HP Assessment Management Platform™

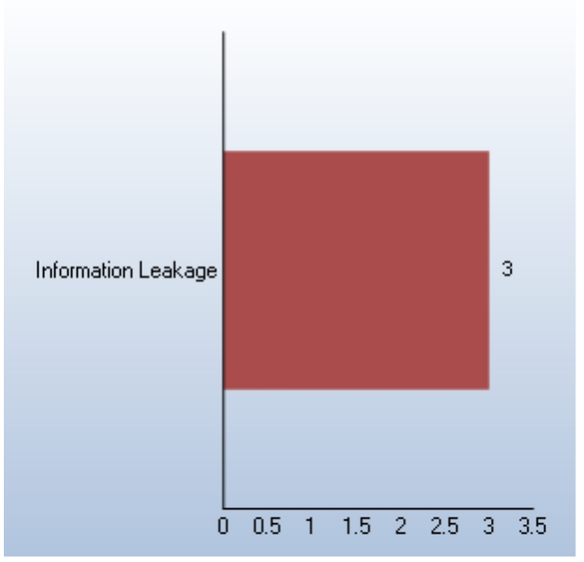
Aggregate Scan

Executive Summary

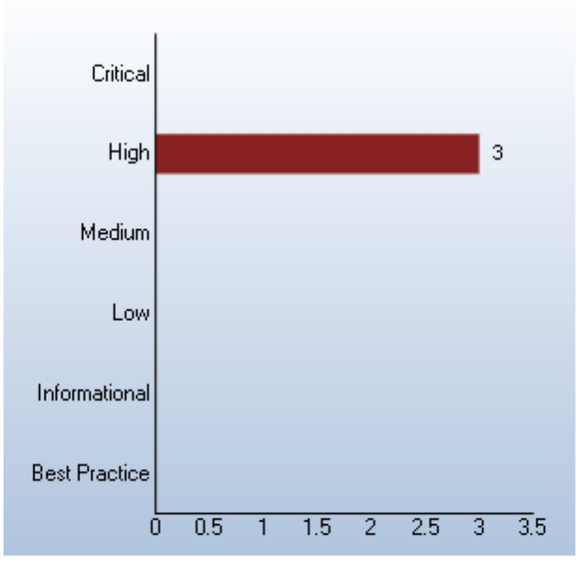
Created on 12/7/2011 8:02:17 AM with the following scans:

Scan Name:	Policy:	Scan Date:	Scan Version:
MPT MTS Knova Analytics Dev - 2011-12-07 16:00:00Z	Passive Scan	12/7/2011 8:01:25 AM	9.10.78.0

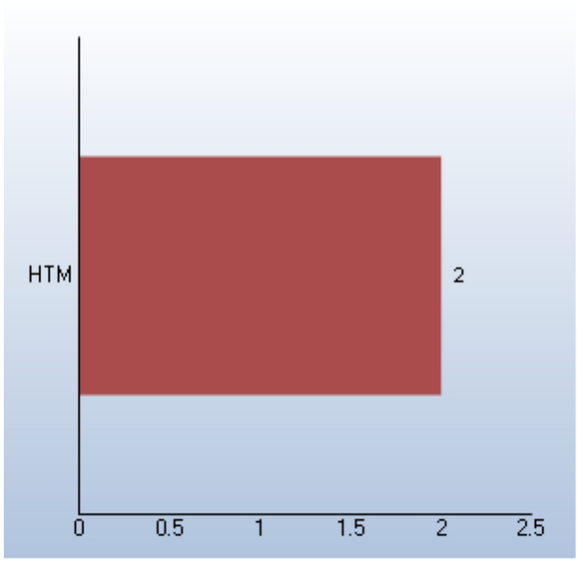
Vulnerabilities By Threat Class (Top 12)



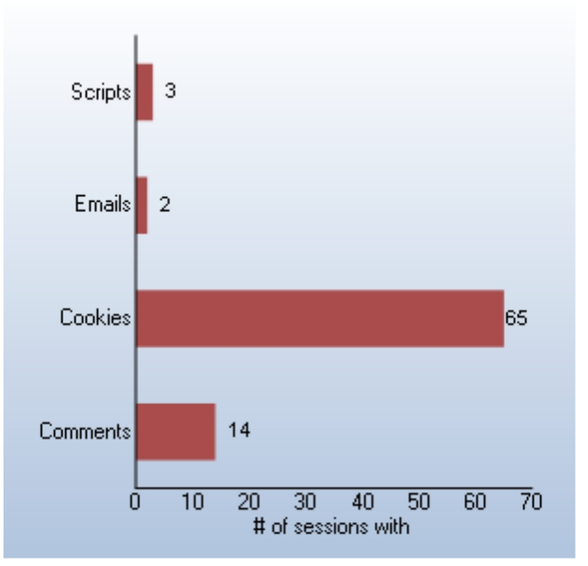
Vulnerability By Severity



Vulnerabilities By File Extension (Top 12)



Site Structure

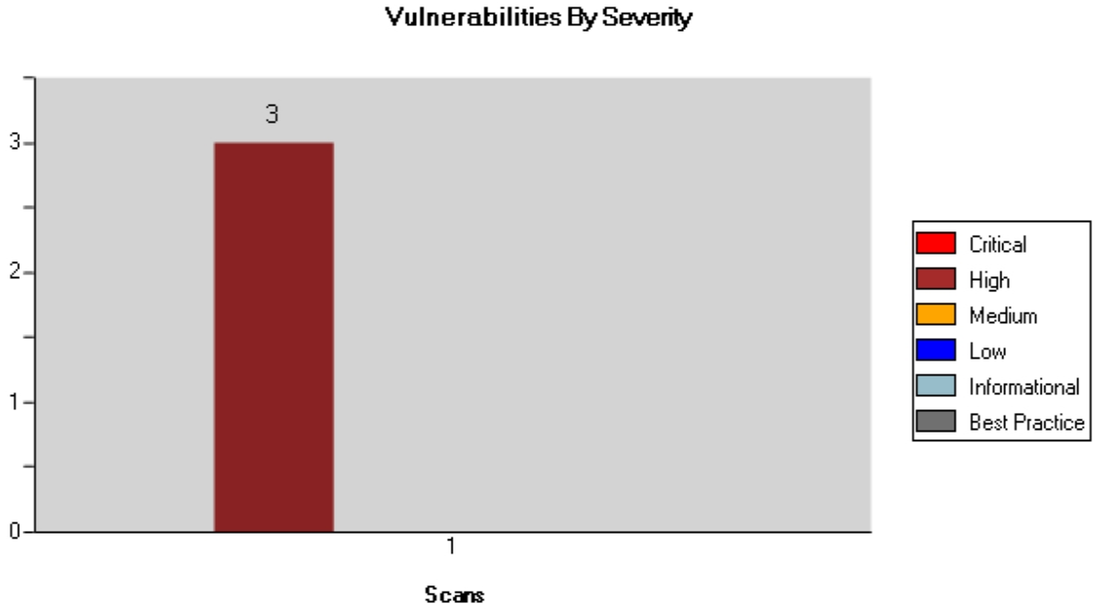


Vulnerability

Created on 12/7/2011 8:02:22 AM with the following scans:

Scan Name:	Policy:	Scan Date:	Scan Version:
MPT MTS Knova Analytics Dev - 2011-12-07 16:00:00Z	Passive Scan	12/7/2011 8:01:25 AM	9.10.78.0

Server: http://ddcwz30297:80 MPT MTS Knova Analytics Dev - 2011-12-07 16:00:00Z



High	**Possible Username or Password Disclosure**
File Names:	http://ddcwz30297:80/Analytics/SH_ACT_WF.htm
Summary:	A username or password was found during "unknown" application testing. Unknown application testing seeks to uncover new vulnerabilities in both custom and commercial software. Because of this, there are no specific patches or descriptions for this issue. Please note that this vulnerability may be a false positive if the page it is flagged on is technical documentation. Recommendations include removing the information from the production server, or otherwise restricting access.
Execution:	Click http://ddcwz30297:80/Analytics/SH_ACT_WF.htm to verify the vulnerability in a web browser.
Implication:	This information could allow an attacker to access sensitive applications and information on a site, or to perform functions according to the privilege level of the login information. Gaining information critical to the success of escalated attacks would also be a likely impact of exploitation.
Fix:	Remove the information from the web server, if possible, or otherwise restrict access.
Reference:	**Microsoft:** IIS Authentication Authentication in IIS 6.0 (IIS 6.0) How to configure IIS Web site authentication in Windows Server 2003 **Apache:** Apache HTTP Server Version 1.3 - Authentication, Authorization, and Access Control Apache HTTP Server Version 2.0 - Authentication, Authorization, and Access Control
Attack Request:	GET /Analytics/SH_ACT_WF.htm HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) Accept: */* Pragma: no-cache Host: ddcwz30297 X-Scan-Memo: Category="Crawl"; Function="CreateStateRequest";

SID="AAE7DAA0D9D5211A830090E2DA35E093";
SessionType="ExternalAddedToCrawl"; CrawlType="None"; AttackType="None";
OriginatingEngineID="00000000-0000-0000-0000-000000000000"; ThreadId="60"
ThreadType="CrawlBreadthFirstDBReader";
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect0

Attack Response:

HTTP/1.1 200 OK
Content-Length: 17919
Content-Type: text/html
Last-Modified: Tue, 15 Feb 2011 02:23:44 GMT
Accept-Ranges: bytes
ETag: "078195eb7cccb1:56d"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 07 Dec 2011 16:00:30 GMT

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns:zfp="http://www.qliktech.com/zfp" xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>7.3</title>
<link rel="stylesheet" type="text/css" media="screen"
href="/QvAjaxZfc/htc/default.css"/>
<link rel="stylesheet" type="text/css" href="/QvAjaxZfc/htc/tabcontent.css"/>
<link rel="stylesheet" type="text/css" href="/QvAjaxZfc/htc/avq.css"/>
<link rel="stylesheet" type="text/css" media="screen"
href="/QvAjaxZfc/htc/modal/modal.css" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""><![CDATA[<script
language="javascript" type="text/javascript" src="/QvAjaxZfc/htc/QvAjax.js"
xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:zfp="uri:zfp"
xmlns:user="uri:user" xmlns=""></script>]]><![CDATA[<script
language="javascript" type="text/javascript" src="/QvAjaxZfc/htc/QvAjaxTrace.js"
xmlns:msxsl="urn:schemas-microsoft-com:xslt" xmlns:zfp="uri:zfp"
xmlns:user="uri:user" xmlns=""></script>]]><![CDATA[<script
language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxBaseMgr.js" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxTableMgr.js" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxScan.js" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxModal.js" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><link
rel="stylesheet" type="text/css" media="all"
href="/QvAjaxZfc/htc/calendar/skins/aqua/theme.css" xmlns:msxsl="urn:schemas-
microsoft-com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/calendar/calendar.js" xmlns:msxsl="urn:schemas-microsoft-

```
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/calendar/lang/calendar-en.js" xmlns:msxsl="urn:schemas-
microsoft-com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]
><![CDATA[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/calendar/QvAjaxCalendar.js" xmlns:msxsl="urn:schemas-
microsoft-com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]
><![CDATA[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxGraphics.js" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxSlider.js" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxGraph.js" xmlns:msxsl="urn:schemas-microsoft-
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript"
src="/QvAjaxZfc/htc/QvAjaxCollaboration.js" xmlns:msxsl="urn:schemas-microsoft
com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA
[<script language="javascript" type="text/javascript" xmlns:msxsl="urn:schemas-
microsoft-com:xslt" xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns="">
        var qva = new Qva.PageBinding();
        qva.View = "7.3";
        qva.Autoview = "SH_ACT_WF";
        qva.Trace = new Qva.Trace(qva);
        qva.Modal = new Qva.Modal(qva);
        //qva.JSON = true;

        qva.OnUpdateComplete = function () { qva.SetNewSheet(); }

        new Qva.Collaboration(qva);
        new Qva.Scanner(qva);
        window.onresize = function () { Qva.SetBackgroundSize(); }
    </script>]]><![CDATA[<script language="javascript" type="text/javascript"
src="PageModifications.js" xmlns:msxsl="urn:schemas-microsoft-com:xslt"
xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><style
type="text/css">
            #SH_ACT_WF { background-color: #f8f8f8; color:#000000; }

            #SH_WF_AN { background-color: #f8f8f8; color:#000000; }

            #SH_REV_PROD { background-color: #f8f8f8; color:#000000; }

            #SH_REV_EFF { background-color: #f8f8f8; color:#000000; }

            #SH_KN_EFF { background-color: #f8f8f8; color:#000000; }

            #SH_KN_EFF_TR { background-color: #f8f8f8; color:#000000; }

            #SH_RECOM { background-color: #f8f8f8; color:#000000; }

            #SH_SITE_AN { background-color: #f8f8f8; color:#000000; }
```

```
                #SH_TSE { background-color: #f8f8f8; color:#000000; }

                #SH_RESFLOW { background-color: #f8f8f8; color:#000000; }

                #SH_RW { background-color: #f8f8f8; color:#000000; }
               </style>
</head>
<body onload="Qva.SetBackgroundSize(); Qva.Start();" class="QvPageBody"
style="background-color:#f8f8f8;">
<div class="shadetabs" avq="label:.TabRow">
<a id="SH_ACT_WF" avq="bind:.SH_ACT_WF"> </a>
<a id="SH_WF_AN" avq="bind:.SH_WF_AN"> </a>
<a id="SH_REV_PROD" avq="bind:.SH_REV_PROD"> </a>
<a id="SH_REV_EFF" avq="bind:.SH_REV_EFF"> </a>
<a id="SH_KN_EFF" avq="bind:.SH_KN_EFF"> </a>
<a id="SH_KN_EFF_TR" avq="bind:.SH_KN_EFF_TR"> </a>
<a id="SH_RECOM" avq="bind:.SH_RECOM"> </a>
<a id="SH_SITE_AN" avq="bind:.SH_SITE_AN"> </a>
<a id="SH_TSE" avq="bind:.SH_TSE"> </a>
<a id="SH_RESFLOW" avq="bind:.SH_RESFLOW"> </a>
<a id="SH_RW" avq="bind:.SH_RW"> </a>
</div>
<div id="PageContainer">
<div id="BackgroundContainer" style="background-image: url(SH_ACT_WF.png);
background-position: ; background-repeat:no-repeat;"/>
<div id="MainContainer">
<div id="Main">
<div avq="label:.TX17" style="display:none; left:1pt;top:5pt;width:181pt;
height:23pt; z-index:0;" class="TextObject TX17_bkg Frame" id="TX17_bkg"
xmlns="">
</div>
<div avq="frame:.TX17" style="display:none; left:1pt;top:5pt;width:181pt;
height:23pt;z-index:0;" class="TextObject Frame" id="TX17_frame">
<div class="caption" avq="caption:.TX17.Caption" xmlns="">
</div>
<div avq="label:.TX17.Content" class="content" xmlns="">
<table class="TextObject" style="width:181.44pt; height: 23.28pt; color:#0e5899;">
<tr>
<td style="width:100%; height:100%;" avq="text:.TX17.Content">
</td>
</tr>
</table>
</div>
</div>
<div avq="frame:.BU125" style="display:none; left:813pt;top:429pt;width:125pt;
height:18pt;z-index:0;" class="Button Frame" id="BU125_frame">
<div class="caption" avq="caption:.BU125.Caption" xmlns="">
</div>
<div avq="label:.BU125.Content" class="content" xmlns=""><button
style="width:auto; height:auto;"
avq="binaryaction:.BU125.Content"></button></div>
</div>
<div avq="frame:.BU96" style="display:none; left:881pt;top:12pt;width:53pt;
```

```
height:18pt;z-index:0;" class="Button Frame" id="BU96_frame">
<div class="caption" avq="caption:.BU96.Caption" xmlns="">
</div>
<div avq="label:.BU96.Content" class="content" xmlns=""><button
style="width:auto; height:auto;" avq="binaryaction:.BU96.Content"></button></div>
</div>
<div avq="frame:.CH19" style="display:none; left:304pt;top:45pt;width:300pt;
height:208pt;z-index:0;" class="Chart Frame" id="CH19_frame">
<div class="caption" avq="caption:.CH19.Caption" xmlns="">
</div>
<div avq="label:.CH19.Head" id="CH19_header" class="header" xmlns="">
<table style="width:auto; height:inherit;" avq="table:.CH19" avqheader="true"
id="CH19" class="Chart">
</table>
</div>
<div style="height:207.84pt;" avq="label:.CH19.Body" class="body" xmlns="">
<table style="width:auto;" avq="table" avqbody="true" AvqAsync="20:.CH19"
class="Chart">
</table>
</div>
<div avq="label:.CH19.Graph" class="graph" xmlns=""><img style="width:auto;
height:auto;" galleryimg="no" avq="binary:.CH19.Graph"></div>
</div>
<div style="
        left:151pt;
        top:1035pt;

       width:103pt;
       height:25pt;
       display:none;" avq="restore:.CH19.RE" class="Frame" xmlns="">
<div><button style="width:auto; height:auto;"
avq="binaryaction:.CH19.RE"></button></div>
</div>
<div avq="frame:.LB169" style="display:none; left:781pt;top:247pt;width:161pt;
height:107pt;z-index:0;" class="ListBox Frame" id="LB169_frame">
<d
```

High	**Possible Username or Password Disclosure**
File Names:	http://ddcwz30297:80/Analytics/

Summary: A username or password was found during "unknown" application testing. Unknown application testing seeks to uncover new vulnerabilities in both custom and commercial software. Because of this, there are no specific patches or descriptions for this issue. Please note that this vulnerability may be a false positive if the page it is flagged on is technical documentation. Recommendations include removing the information from the production server, or otherwise restricting access.

Execution: Click http://ddcwz30297:80/Analytics/ to verify the vulnerability in a web browser.

Implication: This information could allow an attacker to access sensitive applications and information on a site, or to perform functions according to the privilege level of the login information. Gaining information critical to the success of escalated attacks would also be a likely impact of exploitation.

Fix: Remove the information from the web server, if possible, or otherwise restrict access.

Reference:

Microsoft:
IIS Authentication
Authentication in IIS 6.0 (IIS 6.0)
How to configure IIS Web site authentication in Windows Server 2003

Apache:
Apache HTTP Server Version 1.3 - Authentication, Authorization, and Access Control
Apache HTTP Server Version 2.0 - Authentication, Authorization, and Access Control

Attack Request:

```
GET /Analytics/ HTTP/1.1
Referer: http://ddcwz30297:80/Analytics/SH_ACT_WF.htm
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR
1.1.4322)
Accept: */*
Pragma: no-cache
Host: ddcwz30297
X-Scan-Memo: Category="Audit";
Function="createStateRequestFromAttackDefinition";
SID="336B4B317E4CA2DFD0F9F3AB41B4B019";
PSID="AAE7DAA0D9D5211A830090E2DA35E093";
SessionType="PathTruncation"; CrawlType="None"; AttackType="None";
OriginatingEngineID="398bfe9e-1b77-4458-9691-603eea06e341";
AttackSequence="0"; AttackParamDesc=""; AttackParamIndex="0";
AttackParamSubIndex="0"; CheckId="(null)"; Engine="Path+Truncation";
Retry="False"; SmartMode="NonServerSpecificOnly"; ThreadId="31";
ThreadType="AuditDBReaderSessionDrivenAudit";
Connection: Keep-Alive
Cookie: CustomCookie=WebInspect0
```

Attack Response:

```
HTTP/1.1 200 OK
Content-Length: 1532
Content-Type: text/html
Content-Location: http://ddcwz30297/Analytics/Default.htm
Last-Modified: Thu, 09 Jul 2009 19:19:52 GMT
Accept-Ranges: bytes
ETag: "07cca3bca0ca1:56d"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 07 Dec 2011 16:01:22 GMT

...TRUNCATED...mas-microsoft-com:xslt" xmlns:zfp="uri:zfp"
xmlns:user="uri:user" xmlns=""></script><![CDATA[<script language="javascript"
t...TRUNCATED...mas-microsoft-com:xslt" xmlns:zfp="uri:zfp"
```

```
xmlns:user="uri:user" xmlns=""></script>]]><![CDATA[<script
language="javascript" t...TRUNCATED...mas-microsoft-com:xslt"
xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA[<script
language="javascript" t...TRUNCATED...mas-microsoft-com:xslt"
xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns="">
      var qva = new Qva.PageBinding(...TRUNCATED...mas-microsoft-com:xslt"
xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]></head>
<body onload="Qva.Star...TRUNCATED...
```

High	**Possible Username or Password Disclosure**
File Names:	http://ddcwz30297:80/Analytics/Default.htm
Summary:	A username or password was found during "unknown" application testing. Unknown application testing seeks to uncover new vulnerabilities in both custom and commercial software. Because of this, there are no specific patches or descriptions for this issue. Please note that this vulnerability may be a false positive if the page it is flagged on is technical documentation. Recommendations include removing the information from the production server, or otherwise restricting access.
Execution:	Click http://ddcwz30297:80/Analytics/Default.htm to verify the vulnerability in a web browser.
Implication:	This information could allow an attacker to access sensitive applications and information on a site, or to perform functions according to the privilege level of the login information. Gaining information critical to the success of escalated attacks would also be a likely impact of exploitation.
Fix:	Remove the information from the web server, if possible, or otherwise restrict access.
Reference:	**Microsoft:** IIS Authentication Authentication in IIS 6.0 (IIS 6.0) How to configure IIS Web site authentication in Windows Server 2003 **Apache:** Apache HTTP Server Version 1.3 - Authentication, Authorization, and Access Control Apache HTTP Server Version 2.0 - Authentication, Authorization, and Access Control
Attack Request:	GET /Analytics/Default.htm HTTP/1.1 Referer: http://ddcwz30297:80/Analytics/ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322) Accept: */* Pragma: no-cache Host: ddcwz30297 X-Scan-Memo: Category="Crawl"; Function="CreateStateRequest"; SID="978F4B6441E6C4F7BC64414DF0030F69"; PSID="336B4B317E4CA2DFD0F9F3AB41B4B019"; SessionType="Crawl"; CrawlType="HTML"; AttackType="None"; OriginatingEngineID="00000000-0000-0000-0000-000000000000"; ThreadId="122"; ThreadType="CrawlBreadthFirstDBReader";

Connection: Keep-Alive
Cookie: CustomCookie=WebInspect0

Attack Response:

HTTP/1.1 200 OK
Content-Length: 1532
Content-Type: text/html
Last-Modified: Thu, 09 Jul 2009 19:19:52 GMT
Accept-Ranges: bytes
ETag: "07cca3bca0ca1:56d"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 07 Dec 2011 16:01:23 GMT

...TRUNCATED...mas-microsoft-com:xslt" xmlns:zfp="uri:zfp"
xmlns:user="uri:user" xmlns=""></script><![CDATA[<script language="javascript"
t...TRUNCATED...mas-microsoft-com:xslt" xmlns:zfp="uri:zfp"
xmlns:user="uri:user" xmlns=""></script>]]><![CDATA[<script
language="javascript" t...TRUNCATED...mas-microsoft-com:xslt"
xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]><![CDATA[<script
language="javascript" t...TRUNCATED...mas-microsoft-com:xslt"
xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns="">
    var qva = new Qva.PageBinding(...TRUNCATED...mas-microsoft-com:xslt"
xmlns:zfp="uri:zfp" xmlns:user="uri:user" xmlns=""></script>]]></head>
<body onload="Qva.Star...TRUNCATED...

Attack Status

Created on 12/7/2011 8:02:34 AM with the following scans:

Scan Name:	Policy:	Scan Date:	Scan Version:
MPT MTS Knova Analytics Dev - 2011-12-07 16:00:00Z	Passive Scan	12/7/2011 8:01:25 AM	9.10.78.0

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
1435	Shell Error Message	Critical	Yes	Pass	-
1436	Shell Error Message	Critical	Yes	Pass	-
1451	Shell Error Message	Critical	Yes	Pass	-
3185	Possible Database Connection String (ODBC DSN or OleDB for Access, MS SQL, ORACLE, IBM DB2, MySQL, Sybase, Informix, or Interbase)	Critical	Yes	Pass	-
3490	PHP Multi-Part Form Data Arbitrary Command Execution	Critical	Yes	Pass	-
3527	L-Forum Multiple Vunerabilities	Critical	Yes	Pass	-
3531	Cafelog b2 Weblog Multiple Possible Vulnerabilties	Critical	Yes	Pass	-
5613	Possible Database Connection String (MSSQL ODBC Trusted Connection)	Critical	Yes	Pass	-
5615	Possible Database Connection String (MSSQL OleDb Trusted Connection)	Critical	Yes	Pass	-
5616	Possible Database Connection String (MSSQL OleDb via IP Address)	Critical	Yes	Pass	-
5617	Possible Database Connection String (MSSQL .NET DataProvider Standard Connection or Sybase .NET DataProvider)	Critical	Yes	Pass	-
5618	Possible Database Connection String (MSSQL .NET DataProvider Trusted Connection)	Critical	Yes	Pass	-
5619	Possible Database Connection String (MSSQL .NET DataProvider via IP Address)	Critical	Yes	Pass	-
5621	Possible Database Connection String (Access and Oracle ODBC)	Critical	Yes	Pass	-
5622	Possible Database Connection String (Access ODBC Workgroup - System Database)	Critical	Yes	Pass	-
5623	Possible Database Connection String (Access ODBC Exclusive Use)	Critical	Yes	Pass	-
5625	Possible Database Connection String (Access OleDb with MS Jet Workgroup - System Database)	Critical	Yes	Pass	-
5626	Possible Database Connection String (Access OleDb with MS Jet With Password)	Critical	Yes	Pass	-
5627	Possible Database Connection String (Oracle ODBC New Microsoft Driver)	Critical	Yes	Pass	-
5628	Possible Database Connection String (Oracle ODBC Old Microsoft Driver)	Critical	Yes	Pass	-

5629	Possible Database Connection String (Oracle OleDb Microsoft Driver and Oracle Driver - possible trusted connection)	Critical	Yes	Pass	-
5630	Possible Database Connection String (Oracle OleDb Oracle Driver - Trusted Connection)	Critical	Yes	Pass	-
5631	Possible Database Connection String (Oracle .NET DataProvider from Microsoft and Oracle - Standard Connection)	Critical	Yes	Pass	-
5632	Possible Database Connection String (Oracle .NET DataProvider from Microsoft and Oracle - Trusted Connection)	Critical	Yes	Pass	-
5633	Possible Database Connection String (IBM DB2 ODBC without DSN and OleDb IBM Driver)	Critical	Yes	Pass	-
5634	Possible Database Connection String (IBM DB2 OleDb Microsoft Driver)	Critical	Yes	Pass	-
5635	Possible Database Connection String (IBM DB2 .NET DataProvider from IBM)	Critical	Yes	Pass	-
5636	Possible Database Connection String (MySQL ODBC MyODBC Driver - local database)	Critical	Yes	Pass	-
5637	Possible Database Connection String (MySQL ODBC MyODBC Driver - remote database)	Critical	Yes	Pass	-
5640	Possible Database Connection String (MySQL .NET DataProvider from CoreLab)	Critical	Yes	Pass	-
5641	Possible Database Connection String (Sybase ODBC Sybase System 12 (12.5) ODBC Driver)	Critical	Yes	Pass	-
5642	Possible Database Connection String (Sybase ODBC Sybase System 11 ODBC Driver or Intersolv 3.10 ODBC Driver)	Critical	Yes	Pass	-
5643	Possible Database Connection String (Sybase ODBC SQL Anywhere)	Critical	Yes	Pass	-
5644	Possible Database Connection String (Sybase OleDb Sybase Adaptive Server Enterprise (ASE))	Critical	Yes	Pass	-
5646	Possible Database Connection String (Informix ODBC DSN INFORMIX 3.30 ODBC Driver)	Critical	Yes	Pass	-
5647	Possible Database Connection String (Informix ODBC without DSN INFORMIX 3.30 ODBC Driver)	Critical	Yes	Pass	-
5648	Possible Database Connection String (Informix OleDb IBM Informix OleDb Provider)	Critical	Yes	Pass	-
742	Database Server Error Message	Critical	Yes	Pass	-
10050	Personal Identification Number Disclosed	Critical	Yes	Pass	-
10186	Possible MPack Infection	Critical	Yes	Pass	-
10237	Possible Credit Card Numbers In Cookie(s)	Critical	Yes	Pass	-
10299	Possible XSS-Proxy Infection	Critical	Yes	Pass	-
10662	phpMyAdmin Arbitrary Command Execution	Critical	Yes	Pass	-
10749	Insecure Security.allowInsecureDomain() usage	Critical	Yes	Pass	-
10750	Insecure Security.allowDomain() usage	Critical	Yes	Pass	-

10757	Insecure LocalConnection.allowDomain() usage	Critical	Yes	Pass	-
10765	Application Source Available	Critical	Yes	Pass	-
10778	Possible Credit Card Number Disclosure	Critical	Yes	Pass	-
10823	Insecure LocalConnection.allowInsecureDomain() usage	Critical	Yes	Pass	-
10825	Credit Card Numbers Disclosed	Critical	Yes	Pass	-
10834	Social Security Number Disclosure	Critical	Yes	Pass	-
1384	Possible PHP Source Code Disclosure	High	Yes	Pass	-
1389	WebTrends Statistics Information Disclosure	High	Yes	Pass	-
1429	Possible Debug Application	High	Yes	Pass	-
3412	Rapid Web Publisher Administrative Interface	High	Yes	Pass	-
3699	Jetty CGI-BIN Arbitrary Command Execution	High	Yes	Pass	-
4722	Logins Sent Over Unencrypted Connection	High	Yes	Pass	-
5241	Perl Source Code Disclosure	High	Yes	Pass	-
2229	Possible ASP.NET Source Code Disclosure	High	Yes	Pass	-
3051	Microsoft JScript Runtime Error Message	High	Yes	Pass	-
10049	California Driver's License Number Disclosed	High	Yes	Pass	-
10167	Password in Query or Cookie Data	High	Yes	Pass	-
10512	HTTP Basic Logins Sent Over Unencrypted Connection	High	Yes	Pass	-
10551	Possible Username or Password Disclosure	High	Yes	**Fail**	3
10595	Unencrypted Login Form	High	Yes	Pass	-
10753	Insecure Flash Storage Object	High	Yes	Pass	-
10755	ENABLEDEBUGGER Tag Detected	High	Yes	Pass	-
10763	Possible Social Security Number	High	Yes	Pass	-
10772	Possible Database Connection String (MSSQL ODBC Trusted Connection)	High	Yes	Pass	-
10773	Possible Database Connection String (MSSQL OleDb Trusted Connection)	High	Yes	Pass	-
10774	Possible Database Connection String (MSSQL OleDb via IP Address)	High	Yes	Pass	-
10775	Possible Database Connection String (MSSQL .NET DataProvider Standard Connection or Sybase .NET DataProvider)	High	Yes	Pass	-
10776	Possible Database Connection String (MSSQL .NET DataProvider Trusted Connection)	High	Yes	Pass	-
10777	Possible Database Connection String (MSSQL .NET DataProvider via IP Address)	High	Yes	Pass	-
10781	PGP Private Key Block	High	Yes	Pass	-

10783	Possible Database Connection String (Access and Oracle ODBC -- Standard Security for MS Access and ODBC Oracle Driver	High	Yes	Pass	-
10784	Possible Database Connection String (Access ODBC Workgroup - System Database)	High	Yes	Pass	-
10785	Possible Database Connection String (Access OleDb with MS Jet Workgroup - System Database)	High	Yes	Pass	-
10786	Possible Database Connection String (Access OleDb with MS Jet With Password)	High	Yes	Pass	-
10787	Possible Database Connection String (Oracle ODBC New Microsoft Driver	High	Yes	Pass	-
10788	Possible Database Connection String (Oracle ODBC Old Microsoft Driver	High	Yes	Pass	-
10789	Possible Database Connection String (Oracle OleDb Microsoft Driver and Oracle Driver - possible trusted connection)	High	Yes	Pass	-
10790	Possible Database Connection String (Oracle OleDb Oracle Driver - Trusted Connection)	High	Yes	Pass	-
10791	Possible Database Connection String (Oracle .NET DataProvider from Microsoft and Oracle - Standard Connection)]	High	Yes	Pass	-
10792	Possible Database Connection String (Oracle .NET DataProvider from Microsoft and Oracle - Trusted Connection)	High	Yes	Pass	-
10793	Possible Database Connection String (IBM DB2 ODBC without DSN and OleDb IBM Driver	High	Yes	Pass	-
10794	Possible Database Connection String (IBM DB2 OleDb Microsoft Driver)	High	Yes	Pass	-
10795	Possible Database Connection String (IBM DB2 .NET DataProvider from IBM)	High	Yes	Pass	-
10796	Possible Database Connection String (MySQL ODBC MyODBC Driver - local database)	High	Yes	Pass	-
10797	Possible Database Connection String (MySQL ODBC MyODBC Driver - remote database)	High	Yes	Pass	-
10798	Possible Database Connection String (MySQL .NET DataProvider from CoreLab)	High	Yes	Pass	-
10799	Possible Database Connection String (Sybase ODBC Sybase System 12 (12.5) ODBC Driver)	High	Yes	Pass	-
10800	Possible Database Connection String (Sybase ODBC Sybase System 11 ODBC Driver or Intersolv 3.10 ODBC Driver)	High	Yes	Pass	-
10801	Possible Database Connection String (Sybase ODBC SQL Anywhere)	High	Yes	Pass	-
10802	Possible Database Connection String (Sybase OleDb Sybase Adaptive Server Enterprise (ASE))	High	Yes	Pass	-
10803	Possible Database Connection String (Informix ODBC DSN INFORMIX 3.30 ODBC Driver)	High	Yes	Pass	-
10804	Possible Database Connection String (Informix ODBC without DSN INFORMIX 3.30 ODBC Driver)	High	Yes	Pass	-
10805	Possible Database Connection String (Informix OleDb IBM Informix OleDb Provider)	High	Yes	Pass	-

10811	FlashVars Cross-Site Scripting	High	Yes	Pass	-
10812	FlashVars Cross-Site Scripting / Request Forgery	High	Yes	Pass	-
10813	ASNative Function Usage Detected	High	Yes	Pass	-
10817	Use of FlashVars in System.security.loadPolicyFile Detected	High	Yes	Pass	-
10818	Use of FlashVars in loadMovie Detected	High	Yes	Pass	-
10819	Possible FlashVars Cross-Site Scripting in htmlText property of a TextField	High	Yes	Pass	-
10820	Possible FlashVars Cross-Site Scripting in htmlText property bound to an Uninitialized Variable	High	Yes	Pass	-
10821	FlashVar usage in ExternalInterface.call method	High	Yes	Pass	-
10822	Possible Cross-Site Scripting in getURL using "GET" method	High	Yes	Pass	-
10978	Joomla's Contact Component Spam Vulnerability	High	Yes	Pass	-
745	Runtime Error Message	Medium	Yes	Pass	-
1385	ColdFusion Error Message	Medium	Yes	Pass	-
1430	Server Statistics Information Disclosure	Medium	Yes	Pass	-
1498	Exception Error Message	Medium	Yes	Pass	-
2077	Java Runtime Error Message	Medium	Yes	Pass	-
2172	Websphere Net.Data Error Message	Medium	Yes	Pass	-
2256	Servlet Runtime Error Message	Medium	Yes	Pass	-
3064	ASP Runtime Error Message	Medium	Yes	Pass	-
3186	SOAP Exception Error Message	Medium	Yes	Pass	-
4423	LDAP Error Message	Medium	Yes	Pass	-
4625	Webalizer webalizer.conf Configuration Disclosure	Medium	Yes	Pass	-
4720	SSL Cookie Not Used	Medium	Yes	Pass	-
4725	Certificate Hostname Discrepency	Medium	Yes	Pass	-
4728	Persistent Cookies	Medium	Yes	Pass	-
4939	.NET Error Message	Medium	Yes	Pass	-
5153	ASP.NET Unhashed Viewstate Agent	Medium	Yes	Pass	-
5541	XPath Error Message	Medium	Yes	Pass	-
746	Directory Listing	Medium	Yes	Pass	-
4724	Password Field Masked	Medium	Yes	Pass	-
10261	Source Code Viewing Example Application	Medium	Yes	Pass	-
10263	Outlook .PST File Disclosure	Medium	Yes	Pass	-

10269	.NET Verbose Errors Enabled	Medium	Yes	Pass	-
10290	InfoSoft FusionCharts/PowerCharts Possible Remote SWF Inclusion	Medium	Yes	Pass	-
10292	Camtasia Studio Possible Remote SWF Inclusion	Medium	Yes	Pass	-
10293	Acrobat Connect SWF Possible Cross-Site Scripting	Medium	Yes	Pass	-
10479	Phpinfo() Information Disclosure	Medium	Yes	Pass	-
10506	Apache Header Line Abort Denial of Service	Medium	Yes	Pass	-
10666	Oracle Application Server Portal Authentication Bypass	Medium	Yes	Pass	-
10703	Certificate Expired	Medium	Yes	Pass	-
10722	SQL Query in Query String or Post Data	Medium	Yes	Pass	-
10729	ASP.NET Stack Trace Disclosure	Medium	Yes	Pass	-
10744	JRun web.xml Server Configuration Information Disclosure	Medium	Yes	Pass	-
10747	MD5 Hash Detected	Medium	Yes	Pass	-
10748	Potential User Account Information Disclosure	Medium	Yes	Pass	-
10752	Debug Messaging	Medium	Yes	Pass	-
10764	ActionScript Source Path Disclosure	Medium	Yes	Pass	-
10766	SHA-0/SHA-1 Hash Detected	Medium	Yes	Pass	-
10926	Sun Communications Express search.xml Cross-Site Scripting	Medium	Yes	Pass	-
10927	Sun Communications Express UWCMain Cross-Site Scripting	Medium	Yes	Pass	-
10929	IBM Tivoli FilepathLogin.html Cross-Site Scripting	Medium	Yes	Pass	-
10943	HTTPS Privacy/Trust Violation	Medium	Yes	Pass	-
10965	User Data in Query or Cookie	Medium	Yes	Pass	-
2291	Environmental Variables Disclosure	Low	Yes	Pass	-
3508	Internal IP Disclosure	Low	Yes	Pass	-
3636	Verity Search97 Error Message	Low	Yes	Pass	-
3789	Oracle Application Server PL/SQL Error Message	Low	Yes	Pass	-
4250	VBScript Runtime Error Message	Low	Yes	Pass	-
4823	Jrun Server Error Message	Low	Yes	Pass	-
810	Possible Server Path Disclosure (unix)	Low	Yes	Pass	-
909	Possible File Upload Capability	Low	Yes	Pass	-
4919	Unexecuted Server Side Include	Low	Yes	Pass	-
10190	Possible VBScript Runtime Error Message	Low	Yes	Pass	-
10208	PHP Error Message	Low	Yes	Pass	-

10256	Webbler Web Root Path Disclosure	Low	Yes	Pass	-
10526	CuteNews "cutepath" Remote File Include	Low	Yes	Pass	-
10527	Bitweaver TEST Mode Enabled	Low	Yes	Pass	-
10571	PHP open_basedir And display_errors Path Disclosure	Low	Yes	Pass	-
10600	Moodle blogpage.php Path Disclosure	Low	Yes	Pass	-
10649	FlashStaticAnalysis	Low	Yes	Pass	-
10675	Questionable Material Directories	Low	Yes	Pass	-
10682	Wordpress wp-app.log Information Disclosure	Low	Yes	Pass	-
10683	Wordpress xmlrpc.log Information Disclosure	Low	Yes	Pass	-
10684	Wordpress enclosures.log Information Disclosure	Low	Yes	Pass	-
10695	Subversion Keyword Information Disclosure	Low	Yes	Pass	-
10735	Possible Server Path Disclosure (win32)	Low	Yes	Pass	-
10736	ASP.NET Stack Trace (VB)	Low	Yes	Pass	-
10740	Apache Cocoon Stack Trace	Low	Yes	Pass	-
10751	LoadBytes Usage	Low	Yes	Pass	-
10754	Shared Flash Storage Object	Low	Yes	Pass	-
10758	Potentially Interesting Name Encountered	Low	Yes	Pass	-
10759	Possible Application Information Disclosure	Low	Yes	Pass	-
10760	Potential Personal Information Disclosure	Low	Yes	Pass	-
10761	Possible Cryptographic Data	Low	Yes	Pass	-
10762	Possible Commerce Information	Low	Yes	Pass	-
10767	Possible Server Path Disclosure (win32)	Low	Yes	Pass	-
10768	Possible Server Path Disclosure (unix)	Low	Yes	Pass	-
10769	Possible SQL Query	Low	Yes	Pass	-
10770	Possible LDAP Query	Low	Yes	Pass	-
10779	Internal IP Disclosure	Low	Yes	Pass	-
10780	PGP Public Key Block	Low	Yes	Pass	-
10782	Possible XPath Query	Low	Yes	Pass	-
10842	Possible LDAP Query	Low	Yes	Pass	-
10845	Possible XPath Query	Low	Yes	Pass	-
10855	PHP Error Header Information Disclosure	Low	Yes	Pass	-
10856	BEA AquaLogic Interaction Plumtree Portal Information Disclosure	Low	Yes	Pass	-

10869	XDomainRequestAllowed Header Found	Low	Yes	Pass	-
10925	ActiveX Control Discovery	Low	Yes	Pass	-
10932	Server Error Response	Low	Yes	Pass	-
11217	PHP Admin Application (admin.php3)	Low	Yes	Pass	-
7	Comment Checks	Informational	Yes	Pass	-
2888	Default Apache Page	Informational	Yes	Pass	-
2897	IIS Default Install Page	Informational	Yes	Pass	-
2898	IIS Default Install Page	Informational	Yes	Pass	-
2903	iPlanet 6.0 Default Install	Informational	Yes	Pass	-
3850	Site Search	Informational	Yes	Pass	-
3853	Potential filename found in comments	Informational	Yes	Pass	-
3856	Known Vulnerabilities	Informational	Yes	Pass	-
3869	Adaptive Agents	Informational	Yes	Pass	-
4306	Possible Login Form	Informational	Yes	Pass	-
4727	Hidden Form Value	Informational	Yes	Pass	-
10026	Keyword Search	Informational	Yes	Pass	-
10027	Request Inspect	Informational	Yes	Pass	-
10028	Request Modification	Informational	Yes	Pass	-
10264	Installed Application: Squirrelmail	Informational	Yes	Pass	-
10267	Installed Application: Drupal	Informational	Yes	Pass	-
10268	Installed Application: Roller	Informational	Yes	Pass	-
10273	Warning: IIS Server Overloaded	Informational	Yes	Pass	-
10278	Installed Application: HacmeCasino	Informational	Yes	Pass	-
10280	Price-Related Form Fields	Informational	Yes	Pass	-
10374	Struts Framework in Use	Informational	Yes	Pass	-
10376	QuickCaptcha Detected	Informational	Yes	Pass	-
10377	Cryptographp CAPTCHA Detected	Informational	Yes	Pass	-
10378	AnimatedCaptcha Detected	Informational	Yes	Pass	-
10379	AnimatedImage CAPTCHA Detected	Informational	Yes	Pass	-
10380	Idut Human Checker CAPTCHA Detected	Informational	Yes	Pass	-
10381	SecurImage CAPTCHA Detected	Informational	Yes	Pass	-
10382	phpOpenCaptcha Detected	Informational	Yes	Pass	-

10383	TheCAPTCHA Detected	Informational	Yes	Pass	-
10384	Simple PHP-CAPTCHA Detected	Informational	Yes	Pass	-
10385	Simple Captcha Detected	Informational	Yes	Pass	-
10386	Micro Captcha Detected	Informational	Yes	Pass	-
10387	Fusebox Framework in Use	Informational	Yes	Pass	-
10388	Security Image CAPTCHA Detected	Informational	Yes	Pass	-
10389	ZDR Captcha Detected	Informational	Yes	Pass	-
10391	Freecap CAPTCHA Detected	Informational	Yes	Pass	-
10392	HN Captcha Detected	Informational	Yes	Pass	-
10393	Captcha PHP Detected	Informational	Yes	Pass	-
10412	CAPTCHA for ASP Detected	Informational	Yes	Pass	-
10413	HumanVerify CAPTCHA Detected	Informational	Yes	Pass	-
10414	ASP Security Image Generator (CAPTCHA) Detected	Informational	Yes	Pass	-
10415	ASP CAPTCHA Project Detected	Informational	Yes	Pass	-
10416	CAPTCHA Server Control for ASP.NET Detected	Informational	Yes	Pass	-
10417	CAPTCHA Image for ASP Detected	Informational	Yes	Pass	-
10418	CIS Image Verification CAPTCHA Detected	Informational	Yes	Pass	-
10419	ASP Form Image Code Verification (CAPTCHA) Detected	Informational	Yes	Pass	-
10420	CaptchaControl Detected	Informational	Yes	Pass	-
10421	DotNetNuke Captcha Control Detected	Informational	Yes	Pass	-
10422	Lanapsoft BotDetect CAPTCHA Detected	Informational	Yes	Pass	-
10434	LylaCaptcha Detected	Informational	Yes	Pass	-
10435	Use of captchas.net Service Detected	Informational	Yes	Pass	-
10436	Flash Object Detected	Informational	Yes	Pass	-
10437	Silverlight Application Detected	Informational	Yes	Pass	-
10534	Java Applet Detected	Informational	Yes	Pass	-
10628	Possible Authentication Misconfiguration (Status Code)	Informational	Yes	Pass	-
10629	Possible Authentication Misconfiguration (WWW-Authenticate)	Informational	Yes	Pass	-
10656	BitTorrent File Found	Informational	Yes	Pass	-
10713	PHProxy Detected	Informational	Yes	Pass	-
10719	PHP-Nuke SQL Injection Probing	Informational	Yes	Pass	-
10808	PROTECT Tag detected	Informational	Yes	Pass	-

10809	ENABLEDEBUGGER2 Tag Detected	Informational	Yes	Pass	-
10861	Header May Reveal Server Name	Informational	Yes	Pass	-
10936	Unsafe Flash Embed Settings - AllowScriptAccess	Informational	Yes	Pass	-
10937	File Open Error Messages Detected	Informational	Yes	Pass	-
2887	Default Apache Page	Best Practice	Yes	Pass	-
4723	Logins Sent Over Query	Best Practice	Yes	Pass	-
4729	User supplied data without POST	Best Practice	Yes	Pass	-
5597	Form Auto Complete Active	Best Practice	Yes	Pass	-
10344	Possible Insecure Cryptographic Hash (MD Family)	Best Practice	Yes	Pass	-
10346	Possible Insecure Cryptographic Hash (SHA-0/SHA-1)	Best Practice	Yes	Pass	-
10543	Set-Cookie does not use HTTPOnly Keyword	Best Practice	Yes	Pass	-
10691	Encrypted Page Includes Insecure Content	Best Practice	Yes	Pass	-
10756	Minimum Stage Size	Best Practice	Yes	Pass	-
10814	Suggested Security Controls for Embedding SWF Files in HTML	Best Practice	Yes	Pass	-