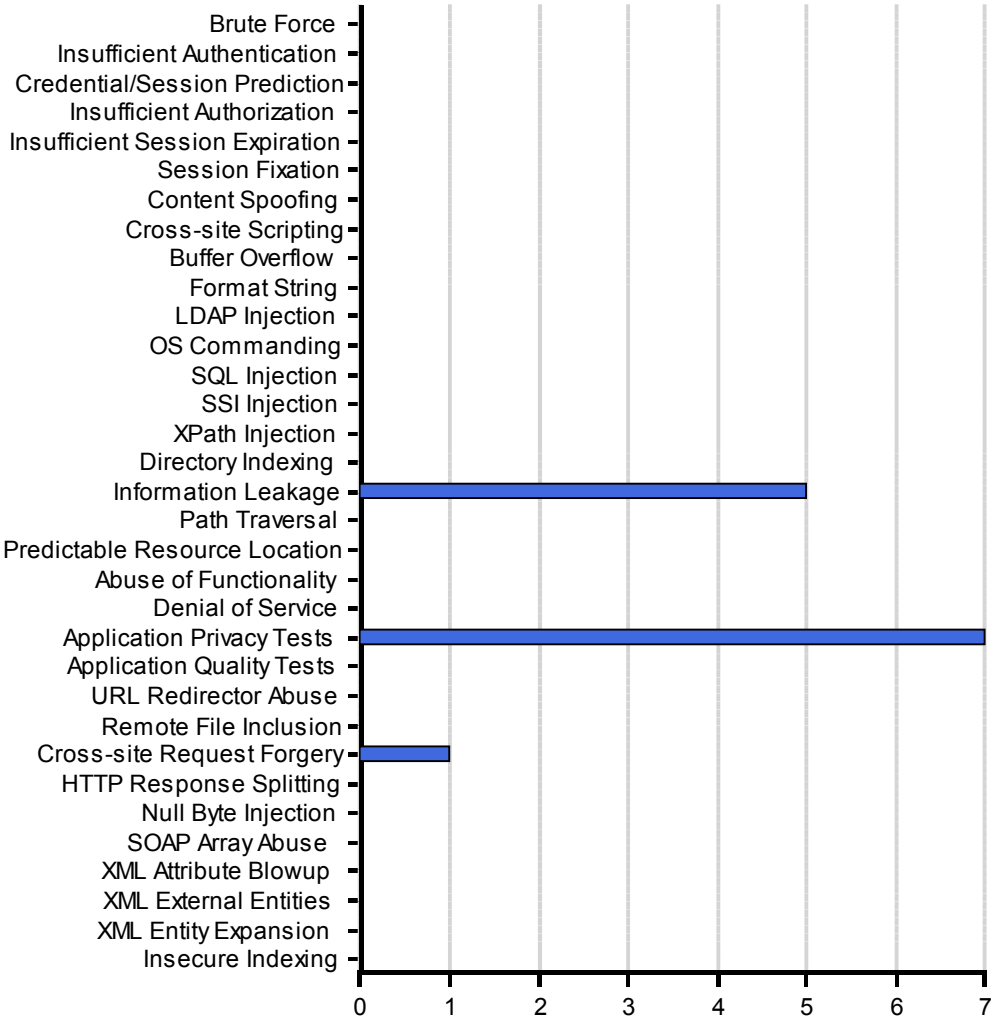
- https://registryplustest.dshs.state.tx.us/homeallex.aspx (3)
- https://registryplustest.dshs.state.tx.us/localreports.aspx (2)
- https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx (1)
- https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx (1)
- https://registryplustest.dshs.state.tx.us/releaselog.aspx (1)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
https://registryplustest.dshs.state.tx.us/	0	1	12	0	13
Total	**0**	**1**	**12**	**0**	**13**

Security Issue Distribution per Threat Class

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



Security Issue Cause Distribution

61% Application-related Security Issues (8 out of a total of 13 issues).
Application-related Security Issues can usually be fixed by application developers, as they result from defects in the application code.
39% Infrastructure and Platform Security Issues (5 out of a total 13 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://registryplustest.dshs.state.tx.us/homeallex.aspx

Total of 3 security issues in this URL

[1 of 3] Query Parameter in SSL Request

Severity:	Low
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/homeallex.aspx (Parameter: Role)
CVE ID(s):	N/A
CWE ID(s):	598
Remediation Tasks:	Always use SSL and POST (body) parameters when sending sensitive information.

Variant 1 of 1 [ID=8667]

The following may require user attention:

```
GET /homeallex.aspx?FacilityID=2222222222&DisplayID=50&Role=1 HTTP/1.1
Cookie:
sqlAuthCookie=34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0
D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629
F04091F5AF473E537E038BEBF3FBFD5FC5471;
ASP.NET_SessionId=xwu3mavx0voahsyg20eedy55; __LOGINCOOKIE__=
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homeallex.aspx


HTTP/1.1 302 Found
Content-Length: 145
Date: Mon, 14 May 2012 20:41:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Location: /HomeFacilityAbstractor.aspx
Cache-Control: private
Content-Type: text/html; charset=utf-8

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/HomeFacilityAbstractor.aspx">here</a>.</h2>
</body></html>
```

```
GET /homefacilityabstractor.aspx HTTP/1.1
Cookie:
sqlAuthCookie=34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0
D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629
F04091F5AF473E537E038BEBF3FBFD5FC5471;
ASP.NET_SessionId=xwu3mavx0voahsyg20eedy55; __LOGINCOOKIE__=
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homeallex.aspx?
FacilityID=2222222222&DisplayID=50&Role=1


HTTP/1.1 200 OK
Content-Length: 6917
Date: Mon, 14 May 2012 20:41:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<h1>Web Plus</h1><head>
<style type="text/css">
.mainmenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mainmenu a:link{color: #fff; text-decoration: none}
.mainmenu a:visited{color: #fff; text-decoration: none}
.mainmenu a:hover{color: #000; text-decoration: none}
.mainmenu a:active{color: #fff; text-decoration: none}
.mymainhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mymainhover a:link{color: #fff; text-decoration: none}
.mymainhover a:visited{color: #000; text-decoration: none}
```

```
.mymainhover a:hover{color: #000; text-decoration: none}
.mymainhover a:active{color: #000; text-decoration: none}
.submenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.submenu a:link{color: #fff; text-decoration: none}
.submenu a:visited{color: #fff; text-decoration: none}
.submenu a:hover{color: #000; text-decoration: none}
.submenu a:active{color: #fff; text-decoration: none}
.mysubhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.mysubhover a:link{color: #fff; text-decoration: none}
.mysubhover a:visited{color: #000; text-decoration: none}
.mysubhover a:hover{color: #000; text-decoration: none}
.mysubhover a:active{color: #000; text-decoration: none}

</style>
<script language="javascript">

var prevmenu;
function showmenu(menu, submenu) {if(prevmenu) document.getElementById
(prevmenu).style.visibility='hidden';if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='visible';document.getElementById
(submenu).style.zIndex=5000;document.getElementById
(submenu).style.left=document.getElementById
(menu).offsetLeft+10;document.getElementById
(submenu).style.top=document.getElementById
('main').offsetTop+document.getElementById('main').offsetHeight;prevmenu = submenu;}}
function hidemenu(submenu) {if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='hidden'}}
function makeactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='pointer';}}
function makeinactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='auto';}}

</script>

</head>
```

```
<body>
<div id=main style='top:40px;left:'; width:100%>
<table width=100%>
<tr>
<td class="mainmenu" id = "homemain" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('homemain','mymainhover')" onmouseout="makeinactive
('homemain','mainmenu')"><a href=HomeAllEx.aspx>Home</a></td>
<td class="ma...
```

Validation In Response:

N/A

Reasoning:

AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

CWE ID:

598

[2 of 3] Query Parameter in SSL Request

Severity:	Low
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/homeallex.aspx (Parameter: DisplayID)
CVE ID(s):	N/A
CWE ID(s):	598
Remediation Tasks:	Always use SSL and POST (body) parameters when sending sensitive information.

Variant 1 of 1 [ID=8444]

The following may require user attention:

```
GET /homeallex.aspx?FacilityID=2222222222&DisplayID=50&Role=1 HTTP/1.1
Cookie:
sqlAuthCookie=34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0
D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629
F04091F5AF473E537E038BEBF3FBFD5FC5471;
ASP.NET_SessionId=xwu3mavx0voahsyg20eedy55; __LOGINCOOKIE__=
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homeallex.aspx


HTTP/1.1 302 Found
Content-Length: 145
Date: Mon, 14 May 2012 20:41:00 GMT
```

Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Location: /HomeFacilityAbstractor.aspx
Cache-Control: private
Content-Type: text/html; charset=utf-8

<html><head><title>Object moved</title></head><body>
<h2>Object moved to here.</h2>
</body></html>

GET /homefacilityabstractor.aspx HTTP/1.1
Cookie:
sqlAuthCookie=34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0
D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629
F04091F5AF473E537E038BEBF3FBFD5FC5471;
ASP.NET_SessionId=xwu3mavx0voahsyg20eedy55; __LOGINCOOKIE__=
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homeallex.aspx?
FacilityID=2222222222&DisplayID=50&Role=1

HTTP/1.1 200 OK
Content-Length: 6917
Date: Mon, 14 May 2012 20:41:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<h1>Web Plus</h1><head>
<style type="text/css">
.mainmenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mainmenu a:link{color: #fff; text-decoration: none}
.mainmenu a:visited{color: #fff; text-decoration: none}
.mainmenu a:hover{color: #000; text-decoration: none}
.mainmenu a:active{color: #fff; text-decoration: none}

```
.mymainhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mymainhover a:link{color: #fff; text-decoration: none}
.mymainhover a:visited{color: #000; text-decoration: none}
.mymainhover a:hover{color: #000; text-decoration: none}
.mymainhover a:active{color: #000; text-decoration: none}
.submenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.submenu a:link{color: #fff; text-decoration: none}
.submenu a:visited{color: #fff; text-decoration: none}
.submenu a:hover{color: #000; text-decoration: none}
.submenu a:active{color: #fff; text-decoration: none}
.mysubhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.mysubhover a:link{color: #fff; text-decoration: none}
.mysubhover a:visited{color: #000; text-decoration: none}
.mysubhover a:hover{color: #000; text-decoration: none}
.mysubhover a:active{color: #000; text-decoration: none}

</style>
<script language="javascript">

var prevmenu;
function showmenu(menu, submenu) {if(prevmenu) document.getElementById
(prevmenu).style.visibility='hidden';if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='visible';document.getElementById
(submenu).style.zIndex=5000;document.getElementById
(submenu).style.left=document.getElementById
(menu).offsetLeft+10;document.getElementById
```

```
(submenu).style.top=document.getElementById
('main').offsetTop+document.getElementById('main').offsetHeight;prevmenu = submenu;}}
function hidemenu(submenu) {if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='hidden'}}
function makeactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='pointer';}}
function makeinactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='auto';}}

</script>

</head>
<body>
<div id=main style='top:40px;left:'; width:100%>
<table width=100%>
<tr>
<td class="mainmenu" id = "homemain" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('homemain','mymainhover')" onmouseout="makeinactive
('homemain','mainmenu')"><a href=HomeAllEx.aspx>Home</a></td>
<td class="ma...
```

Validation In Response:

N/A

Reasoning:

AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

CWE ID:

598

[3 of 3] Query Parameter in SSL Request

Severity:	Low
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/homeallex.aspx (Parameter: FacilityID)
CVE ID(s):	N/A
CWE ID(s):	598
Remediation Tasks:	Always use SSL and POST (body) parameters when sending sensitive information.

Variant 1 of 1 [ID=8221]

The following may require user attention:

```
GET /homeallex.aspx?FacilityID=2222222222&DisplayID=50&Role=1 HTTP/1.1
Cookie:
sqlAuthCookie=34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0
D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629
F04091F5AF473E537E038BEBF3FBFD5FC5471;
ASP.NET_SessionId=xwu3mavx0voahsyg20eedy55; __LOGINCOOKIE__=
```

Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homeallex.aspx

HTTP/1.1 302 Found
Content-Length: 145
Date: Mon, 14 May 2012 20:41:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Location: /HomeFacilityAbstractor.aspx
Cache-Control: private
Content-Type: text/html; charset=utf-8

<html><head><title>Object moved</title></head><body>
<h2>Object moved to here.</h2>
</body></html>

GET /homefacilityabstractor.aspx HTTP/1.1
Cookie:
sqlAuthCookie=34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629F04091F5AF473E537E038BEBF3FBFD5FC5471;
ASP.NET_SessionId=xwu3mavx0voahsyg20eedy55; __LOGINCOOKIE__=
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homeallex.aspx?FacilityID=2222222222&DisplayID=50&Role=1

HTTP/1.1 200 OK
Content-Length: 6917
Date: Mon, 14 May 2012 20:41:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<h1>Web Plus</h1><head>
<style type="text/css">
.mainmenu{
font: 11px arial, verdana, helvetica;

```
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mainmenu a:link{color: #fff; text-decoration: none}
.mainmenu a:visited{color: #fff; text-decoration: none}
.mainmenu a:hover{color: #000; text-decoration: none}
.mainmenu a:active{color: #fff; text-decoration: none}
.mymainhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mymainhover a:link{color: #fff; text-decoration: none}
.mymainhover a:visited{color: #000; text-decoration: none}
.mymainhover a:hover{color: #000; text-decoration: none}
.mymainhover a:active{color: #000; text-decoration: none}
.submenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.submenu a:link{color: #fff; text-decoration: none}
.submenu a:visited{color: #fff; text-decoration: none}
.submenu a:hover{color: #000; text-decoration: none}
.submenu a:active{color: #fff; text-decoration: none}
.mysubhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.mysubhover a:link{color: #fff; text-decoration: none}
.mysubhover a:visited{color: #000; text-decoration: none}
.mysubhover a:hover{color: #000; text-decoration: none}
```

```
.mysubhover a:active{color: #000; text-decoration: none}

</style>
<script language="javascript">

var prevmenu;
function showmenu(menu, submenu) {if(prevmenu) document.getElementById
(prevmenu).style.visibility='hidden';if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='visible';document.getElementById
(submenu).style.zIndex=5000;document.getElementById
(submenu).style.left=document.getElementById
(menu).offsetLeft+10;document.getElementById
(submenu).style.top=document.getElementById
('main').offsetTop+document.getElementById('main').offsetHeight;prevmenu = submenu;}}
function hidemenu(submenu) {if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='hidden'}}
function makeactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='pointer';}}
function makeinactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='auto';}}

</script>

</head>
<body>
<div id=main style='top:40px;left:'; width:100%>
<table width=100%>
<tr>
<td class="mainmenu" id = "homemain" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('homemain','mymainhover')" onmouseout="makeinactive
('homemain','mainmenu')"><a href=HomeAllEx.aspx>Home</a></td>
<td class="ma...
```

Validation In Response:

N/A

Reasoning:

AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

CWE ID:

598

Vulnerable URL: https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx

Total of 1 security issues in this URL

[1 of 1] Cacheable SSL Page Found

Severity:	Low
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
CVE ID(s):	N/A
CWE ID(s):	525
Remediation Tasks:	Do not allow caching of SSL pages

Variant 1 of 1 [ID=142]

Request/Response:

```
GET /homefacilityabstractor.aspx HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=kuzsjo55yececl55xdyxtr45;
sqlAuthCookie=2B6C2288C531209415728D52716A105367314C2C1A7A4EEE5B7CB6EF4825F4279A841C
35447331F0783CB25FF0C7631FDB6F168BFE08E34F056C911B7F6A66EDF092DE7F423CA69D7789496833
F37223
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homeallex.aspx?
FacilityID=2222222222&DisplayID=50&Role=1


HTTP/1.1 200 OK
Content-Length: 6917
Date: Mon, 14 May 2012 21:09:27 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<h1>Web Plus</h1><head>
<style type="text/css">
.mainmenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mainmenu a:link{color: #fff; text-decoration: none}
.mainmenu a:visited{color: #fff; text-decoration: none}
.mainmenu a:hover{color: #000; text-decoration: none}
.mainmenu a:active{color: #fff; text-decoration: none}
.mymainhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mymainhover a:link{color: #fff; text-decoration: none}
.mymainhover a:visited{color: #000; text-decoration: none}
```

```
.mymainhover a:hover{color: #000; text-decoration: none}
.mymainhover a:active{color: #000; text-decoration: none}
.submenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.submenu a:link{color: #fff; text-decoration: none}
.submenu a:visited{color: #fff; text-decoration: none}
.submenu a:hover{color: #000; text-decoration: none}
.submenu a:active{color: #fff; text-decoration: none}
.mysubhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.mysubhover a:link{color: #fff; text-decoration: none}
.mysubhover a:visited{color: #000; text-decoration: none}
.mysubhover a:hover{color: #000; text-decoration: none}
.mysubhover a:active{color: #000; text-decoration: none}

</style>
<script language="javascript">

var prevmenu;
function showmenu(menu, submenu) {if(prevmenu) document.getElementById
(prevmenu).style.visibility='hidden';if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='visible';document.getElementById
(submenu).style.zIndex=5000;document.getElementById
(submenu).style.left=document.getElementById
(menu).offsetLeft+10;document.getElementById
(submenu).style.top=document.getElementById
('main').offsetTop+document.getElementById('main').offsetHeight;prevmenu =
submenu;}}
function hidemenu(submenu) {if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='hidden'}}
function makeactive(itm, style) {if (document.getElementById(itm))
{document.getElementById
(itm).className=style;document.body.style.cursor='pointer';}}
function makeinactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='auto';}}

</script>

</head>
<body>
<div id=main style='top:40px;left:'; width:100%>
<table width=100%>
<tr>
<td class="mainmenu" id = "homemain" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('homemain','mymainhover')" onmouseout="makeinactive
('homemain','mainmenu')"><a href=HomeAllEx.aspx>Home</a></td>
<td class="mainmenu" id = "newabstract" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('newabstract','mymainhover')"
onmouseout="makeinactive('newabstract','mainmenu')"><a href=dataentrytype1.aspx?
absrefid=0>New Abstract</a></td>
<td class="mainmenu" id = "findabstract" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('findabstract','mymainhover')"
onmouseout="makeinactive('findabstract','mainmenu')"><a
href=frmfindabstracthospitaluser.aspx>Find/Open Abstract</a></td>
<td class="mainmenu" id = "releaseabstracts" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('releaseabstracts','mymainhover')"
```

```
onmouseout="makeinactive('releaseabstracts','mainmenu')"><a
href=releaseabstracts.aspx>Release Abstracts</a></td>
<td class="mainmenu" id = "reports" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('reports','mymainhover')" onmouseout="makeinactive
('reports','mainmenu')"><a href=localreports.aspx>Reports</a></td>
<td class="mainmenu" id = "changepassword" colspan=1  onmouseover="showmenu('no...
```

Validation In Response:

```
N/A
```

Reasoning:

The application has responded with a response that indicates the page should be cached.

CWE ID:

525

Vulnerable URL: https://registryplustest.dshs.state.tx.us/localreports.aspx

Total of 2 security issues in this URL

[1 of 2] Cross-Site Request Forgery

Severity:	Medium
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/localreports.aspx
CVE ID(s):	N/A
CWE ID(s):	352
Remediation Tasks:	Decline malicious requests

Variant 1 of 1 [ID=255]

The following changes were applied to the original request:

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

Request/Response:

```
POST /localreports.aspx HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=kuzsjo55yececl55xdyxtr45;
sqlAuthCookie=2B6C2288C5312O9415728D52716A105367314C2C1A7A4EEE5B7CB6EF4825F4279A841C
35447331F0783CB25FF0C7631FDB6F168BFE08E34F056C911B7F6A66EDF092DE7F423CA69D7789496833
F37223
Content-Length: 444
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Content-Type: application/x-www-form-urlencoded
Referer: http://bogus.referer.ibm.com

__VIEWSTATE=I774L6WD4V0yESV%2FbeEyZEVx%2F3NQVkiFulR60KR4cJdeaQFXH2iIo440g8%
2BBjIgysWJLO1i7vVMGYsJ6%2BZBerDg5XNZokx8gmC2OcYLWC%2FZGVc%
2FtQ7TQycfA6pGnp538w2AfmMNfg3sX%2BThD8K%2Bwc1vTsYF%2BtzcQltRM5NfeN4DkPPQA2nu76r%
2BJEfnjhgGoRWsa7LfmGgeMxrHWd1HIlh5OMhEMJpeRubTmZwBhkkIgvxbpvdnDW%2BpmS%2BfGUviOB%
2FxFXlg4I2xce7LOefmXJq7AtnRdC5rxRdJK2vE%2FEWKtsKmTeHDcFvsPPdeB2MHum%2FXu%2BhbXw7%
2FzLZ%2FBMP23qSzLH954yAAEnNULR%2FyU4D1%2BiXcFE64NXA%3D%3D&txtTimeout=
HTTP/1.1 200 OK
Content-Length: 9297
Date: Mon, 14 May 2012 21:21:37 GMT
```

```
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<h1>Web Plus</h1><head>
<style type="text/css">
.mainmenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mainmenu a:link{color: #fff; text-decoration: none}
.mainmenu a:visited{color: #fff; text-decoration: none}
.mainmenu a:hover{color: #000; text-decoration: none}
.mainmenu a:active{color: #fff; text-decoration: none}
.mymainhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mymainhover a:link{color: #fff; text-decoration: none}
.mymainhover a:visited{color: #000; text-decoration: none}
.mymainhover a:hover{color: #000; text-decoration: none}
.mymainhover a:active{color: #000; text-decoration: none}
.submenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.submenu a:link{color: #fff; text-decoration: none}
.submenu a:visited{color: #fff; text-decoration: none}
.submenu a:hover{color: #000; text-decoration: none}
.submenu a:active{color: #fff; text-decoration: none}
.mysubhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.mysubhover a:link{color: #fff; text-decoration: none}
.mysubhover a:visited{color: #000; text-decoration: none}
.mysubhover a:hover{color: #000; text-decoration: none}
.mysubhover a:active{color: #000; text-decoration: none}

</style>
<script language="javascript">

var prevmenu;
function showmenu(menu, submenu) {if(prevmenu) document.getElementById
(prevmenu).style.visibility='hidden';if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='visible';document.getElementById
```

```
(submenu).style.zIndex=5000;document.getElementById
(submenu).style.left=document.getElementById
(menu).offsetLeft+10;document.getElementById
(submenu).style.top=document.getElementById
('main').offsetTop+document.getElementById('main').offsetHeight;prevmenu =
submenu;}}
function hidemenu(submenu) {if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='hidden'}}
function makeactive(itm, style) {if (document.getElementById(itm))
{document.getElementById
(itm).className=style;document.body.style.cursor='pointer';}}
function makeinactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='auto';}}

</script>

</head>
<body>
<div id=main style='top:40px;left:'; width:100%>
<table width=100%>
<tr>
<td class="mainmenu" id = "homemain" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('homemain','mymainhover')" onmouseout="makeinactive
('homemain','mainmenu')"><a href=HomeAllEx.aspx>Home</a></td>
<td class="mainmenu" id = "newabstract" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('newabstract','mymainhover')"
onmouseout="makeinactive('newabstract','mainmenu')"><a href=dataentrytype1.aspx?
absrefid=0>New Abstract</a></td>
<td class="mainmenu" id = "findabstract" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('findabstract','mymainhover')"
onmouseout="makeinactive('findabstract','mainmenu')"><a
href=frmfindabstracthospitaluser.aspx>Find/Open Abstract</a></td>
<td class="mainmenu" id = "releaseabstracts" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('releaseabstr...
```

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

[2 of 2] Cacheable SSL Page Found

Severity:	Low
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/localreports.aspx
CVE ID(s):	N/A
CWE ID(s):	525
Remediation Tasks:	Do not allow caching of SSL pages

Variant 1 of 1 [ID=156]

Request/Response:

```
GET /localreports.aspx HTTP/1.1
```

```
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=kuzsjo55yececl55xdyxtr45;
sqlAuthCookie=2B6C2288C531209415728D52716A105367314C2C1A7A4EEE5B7CB6EF4825F4279A841C
35447331F0783CB25FF0C7631FDB6F168BFE08E34F056C911B7F6A66EDF092DE7F423CA69D7789496833
F37223
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx


HTTP/1.1 200 OK
Content-Length: 9297
Date: Mon, 14 May 2012 21:12:07 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<h1>Web Plus</h1><head>
<style type="text/css">
.mainmenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mainmenu a:link{color: #fff; text-decoration: none}
.mainmenu a:visited{color: #fff; text-decoration: none}
.mainmenu a:hover{color: #000; text-decoration: none}
.mainmenu a:active{color: #fff; text-decoration: none}
.mymainhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mymainhover a:link{color: #fff; text-decoration: none}
.mymainhover a:visited{color: #000; text-decoration: none}
.mymainhover a:hover{color: #000; text-decoration: none}
.mymainhover a:active{color: #000; text-decoration: none}
.submenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.submenu a:link{color: #fff; text-decoration: none}
.submenu a:visited{color: #fff; text-decoration: none}
.submenu a:hover{color: #000; text-decoration: none}
.submenu a:active{color: #fff; text-decoration: none}
.mysubhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: left;
```

```
padding: 3px;
width: 140px;
text-decoration: none;
}
.mysubhover a:link{color: #fff; text-decoration: none}
.mysubhover a:visited{color: #000; text-decoration: none}
.mysubhover a:hover{color: #000; text-decoration: none}
.mysubhover a:active{color: #000; text-decoration: none}

</style>
<script language="javascript">

var prevmenu;
function showmenu(menu, submenu) {if(prevmenu) document.getElementById
(prevmenu).style.visibility='hidden';if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='visible';document.getElementById
(submenu).style.zIndex=5000;document.getElementById
(submenu).style.left=document.getElementById
(menu).offsetLeft+10;document.getElementById
(submenu).style.top=document.getElementById
('main').offsetTop+document.getElementById('main').offsetHeight;prevmenu =
submenu;}}
function hidemenu(submenu) {if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='hidden'}}
function makeactive(itm, style) {if (document.getElementById(itm))
{document.getElementById
(itm).className=style;document.body.style.cursor='pointer';}}
function makeinactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='auto';}}

</script>

</head>
<body>
<div id=main style='top:40px;left:'; width:100%>
<table width=100%>
<tr>
<td class="mainmenu" id = "homemain" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('homemain','mymainhover')" onmouseout="makeinactive
('homemain','mainmenu')"><a href=HomeAllEx.aspx>Home</a></td>
<td class="mainmenu" id = "newabstract" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('newabstract','mymainhover')"
onmouseout="makeinactive('newabstract','mainmenu')"><a href=dataentrytype1.aspx?
absrefid=0>New Abstract</a></td>
<td class="mainmenu" id = "findabstract" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('findabstract','mymainhover')"
onmouseout="makeinactive('findabstract','mainmenu')"><a
href=frmfindabstracthospitaluser.aspx>Find/Open Abstract</a></td>
<td class="mainmenu" id = "releaseabstracts" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('releaseabstracts','mymainhover')"
onmouseout="makeinactive('releaseabstracts','mainmenu')"><a
href=releaseabstracts.aspx>Release Abstracts</a></td>
<td class="mainmenu" id = "reports" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('reports','mymainhover')" onmouseout="makeinactive
('reports','mainmenu')"><a href=localreports.aspx>Reports</a></td>
<td class="mainmenu" id = "changepassword" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('changepas...
```

Validation In Response:

N/A

Reasoning:

The application has responded with a response that indicates the page should be cached.

CWE ID:

525

Vulnerable URL: https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx

Total of 1 security issues in this URL

[1 of 1] Cacheable SSL Page Found

Severity:	Low
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
CVE ID(s):	N/A
CWE ID(s):	525
Remediation Tasks:	Do not allow caching of SSL pages

Variant 1 of 1 [ID=184]

Request/Response:

```
GET /releaseabstracts.aspx HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=kuzsjo55yececl55xdyxtr45;
sqlAuthCookie=2B6C2288C531209415728D52716A105367314C2C1A7A4EEE5B7CB6EF4825F4279A841C
35447331F0783CB25FF0C7631FDB6F168BFE08E34F056C911B7F6A66EDF092DE7F423CA69D7789496833
F37223
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx


HTTP/1.1 200 OK
Content-Length: 10040
Date: Mon, 14 May 2012 21:21:18 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8

<h1>Web Plus</h1><head>
<style type="text/css">
.mainmenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: center;
padding: 3px;
width: 10%;
text-decoration: none;
}
.mainmenu a:link{color: #fff; text-decoration: none}
.mainmenu a:visited{color: #fff; text-decoration: none}
.mainmenu a:hover{color: #000; text-decoration: none}
.mainmenu a:active{color: #fff; text-decoration: none}
.mymainhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: center;
padding: 3px;
```

```
width: 10%;
text-decoration: none;
}
.mymainhover a:link{color: #fff; text-decoration: none}
.mymainhover a:visited{color: #000; text-decoration: none}
.mymainhover a:hover{color: #000; text-decoration: none}
.mymainhover a:active{color: #000; text-decoration: none}
.submenu{
font: 11px arial, verdana, helvetica;
color: #fff;
border: 1 px solid #fff;
background-color: #0C457E;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.submenu a:link{color: #fff; text-decoration: none}
.submenu a:visited{color: #fff; text-decoration: none}
.submenu a:hover{color: #000; text-decoration: none}
.submenu a:active{color: #fff; text-decoration: none}
.mysubhover{
font: 11px arial, verdana, helvetica;
color: #000;
border: 1 px solid #fff;
background-color: #CFDFEB;
text-align: left;
padding: 3px;
width: 140px;
text-decoration: none;
}
.mysubhover a:link{color: #fff; text-decoration: none}
.mysubhover a:visited{color: #000; text-decoration: none}
.mysubhover a:hover{color: #000; text-decoration: none}
.mysubhover a:active{color: #000; text-decoration: none}

</style>
<script language="javascript">

var prevmenu;
function showmenu(menu, submenu) {if(prevmenu) document.getElementById
(prevmenu).style.visibility='hidden';if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='visible';document.getElementById
(submenu).style.zIndex=5000;document.getElementById
(submenu).style.left=document.getElementById
(menu).offsetLeft+10;document.getElementById
(submenu).style.top=document.getElementById
('main').offsetTop+document.getElementById('main').offsetHeight;prevmenu =
submenu;}}
function hidemenu(submenu) {if (document.getElementById(submenu))
{document.getElementById(submenu).style.visibility='hidden'}}
function makeactive(itm, style) {if (document.getElementById(itm))
{document.getElementById
(itm).className=style;document.body.style.cursor='pointer';}}
function makeinactive(itm, style) {if (document.getElementById(itm))
{document.getElementById(itm).className=style;document.body.style.cursor='auto';}}

</script>

</head>
<body>
<div id=main style='top:40px;left:'; width:100%>
<table width=100%>
<tr>
<td class="mainmenu" id = "homemain" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('homemain','mymainhover')" onmouseout="makeinactive
('homemain','mainmenu')"><a href=HomeAllEx.aspx>Home</a></td>
<td class="mainmenu" id = "newabstract" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('newabstract','mymainhover')"
onmouseout="makeinactive('newabstract','mainmenu')"><a href=dataentrytype1.aspx?
absrefid=0>New Abstract</a></td>
<td class="mainmenu" id = "findabstract" colspan=1  onmouseover="showmenu
```

```
('nothing','nothing');makeactive('findabstract','mymainhover')"
onmouseout="makeinactive('findabstract','mainmenu')"><a
href=frmfindabstracthospitaluser.aspx>Find/Open Abstract</a></td>
<td class="mainmenu" id = "releaseabstracts" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('releaseabstracts','mymainhover')"
onmouseout="makeinactive('releaseabstracts','mainmenu')"><a
href=releaseabstracts.aspx>Release Abstracts</a></td>
<td class="mainmenu" id = "reports" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('reports','mymainhover')" onmouseout="makeinactive
('reports','mainmenu')"><a href=localreports.aspx>Reports</a></td>
<td class="mainmenu" id = "changepassword" colspan=1  onmouseover="showmenu
('nothing','nothing');makeactive('chan...
```

Validation In Response:

N/A

Reasoning:

The application has responded with a response that indicates the page should be cached.

CWE ID:

525

Vulnerable URL: https://registryplustest.dshs.state.tx.us/releaselog.aspx

Total of 1 security issues in this URL

[1 of 1] Query Parameter in SSL Request

Severity:	Low
Test Type:	Application
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/releaselog.aspx (Parameter: facilityid)
CVE ID(s):	N/A
CWE ID(s):	598
Remediation Tasks:	Always use SSL and POST (body) parameters when sending sensitive information.

Variant 1 of 1 [ID=8890]

The following may require user attention:

```
GET /releaselog.aspx?facilityid=2222222222 HTTP/1.1
Cookie:
sqlAuthCookie=34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0
D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629
F04091F5AF473E537E038BEBF3FBFD5FC5471;
ASP.NET_SessionId=xwu3mavx0voahsyg20eedy55; __LOGINCOOKIE__=
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us
Referer: https://registryplustest.dshs.state.tx.us/localreports.aspx
```

```
HTTP/1.1 200 OK
Content-Length: 5074
Date: Mon, 14 May 2012 20:41:02 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
    <head>
        <title>Web Plus</title>
        <meta http-equiv="Pragma" content="no-cache" />
        <meta http-equiv="Cache-Control" content="no-store,no-cache" />
        <meta content="Microsoft Visual Studio .NET 7.1" name="GENERATOR">
        <meta content="Visual Basic .NET 7.1" name="CODE_LANGUAGE">
        <meta content="JavaScript" name="vs_defaultClientScript">
        <meta content="http://schemas.microsoft.com/intellisense/ie5"
name="vs_targetSchema">
        <script type="text/javascript">
    function getDateFrom()
    {

       w = screen.width/2
         h = screen.availHeight-10
         t = 1
         l = screen.availWidth/2-10
         val=document.getElementById("txtFrom").value
         strStyle='width='+ w +',height=' + h/2 + ',top=1,left=' + l + ', scrollbars=no,
resizable=no'
         WindowName = window.open("calendar.aspx?
id=txtFrom&date="+val,'help',strStyle);
         WindowName.focus()
    }

    function getDateTo()
    {

       w = screen.width/2
         h = screen.availHeight-10
         t = 1
         l = screen.availWidth/2-10
         val=document.getElementById("txtTo").value
         strStyle='width='+ w +',height=' + h/2 + ',top=1,left=' + l + ', scrollbars=no,
resizable=no'
         WindowName = window.open("calendar.aspx?id=txtTo&date="+val,'help',strStyle);
         WindowName.focus()
    }
        </script>
    </head>
```

value="I774L6WD4V0eEqcfOVTcZbB87Hi1f+xK9SvCBHHAiDGy8O0oZjj1I/WVh/7MNEz6T
UBKzFw0JAivEVceyu10X3Fmi5Nxk/gyCRur9Dxt4NrORpxjCIovX5JbKIreCzCfnaZUbpu9ur
OHD4wedpAJ1tEY3vRu7IXAT5UrjkegkeXg2yCFKxctCUlFO4nRm2o/xw/U/EaobLyHEtyfo+
35xBVzdJEWimVzLdJFdxnqCKaC5kgjXnd6ED22ryG7pq6ZwL1bxgAvjH5nUzBY5RmE2fth
34rT94C39HSkVYOkptFGWsFyBo+O/O6ltpxJGEIT6qGVhWd1mMinP2T50gILko2NwOUuu
EJCMC9SZvyu2dVIn6xRa/+nqTEfXqCeVCEjR79VCIOthu3d6+qpSyF+/bwH3uoUN/vhBkTy
GYAt2Kn7WKLploaLHZ7VD84Ruz4a" />

<input name="txtTimeout" type="hidden" id="txtTimeout" style="Z-INDEX: 112; LEFT: 8px; WIDTH: 16px; POSITION: absolute; TOP: 8px; HEIGHT: 16px" size="1" />
Abstract Release LogChoose a date range:From:<input name="txtFrom" type="text" value="04/14/2012" id="txtFrom" style="height:20px;width:90px;Z-INDEX: 103; LEFT: 224px; POSITION: absolute; TOP: 48px" /><IMG id="calendar1" style="Z-INDEX: 105; LEFT: 312px; WIDTH: 24px; POSITION: absolute; TOP: 48px"
onclick="getDateFrom()" height="20" alt="" src="images/calendar.jpg" width="24">
To:<input name="txtTo" type="text" value="05/14/2012" id="txtTo" style="height:20px;width:90px;Z-INDEX: 104; LEFT: 408px; POSITION: absolute; TOP: 48px" /><IMG id="calendar2" style="Z-INDEX: 107; LEFT: 496px; WIDTH: 24px; POSITION: absolute; TOP: 48px"
onclick="getDateTo()" height="20" alt="" src="images/calendar.jpg" width="24">
<input type="submit" name="btnRun" value="Select" id="btnRun" style="height:20px;width:48px;Z-INDEX: 110; LEFT: 544px; POSITION: absolute; TOP: 48px" />Date Report Run: 5/14/2012 3:41:02 PM<table id="tblReport" border="0" style="height:24px;width:100%;Z-INDEX: 101; LEFT: 16px; POSITION: absolute; TOP: 152px">
<tr>
<th align="left" style="font-family:Arial;font-size:9pt;">AbsRefID</th><th align="left" style="font-family:Arial;font-size:9pt;">UserID</th><th align="left" style="font-family:Arial;font-si...

Validation In Response:

N/A

Reasoning:

AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

CWE ID:
598

Vulnerable URL: https://registryplustest.dshs.state.tx.us/data/

Total of 1 security issues in this URL

[1 of 1] Hidden Directory Detected

Severity:	Low
Test Type:	Infrastructure
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/data/
CVE ID(s):	N/A
CWE ID(s):	N/A
Remediation Tasks:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Variant 1 of 1 [ID=3557]

The following changes were applied to the original request:
• Set path to 'data/'

Request/Response:

```
GET /data/ HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=driwnue3ubwsdx55czuok445;
sqlAuthCookie=C542B249324C2E7AC2A89D1CA3FAAD33C69662CC5ADD27544182433DD34B58C42CE746
C25018ED28FACC83C9EF236E126D07B93D32FF54A2B10F4ED5F27E8B99C80F2A2161E226BCA1D29240A9
53DF65
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 14 May 2012 21:58:55 GMT

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

Validation In Response:

- `HTTP/1.1` **`403`** `Forbidden`

Reasoning:

The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

CWE ID:
N/A

Vulnerable URL: https://registryplustest.dshs.state.tx.us/help/

Total of 1 security issues in this URL

[1 of 1] Hidden Directory Detected

Severity:	Low
Test Type:	Infrastructure
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/help/
CVE ID(s):	N/A
CWE ID(s):	N/A
Remediation Tasks:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Variant 1 of 1 [ID=3620]

The following changes were applied to the original request:
• Set path to 'help/'

Request/Response:

```
GET /help/ HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=driwnue3ubwsdx55czuok445;
sqlAuthCookie=C542B249324C2E7AC2A89D1CA3FAAD33C69662CC5ADD27544182433DD34B58C42CE746
C25018ED28FACC83C9EF236E126D07B93D32FF54A2B10F4ED5F27E8B99C80F2A2161E226BCA1D29240A9
53DF65
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 14 May 2012 21:58:56 GMT

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

Validation In Response:

- `HTTP/1.1` **`403`** `Forbidden`

Reasoning:

The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

CWE ID:
N/A

Vulnerable URL: https://registryplustest.dshs.state.tx.us/images/

Total of 1 security issues in this URL

[1 of 1] Hidden Directory Detected

Severity:	Low
Test Type:	Infrastructure
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/images/
CVE ID(s):	N/A
CWE ID(s):	N/A
Remediation Tasks:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Variant 1 of 1 [ID=3638]

The following changes were applied to the original request:
• Set path to 'images/'

Request/Response:

```
GET /images/ HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=driwnue3ubwsdx55czuok445;
sqlAuthCookie=C542B249324C2E7AC2A89D1CA3FAAD33C69662CC5ADD27544182433DD34B58C42CE746
C25018ED28FACC83C9EF236E126D07B93D32FF54A2B10F4ED5F27E8B99C80F2A2161E226BCA1D29240A9
53DF65
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 14 May 2012 21:58:56 GMT

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

Validation In Response:

- `HTTP/1.1` **`403`** `Forbidden`

Reasoning:

The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

CWE ID:
N/A

Vulnerable URL: https://registryplustest.dshs.state.tx.us/scripts/

Total of 1 security issues in this URL

[1 of 1] Hidden Directory Detected

Severity:	Low
Test Type:	Infrastructure
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/scripts/
CVE ID(s):	N/A
CWE ID(s):	N/A
Remediation Tasks:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Variant 1 of 1 [ID=3763]

The following changes were applied to the original request:
• Set path to 'scripts/'

Request/Response:

```
GET /scripts/ HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=driwnue3ubwsdx55czuok445;
sqlAuthCookie=C542B249324C2E7AC2A89D1CA3FAAD33C69662CC5ADD27544182433DD34B58C42CE746
C25018ED28FACC83C9EF236E126D07B93D32FF54A2B10F4ED5F27E8B99C80F2A2161E226BCA1D29240A9
53DF65
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 14 May 2012 21:58:58 GMT

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

Validation In Response:

- `HTTP/1.1` **`403`** `Forbidden`

Reasoning:

The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

CWE ID:
N/A

Vulnerable URL: https://registryplustest.dshs.state.tx.us/styles/

Total of 1 security issues in this URL

[1 of 1] Hidden Directory Detected

Severity:	Low
Test Type:	Infrastructure
Vulnerable URL:	https://registryplustest.dshs.state.tx.us/styles/
CVE ID(s):	N/A
CWE ID(s):	N/A
Remediation Tasks:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Variant 1 of 1 [ID=3814]

The following changes were applied to the original request:
• Set path to 'styles/'

Request/Response:

```
GET /styles/ HTTP/1.1
Cookie: __LOGINCOOKIE__=; ASP.NET_SessionId=driwnue3ubwsdx55czuok445;
sqlAuthCookie=C542B249324C2E7AC2A89D1CA3FAAD33C69662CC5ADD27544182433DD34B58C42CE746
C25018ED28FACC83C9EF236E126D07B93D32FF54A2B10F4ED5F27E8B99C80F2A2161E226BCA1D29240A9
53DF65
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: registryplustest.dshs.state.tx.us


HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 14 May 2012 21:58:58 GMT

<html><head><title>Error</title></head><body><head><title>Directory Listing
Denied</title></head>
<body><h1>Directory Listing Denied</h1>This Virtual Directory does not allow
contents to be listed.</body></body></html>
```

Validation In Response:

- `HTTP/1.1` **`403`** `Forbidden`

Reasoning:

The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

CWE ID:

N/A

Remediation Tasks

URL	Remediation Tasks	Addressed Security Issues
https://registryplustest.dshs.state.tx.us/homeallex.aspx (1)		
	Always use SSL and POST (body) parameters when sending sensitive information. (Low) Parameter: DisplayID Parameter: FacilityID Parameter: Role	Query Parameter in SSL Request
https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx (1)		
	Do not allow caching of SSL pages (Low)	Cacheable SSL Page Found
https://registryplustest.dshs.state.tx.us/localreports.aspx (2)		
	Decline malicious requests (Medium)	Cross-Site Request Forgery
	Do not allow caching of SSL pages (Low)	Cacheable SSL Page Found
https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx (1)		
	Do not allow caching of SSL pages (Low)	Cacheable SSL Page Found
https://registryplustest.dshs.state.tx.us/releaselog.aspx (1)		
	Always use SSL and POST (body) parameters when sending sensitive information. (Low) Parameter: facilityid	Query Parameter in SSL Request
https://registryplustest.dshs.state.tx.us/data/ (1)		
	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely (Low)	Hidden Directory Detected
https://registryplustest.dshs.state.tx.us/help/ (1)		
	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely (Low)	Hidden Directory Detected

https://registryplustest.dshs.state.tx.us/images/ (1)

Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely (Low)	Hidden Directory Detected

https://registryplustest.dshs.state.tx.us/scripts/ (1)

Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely (Low)	Hidden Directory Detected

https://registryplustest.dshs.state.tx.us/styles/ (1)

Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely (Low)	Hidden Directory Detected

Application Data

Script Parameters

URL	Name	Type	Value
https://registryplustest.dshs.state.tx.us/about.aspx			
	__VIEWSTATE	Hidden	V0y2cDToxq7Cv+3hoIV1vgtALIAIREK3xXFE+InEkLNXP/jdPNl/66rcITMmULA/C2jICZXMODfyv1VhUaX3/4jNn/6livEjp4jA9eXFxSXuSBiGuLusilGQYQKa/b6axz47pFCgaeH8n/j87uM9/YkLudwP6PZeay3UpwBJ9MoPDEREik2pPisWHRDpoO5gTO9wIwKioYRQziXdu0D+qtRxpnZLbDrkCoJLdw5pFI1Bwz0W4xjx47z38/df6yA5HkpEkdh287pHAU9tzB+sKb5pAiMFeG7eBT1PoHMYxwLgnOx+lQpEknRDuhzAZHza4SUngeFNoKHIUum/GEgkEpqANIM+WD85GI6jizXKHa0dD57sP7tXlaaFbl9jdHAcO1JhxqysuGSC03mzO9RNAw==
https://registryplustest.dshs.state.tx.us/abstractdeletelog.aspx			
	facilityid	Simple Link	1111111111
	facilityid	Simple Link	1111111111
	__VIEWSTATE	Hidden	I774L6WD4V17RcLG1EQVjOzAi/tKkF/lBp98+v0Hs+vyQhX484EhtHXJpi+SH9ozrznaULeYes2Ct9/SGlzMP/TCbDA/yz8OVnjYLxsbPL1G7mao0M/uNpahadFfjcPzxTMPAYTg5cinViE5GTkuMKbCTC+QlatLqEOqay1ts43YciaW4Ttn5TxUUBH36jftYwNeMq+o828K5LlcvS9cbmFjLZ/L/KeevswqMSrQQXqS3yuBMlClCSM61NcUsVU/Pm1DGlfQUjQ+AHbDxGB4x9wWy94Lfa8O
	txtTimeout	Hidden	
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Select
https://registryplustest.dshs.state.tx.us/abstractdeletelog_prnt.aspx			
	Fromdate	Simple Link	04/02/2012
	Todate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	Fromdate	Simple Link	04%2f02%2f2012
	Todate	Simple Link	05%2f02%2f2012

URL	Name	Type	Value
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	ekkz6DH/oSnVbNAigoe9o1wTVSOrcrA0TH n+cXWcpC1zK6eiE0aUM0fKIhEOp66KkP4 mmdWzDhSfbHy0ixBgAD61Gm/JSJQ7HW PPZgXyQrdlDU+RIlodfH3plmVuVsBK
	txtTimeout	Hidden	
https://registryplustest.dshs.state.tx.us/abstractsearchlog.aspx			
	facilityid	Simple Link	2222222222
https://registryplustest.dshs.state.tx.us/abstractupdatelog.aspx			
	facilityid	Simple Link	1111111111
	facilityid	Simple Link	1111111111
	__VIEWSTATE	Hidden	BhQFE5hI+t+tV69Rc9nqxX5vzqW7EFeOa Bq2MLCFVmCFc7x6/Bc3XTZxUqpV0FhT+ 4QaZefNcc3S/57J5pSHWu51HMZrW3uYJ LU4qeoOpsB5zO8gavYm2RBhvNmFaKmq 56ksUqA9dXglvEhUPdXLioI4YAtDdjfhYMKj xCbxaBWumQZcoa5lZjy3CZFEZkNMQyn7 nnCFGAB898Eia8oHMZEyEN9P7B846gd0 KV9O4b/SZQE+VkNG9siaoaxObKHUW6S FCI0P8Ag8KYANQJvZeHmq1+N6y4pm
	txtTimeout	Hidden	
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Select
https://registryplustest.dshs.state.tx.us/abstractupdatelog_prnt.aspx			
	Fromdate	Simple Link	04/02/2012
	Todate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	Fromdate	Simple Link	04%2f02%2f2012
	Todate	Simple Link	05%2f02%2f2012
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	V0y2cDToxq54vnjvyKko/OOy8FBOBMQad 3o1/nyoxvXfaugeWuZiA9X/RiEv9mfY3gND +ElDmwURiXX3mSBdn51VWFy9Lg1VdYT yaScMDLq/Oe0kLkuN3wWPZ7lXzUp774W g4W5dJKjPyNA+9hoy4Q==
	txtTimeout	Hidden	

URL	Name	Type	Value
https://registryplustest.dshs.state.tx.us/auditlogins.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	C6BgDnb0tNASfblxVnABVZrgaSxEeZRzS3+Ady6Me4aw4iLb/FoB5xS5O5sikd/8AwKdeho/fWiKg2z1vim9Qtxt8OoRMhun8G5c2Nut/9rkTA/smqLZ5qA761oNR3TZoMYOOXfsr9lDmDV2VpwPs7QAff9giK2+N6UUDR/aX5xjfcZS9NbSE+e5gdDuYYsC+YEAQp1X/Rdp1e/R7O1HaC39YRD9gShR+X6vE+Lxgc2c44TREhBlrGSS4X5K+JpVfn9SBbRpJM/1hYeIZWM+eQ==
	txtTimeout	Hidden	
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Select
https://registryplustest.dshs.state.tx.us/auditlogins_prnt.aspx			
	Fromdate	Simple Link	04/02/2012
	Todate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	Fromdate	Simple Link	04%2f02%2f2012
	Todate	Simple Link	05%2f02%2f2012
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	4fiXlevNNHXEgFF5DRjsR8mOHiV7scfRJ3UugaN2CNFalPYyfITiUzdl1kc3NawbC7KpiwfsVPEusqx0ns/xPUKlWxXKj832EzmMxzSY0eBrQ5TBWWinAaVCelbgeLDlRxB0UTxVnseuOw+F/RJDhg==
	txtTimeout	Hidden	
https://registryplustest.dshs.state.tx.us/calendar.aspx			
	id	Simple Link	UcReportHeader1:txtFrom
	date	Simple Link	
	id	Simple Link	txtFrom
	date	Simple Link	
	__EVENTTARGET	Hidden	

URL	Name	Type	Value
	__EVENTARGUMENT	Hidden	
	__VIEWSTATE	Hidden	/WbA1u0RqEFQSbaOPZrOroqOa4XbL4345mvgehQXlhbdOjN36tQRWvBmDhhlieP70+TLhwoyRQUe8KmrPAKPwdKoMwNgKD5nHNQBA4VLsmnTpO/WvOd6/Q==
	txtDate	Hidden	
	txtID	Hidden	txtFrom
	txtUnload	Text	1234
	id	Simple Link	txtFrom
https://registryplustest.dshs.state.tx.us/casesaccessed.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	J+YXNcYrJwUp9dUgyOBnXmhFK0XdD+UhC1Ylb4GvPrRv7HsZkHsyofSGa7oCqUSBXPpkN+CBV7Nhyz2DvTFtKOXfum1VqzhmvZoKzaGq6Sjtflc2uZv+7QRcgqewWsJOr2nhCqyIHf0+Uk/32U7Wt5R8ezcAzXsqtFKJ/jIFSxEjmCSwfVIgtY5nmZKEhfDvZmO6o1z7LwLmfMQXgc33EwJICeqgn/UapqcgueneMLvdFF6hH/h9CxuSM5PYJrPg4epXh5hUlackxt+aXoEKCizjwPkhgL+MM4OQTVxQNVAO2pvi+Yi/kmsBm+ID6UhFKHGbbEThzi7WwjMaNZVcOFRkWfWdhOcq/KE8GjpucHrkxrvQwPoLVeTBOjE4UvMhiXQTzzLVtRCEaFrviGT4RQ==
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Select
	txtTimeout	Hidden	
https://registryplustest.dshs.state.tx.us/casesaccessed_prt.aspx			
	Fromdate	Simple Link	04/02/2012
	Todate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	Fromdate	Simple Link	04%2f02%2f2012
	Todate	Simple Link	05%2f02%2f2012
	FacilityID	Simple Link	1111111111

URL	Name	Type	Value
	__VIEWSTATE	Hidden	LOz0k1u8SLPaSJUdu0VSMWRsP+cdBvWa/fVkC7bNRUnzbFWwZMPi8lxyWUu4EaFBdPuujWDYZL3CUajJFSumPhbe+NlULok8D2Q9Ik/U9Z4/yJoQt3XcS/zQUh2JbLMXFVJhvKRIL8wb4oU+n4tlEok2iEsG50P2MhJ0q/XnuYPvlFLtlHMwtkut9SUinnLnKKlpV701w4Oy+Rt/45uW+Z02tnI1Yrr2C4EKRXLiYgRVGDBnURmXxBKdRILUvrSvEzU+I5M4MzwQcVVGLVHsn7SqH83OFUxybSUVa0sVqUIMhJCkUdI1aNNTw4gZDlsuHK8pQW08m7+leJvKQAdR8nPdefVv0aT4Izco6Q69X7g=
https://registryplustest.dshs.state.tx.us/casesbyuserid.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	I774L6WD4V0RSUHAOPUpZTVX0dFu4fEXr+Kab4XMh0PTZy+LLt0WF3u5ZbcYYjHjXseTUsy4QrVS7vemYsD6isLNxd6FzPPqFwVCE6vkhUJvGmF0NeQQuRNw9h9XQdlKc/bb9SESdgTjQMZvKqVkjTSgqlLF8MLGhemzBZGCgfgJ77SzbQ2lJ79FqfFT34G1RD8p/bobnU8abmr3azCuez1CS/NPOUj29l6w02/BFTLbDrK/Q1Ng+at/8P/8KfrmVb+Oflk95yCju9479wUGfMJK6zccf9PvHjktyD6BOEY9mwio4HiEkK+YT2tgeKOxB9oL7xaxRs9lwmITmwrKV+aww0WquQ20VTha+cUeegDVlYKha5DAzc9TRPd9S1Yi
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Select
	txtTimeout	Hidden	
https://registryplustest.dshs.state.tx.us/casesbyuserid_prt.aspx			
	Fromdate	Simple Link	04/02/2012
	Todate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	Fromdate	Simple Link	04%2f02%2f2012
	Todate	Simple Link	05%2f02%2f2012
	FacilityID	Simple Link	1111111111

URL	Name	Type	Value
	__VIEWSTATE	Hidden	I774L6WD4V3DyK0y15wKNi2qJW0mboJaauyZatoO+6yt0S1Q6qBzzUPD3urb/tEpIRUm02p+snwNDj5w+kdXQr93Nbi68TVHrmHhs1Ym9QstCJPKcy3rxOxhY7v+bGc8WfZMXB/ZRCUeqG6BG9+fbjcKz8Vih5bqDa0ZKZcfeRDd3igsob7wlw32/DWmY9anc5ZhK6aq/Xnx8M1Ycpg+yXM/xcV5aDVHs+1HcO5gEpEN6T9ipkKOKQ45Tt5BDaODYDmmwEJgK59xYOrVlWQHEJrQsPQUJ6iwb7K331iGEZs+MmpaUBsoU9Lk0rIBObnTzcRP8fa+R+VGO4aUl0/wjw==
https://registryplustest.dshs.state.tx.us/frmmsg.aspx			
	__VIEWSTATE	Hidden	I774L6WD4V1izXdSV8rAzySKR/bOGbA1uANVhzXPYxxdpl4TmlPSgDwCZmygKk9HE9e5DCjTHnyiGZKYXqF3cm1Yn3DW8Sd5Z0e7Pyh3PB61mWTVd+/lOV73VJX7cKSxH1BKT2WlSdiZskL2z95LYQ==
https://registryplustest.dshs.state.tx.us/homeallex.aspx			
	FacilityID	Simple Link	2222222222
	DisplayID	Simple Link	50
	Role	Simple Link	1
https://registryplustest.dshs.state.tx.us/localreports.aspx			
	__VIEWSTATE	Hidden	I774L6WD4V0yESV/beEyZEVx/3NQVkiFulR60KR4cJdeaQFXH2ilo440g8+BjlgysWJLO1i7vVMGYsJ6+ZBerDg5XNZokx8gmC20cYLWC/ZGVc/tQ7TQycfA6pGnp538w2AfmMNfg3sX+ThD8K+wc1vTsYF+tzcQltRM5NfeN4DkPPQA2nu76r+JEfnjhgGoRWsa7LfmGgeMxrHWd1HIlh5OMhEMJpeRubTmZwBhkkIgvxbpvdnDW+pmS+fGUviOB/xFXlg4I2xce7LOefmXJq7AtnRdC5rxRdJK2vE/EWKtsKmTeHDcFvsPPdeB2MHum/Xu+hbXw7/zLZ/BMP23qSzLH954yAAEnNULR/yU4D1+iXcFE64NXA==
	txtTimeout	Hidden	
https://registryplustest.dshs.state.tx.us/logonen.aspx			

URL	Name	Type	Value
	__VIEWSTATE	Hidden	I774L6WD4V20lxT3qy27vIN9gepxElp6YUt7lVVQcuHGPQ0AlkrRRm1U9E0+u9HrkT1I5otixRQZ63SBQ6l+3MZPLLRsDBG/fldas+LJ86TnjrOhR662WAAxg+JPU1gFDJRsnlcU/3c5Dnwm7XVTH8z6RAjgIlWNLpesqixtz6UInhi6BWMgf/q7HYIc/a5q7WaIgDr1tId4FPubOh8qBdQ1wwtmW1jMyccWJBDcDeyuy6swPoULBvGAwpfb3TIOY7xBasz/pOGJkRMLhcCC4bdPW1TnwgmlFcGBVarCZnbWBEwEV+HuDRAqrgOCF20DfoMarTYXc6fLaHGfzu6bQoaI58HorZVOX4mhqI2d4JXR4KAidcgtXZbDJuenzz05hZYWcMZA6LRf24gz3ZmquWrWqBXU+Tc6S8KRC2/2kVzhwzmqdbvXkge9cSwJd4LbMucBYGSAwkFUauy98d4kqykhvglt5DvQQtpus5FSyuMEohuu423X...
	txtUserID	Text	johndoe
	txtPassword	Password	abstract2
	btnLogIn	Submit	Log in
	logoff	Simple Link	1
	logoff	Simple Link	1
	__VIEWSTATE	Hidden	I774L6WD4V20lxT3qy27vIN9gepxElp6YUt7lVVQcuHGPQ0AlkrRRm1U9E0+u9HrkT1I5otixRQZ63SBQ6l+3MZPLLRsDBG/fldas+LJ86TnjrOhR662WAAxg+JPU1gFDJRsnlcU/3c5Dnwm7XVTH8z6RAjgIlWNLpesqixtz6UInhi6BWMgf/q7HYIc/a5q7WaIgDr1tId4FPubOh8qBdQ1wwtmW1jMyccWJBDcDeyuy6swPoULBvGAwpfb3TIOY7xBasz/pOGJkRMLhcCC4bdPW1TnwgmlFcGBVarCZnbWBEwEV+HuDRAqrgOCF20DfoMarTYXc6fLaHGfzu6bQoaI58HorZVOX4mhqI2d4JXR4KAidcgtXZbDJuenzz05hZYWcMZA6LRf24gz3ZmquWrWqBXU+Tc6S8KRC2/2kVzhwzmqdbvXkge9cSwJd4LbMucBYGSAwkFUauy98d4kqykhvglt5DvQQtpus5FSyuMEohuu423X...
	txtUserID	Text	johndoe
	txtPassword	Password	abstract2
	btnLogIn	Submit	Log in
https://registryplustest.dshs.state.tx.us/releaselog.aspx			
	facilityid	Simple Link	1111111111
	facilityid	Simple Link	1111111111

URL	Name	Type	Value
	__VIEWSTATE	Hidden	I774L6WD4V0eEqcfOVTcZbB87Hi1f+xK9SvCBHHAiDGy8O0oZjj1I/WVh/7MNEz6TUBKzFw0JAivEVceyu10X3Fmi5Nxk/gyCRur9Dxt4NrORpxjCIovX5JbKIreCzCfnaZUbpu9urOHD4wedpAJ1tEY3vRu7IXAT5UrjkegkeXg2yCFKxctCUlFO4nRm2o/xw/U/EaobLyHEtyfo+35xBVzdJEWimVzLdJFdxnqCKaC5kgjXnd6ED22ryG7pq6ZwL1bxgAvjH5nUzBY5RmE2fth34rT94C39HSkVYOkptFGWsFyBo+O/O6ltpxJGEIT6qGVhWd1mMinP2T50gILko2NwOUuuEJCMC9SZvyu2dVIn6xRa/+nqTEfXqCeVCEjR79VCIOthu3d6+qpSyF+/bwH3uoUN/vhBkTyGYAt2Kn7WKLploaLHZ7VD84Ruz4a
	txtTimeout	Hidden	
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Select
	OrderBy	Select	DateTimeStamp
https://registryplustest.dshs.state.tx.us/releaselog_prnt.aspx			
	Fromdate	Simple Link	04/14/2012
	Todate	Simple Link	05/14/2012
	FacilityID	Simple Link	1111111111
	OrderBy	Simple Link	DateTimeStamp
	Fromdate	Simple Link	04%2f14%2f2012
	Todate	Simple Link	05%2f14%2f2012
	FacilityID	Simple Link	1111111111
	OrderBy	Simple Link	DateTimeStamp
	__VIEWSTATE	Hidden	V0y2cDToxq6ftOzeHxGVaE8PV4Aocs8HqM69cfuGpzmkxnJglb3TCVanmQtEfnum+ljSVEAHtSJmq6pRcOXhEj3Q7CMJhfphJOgcenvlij0e7hFNNP3INGqYnxKBzMDImCjx+Pz+JhWW68vhyLIH2Q==
	Fromdate	Simple Link	04/02/2012
	Todate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	orderby	Simple Link	DateTimeStamp

URL	Name	Type	Value
	Fromdate	Simple Link	04%2f02%2f2012
	Todate	Simple Link	05%2f02%2f2012
	FacilityID	Simple Link	1111111111
	orderby	Simple Link	DateTimeStamp
	__VIEWSTATE	Hidden	V0y2cDToxq6ftOzeHxGVaE8PV4Aocs8HqM69cfuGpzmkxnJglb3TCVanmQtEfnum+ljSVEAHtSJmq6pRcOXhEj3Q7CMJhfphWr+JS0v6JeV4cdEwd60aCJGqj3c7c28pB0LXZe0WcE/XTS8yM5CbPQ==
https://registryplustest.dshs.state.tx.us/rptactivity.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	ekkz6DH/oSls7UbRY5+hcT+hxLXQARLY/8X819K6HT/Nr0NXmyEJZosfLs8EOKofFEsIWXBGF5GxQQQ8b/97uJph8mORdykpcbwxUr3/wbs8HZBgH+5XZ/wNK3HTdyfJ5iK6gOepwB1D6vRpce4jjKmi8RltuFHtOTxkxNw6nFwX9f7K3XYzqHo01XV6oquwPuiRUkQq+5LkIcUVSVfoiSXtKHZz8PfXbTG93OoeGQRRY/fkpRhPdTpZJFTswmIvI6HxDBUmyQPEBGMQjPgXFVsx8OJXhp9FxN3+NWdqr5iDd13Nhp2WW8MTb0YqgPcrmpnGLrJ58V5HO+XVKWaki4MMKZhNqVJ16Jz2PR4irUiYqwOtiYA8BhkRqmEGj7NlL3wGEzFtPmIX2u8o1toEieyxnZ+lsHSZW4G+CRiGrdL27zBUCCSB4NUKlOApeUwIF4DDJ4ZVJCC30qeHS0oXp9GIv6fTyJ0bX7N5cTezDFo=
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Run
	physgroup	Radio	rdPhysNo
	physgroup	Checkbox	rdPhysNo
https://registryplustest.dshs.state.tx.us/rptactivity_prnt.aspx			
	Fromdate	Simple Link	04/02/2012
	Todate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	Group	Simple Link	False
	Fromdate	Simple Link	04%2f02%2f2012

URL	Name	Type	Value
	Todate	Simple Link	05%2f02%2f2012
	FacilityID	Simple Link	1111111111
	Group	Simple Link	False
	__VIEWSTATE	Hidden	LOz0k1u8SLPaSJUdu0VSMWRsP+cdBvWamV2QMjNJL1pOrdBF/L1YisRpoDx9uAqh/t1mS5jHjfXB2nzY3rKVTLr7fRrIgFD11dNVcAS7buwKPaAYIEjNyKUcEjXjLM5e0bwunusUGozqn5ckcXEWLm2zVmMQXuWyxwrYCdHNWFS/t8CqaIP19sGwVDD+tVmc0QKDttrH6afWg0xLM+JdQrresaB+sxeXn5SLKD4iaHItNdTPnRE0RW+zejMoWJcCRI5xdSxDZenAF5ZHoITs/V6YGPPZp9wyx/1r75yANzS8j1xTm6vhQ9rkdhsAvwzBJWAq7Q4Ir6/w8JUEswEnkA==
https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingdcoabstracts.aspx			
	FacilityID	Simple Link	2222222222
https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingpathabstracts.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	fZQuyTfF+RNPUC5R7YTHBhBGsWekBVf1kRxr/bw2iKQhC+IuAjku1KmE1TtZgDPcTPFZE5qoFT3b6PXMgF/UG7sJ4Sr0Iba/aPLMOSDZWcFNm+Z/y+jOTYCYnHc46XRlGPduame24m9Kq4Wni2oTQtkIWaWex64YCO4YvmeAk9jWk8zInfqMrp+3CX92YkzkcjYuiCqfbMvxxLHn9RwBmXbav4Rcdokhiml6P4yWmldB56C68hwbZ3yA314PAS/3yZ2SBznw4lF6LrUBtjCMiO8QwGrCaNrDj+YqvV0Rdjt2HELhff7fOgVddpE9Jax6S4BkHRezLfYu/GfzkRPHbO4nBPn63hUkifz/hK7ahpteJhbMYQQk386vnVTqFDeBvXCDddvcmEkXxGzOJVzuYtzpHHngtgfBKwkXiuEoAmWeDsuwSw3FPHSwlL+hYtgW
https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingpathabstracts_prnt.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111

URL	Name	Type	Value
	__VIEWSTATE	Hidden	stau725jhPnxWzyFFznuUQmOxreAF+KtMI+ny75s+RKJouw3kEwdgIOFFFSSSgsxxNXu0B6eNuZ6ELI10a6Qg+DHIzHSFnpmDP1tBtvWMBmRaiF9NaxJnB9iG/oCo2UIQcyhaQ9cXboS7xkIUyjKjHtffGCb2FH0qUE/QMoLx4twqbI1vdtZSfZ2CZfscIbDSUTuaf1jPCCeffMTuhzqF43m4nhDA6vg+E0E4KiKnTeUHaP1Vkcchifw8q1A2NKVtIvF5FAHDOrU/N0qAm6UJQ==
https://registryplustest.dshs.state.tx.us/rptdisclosure.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	I774L6WD4V3NDyttmAB9tDIoQOHxFhLIo2I0X9eL71pcxJ8kTZa3j1fqvnEVCcHsvFpgMjX4MA3O8h099QKBH1m/mFIBKHv8ikHz3lggSRcI+bYbHFv8Od/bmlHmcey2fUWOkeoBNCQXPFEWBsf4N31Glswuiwzo3jz6NQZiwcbwKgy6WqWn3X7h7xFdvSfSNVX1jEzjOgOqeXjbZgHMRdT3skqzX6JlaWLDiGs+TIetYIW8zv6/VEHf48yGh86D83w459o2PcMJG3pWKUIQSLwagDfhaSCpAsK4ZvsFF0WNQLMCWxuaUYzv/MGSBiRyj9UaU9hfrvaGaGy03czMt+e9Ru2lUM/I7CVt0Qz8lhHZboQbPQt+kWLHRV+E4acm2IKj7LYILjeM0BZhtXzIKguSLV4vdkJU1tVXevj77MGbeMu8jmmhQA==
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	btnRun	Submit	Run
https://registryplustest.dshs.state.tx.us/rptdisclosure_prnt.aspx			
	FromDate	Simple Link	04/02/2012
	ToDate	Simple Link	05/02/2012
	FacilityID	Simple Link	1111111111
	FromDate	Simple Link	04%2f02%2f2012
	ToDate	Simple Link	05%2f02%2f2012
	FacilityID	Simple Link	1111111111

URL	Name	Type	Value
	__VIEWSTATE	Hidden	5Ok+gpMtBhMe00gN71Muh9YKJnEvoq4et/NXtx04UsGu7O5H7gKf1NFXu+8FKIhn7UHJDxUx3KHoiyJgsOPAhPoHXXj9qTr8O4B5ReaJCgUAyXnFUexGkkIhUT+ME6fHsF3pelyoCq1/wHXv/WjEaWkn3Hx+ZflLZYpqx4KpygQQ2ydCA7YuLwgh5NvanpP8IeHpfyvU6sJHA7TCpEoxO5E5zjdl/3m9lUa9wzrEmKlKDJhOf7JQtFVpvib7UfFOIah+C9FEu1s7AAcBb5nxSYETQhzg/4wntEPHdFh80avPaL8dylfp82LR0YeMY6sB3R+odtFv/JKFG8vXKX81wFo9n1gh6m5JcK/6/CjWuSHMySiuVQvmN6oFBQZoJlJGYlYy0DeP2IC5fXIIXxE/BQ==
https://registryplustest.dshs.state.tx.us/rptfrequency.aspx			
	FacilityID	Simple Link	1111111111
	FacilityID	Simple Link	1111111111
	__VIEWSTATE	Hidden	FnY9Kc54vWRaG/Vhigmmrfh87Ka2SGBpdp2zgm5SZc2Z/zBnbtvfcdU/C/w33ILX1jT3+1ww7Ddo+Ulni8qo2E/DSjAMA9whelVbAeb11oMRfsCbaxKXuqXwoSyPcKGNyXSMhl2BUGn3zGcoiG7z3lwNIOQGS9TQcGglKr4jLRXSjwi37mGjz1wvt493YyOPycWilRrZ0h363cqKIc3i38wPy9DzQSk4qD4wJmklYp/o+vhwh3hUDO61vYjxK3t9E6slirO8mjp8FkKxKG0W3LaV531pSOrGnyngqhtT0CPtW0bBFGASXkeUPLZnfUZbck+mTdLQ4hyZXr6rED6MndhuiqpCh4Fc6EBuP9O324JATRjvDkk2yJKfLB3vuSujH3BSwcKVzsj2Oxro81uE1vOPjERQ204niNe4maYpQ4VvgunqTPlQbDxtaqMoEaNn3pieMF95UAtwMIffSiL4X1hwsSFwFvrCko9MdLYc7SlJMw/3NoVW...
	txtFrom	Text	04/02/2012
	txtTo	Text	05/02/2012
	chkSelectall	Checkbox	on
	lstSitegroups	Select	2
	btnRun	Submit	Run
	physgroup	Radio	rdPhysNo
	physgroup	Checkbox	rdPhysNo
	sitegroup	Radio	radNo
	sitegroup	Checkbox	radNo
https://registryplustest.dshs.state.tx.us/rptfrequencyprt.aspx			

URL	Name	Type	Value
	From	Simple Link	04/02/2012
	To	Simple Link	05/02/2012
	gl	Simple Link	1
	sp	Simple Link	False
	AllReleased	Simple Link	False
	ShowAll	Simple Link	False
	F	Simple Link	1111111111
	sg	Simple Link	False
	From	Simple Link	04%2f02%2f2012
	To	Simple Link	05%2f02%2f2012
	gl	Simple Link	1
	sp	Simple Link	False
	AllReleased	Simple Link	False
	ShowAll	Simple Link	False
	F	Simple Link	1111111111
	sg	Simple Link	False
	__VIEWSTATE	Hidden	LOz0k1u8SLMyoAD8Xrndh7W6TSt7L5n5bRGiXfaPWyVFWEWPar+0rWDEoCrq5ISEAl0KbFFVTf0aAFRPtBLyLecU6rwtRGCfoFoS07SEQbGHAc/cljFLZus7J2lZguzmhWT6lEwWjYmfZtKvOZg2EYlYEVeiYtBtKexT+EVUiUvwqCM6+bNRQ3DGbfYhaC9u3re0oc5UsEX217/A871N6v5qu0dHn92DJe15VtRuxbLySDUiNQ2voaxXtWjsRL5Z3YipIMVY3CHRcIgO7wRgH9F9YTFpoPMv5UkNvomPAUq+ntISDjvnjg==

Broken Links

Reason	URL
Time Out	https://registryplustest.dshs.state.tx.us/homealleax.aspx
Time Out	https://registryplustest.dshs.state.tx.us/homealleax.aspx
Time Out	https://registryplustest.dshs.state.tx.us/homealleax.aspx
Time Out	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx

Reason	URL
Time Out	https://registryplustest.dshs.state.tx.us/frmfindabstracthospitaluser.aspx
Time Out	https://registryplustest.dshs.state.tx.us/dataentrytype1.aspx
Time Out	https://registryplustest.dshs.state.tx.us/changepassword.aspx
Time Out	https://registryplustest.dshs.state.tx.us/casesaccessed.aspx
Time Out	https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingpathabstracts.aspx
Time Out	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
Time Out	https://registryplustest.dshs.state.tx.us/downloadfiles.aspx
Time Out	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
Time Out	https://registryplustest.dshs.state.tx.us/calendar.aspx
Time Out	https://registryplustest.dshs.state.tx.us/abstractsearchlog.aspx
Time Out	https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingdcoabstracts.aspx

JavaScripts

Script	URL

Script	URL

`function getDateFrom()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`val=document.getElementById`
`("txtFrom").value`
`strStyle='width='+ w +',height=' + h/2`
`+ ',top=1,left=' + l + ', scrollbars=no,`
`resizable=no'`
`WindowName = window.open`
`("calendar.aspx?`
`id=txtFrom&date="+val,'help',strStyle);`
`WindowName.focus()`
`}`
 	
`function getDateTo()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`val=document.getElementById`
`("txtTo").value`
`strStyle='width='+ w +',height=' + h/2`
`+ ',top=1,left=' + l + ', scrollbars=no,`
`resizable=no'`
`WindowName = window.open`
`("calendar.aspx?`
`id=txtTo&date="+val,'help',strStyle);`
`WindowName.focus()`
`}`
	https://registryplustest.dshs.state.tx.us/abstractdeletelog.aspx

`getDateFrom()`	https://registryplustest.dshs.state.tx.us/abstractdeletelog.aspx
`getDateTo()`	https://registryplustest.dshs.state.tx.us/abstractdeletelog.aspx

`window.resizeTo(260,270)`
`function getDate()`
`{`
`id = document.getElementById`
`("txtID").value`
`txt = opener.document.getElementById`
`(id)`
`if (txt)`
`{`
`txt.value=document.getElementById`
`("txtDate").value`
`}`
`if (document.getElementById`
`("txtUnload").value==1)`
`window.close();`
`}`
	https://registryplustest.dshs.state.tx.us/calendar.aspx

`getDate()`	https://registryplustest.dshs.state.tx.us/calendar.aspx

Script	URL

<!--
var theForm = document.forms['Form1'];
if (!theForm) {
    theForm = document.Form1;
}
function __doPostBack(eventTarget,
eventArgument) {
    if (!theForm.onsubmit ||
(theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value =
eventTarget;
        theForm.__EVENTARGUMENT.value =
eventArgument;
        theForm.submit();
    }
}
// -->
	https://registryplustest.dshs.state.tx.us/calendar.aspx

__doPostBack('Calendar1','V4474')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','V4535')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4502')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4503')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4504')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4505')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4506')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4507')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4508')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4509')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4510')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4511')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4512')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4513')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4514')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4515')	https://registryplustest.dshs.state.tx.us/calendar.aspx

Script	URL
__doPostBack('Calendar1','4516')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4517')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4518')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4519')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4520')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4521')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4522')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4523')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4524')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4525')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4526')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4527')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4528')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4529')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4530')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4531')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4532')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4533')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4534')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4535')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4536')	https://registryplustest.dshs.state.tx.us/calendar.aspx
__doPostBack('Calendar1','4537')	https://registryplustest.dshs.state.tx.us/calendar.aspx

Script	URL
`__doPostBack('Calendar1','4538')`	https://registryplustest.dshs.state.tx.us/calendar.aspx
`__doPostBack('Calendar1','4539')`	https://registryplustest.dshs.state.tx.us/calendar.aspx
`__doPostBack('Calendar1','4540')`	https://registryplustest.dshs.state.tx.us/calendar.aspx
`__doPostBack('Calendar1','4541')`	https://registryplustest.dshs.state.tx.us/calendar.aspx
`__doPostBack('Calendar1','4542')`	https://registryplustest.dshs.state.tx.us/calendar.aspx
`__doPostBack('Calendar1','4543')`	https://registryplustest.dshs.state.tx.us/calendar.aspx
`function setfocusonpassword() { document.getElementById ("txtOldPassword").focus() }`	https://registryplustest.dshs.state.tx.us/changepassword.aspx
`var prevmenu; function showmenu(menu, submenu) {if (prevmenu) document.getElementById (prevmenu).style.visibility='hidden';if (document.getElementById(submenu)) {document.getElementById (submenu).style.visibility='visible';document .getElementById (submenu).style.zIndex=5000;document.getEleme ntById (submenu).style.left=document.getElementById (menu).offsetLeft+10;document.getElementById (submenu).style.top=document.getElementById ('main').offsetTop+document.getElementById ('main').offsetHeight;prevmenu = submenu;}} function hidemenu(submenu) {if (document.getElementById(submenu)) {document.getElementById (submenu).style.visibility='hidden'}} function makeactive(itm, style) {if (document.getElementById(itm)) {document.getElementById (itm).className=style;document.body.style.cur sor='pointer';}} function makeinactive(itm, style) {if (document.getElementById(itm)) {document.getElementById (itm).className=style;document.body.style.cur sor='auto';}}`	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
`showmenu('nothing','nothing');makeactive ('homemain','mymainhover')`	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
`showmenu('nothing','nothing');makeactive ('newabstract','mymainhover')`	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
`showmenu('nothing','nothing');makeactive ('findabstract','mymainhover')`	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx

Script	URL
showmenu('nothing','nothing');makeactive ('releaseabstracts','mymainhover')	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
showmenu('nothing','nothing');makeactive ('reports','mymainhover')	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
showmenu('nothing','nothing');makeactive ('changepassword','mymainhover')	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
showmenu('helpmain', 'help');makeactive ('helpmain','mymainhover')	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
showmenu('nothing','nothing');makeactive ('logout','mymainhover')	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
showmenu('helpmain', 'help')	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
makeactive('about', 'mysubhover')	https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx

function checkresolution()
{
if (parseInt(screen.width) < 1024 ‖ parseInt(screen.height) < 768)
var id = document.getElementById ("information").innerHTML="Low screen resolution (" + screen.width + " X " + screen.height + ") detected.\n While you may still be able to use Web Plus at this resolution it has been designed to be viewed best at 1024 X 768 or higher resolution."
document.getElementById ("information").style.color="red"
}
function testparm(parm)
{
alert(parm)
}
function test()
{
document.getElementById ("lblMsg").innerHTML="Logging you in. Please wait ..."
}
 	
function setfocus()
{
if (document.getElementById("txtUserID"))
document.getElementById ("txtUserID").focus();
}
 	
function submit()
{
 	
if (event.keyCode == 13)
{
//cancel the default submit
...
	https://registryplustest.dshs.state.tx.us/logonen.aspx

checkresolution()	https://registryplustest.dshs.state.tx.us/logonen.aspx

Script	URL
showmenu('nothing','nothing');makeactive ('fileupload','mymainhover')	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
showmenu('previousuploads', 'uploads');makeactive ('previousuploads','mymainhover')	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
showmenu('nothing','nothing');makeactive ('downloadfiles','mymainhover')	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
showmenu('previousuploads', 'uploads')	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
makeactive('TrackFileUploads', 'mysubhover')	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx

function selectAll()
{
for (i=0;i<window.document.forms (0).elements.length;i++)
{
if (window.document.forms(0).elements (i).id.substr(0,3)=="chk")
window.document.forms(0).elements (i).checked=true;
}
}
 	
function unselectAll()
{
for (i=0;i<window.document.forms (0).elements.length;i++)
{
if (window.document.forms(0).elements (i).id.substr(0,3)=="chk")
window.document.forms(0).elements (i).checked=false;
}
}
	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx

selectAll()	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
unselectAll()	https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx

Script	URL

`function getDateFrom()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`val=document.getElementById`
`("UcReportHeader1:txtFrom").value`
`strStyle='width='+ w +',height=' + h/2`
`+ ',top=1,left=' + l + ', scrollbars=no,`
`resizable=no'`
`WindowName = window.open`
`("calendar.aspx?`
`id=UcReportHeader1:txtFrom&date="+val,'help',`
`strStyle);`
`WindowName.focus()`
`}`
 	
`function getDateTo()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`val=document.getElementById`
`("UcReportHeader1:txtTo").value`
`strStyle='width='+ w +',height=' + h/2`
`+ ',top=1,left=' + l + ', scrollbars=no,`
`resizable=no'`
`WindowName = window.open`
`("calendar.aspx?`
`id=UcReportHeader1:txtTo&date="+val,'help',st`
`rStyle);`
`WindowName.focus()`
`}`
	https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingpathabstracts.aspx

Script	URL

`function getDateFrom()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`val=document.getElementById`
`("txtFrom").value`
`strStyle='width='+ w +',height=' + h/2`
`+ ',top=1,left=' + l + ', scrollbars=no,`
`resizable=no'`
`WindowName = window.open`
`("calendar.aspx?`
`id=txtFrom&date="+val,'help',strStyle);`
`WindowName.focus()`
`}`
 	
`function getDateTo()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`val=document.getElementById`
`("txtTo").value`
`strStyle='width='+ w +',height=' + h/2`
`+ ',top=1,left=' + l + ', scrollbars=no,`
`resizable=no'`
`WindowName = window.open`
`("calendar.aspx?`
`id=txtTo&date="+val,'help',strStyle);`
`WindowName.focus()`
`}`
 	
`function cleardate()`
`{`
 	
`...`
	https://registryplustest.dshs.state.tx.us/rptdisclosure.aspx

`cleardate()`	https://registryplustest.dshs.state.tx.us/rptfrequency.aspx

Script	URL

`function getDateFrom()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`strStyle='width='+ w +',height=' + h/2 + ',top=1,left=' + l + ', scrollbars=no, resizable=no'`
`WindowName = window.open ("calendar.aspx?id=txtFrom",'help',strStyle);`
`WindowName.focus()`
`}`
 	
`function getDateTo()`
`{`
 	
`w = screen.width/2`
`h = screen.availHeight-10`
`t = 1`
`l = screen.availWidth/2-10`
`strStyle='width='+ w +',height=' + h/2 + ',top=1,left=' + l + ', scrollbars=no, resizable=no'`
`WindowName = window.open ("calendar.aspx?id=txtTo",'help',strStyle);`
`WindowName.focus()`
`}`
 	
`function cleardate()`
`{`
 	
`chk=document.getElementById ("chkSelectall")`
`if (chk.checked)`
...
	https://registryplustest.dshs.state.tx.us/rptfrequencyprt.aspx

Comments

Comment	URL

Comment	URL
 Select a Date Range: From: <input name="UcReportHeader1:txtFrom" type="text" id="UcReportHeader1_txtFrom" style="font-family:Arial;font-size:Smaller;height:20px;width:104px;" /> To: <input name="UcReportHeader1:txtTo" type="text" id="UcReportHeader1_txtTo" style="font-family:Arial;font-size:Smaller;height:20px;width:104px;" /> <input type="submit" name="UcReportHeader1:btnRun" value="Run Report" id="UcReportHeader1_btnRun" style="LEFT:90%; POSITION:absolute" /> 	https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingpathabstracts.aspx

Cookies

Name	Value	URL
sqlAuthCookie	493E9B89B2D82FBC9F5AFEB7311AF6A7AA037FF983C272342BF95536823FCE4F4EB7D58D95C9E524A3B7B9900DA02B225B45965985F0DE9D62751EB06F40657EF5501CF842158296C2C5176221949167	

Name	Value	URL
ASP.NET_SessionId	xwu3mavx0voahsyg20eedy55	https://registryplustest.dshs.state.tx.us/logonen.aspx
ASP.NET_SessionId		https://registryplustest.dshs.state.tx.us/logonen.aspx
ASP.NET_SessionId	0r0x2u2sqprdrjz0tgully45	https://registryplustest.dshs.state.tx.us/logonen.aspx
__LOGINCOOKIE__		https://registryplustest.dshs.state.tx.us/logonen.aspx
__LOGINCOOKIE__	EF5F078770115DA01F3FDD188B5D2FFCA005FB99149469FACF48C2D050C609F87673A1B9AE55BE358960D17EEBC25D436416FEF3B3D243995CADDC26815FEBE6	https://registryplustest.dshs.state.tx.us/logonen.aspx
__LOGINCOOKIE__	C279100AFC249839CC66C2013ADF14A4EC044A9E1A5B2A5760ED239F53CE2A03DAED2D17B3047AA9AC2531F6F08338F395A8FA8754063BAF52B1B047277411F6	https://registryplustest.dshs.state.tx.us/logonen.aspx
sqlAuthCookie	34D428E5190CBBDF334490FFF072074C2ABC5E3041F5D414A42431F0D8D935CD4F012F7CB08A615821590B1F59EE07C9AD52BF5EBE6517E112187EF3629F04091F5AF473E537E038BEBF3FBFD5FC5471	https://registryplustest.dshs.state.tx.us/logonen.aspx
__LOGINCOOKIE__	0040ED79F0D12EA4776464E85789AB48F30C5F4BDA9E4B467121BC9D18ACFE5916A35771426E2D70AA64F3DE413F97554DF9847E16D57B0CA649FA0E93DDC35F	https://registryplustest.dshs.state.tx.us/logonen.aspx?logoff=1

Name	Value	URL
sqlAuthCookie	4DB2F0141AE706E8 6279B3AA0E0EDD7B 1DCD3C84F66DEFA A3BBABCAD78F828F 6FCC9A8E90D7D2B E78DBAAF56D3A35A 988276C5931B63E71 CE5C69F1709F6E48 17B8527874BB77E80 F27ED12B4F50E01F	https://registryplustest.dshs.state.tx.us/logonen.aspx?logoff=1

Application URLs

- https://registryplustest.dshs.state.tx.us/
- https://registryplustest.dshs.state.tx.us/about.aspx
- https://registryplustest.dshs.state.tx.us/abstractdeletelog.aspx
- https://registryplustest.dshs.state.tx.us/abstractdeletelog_prnt.aspx
- https://registryplustest.dshs.state.tx.us/abstractsearchlog.aspx
- https://registryplustest.dshs.state.tx.us/abstractupdatelog.aspx
- https://registryplustest.dshs.state.tx.us/abstractupdatelog_prnt.aspx
- https://registryplustest.dshs.state.tx.us/auditlogins.aspx
- https://registryplustest.dshs.state.tx.us/auditlogins_prnt.aspx
- https://registryplustest.dshs.state.tx.us/calendar.aspx
- https://registryplustest.dshs.state.tx.us/casesaccessed.aspx
- https://registryplustest.dshs.state.tx.us/casesaccessed_prt.aspx
- https://registryplustest.dshs.state.tx.us/casesbyuserid.aspx
- https://registryplustest.dshs.state.tx.us/casesbyuserid_prt.aspx
- https://registryplustest.dshs.state.tx.us/changepassword.aspx
- https://registryplustest.dshs.state.tx.us/frmmsg.aspx
- https://registryplustest.dshs.state.tx.us/homeallex.aspx
- https://registryplustest.dshs.state.tx.us/homefacilityabstractor.aspx
- https://registryplustest.dshs.state.tx.us/localreports.aspx
- https://registryplustest.dshs.state.tx.us/logonen.aspx
- https://registryplustest.dshs.state.tx.us/previousuploads.aspx
- https://registryplustest.dshs.state.tx.us/releaseabstracts.aspx
- https://registryplustest.dshs.state.tx.us/releaselog.aspx
- https://registryplustest.dshs.state.tx.us/releaselog_prnt.aspx
- https://registryplustest.dshs.state.tx.us/rptactivity.aspx
- https://registryplustest.dshs.state.tx.us/rptactivity_prnt.aspx
- https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingdcoabstracts.aspx
- https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingpathabstracts.aspx
- https://registryplustest.dshs.state.tx.us/rptcurrentoutstandingpathabstracts_prnt.aspx
- https://registryplustest.dshs.state.tx.us/rptdisclosure.aspx
- https://registryplustest.dshs.state.tx.us/rptdisclosure_prnt.aspx
- https://registryplustest.dshs.state.tx.us/rptfrequency.aspx

- https://registryplustest.dshs.state.tx.us/rptfrequencyprt.aspx
- https://registryplustest.dshs.state.tx.us/upload.aspx
- https://registryplustest.dshs.state.tx.us/data/
- https://registryplustest.dshs.state.tx.us/help/
- https://registryplustest.dshs.state.tx.us/images/
- https://registryplustest.dshs.state.tx.us/scripts/
- https://registryplustest.dshs.state.tx.us/styles/

Advisories & Fix Recommendations

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

Even well-formed, valid, consistent requests may have been sent without the user's knowledge. Web applications should therefore examine all requests for signs that they are not legitimate. The result of this test indicates that the application being scanned does not do this.
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 page.
When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, then it might be possible for an attacker to trick a client into making an unintentional request to the web server which will be treated as an authentic request. This can be done via a URL, image load, XMLHttpRequest, etc., and can result in exposure of data or unintended code execution.
If the user is currently logged-in to the victim site, the request will automatically use the user's credentials including session cookies, 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.

General Fix Recommendations

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness, or provides constructs that make it easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard - http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
Another example is the ESAPI Session Management control, which includes a component for CSRF -

http://www.owasp.org/index.php/ESAPI
[2] Ensure that your application is free of cross-site scripting issues (CWE-79), because most CSRF defenses can be bypassed using attacker-controlled script.
[3] Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330) - http://www.cgisecurity.com/articles/csrf-faq.shtml
Note that this can be bypassed using XSS (CWE-79).
[4] Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
Note that this can be bypassed using XSS (CWE-79).
[5] Use the "double-submitted cookie" method as described by Felten and Zeller:
When a user visits a site, the site should generate a pseudorandom value and set it as a cookie on the user's machine. The site should require every form submission to include this value as both a form and a cookie value. When a POST request is sent to the site, the request should only be considered valid if the form and cookie values are the same.
Because of same-origin policy, an attacker cannot read or modify the value stored in the cookie. To successfully submit a form on behalf of the user, the attacker would have to correctly guess the pseudorandom value. If the pseudorandom value is cryptographically strong, this will be prohibitively difficult.
This technique requires Javascript, so it may not work for browsers that have Javascript disabled - http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.147.1445
Note that this can probably be bypassed using XSS (CWE-79), or when using web technologies that enable the attacker to read raw headers from HTTP requests.
[6] Do not use the GET method for any request that triggers a state change.
[7] Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Note that this can be bypassed using XSS (CWE-79). An attacker could use XSS to generate a spoofed Referer, or to generate a malicious request from a page whose Referer would be allowed.

References and Relevant Links

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

Cacheable SSL Page Found

Application

WASC Threat Classification

Application Privacy Tests

CVE ID(s)

N/A

CWE ID(s)

525

Security Risks

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Possible Causes

Sensitive information might have been cached by your browser

Technical Description

Most web browsers are configured by default to cache the user's pages during use. This means that SSL pages are cached as well.
It is not recommended to enable the web browser to save any SSL information, since this information might be compromised when a vulnerability exists.

General Fix Recommendations

Disable caching on all SSL pages or all pages that contain sensitive data.
For example, you can add "Cache-Control: no-cache, no-store" to your login page headers.

References and Relevant Links

N/A

Hidden Directory Detected

Infrastructure

WASC Threat Classification

Information Leakage

http://projects.webappsec.org/Information-Leakage

CVE ID(s)

N/A

CWE ID(s)

N/A

Security Risks

It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Possible Causes

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

Technical Description

The web application has exposed the presence of a directory in the site. Although the directory does not list its content, the information may help an attacker to develop further attacks against the site. For example, by knowing the directory name, an attacker can guess its content type and possibly file names that reside in it, or sub directories under it, and try to access them.
The more sensitive the content is, the more severe this issue may be.

General Fix Recommendations

If the forbidden resource is not required, remove it from the site.
If possible, issue a "404 - Not Found" response status code instead of "403 - Forbidden". This change will obfuscate the presence of the directory in the site, and will prevent the site structure from being exposed.

References and Relevant Links

N/A

Query Parameter in SSL Request

Application

WASC Threat Classification

Application Privacy Tests

CVE ID(s)

N/A

CWE ID(s)

598

Security Risks

It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Possible Causes

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

Technical Description

During the application test, it was detected that a request, which was sent over SSL, contained parameters that were transmitted in the Query part of an HTTP request.
When sending requests, the browser's history can be used to reveal the URLs, which contain the query parameter names and values.
Due to the sensitivity of encrypted requests, it is suggested to use HTTP POST (without parameters in the URL string) when possible, in order to avoid the disclosure of URLs and parameter values to others.

General Fix Recommendations

Make sure that sensitive information such as:
- Username
- Password
- Social Security number
- Credit Card number
- Driver's License number
- e-mail address
- Phone number
- Zip code

is always sent in the body part of an HTTP POST request.

References and Relevant Links

Financial Privacy: The Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act (HIPAA)
Sarbanes-Oxley Act
California SB1386