Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 9.0.3, Rules: 1957
Scan started: 8/16/2017 5:42:35 PM

Table of Contents

Introduction

Summary

Issues Sorted by Issue Type

Fix Recommendations

- Add the 'Secure' attribute to all sensitive cookies
- Change session identifier values after login
- Configure your server to allow only required HTTP methods
- Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form
- Always use SSL and POST (body) parameters when sending sensitive information.
- Apply proper authorization to administration scripts
- Config your server to use the "Content-Security-Policy" header
- Config your server to use the "X-Content-Type-Options" header
- Config your server to use the "X-Frame-Options" header
- Config your server to use the "X-XSS-Protection" header
- Correctly set the "autocomplete" attribute to "off"
- Disable Debugging on Microsoft ASP.NET
- Implement the HTTP Strict-Transport-Security policy
- Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely
- Modify your Web.Config file to encrypt the VIEWSTATE parameter
- Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.
- Remove business and security logic from the client side
- Remove old versions of files from the virtual directory
- Remove test scripts from the server

Advisories

- Authentication Bypass Using HTTP Verb Tampering
- Cross-Site Request Forgery
- Missing Secure Attribute in Encrypted Session (SSL) Cookie
- Session Identifier Not Updated
- Autocomplete HTML Attribute Not Disabled for Password Field
- Cacheable SSL Page Found
- Direct Access to Administration Pages
- Hidden Directory Detected
- Microsoft ASP.NET Debugging Enabled
- Missing "Content-Security-Policy" header
- Missing "X-Content-Type-Options" header
- Missing "X-XSS-Protection" header
- Missing Cross-Frame Scripting Defence
- Missing HTTP Strict-Transport-Security Header
- Query Parameter in SSL Request
- Temporary File Download
- Unencrypted __VIEWSTATE Parameter
- Application Test Script Detected
- Client-Side (JavaScript) Cookie References

Application Data

- Cookies
- JavaScripts
- Parameters
- Comments
- Visited URLs
- Failed Requests
- Filtered URLs

Introduction

This report contains the results of a web application security scan performed by IBM Security AppScan Standard.

Medium severity issues:	5
Low severity issues:	77
Informational severity issues:	3
Total security issues included in the report:	85
Total security issues discovered in the scan:	85

General Information

Scan file name:	Untitled
Scan started:	8/16/2017 5:42:35 PM
Test policy:	Default
Host	md1npdvpadss02.dev.corp.local
Operating system:	Win32
Web server:	IIS
Application server:	Any

Login Settings

Login method:	Automatic
Concurrent logins:	Enabled
JavaScript execution:	Disabled
In-session detection:	Enabled
In-session pattern:	
Tracked or session ID cookies:	
Tracked or session ID parameters:	
Login sequence:	

Summary

Issue Types 19

TOC

	Issue Type	Number of Issues
M	Authentication Bypass Using HTTP Verb Tampering	1
M	Cross-Site Request Forgery	2
M	Missing Secure Attribute in Encrypted Session (SSL) Cookie	1
M	Session Identifier Not Updated	1
L	Autocomplete HTML Attribute Not Disabled for Password Field	2
L	Cacheable SSL Page Found	5
L	Direct Access to Administration Pages	2
L	Hidden Directory Detected	10
L	Microsoft ASP.NET Debugging Enabled	1
L	Missing "Content-Security-Policy" header	11
L	Missing "X-Content-Type-Options" header	11
L	Missing "X-XSS-Protection" header	11
L	Missing Cross-Frame Scripting Defence	2
L	Missing HTTP Strict-Transport-Security Header	11
L	Query Parameter in SSL Request	8
L	Temporary File Download	1
L	Unencrypted __VIEWSTATE Parameter	2
I	Application Test Script Detected	2
I	Client-Side (JavaScript) Cookie References	1

Vulnerable URLs 21

TOC

	URL	Number of Issues
M	https://md1npdvpadss02.dev.corp.local/dxr.axd	9
M	https://md1npdvpadss02.dev.corp.local/login.aspx	17
M	https://md1npdvpadss02.dev.corp.local/logout.aspx	6

L	https://md1npdvpadss02.dev.corp.local/scriptresource.axd	8
L	https://md1npdvpadss02.dev.corp.local/webresource.axd	7
L	https://md1npdvpadss02.dev.corp.local/	3
L	https://md1npdvpadss02.dev.corp.local/css/	1
L	https://md1npdvpadss02.dev.corp.local/cvs/	1
L	https://md1npdvpadss02.dev.corp.local/data/	1
L	https://md1npdvpadss02.dev.corp.local/help/	2
L	https://md1npdvpadss02.dev.corp.local/images/	1
L	https://md1npdvpadss02.dev.corp.local/reports/	1
L	https://md1npdvpadss02.dev.corp.local/scripts/	1
L	https://md1npdvpadss02.dev.corp.local/services/	1
L	https://md1npdvpadss02.dev.corp.local/templates/	1
L	https://md1npdvpadss02.dev.corp.local/uploads/	1
L	https://md1npdvpadss02.dev.corp.local/admin.aspx	4
L	https://md1npdvpadss02.dev.corp.local/admin/scriptresource.axd	6
L	https://md1npdvpadss02.dev.corp.local/error_handling.aspx	5
L	https://md1npdvpadss02.dev.corp.local/salestrends.aspx	4
L	https://md1npdvpadss02.dev.corp.local/timeout.aspx	5

Fix Recommendations 19

TOC

	Remediation Task	Number of Issues
M	Add the 'Secure' attribute to all sensitive cookies	1
M	Change session identifier values after login	1
M	Configure your server to allow only required HTTP methods	1
M	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form	2
L	Always use SSL and POST (body) parameters when sending sensitive information.	8
L	Apply proper authorization to administration scripts	2
L	Config your server to use the "Content-Security-Policy" header	11
L	Config your server to use the "X-Content-Type-Options" header	11
L	Config your server to use the "X-Frame-Options" header	2
L	Config your server to use the "X-XSS-Protection" header	11
L	Correctly set the "autocomplete" attribute to "off"	2
L	Disable Debugging on Microsoft ASP.NET	1
L	Implement the HTTP Strict-Transport-Security policy	11
L	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely	10

L	Modify your Web.Config file to encrypt the VIEWSTATE parameter	2
L	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	5
L	Remove business and security logic from the client side	1
L	Remove old versions of files from the virtual directory	1
L	Remove test scripts from the server	2

Security Risks 10

TOC

	Risk	Number of Issues
M	It might be possible to escalate user privileges and gain administrative permissions over the web application	3
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	55
M	It may be 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	3
M	It may be possible to steal user and session information (cookies) that was sent during an encrypted session	1
L	It may be possible to bypass the web application's authentication mechanism	2
L	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site	10
L	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	46
L	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted	8
L	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords	3
I	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side	1

Causes 8

TOC

	Cause	Number of Issues
M	Insecure web application programming or configuration	53
M	Insufficient authentication method was used by the application	2
M	The web application sends non-secure cookies over SSL	1

L	Sensitive information might have been cached by your browser	5
L	The web server or application server are configured in an insecure way	12
L	Query parameters were passed over SSL, and may contain sensitive information	8
L	Temporary files were left in production environment	3
I	Cookies are created at the client side	1

WASC Threat Classification

TOC

Threat	Number of Issues
Cross-site Request Forgery	2
Information Leakage	76
Insufficient Authentication	1
Predictable Resource Location	5
Session Fixation	1

Issues Sorted by Issue Type

M Authentication Bypass Using HTTP Verb Tampering 1 TOC

Issue 1 of 1 TOC

Authentication Bypass Using HTTP Verb Tampering	
Severity:	**Medium**
CVSS Score:	6.4
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	DXR.axd (Page)
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Configure your server to allow only required HTTP methods

Difference: **Method** manipulated from: `GET` to: `BOGUS`
Cookie removed from request: `2tayzw3g1nhtsf00fxfxc512`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the verb tampering was able to bypass the site authentication

Test Requests and Responses:

```
BOGUS /DXR.axd?r=1_147-i3tS8 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
```

```
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:14:07 GMT
Content-Length: 34742

var __aspxStateItemsExist = false;
var __aspxFocusedItemKind = "FocusedStateItem";
var __aspxHoverItemKind = "HoverStateItem";
var __aspxPressedItemKind = "PressedStateItem";
var __aspxSelectedItemKind = "SelectedStateItem";
var __aspxDisabledItemKind = "DisabledStateItem";
var __aspxCachedStatePrefix = "cached";
ASPxStateItem = _aspxCreateClass(null, {
 constructor: function(name, classNames, cssTexts, postfixes, imageObjs, imagePostfixes, kind,
disableApplyingStyleToLink){
  this.name = name;
  this.classNames = classNames;
  this.customClassNames = [];
  this.resultClassNames = [];
  this.cssTexts = cssTexts;
  this.postfixes = postfixes;
  this.imageObjs = imageObjs;
  this.imagePostfixes = imagePostfixes;
  this.kind = kind;
  this.classNamePostfix = kind.substr(0, 1).toLowerCase();
  this.enabled = true;
  this.needRefreshBetweenElements = false;
  this.elements = null;
  this.images = null;
  this.linkColor = null;
  this.lintTextDecoration = null;
  this.disableApplyingStyleToLink = !!disableApplyingStyleToLink;
 },
 GetCssText: function(index){
  if(_aspxIsExists(this.cssTexts[index]))
   return this.cssTexts[index];
  return this.cssTexts[0];
 },
 CreateStyleRule: function(index){
  if(this.GetCssText(index) == "") return "";
  var styleSheet = _aspxGetCurrentStyleSheet();
  if(styleSheet)
   return _aspxCreateImportantStyleRule(styleSheet, this.GetCssText(index),
this.classNamePostfix);
  return "";
 },
 GetClassName: function(index){
  if(_aspxIsExists(this.classNames[index]))
   return this.classNames[index];
  return this.classNames[0];
 },
 GetResultClassName: function(index){
  if(!_aspxIsExists(this.resultClassNames[index])) {
   if(!_aspxIsExists(this.customClassNames[index]))
    this.customClassNames[index] = this.CreateStyleRule(index);
   if(this.GetClassName(index) != "" && this.customClassNames[index] != "")
    this.resultClassNames[index] = this.GetClassName(index) + " " + this.customClassNames[index];
   else if(this.GetClassName(index) != "")
    this.resultClassNames[index] = this.GetClassName(index);
   else if(this.customClassNames[index] != "")
    this.resultClassNames[index] = this.customClassNames[index];
   else
    this.resultClassNames[index] = "";
  }
  return this.resultClassNames[index];
 },
 GetElements: function(element){
  if(!this.elements || !_aspxIsValidElements(this.elements)){
   if(this.postfixes && this.postfixes.length > 0){
    this.elements = [ ];
    var parentNode = element.parentNode;
    if(parentNode){
     for(var i = 0; i < this.postfixes.length; i++){
      var id = this.name + this.postfixes[i];
      this.elements[i] = _aspxGetChildById(parentNode, id);
      if(!this.elements[i])
       this.elements[i] = _aspxGetElementById(id);
     }
    }
   }
   else
    this.elements = [element];
  }
  return this.elements;
 },
 GetImages: function(element){
  if(!this.images || !_aspxIsValidElements(this.images)){
   this.images = [ ];
   if(this.imagePostfixes && this.imagePostfixes.length > 0){
    var elements = this.GetElements(element);
    for(var i = 0; i < this.imagePostfixes.length; i++){
     var id = this.name + this.imagePostfixes[i];
     for(var j = 0; j < elements.length; j++){
      if(!elements[j]) continue;
      if(elements[j].id == id)
       this.images[i] = elements[j];
      else
       this.images[i] = _aspxGetChildById(elements[j], id);
      if(this.images[i])
       break;
     }
    }
   }
  }
  return this.images;
 },
 Apply: function(element){
  if(!this.enabled) return;
  try{
   this.ApplyStyle(element);
   if(this.imageObjs && this.imageObjs.length > 0)
    this.ApplyImage(element);
  }
  catch(e){
  }
 },
 ApplyStyle: function(element){
  var elements = this.GetElements(element);
  for(var i = 0; i < elements.length; i++){
   if(!elements[i]) continue;
   var className = elements[i].className.replace(this.GetResultClassName(i), "");
   elements[i].className = _aspxTrim(className) + " " + this.GetResultClassName(i);
   if(!__aspxOpera || __aspxBrowserVersion >= 9)
    this.ApplyStyleToLinks(elements, i);
  }
 },
 ApplyStyleToLinks: function(elements, index){
  if(this.disableApplyingStyleToLink)
   return;
  var linkCount = 0;
  var savedLinkCount = -1;
  if(_aspxIsExist
...
...
...
```

M Cross-Site Request Forgery 2 TOC

Issue 1 of 2 TOC

Cross-Site Request Forgery

Severity:	Medium
CVSS Score:	6.4
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	It may be 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
Causes:	Insufficient authentication method was used by the application
Fix:	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Difference: **Header** manipulated from: `https://md1npdvpadss02.dev.corp.local/Login.aspx` to: `http://bogus.referer.ibm.com`
Cookie removed from request: `2tayzw3g1nhtsf00fxfxc512`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

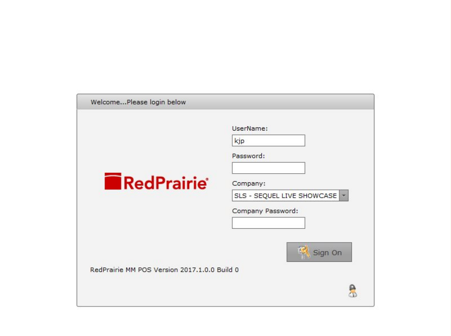
Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://bogus.referer.ibm.com
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:14:36 GMT
Content-Length: 38128
Set-Cookie: ASP.NET_SessionId=sezxhdrnjd0xqeeu4qkcz2ky; path=/; HttpOnly


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
```

```
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">
```

```
          </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padd
...
...
...
```

Original Response



Welcome...Please login below

UserName: kjp

Password:

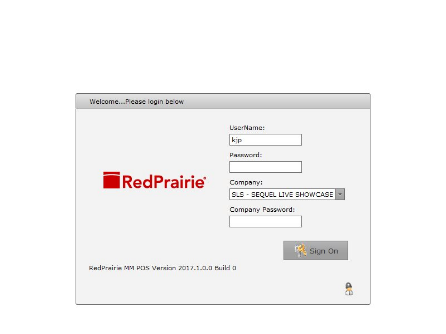
Company: SLS - SEQUEL LIVE SHOWCASE

Company Password:

RedPrairie MM POS Version 2017.1.0.0 Build 0

≈

Test Response



Welcome...Please login below

UserName: kjp

Password:

Company: SLS - SEQUEL LIVE SHOWCASE

Company Password:

RedPrairie MM POS Version 2017.1.0.0 Build 0

Issue 2 of 2

TOC

Cross-Site Request Forgery

Severity:	Medium
CVSS Score:	6.4
URL:	https://md1npdvpadss02.dev.corp.local/logout.aspx
Entity:	logout.aspx (Page)
Risk:	It may be 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
Causes:	Insufficient authentication method was used by the application
Fix:	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Difference: **Header** manipulated from: `https://md1npdvpadss02.dev.corp.local/timeout.aspx` to: `http://bogus.referer.ibm.com`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
GET /logout.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Referer: http://bogus.referer.ibm.com
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:44 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>

...
...
...
```

M Missing Secure Attribute in Encrypted Session (SSL) Cookie 1 TOC

Issue 1 of 1 TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Severity:	Medium
CVSS Score:	6.4
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	ASP.NET_SessionId (Cookie)
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Difference:

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
GET /Login.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:47 GMT
Content-Length: 36506
Set-Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512; path=/; HttpOnly


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                    <table border="0" cellpadding="0" cellspacing="0">
                        <tr>
                            <td height="100%" align="left" valign="middle">

...
...
...
```

M Session Identifier Not Updated 1

TOC

Issue 1 of 1

TOC

Session Identifier Not Updated

Severity:	Medium
CVSS Score:	6.4
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	It may be 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
Causes:	Insecure web application programming or configuration
Fix:	Change session identifier values after login

Difference:

Reasoning: The test result seems to indicate a vulnerability because the session identifiers in the Original Request and in the Response are identical. They should have been updated in the response.

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38128


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
```

```
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
```

```
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
...
...
```

L Autocomplete HTML Attribute Not Disabled for Password Field 2

TOC

Issue 1 of 2

TOC

Autocomplete HTML Attribute Not Disabled for Password Field

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Difference:

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38128


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
```

```
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
```

```
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
...
...
```

Issue 2 of 2

TOC

Autocomplete HTML Attribute Not Disabled for Password Field

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	login.aspx (Page)
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Difference:

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.

Test Requests and Responses:

```
GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
```

```
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">
```

```
         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                    <table border="0" cellpadding="0" cellspacing="0">
                        <tr>
                            <td height="100%" align
...
...
...
```

L Cacheable SSL Page Found 5 TOC

Issue 1 of 5 TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	DXR.axd (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /DXR.axd?r=1_147-i3tS8 HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
```

```
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:50 GMT
Content-Length: 34742

var __aspxStateItemsExist = false;
var __aspxFocusedItemKind = "FocusedStateItem";
var __aspxHoverItemKind = "HoverStateItem";
var __aspxPressedItemKind = "PressedStateItem";
var __aspxSelectedItemKind = "SelectedStateItem";
var __aspxDisabledItemKind = "DisabledStateItem";
var __aspxCachedStatePrefix = "cached";
ASPxStateItem = _aspxCreateClass(null, {
 constructor: function(name, classNames, cssTexts, postfixes, imageObjs, imagePostfixes, kind,
disableApplyingStyleToLink){
  this.name = name;
  this.classNames = classNames;
  this.customClassNames = [];
  this.resultClassNames = [];
  this.cssTexts = cssTexts;
  this.postfixes = postfixes;
  this.imageObjs = imageObjs;
  this.imagePostfixes = imagePostfixes;
  this.kind = kind;
  this.classNamePostfix = kind.substr(0, 1).toLowerCase();
  this.enabled = true;
  this.needRefreshBetweenElements = false;
  this.elements = null;
  this.images = null;
  this.linkColor = null;
  this.lintTextDecoration = null;
  this.disableApplyingStyleToLink = !!disableApplyingStyleToLink;
 },
 GetCssText: function(index){
  if(_aspxIsExists(this.cssTexts[index]))
   return this.cssTexts[index];
  return this.cssTexts[0];
 },
 CreateStyleRule: function(index){
  if(this.GetCssText(index) == "") return "";
  var styleSheet = _aspxGetCurrentStyleSheet();
  if(styleSheet)
   return _aspxCreateImportantStyleRule(styleSheet, this.GetCssText(index),
this.classNamePostfix);
  return "";
 },
 GetClassName: function(index){
  if(_aspxIsExists(this.classNames[index]))
   return this.classNames[index];
  return this.classNames[0];
 },
 GetResultClassName: function(index){
  if(!_aspxIsExists(this.resultClassNames[index])) {
   if(!_aspxIsExists(this.customClassNames[index]))
    this.customClassNames[index] = this.CreateStyleRule(index);
   if(this.GetClassName(index) != "" && this.customClassNames[index] != "")
    this.resultClassNames[index] = this.GetClassName(index) + " " + this.customClassNames[index];
   else if(this.GetClassName(index) != "")
    this.resultClassNames[index] = this.GetClassName(index);
   else if(this.customClassNames[index] != "")
    this.resultClassNames[index] = this.customClassNames[index];
   else
    this.resultClassNames[index] = "";
  }
  return this.resultClassNames[index];
 },
 GetElements: function(element){
  if(!this.elements || !_aspxIsValidElements(this.elements)){
   if(this.postfixes && this.postfixes.length > 0){
    this.elements = [ ];
    var parentNode = element.parentNode;
    if(parentNode){
     for(var i = 0; i < this.postfixes.length; i++){
      var id = this.name + this.postfixes[i];
      this.elements[i] = _aspxGetChildById(parentNode, id);
      if(!this.elements[i])
       this.elements[i] = _aspxGetElementById(id);
     }
    }
   }
   else
    this.elements = [element];
  }
  return this.elements;
 },
 GetImages: function(element){
  if(!this.images || !_aspxIsValidElements(this.images)){
   this.images = [ ];
   if(this.imagePostfixes && this.imagePostfixes.length > 0){
    var elements = this.GetElements(element);
    for(var i = 0; i < this.imagePostfixes.length; i++){
     var id = this.name + this.imagePostfixes[i];
     for(var j = 0; j < elements.length; j++){
      if(!elements[j]) continue;
      if(elements[j].id == id)
       this.images[i] = elements[j];
      else
       this.images[i] = _aspxGetChildById(elements[j], id);
      if(this.images[i])
       break;
     }
    }
   }
  }
  return this.images;
 },
 Apply: function(element){
  if(!this.enabled) return;
  try{
   this.ApplyStyle(element);
   if(this.imageObjs && this.imageObjs.length > 0)
    this.ApplyImage(element);
  }
  catch(e){
  }
 },
 ApplyStyle: function(element){
  var elements = this.GetElements(element);
  for(var i = 0; i < elements.length; i++){
   if(!elements[i]) continue;
   var className = elements[i].className.replace(this.GetResultClassName(i), "");
   elements[i].className = _aspxTrim(className) + " " + this.GetResultClassName(i);
   if(!__aspxOpera || __aspxBrowserVersion >= 9)
    this.ApplyStyleToLinks(elements, i);
  }
 },
 ApplyStyleToLinks: function(elements, index){
  if(this.disableApplyingStyleToLink)
   return;
  var linkCount = 0;
  var savedLinkCount = -1;

...
...
...
```

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/webresource.axd
Entity:	WebResource.axd (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m1BKCj... HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript
Expires: Thu, 16 Aug 2018 11:27:34 GMT
Last-Modified: Wed, 30 Nov 2016 06:34:16 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:54 GMT
Content-Length: 23063

function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup,
actionUrl, trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) &&
(active.id.length > 0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback,
useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" +
WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
        var action = theForm.action || document.location.pathname, fragmentIndex =
action.indexOf('#');
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                if (/^https?\:\/\/.*$/gi.test(path)) {

...
...
...
```

Issue 3 of 5

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /Login.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:47 GMT
Content-Length: 36506
Set-Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512; path=/; HttpOnly


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
```

```
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
```

```
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                      </strong>
                  </div>
             </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

          </div></td>
 </tr><tr>
          <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

          </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                      <table border="0" cellpadding="0" cellspacing="0">
                           <tr>
                               <td height="100%" align="left" valign="middle">

...
...
...
```

Issue 4 of 5

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexx... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript; charset=utf-8
Expires: Thu, 16 Aug 2018 11:49:51 GMT
Last-Modified: Wed, 16 Aug 2017 11:49:51 GMT
Server: Microsoft-IIS/8.5
```

```
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:49 GMT
Content-Length: 319864

// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters,
expectedParameters, validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams,
validateParameterCount) {
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) ===
"undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params,
expectedParams, validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }

...
...
...
```

Issue 5 of 5

TOC

Cacheable SSL Page Found

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	login.aspx (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:51 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
```

```
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                    <table border="0" cellpadding="0" cellspacing="0">
                        <tr>
                            <td height="100%" align
...
...
...
```

L Direct Access to Administration Pages 2 TOC

Issue 1 of 2 TOC

Direct Access to Administration Pages

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/
Entity:	admin.aspx (Page)
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Causes:	The web server or application server are configured in an insecure way
Fix:	Apply proper authorization to administration scripts

Difference: **Path** manipulated from: `/Login.aspx` to: `/admin.aspx`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /admin.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:36:55 GMT
Content-Length: 128
Set-Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi; path=/; HttpOnly

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=yj1txs1d1sr5je40ceggariw
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
```

```
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">
```

```
         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>

...
...
...
```

Issue 2 of 2

TOC

Direct Access to Administration Pages

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Causes:	The web server or application server are configured in an insecure way
Fix:	Apply proper authorization to administration scripts

Difference: **Path** manipulated from: `/ScriptResource.axd` to: `admin/ScriptResource.axd`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEK... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:38:29 GMT
Content-Length: 177

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd">here</a>.</h2>
</body></html>


GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></sc
...
...
...
```

L Hidden Directory Detected 10

TOC

Issue 1 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/css/
Entity:	css/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/css/`

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.

Test Requests and Responses:

```
GET /css/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 2 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/data/
Entity:	data/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/data/`

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.

Test Requests and Responses:

```
GET /data/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 3 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/help/
Entity:	help/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/help/`

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.

Test Requests and Responses:

```
GET /help/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 4 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/images/
Entity:	images/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/images/`

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.

Test Requests and Responses:

```
GET /images/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 5 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/reports/
Entity:	reports/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/reports/`

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.

Test Requests and Responses:

```
GET /reports/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 6 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scripts/
Entity:	scripts/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/scripts/`

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.

Test Requests and Responses:

```
GET /scripts/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 7 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/services/
Entity:	services/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/services/`

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.

Test Requests and Responses:

```
GET /services/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 8 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/templates/
Entity:	templates/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/templates/`

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.

Test Requests and Responses:

```
GET /templates/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 9 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/uploads/
Entity:	uploads/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/uploads/`

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.

Test Requests and Responses:

```
GET /uploads/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

Issue 10 of 10

TOC

Hidden Directory Detected

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/cvs/
Entity:	cvs/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/Login.aspx` to: `/cvs/`

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.

Test Requests and Responses:

```
GET /cvs/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:33:27 GMT
Content-Length: 1233
```

L Microsoft ASP.NET Debugging Enabled 1 TOC

Issue 1 of 1 TOC

Microsoft ASP.NET Debugging Enabled

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/
Entity:	AppScan.aspx (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Disable Debugging on Microsoft ASP.NET

Difference: **Header** added to request: `stop-debug`
Path manipulated from: `/Login.aspx` to: `/AppScan.aspx`
Method manipulated from: `GET` to: `DEBUG`

Reasoning: AppScan sent a request in Debug mode. The response indicates that debugging support in ASP.NET can be enabled. This may allow access to information about the server and application.

Test Requests and Responses:

```
DEBUG /AppScan.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Command: stop-debug


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:32:57 GMT
Content-Length: 2

OK
```

L Missing "Content-Security-Policy" header 11 TOC

Issue 1 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	DXR.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /DXR.axd?r=1_147-i3tS8 HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:50 GMT
Content-Length: 34742

var __aspxStateItemsExist = false;
var __aspxFocusedItemKind = "FocusedStateItem";
var __aspxHoverItemKind = "HoverStateItem";
var __aspxPressedItemKind = "PressedStateItem";
var __aspxSelectedItemKind = "SelectedStateItem";
var __aspxDisabledItemKind = "DisabledStateItem";
var __aspxCachedStatePrefix = "cached";
ASPxStateItem = _aspxCreateClass(null, {
 constructor: function(name, classNames, cssTexts, postfixes, imageObjs, imagePostfixes, kind,
disableApplyingStyleToLink){
  this.name = name;
  this.classNames = classNames;
  this.customClassNames = [];
  this.resultClassNames = [];
  this.cssTexts = cssTexts;
  this.postfixes = postfixes;
  this.imageObjs = imageObjs;
  this.imagePostfixes = imagePostfixes;
  this.kind = kind;
  this.classNamePostfix = kind.substr(0, 1).toLowerCase();
  this.enabled = true;
  this.needRefreshBetweenElements = false;
  this.elements = null;
  this.images = null;
  this.linkColor = null;
  this.lintTextDecoration = null;
  this.disableApplyingStyleToLink = !!disableApplyingStyleToLink;
 },
 GetCssText: function(index){
  if(_aspxIsExists(this.cssTexts[index]))
   return this.cssTexts[index];
  return this.cssTexts[0];
 },
 CreateStyleRule: function(index){
  if(this.GetCssText(index) == "") return "";
  var styleSheet = _aspxGetCurrentStyleSheet();
  if(styleSheet)
   return _aspxCreateImportantStyleRule(styleSheet, this.GetCssText(index),
this.classNamePostfix);
  return "";
 },
 GetClassName: function(index){
  if(_aspxIsExists(this.classNames[index]))
   return this.classNames[index];
  return this.classNames[0];
 },
 GetResultClassName: function(index){
  if(!_aspxIsExists(this.resultClassNames[index])) {
   if(!_aspxIsExists(this.customClassNames[index]))
    this.customClassNames[index] = this.CreateStyleRule(index);
   if(this.GetClassName(index) != "" && this.customClassNames[index] != "")
    this.resultClassNames[index] = this.GetClassName(index) + " " + this.customClassNames[index];
   else if(this.GetClassName(index) != "")
    this.resultClassNames[index] = this.GetClassName(index);
   else if(this.customClassNames[index] != "")
    this.resultClassNames[index] = this.customClassNames[index];
   else
    this.resultClassNames[index] = "";
  }
  return this.resultClassNames[index];
 },
 GetElements: function(element){
  if(!this.elements || !_aspxIsValidElements(this.elements)){
   if(this.postfixes && this.postfixes.length > 0){
    this.elements = [ ];
    var parentNode = element.parentNode;
    if(parentNode){
     for(var i = 0; i < this.postfixes.length; i++){
      var id = this.name + this.postfixes[i];
      this.elements[i] = _aspxGetChildById(parentNode, id);
      if(!this.elements[i])
       this.elements[i] = _aspxGetElementById(id);
     }
    }
   }
   else
    this.elements = [element];
  }
  return this.elements;
 },
 GetImages: function(element){
  if(!this.images || !_aspxIsValidElements(this.images)){
   this.images = [ ];
   if(this.imagePostfixes && this.imagePostfixes.length > 0){
    var elements = this.GetElements(element);
    for(var i = 0; i < this.imagePostfixes.length; i++){
     var id = this.name + this.imagePostfixes[i];
     for(var j = 0; j < elements.length; j++){
      if(!elements[j]) continue;
      if(elements[j].id == id)
       this.images[i] = elements[j];
      else
       this.images[i] = _aspxGetChildById(elements[j], id);
      if(this.images[i])
       break;
     }
    }
   }
  }
  return this.images;
 },
 Apply: function(element){
  if(!this.enabled) return;
  try{
   this.ApplyStyle(element);
   if(this.imageObjs && this.imageObjs.length > 0)
    this.ApplyImage(element);
  }
  catch(e){
  }
 },
 ApplyStyle: function(element){
  var elements = this.GetElements(element);
  for(var i = 0; i < elements.length; i++){
   if(!elements[i]) continue;
   var className = elements[i].className.replace(this.GetResultClassName(i), "");
   elements[i].className = _aspxTrim(className) + " " + this.GetResultClassName(i);
   if(!__aspxOpera || __aspxBrowserVersion >= 9)
    this.ApplyStyleToLinks(elements, i);
  }
 },
 ApplyStyleToLinks: function(elements, index){
  if(this.disableApplyingStyleToLink)
   return;
  var linkCount = 0;
  var savedLinkCount = -1;

...
...
...
```

Issue 2 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/webresource.axd
Entity:	WebResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m1BKCj... HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript
Expires: Thu, 16 Aug 2018 11:27:34 GMT
Last-Modified: Wed, 30 Nov 2016 06:34:16 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:54 GMT
Content-Length: 23063

function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup,
actionUrl, trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) &&
(active.id.length > 0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback,
useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" +
WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
        var action = theForm.action || document.location.pathname, fragmentIndex =
action.indexOf('#');
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                if (/^https?\:\/\/.*$/gi.test(path)) {

...
...
...
```

Issue 3 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38128


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
```

```
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
```

```
...
...
```

Issue 4 of 11

TOC

Missing "Content-Security-Policy" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Entity:	salestrends.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /salestrends.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:44 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
```

```
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
```

```
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">

...
...
...
```

Issue 5 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexx... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript; charset=utf-8
Expires: Thu, 16 Aug 2018 11:49:51 GMT
Last-Modified: Wed, 16 Aug 2017 11:49:51 GMT
Server: Microsoft-IIS/8.5
```

```
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:49 GMT
Content-Length: 319864

// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters,
expectedParameters, validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams,
validateParameterCount) {
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) ===
"undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params,
expectedParams, validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }

...
...
...
```

Issue 6 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin.aspx
Entity:	admin.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /admin.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:36:55 GMT
Content-Length: 128
Set-Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi; path=/; HttpOnly

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=2wi0z5rr2gnuyi2xtk4wixco
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>

...
...
...
```

Issue 7 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/timeout.aspx
Entity:	timeout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
POST /timeout.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 571

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
refresh: 120;url=logout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:54 GMT
Content-Length: 15661


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><link rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3027-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=0_3172-iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3174-
iW248" />
    <style type="text/css">
   #progressBackgroundFilter {
    position:fixed;
    top:0px;
    bottom:0px;
    left:0px;
    right:0px;
    overflow:hidden;
    padding:0;
    margin:0;
    background-color:#000;
    filter:alpha(opacity=50);
    opacity:0.5;
    z-index:1000;
}#processMessage {
    position:fixed;
    top:30%;
    left:30%;
    padding:10px;
    width:14%;
    z-index:1001;
    background-color:#fff;
    border:solid 1px #000;
}
 </style>
    <title>

</title></head>
<body>
    <form name="form1" method="post" action="./timeout.aspx" id="form1">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFgYCAw88KwAJAQAPFgIeDl8hVXNlVmlld1N0YXRlZ.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
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();
    }
}
//]]>
</script>


<script src="/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m... type="text/javascript"></script>


<script src="/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQ... type="text/javascript"></script>
<script type="text/javascript">
//<![CDATA[
if (typeof(Sys) === 'undefined') throw new Error('ASP.NET Ajax client-side framework failed to
load.');
//]]>
</script>

<script src="/ScriptResource.axd?d=QboLriYDP1ZrRrfi-
wRmZTLBi570ymPqHln8bdyGSIUmxlNthrWBsBbCYpnaGowWCBQ_2... type="text/javascript"></script>
<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="4D335315" />
</div>
        <script type="text/javascript">
//<![CDATA[
Sys.WebForms.PageRequestManager._initialize('Scriptmanager1', 'form1', ['tUpdatePanel1',''], [],
[], 0, '');
//]]>
</script>

        <div id="UpdatePanel1">

                <div style="padding-left: 0px; padding-top: 3px">
                    <table width="100%" border="0" cellspacing="0" cellpadding="0">
                        <tr>
                            <td>&nbsp;</td>
                            <td width="810px" align="left" valign="middle">
                                <table width="810px" border="1" cellspacing="0" cellpadding="0"
bgcolor="White">
                                    <tr>
```

```
                                        <td height="56">
                                            <table width="100%">
                                                <tr>
                                                    <td align="left" valign="top" width="60%">
                                                        <div style="padding-left: 8px;">
                                                            <table cellpadding="0"
cellspacing="0" border="0">
                                                                <tr>
                                                                    <td>
                                                                        <img
src="images/RedPrairie_logo.png" />
                                                                    </td>
                                                                    <td>

...
...
...
```

Issue 8 of 11

TOC

### Missing "Content-Security-Policy" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:51 GMT
Content-Length: 36506
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
```

```
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                    <table border="0" cellpadding="0" cellspacing="0">
                        <tr>
                            <td height="100%" align
...
...
...
```

Issue 9 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/error_handling.aspx
Entity:	Error_handling.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1c1bhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
```

```
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Bl
...
...
...
```

Issue 10 of 11

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/logout.aspx
Entity:	logout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /logout.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
```

```
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-t
...
...
...
```

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEK... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:38:29 GMT
Content-Length: 177

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd">here</a>.</h2>
</body></html>


GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128
```

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></sc
...
...
...
```

L Missing "X-Content-Type-Options" header 11 TOC

Issue 1 of 11 TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	DXR.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /DXR.axd?r=1_147-i3tS8 HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
```

```
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:50 GMT
Content-Length: 34742

var __aspxStateItemsExist = false;
var __aspxFocusedItemKind = "FocusedStateItem";
var __aspxHoverItemKind = "HoverStateItem";
var __aspxPressedItemKind = "PressedStateItem";
var __aspxSelectedItemKind = "SelectedStateItem";
var __aspxDisabledItemKind = "DisabledStateItem";
var __aspxCachedStatePrefix = "cached";
ASPxStateItem = _aspxCreateClass(null, {
 constructor: function(name, classNames, cssTexts, postfixes, imageObjs, imagePostfixes, kind,
disableApplyingStyleToLink){
  this.name = name;
  this.classNames = classNames;
  this.customClassNames = [];
  this.resultClassNames = [];
  this.cssTexts = cssTexts;
  this.postfixes = postfixes;
  this.imageObjs = imageObjs;
  this.imagePostfixes = imagePostfixes;
  this.kind = kind;
  this.classNamePostfix = kind.substr(0, 1).toLowerCase();
  this.enabled = true;
  this.needRefreshBetweenElements = false;
  this.elements = null;
  this.images = null;
  this.linkColor = null;
  this.lintTextDecoration = null;
  this.disableApplyingStyleToLink = !!disableApplyingStyleToLink;
 },
 GetCssText: function(index){
  if(_aspxIsExists(this.cssTexts[index]))
   return this.cssTexts[index];
  return this.cssTexts[0];
 },
 CreateStyleRule: function(index){
  if(this.GetCssText(index) == "") return "";
  var styleSheet = _aspxGetCurrentStyleSheet();
  if(styleSheet)
   return _aspxCreateImportantStyleRule(styleSheet, this.GetCssText(index),
this.classNamePostfix);
  return "";
 },
 GetClassName: function(index){
  if(_aspxIsExists(this.classNames[index]))
   return this.classNames[index];
  return this.classNames[0];
 },
 GetResultClassName: function(index){
  if(!_aspxIsExists(this.resultClassNames[index])) {
   if(!_aspxIsExists(this.customClassNames[index]))
    this.customClassNames[index] = this.CreateStyleRule(index);
   if(this.GetClassName(index) != "" && this.customClassNames[index] != "")
    this.resultClassNames[index] = this.GetClassName(index) + " " + this.customClassNames[index];
   else if(this.GetClassName(index) != "")
    this.resultClassNames[index] = this.GetClassName(index);
   else if(this.customClassNames[index] != "")
    this.resultClassNames[index] = this.customClassNames[index];
   else
    this.resultClassNames[index] = "";
  }
  return this.resultClassNames[index];
 },
 GetElements: function(element){
  if(!this.elements || !_aspxIsValidElements(this.elements)){
   if(this.postfixes && this.postfixes.length > 0){
    this.elements = [ ];
    var parentNode = element.parentNode;
    if(parentNode){
     for(var i = 0; i < this.postfixes.length; i++){
      var id = this.name + this.postfixes[i];
      this.elements[i] = _aspxGetChildById(parentNode, id);
      if(!this.elements[i])
       this.elements[i] = _aspxGetElementById(id);
     }
    }
   }
   else
    this.elements = [element];
  }
  return this.elements;
 },
 GetImages: function(element){
  if(!this.images || !_aspxIsValidElements(this.images)){
   this.images = [ ];
   if(this.imagePostfixes && this.imagePostfixes.length > 0){
    var elements = this.GetElements(element);
    for(var i = 0; i < this.imagePostfixes.length; i++){
     var id = this.name + this.imagePostfixes[i];
     for(var j = 0; j < elements.length; j++){
      if(!elements[j]) continue;
      if(elements[j].id == id)
       this.images[i] = elements[j];
      else
       this.images[i] = _aspxGetChildById(elements[j], id);
      if(this.images[i])
       break;
     }
    }
   }
  }
  return this.images;
 },
 Apply: function(element){
  if(!this.enabled) return;
  try{
   this.ApplyStyle(element);
   if(this.imageObjs && this.imageObjs.length > 0)
    this.ApplyImage(element);
  }
  catch(e){
  }
 },
 ApplyStyle: function(element){
  var elements = this.GetElements(element);
  for(var i = 0; i < elements.length; i++){
   if(!elements[i]) continue;
   var className = elements[i].className.replace(this.GetResultClassName(i), "");
   elements[i].className = _aspxTrim(className) + " " + this.GetResultClassName(i);
   if(!__aspxOpera || __aspxBrowserVersion >= 9)
    this.ApplyStyleToLinks(elements, i);
  }
 },
 ApplyStyleToLinks: function(elements, index){
  if(this.disableApplyingStyleToLink)
   return;
  var linkCount = 0;
  var savedLinkCount = -1;

...
...
...
```

Issue 2 of 11

TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/webresource.axd
Entity:	WebResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m1BKCj... HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript
Expires: Thu, 16 Aug 2018 11:27:34 GMT
Last-Modified: Wed, 30 Nov 2016 06:34:16 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:54 GMT
Content-Length: 23063

function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup,
actionUrl, trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) &&
(active.id.length > 0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback,
useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" +
WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
        var action = theForm.action || document.location.pathname, fragmentIndex =
action.indexOf('#');
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                if (/^https?\:\/\/.*$/gi.test(path)) {

...
...
...
```

Issue 3 of 11

TOC

Missing "X-Content-Type-Options" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38128


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
```

```
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
```

```
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
...
...
```

Issue 4 of 11

TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Entity:	salestrends.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /salestrends.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

```
Date: Wed, 16 Aug 2017 12:37:44 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">

...
...
...
```

Issue 5 of 11

TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/timeout.aspx
Entity:	timeout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
POST /timeout.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 571

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
refresh: 120;url=logout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:54 GMT
Content-Length: 15661


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><link rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3027-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=0_3172-iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3174-
iW248" />
    <style type="text/css">
   #progressBackgroundFilter {
    position:fixed;
    top:0px;
    bottom:0px;
    left:0px;
    right:0px;
    overflow:hidden;
    padding:0;
    margin:0;
    background-color:#000;
    filter:alpha(opacity=50);
    opacity:0.5;
    z-index:1000;
}#processMessage {
    position:fixed;
    top:30%;
    left:30%;
    padding:10px;
    width:14%;
    z-index:1001;
    background-color:#fff;
    border:solid 1px #000;
}
 </style>
    <title>

</title></head>
<body>
    <form name="form1" method="post" action="./timeout.aspx" id="form1">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFgYCAw88KwAJAQAPFgIeDl8hVXNlVmlld1N0YXRlZ.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
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();
    }
}
//]]>
</script>


<script src="/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m... type="text/javascript"></script>


<script src="/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQ... type="text/javascript"></script>
<script type="text/javascript">
//<![CDATA[
if (typeof(Sys) === 'undefined') throw new Error('ASP.NET Ajax client-side framework failed to
load.');
//]]>
</script>

<script src="/ScriptResource.axd?d=QboLriYDP1ZrRrfi-
wRmZTLBi570ymPqHln8bdyGSIUmxlNthrWBsBbCYpnaGowWCBQ_2... type="text/javascript"></script>
<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="4D335315" />
</div>
        <script type="text/javascript">
//<![CDATA[
Sys.WebForms.PageRequestManager._initialize('Scriptmanager1', 'form1', ['tUpdatePanel1',''], [],
[], 0, '');
//]]>
</script>

        <div id="UpdatePanel1">

                <div style="padding-left: 0px; padding-top: 3px">
                    <table width="100%" border="0" cellspacing="0" cellpadding="0">
                        <tr>
                            <td>&nbsp;</td>
                            <td width="810px" align="left" valign="middle">
                                <table width="810px" border="1" cellspacing="0" cellpadding="0"
bgcolor="White">
                                    <tr>
                                        <td height="56">
                                            <table width="100%">
                                                <tr>
                                                    <td align="left" valign="top" width="60%">
                                                        <div style="padding-left: 8px;">
                                                            <table cellpadding="0"
cellspacing="0" border="0">
                                                                <tr>
                                                                    <td>
                                                                        <img
src="images/RedPrairie_logo.png" />
                                                                    </td>
                                                                    <td>

...
...
...
```

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexx... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript; charset=utf-8
Expires: Thu, 16 Aug 2018 11:49:51 GMT
Last-Modified: Wed, 16 Aug 2017 11:49:51 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:49 GMT
Content-Length: 319864

// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters,
expectedParameters, validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams,
validateParameterCount) {
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) ===
"undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params,
expectedParams, validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }

...
...
...
```

Issue 7 of 11

TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin.aspx
Entity:	admin.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /admin.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:36:55 GMT
Content-Length: 128
Set-Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi; path=/; HttpOnly

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=2wi0z5rr2gnuyi2xtk4wixco
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin.aspx
```

```
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
```

```
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>

...
...
...
```

Issue 8 of 11

TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
```

```
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:51 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
```

```
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                    <table border="0" cellpadding="0" cellspacing="0">
                        <tr>
                            <td height="100%" align
...
...
...
```

Issue 9 of 11

TOC

Missing "X-Content-Type-Options" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/error_handling.aspx
Entity:	Error_handling.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Bl
...
...
...
```

Issue 10 of 11

TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/logout.aspx
Entity:	logout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /logout.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
```

```
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
```

```
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-t
...
...
...
```

Issue 11 of 11

TOC

Missing "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEK... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:38:29 GMT
Content-Length: 177

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd">here</a>.</h2>
</body></html>


GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
```

```
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></sc
...
...
...
```

L Missing "X-XSS-Protection" header 11

TOC

Issue 1 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	DXR.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /DXR.axd?r=1_147-i3tS8 HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:50 GMT
Content-Length: 34742

var __aspxStateItemsExist = false;
var __aspxFocusedItemKind = "FocusedStateItem";
var __aspxHoverItemKind = "HoverStateItem";
var __aspxPressedItemKind = "PressedStateItem";
var __aspxSelectedItemKind = "SelectedStateItem";
var __aspxDisabledItemKind = "DisabledStateItem";
var __aspxCachedStatePrefix = "cached";
ASPxStateItem = _aspxCreateClass(null, {
 constructor: function(name, classNames, cssTexts, postfixes, imageObjs, imagePostfixes, kind,
disableApplyingStyleToLink){
  this.name = name;
  this.classNames = classNames;
  this.customClassNames = [];
  this.resultClassNames = [];
  this.cssTexts = cssTexts;
  this.postfixes = postfixes;
  this.imageObjs = imageObjs;
  this.imagePostfixes = imagePostfixes;
  this.kind = kind;
  this.classNamePostfix = kind.substr(0, 1).toLowerCase();
  this.enabled = true;
  this.needRefreshBetweenElements = false;
  this.elements = null;
  this.images = null;
  this.linkColor = null;
  this.lintTextDecoration = null;
  this.disableApplyingStyleToLink = !!disableApplyingStyleToLink;
 },
 GetCssText: function(index){
  if(_aspxIsExists(this.cssTexts[index]))
   return this.cssTexts[index];
  return this.cssTexts[0];
 },
 CreateStyleRule: function(index){
  if(this.GetCssText(index) == "") return "";
  var styleSheet = _aspxGetCurrentStyleSheet();
  if(styleSheet)
   return _aspxCreateImportantStyleRule(styleSheet, this.GetCssText(index),
this.classNamePostfix);
  return "";
 },
 GetClassName: function(index){
  if(_aspxIsExists(this.classNames[index]))
   return this.classNames[index];
  return this.classNames[0];
 },
 GetResultClassName: function(index){
  if(!_aspxIsExists(this.resultClassNames[index])) {
   if(!_aspxIsExists(this.customClassNames[index]))
    this.customClassNames[index] = this.CreateStyleRule(index);
   if(this.GetClassName(index) != "" && this.customClassNames[index] != "")
```

```
    this.resultClassNames[index] = this.GetClassName(index) + " " + this.customClassNames[index];
   else if(this.GetClassName(index) != "")
    this.resultClassNames[index] = this.GetClassName(index);
   else if(this.customClassNames[index] != "")
    this.resultClassNames[index] = this.customClassNames[index];
   else
    this.resultClassNames[index] = "";
  }
  return this.resultClassNames[index];
 },
 GetElements: function(element){
  if(!this.elements || !_aspxIsValidElements(this.elements)){
   if(this.postfixes && this.postfixes.length > 0){
    this.elements = [ ];
    var parentNode = element.parentNode;
    if(parentNode){
     for(var i = 0; i < this.postfixes.length; i++){
      var id = this.name + this.postfixes[i];
      this.elements[i] = _aspxGetChildById(parentNode, id);
      if(!this.elements[i])
       this.elements[i] = _aspxGetElementById(id);
     }
    }
   }
   else
    this.elements = [element];
  }
  return this.elements;
 },
 GetImages: function(element){
  if(!this.images || !_aspxIsValidElements(this.images)){
   this.images = [ ];
   if(this.imagePostfixes && this.imagePostfixes.length > 0){
    var elements = this.GetElements(element);
    for(var i = 0; i < this.imagePostfixes.length; i++){
     var id = this.name + this.imagePostfixes[i];
     for(var j = 0; j < elements.length; j++){
      if(!elements[j]) continue;
      if(elements[j].id == id)
       this.images[i] = elements[j];
      else
       this.images[i] = _aspxGetChildById(elements[j], id);
      if(this.images[i])
       break;
     }
    }
   }
  }
  return this.images;
 },
 Apply: function(element){
  if(!this.enabled) return;
  try{
   this.ApplyStyle(element);
   if(this.imageObjs && this.imageObjs.length > 0)
    this.ApplyImage(element);
  }
  catch(e){
  }
 },
 ApplyStyle: function(element){
  var elements = this.GetElements(element);
  for(var i = 0; i < elements.length; i++){
   if(!elements[i]) continue;
   var className = elements[i].className.replace(this.GetResultClassName(i), "");
   elements[i].className = _aspxTrim(className) + " " + this.GetResultClassName(i);
   if(!__aspxOpera || __aspxBrowserVersion >= 9)
    this.ApplyStyleToLinks(elements, i);
  }
 },
 ApplyStyleToLinks: function(elements, index){
  if(this.disableApplyingStyleToLink)
   return;
  var linkCount = 0;
  var savedLinkCount = -1;

...
...
```

```
...
```

Issue 2 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/webresource.axd
Entity:	WebResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m1BKCj... HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript
Expires: Thu, 16 Aug 2018 11:27:34 GMT
Last-Modified: Wed, 30 Nov 2016 06:34:16 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:54 GMT
Content-Length: 23063

function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup,
actionUrl, trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) &&
(active.id.length > 0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback,
useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" +
WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
        var action = theForm.action || document.location.pathname, fragmentIndex =
action.indexOf('#');
```

```
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                if (/^https?\:\/\/.*$/gi.test(path)) {

...
...
...
```

Issue 3 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
```

```
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38128


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
```

```
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
...
...
```

Issue 4 of 11

TOC

Missing "X-XSS-Protection" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Entity:	salestrends.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /salestrends.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
```

```
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:44 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
```

```
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">

...
...
...
```

Issue 5 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexx... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript; charset=utf-8
Expires: Thu, 16 Aug 2018 11:49:51 GMT
Last-Modified: Wed, 16 Aug 2017 11:49:51 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:49 GMT
Content-Length: 319864

// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters,
expectedParameters, validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams,
validateParameterCount) {
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) ===
"undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params,
expectedParams, validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }

...
...
...
```

Issue 6 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:51 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
```

```
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
```

```
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                    <table border="0" cellpadding="0" cellspacing="0">
                        <tr>
                            <td height="100%" align
...
...
...
```

Issue 7 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/timeout.aspx
Entity:	timeout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
POST /timeout.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 571

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
refresh: 120;url=logout.aspx
```

```
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:54 GMT
Content-Length: 15661


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><link rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3027-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=0_3172-iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3174-
iW248" />
    <style type="text/css">
   #progressBackgroundFilter {
    position:fixed;
    top:0px;
    bottom:0px;
    left:0px;
    right:0px;
    overflow:hidden;
    padding:0;
    margin:0;
    background-color:#000;
    filter:alpha(opacity=50);
    opacity:0.5;
    z-index:1000;
}#processMessage {
    position:fixed;
    top:30%;
    left:30%;
    padding:10px;
    width:14%;
    z-index:1001;
    background-color:#fff;
    border:solid 1px #000;
}
 </style>
    <title>

</title></head>
<body>
    <form name="form1" method="post" action="./timeout.aspx" id="form1">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFgYCAw88KwAJAQAPFgIeDl8hVXNlVmlld1N0YXRlZ.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
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();
    }
}
//]]>
</script>


<script src="/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m... type="text/javascript"></script>


<script src="/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQ... type="text/javascript"></script>
<script type="text/javascript">
//<![CDATA[
if (typeof(Sys) === 'undefined') throw new Error('ASP.NET Ajax client-side framework failed to
load.');
//]]>
</script>

<script src="/ScriptResource.axd?d=QboLriYDP1ZrRfi-
wRmZTLBi570ymPqHln8bdyGSIUmxlNthrWBsBbCYpnaGowWCBQ_2... type="text/javascript"></script>
<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="4D335315" />
</div>
        <script type="text/javascript">
//<![CDATA[
Sys.WebForms.PageRequestManager._initialize('Scriptmanager1', 'form1', ['tUpdatePanel1',''], [],
[], 0, '');
//]]>
</script>

        <div id="UpdatePanel1">

                <div style="padding-left: 0px; padding-top: 3px">
                    <table width="100%" border="0" cellspacing="0" cellpadding="0">
                        <tr>
                            <td>&nbsp;</td>
                            <td width="810px" align="left" valign="middle">
                                <table width="810px" border="1" cellspacing="0" cellpadding="0"
bgcolor="White">
                                    <tr>
                                        <td height="56">
                                            <table width="100%">
                                                <tr>
                                                    <td align="left" valign="top" width="60%">
                                                        <div style="padding-left: 8px;">
                                                            <table cellpadding="0"
cellspacing="0" border="0">
                                                                <tr>
                                                                    <td>
                                                                        <img
src="images/RedPrairie_logo.png" />
                                                                    </td>
                                                                    <td>

...
...
...
```

Issue 8 of 11

TOC

### Missing "X-XSS-Protection" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin.aspx
Entity:	admin.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /admin.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:36:55 GMT
Content-Length: 128
Set-Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi; path=/; HttpOnly

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=2wi0z5rr2gnuyi2xtk4wixco
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>
```

```
<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>

...
...
...
```

Issue 9 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/logout.aspx
Entity:	logout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /logout.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
```

```
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
```

```
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-t
...
...
...
```

Issue 10 of 11

TOC

Missing "X-XSS-Protection" header	
Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/error_handling.aspx
Entity:	Error_handling.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
```

```
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
```

```
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Bl
...
...
...
```

Issue 11 of 11

TOC

Missing "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEK... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:38:29 GMT
Content-Length: 177

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd">here</a>.</h2>
</body></html>


GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
```

```
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></sc
...
...
...
```

L Missing Cross-Frame Scripting Defence 2 TOC

Issue 1 of 2 TOC

Missing Cross-Frame Scripting Defence

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Frame-Options" header

Difference:

Reasoning: AppScan detected that the X-Frame-Options response header is missing, which may allow Cross-Frame Scripting attacks

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38128


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
```

```
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
```

```
...
...
```

Issue 2 of 2

TOC

Missing Cross-Frame Scripting Defence

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/logout.aspx
Entity:	logout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Frame-Options" header

Difference:

Reasoning: AppScan detected that the X-Frame-Options response header is missing, which may allow Cross-Frame Scripting attacks

Test Requests and Responses:

```
GET /logout.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
```

```
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-t
...
...
...
```

L Missing HTTP Strict-Transport-Security Header 11

TOC

Issue 1 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	DXR.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /DXR.axd?r=1_147-i3tS8 HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 200 OK
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:50 GMT
Content-Length: 34742

var __aspxStateItemsExist = false;
var __aspxFocusedItemKind = "FocusedStateItem";
var __aspxHoverItemKind = "HoverStateItem";
var __aspxPressedItemKind = "PressedStateItem";
var __aspxSelectedItemKind = "SelectedStateItem";
var __aspxDisabledItemKind = "DisabledStateItem";
var __aspxCachedStatePrefix = "cached";
ASPxStateItem = _aspxCreateClass(null, {
 constructor: function(name, classNames, cssTexts, postfixes, imageObjs, imagePostfixes, kind,
disableApplyingStyleToLink){
  this.name = name;
  this.classNames = classNames;
  this.customClassNames = [];
  this.resultClassNames = [];
  this.cssTexts = cssTexts;
  this.postfixes = postfixes;
  this.imageObjs = imageObjs;
  this.imagePostfixes = imagePostfixes;
  this.kind = kind;
  this.classNamePostfix = kind.substr(0, 1).toLowerCase();
  this.enabled = true;
  this.needRefreshBetweenElements = false;
  this.elements = null;
  this.images = null;
  this.linkColor = null;
  this.lintTextDecoration = null;
  this.disableApplyingStyleToLink = !!disableApplyingStyleToLink;
 },
 GetCssText: function(index){
  if(_aspxIsExists(this.cssTexts[index]))
   return this.cssTexts[index];
  return this.cssTexts[0];
 },
 CreateStyleRule: function(index){
  if(this.GetCssText(index) == "") return "";
  var styleSheet = _aspxGetCurrentStyleSheet();
  if(styleSheet)
   return _aspxCreateImportantStyleRule(styleSheet, this.GetCssText(index),
this.classNamePostfix);
  return "";
 },
 GetClassName: function(index){
  if(_aspxIsExists(this.classNames[index]))
   return this.classNames[index];
  return this.classNames[0];
 },
 GetResultClassName: function(index){
  if(!_aspxIsExists(this.resultClassNames[index])) {
   if(!_aspxIsExists(this.customClassNames[index]))
    this.customClassNames[index] = this.CreateStyleRule(index);
   if(this.GetClassName(index) != "" && this.customClassNames[index] != "")
    this.resultClassNames[index] = this.GetClassName(index) + " " + this.customClassNames[index];
   else if(this.GetClassName(index) != "")
    this.resultClassNames[index] = this.GetClassName(index);
   else if(this.customClassNames[index] != "")
    this.resultClassNames[index] = this.customClassNames[index];
   else
    this.resultClassNames[index] = "";
  }
  return this.resultClassNames[index];
 },
 GetElements: function(element){
  if(!this.elements || !_aspxIsValidElements(this.elements)){
   if(this.postfixes && this.postfixes.length > 0){
    this.elements = [ ];
    var parentNode = element.parentNode;
    if(parentNode){
     for(var i = 0; i < this.postfixes.length; i++){
      var id = this.name + this.postfixes[i];
      this.elements[i] = _aspxGetChildById(parentNode, id);
      if(!this.elements[i])
       this.elements[i] = _aspxGetElementById(id);
     }
    }
   }
   else
    this.elements = [element];
  }
  return this.elements;
 },
 GetImages: function(element){
  if(!this.images || !_aspxIsValidElements(this.images)){
   this.images = [ ];
   if(this.imagePostfixes && this.imagePostfixes.length > 0){
    var elements = this.GetElements(element);
    for(var i = 0; i < this.imagePostfixes.length; i++){
     var id = this.name + this.imagePostfixes[i];
     for(var j = 0; j < elements.length; j++){
      if(!elements[j]) continue;
      if(elements[j].id == id)
       this.images[i] = elements[j];
      else
       this.images[i] = _aspxGetChildById(elements[j], id);
      if(this.images[i])
       break;
     }
    }
   }
  }
  return this.images;
 },
 Apply: function(element){
  if(!this.enabled) return;
  try{
   this.ApplyStyle(element);
   if(this.imageObjs && this.imageObjs.length > 0)
    this.ApplyImage(element);
  }
  catch(e){
  }
 },
 ApplyStyle: function(element){
  var elements = this.GetElements(element);
  for(var i = 0; i < elements.length; i++){
   if(!elements[i]) continue;
   var className = elements[i].className.replace(this.GetResultClassName(i), "");
   elements[i].className = _aspxTrim(className) + " " + this.GetResultClassName(i);
   if(!__aspxOpera || __aspxBrowserVersion >= 9)
    this.ApplyStyleToLinks(elements, i);
  }
 },
 ApplyStyleToLinks: function(elements, index){
  if(this.disableApplyingStyleToLink)
   return;
  var linkCount = 0;
  var savedLinkCount = -1;

...
...
...
```

Issue 2 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/webresource.axd
Entity:	WebResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m1BKCj... HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript
Expires: Thu, 16 Aug 2018 11:27:34 GMT
Last-Modified: Wed, 30 Nov 2016 06:34:16 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:54 GMT
Content-Length: 23063

function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup,
actionUrl, trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) &&
(active.id.length > 0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback,
useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" +
WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
        var action = theForm.action || document.location.pathname, fragmentIndex =
action.indexOf('#');
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                 // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                 if (/^https?\:\/\/.*$/gi.test(path)) {

...
...
...
```

Issue 3 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	Login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2639

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38128


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
```

```
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
```

```
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
...
...
```

Issue 4 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Entity:	salestrends.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /salestrends.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:44 GMT
Content-Length: 128

<html><head><title>Object moved</title></head><body>
```

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/salestrends.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">

...
...
...
```

Issue 5 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexx... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
```

```
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript; charset=utf-8
Expires: Thu, 16 Aug 2018 11:49:51 GMT
Last-Modified: Wed, 16 Aug 2017 11:49:51 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:49 GMT
Content-Length: 319864

// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters,
expectedParameters, validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams,
validateParameterCount) {
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) ===
"undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params,
expectedParams, validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }

...
...
...
```

Issue 6 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/error_handling.aspx
Entity:	Error_handling.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
```

```
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
```

```
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Bl
...
...
...
```

Issue 7 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/timeout.aspx
Entity:	timeout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
POST /timeout.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 571

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
refresh: 120;url=logout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:54 GMT
Content-Length: 15661


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><link rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3027-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=0_3172-iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3174-
```

```
iW248" />
    <style type="text/css">
   #progressBackgroundFilter {
    position:fixed;
    top:0px;
    bottom:0px;
    left:0px;
    right:0px;
    overflow:hidden;
    padding:0;
    margin:0;
    background-color:#000;
    filter:alpha(opacity=50);
    opacity:0.5;
    z-index:1000;
}#processMessage {
    position:fixed;
    top:30%;
    left:30%;
    padding:10px;
    width:14%;
    z-index:1001;
    background-color:#fff;
    border:solid 1px #000;
}
 </style>
    <title>

</title></head>
<body>
    <form name="form1" method="post" action="./timeout.aspx" id="form1">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFgYCAw88KwAJAQAPFgIeDl8hVXNlVmlld1N0YXRlZ.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
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();
    }
}
//]]>
</script>


<script src="/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m... type="text/javascript"></script>


<script src="/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQ... type="text/javascript"></script>
<script type="text/javascript">
//<![CDATA[
if (typeof(Sys) === 'undefined') throw new Error('ASP.NET Ajax client-side framework failed to
load.');
//]]>
</script>

<script src="/ScriptResource.axd?d=QboLriYDP1ZrRrfi-
wRmZTLBi570ymPqHln8bdyGSIUmxlNthrWBsBbCYpnaGowWCBQ_2... type="text/javascript"></script>
<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="4D335315" />
</div>
        <script type="text/javascript">
//<![CDATA[
Sys.WebForms.PageRequestManager._initialize('Scriptmanager1', 'form1', ['tUpdatePanel1',''], [],
[], 0, '');
//]]>
</script>

        <div id="UpdatePanel1">

                <div style="padding-left: 0px; padding-top: 3px">
                    <table width="100%" border="0" cellspacing="0" cellpadding="0">
                        <tr>
                            <td>&nbsp;</td>
                            <td width="810px" align="left" valign="middle">
                                <table width="810px" border="1" cellspacing="0" cellpadding="0"
bgcolor="White">
                                    <tr>
                                        <td height="56">
                                            <table width="100%">
                                                <tr>
                                                    <td align="left" valign="top" width="60%">
                                                        <div style="padding-left: 8px;">
                                                            <table cellpadding="0"
cellspacing="0" border="0">
                                                                <tr>
                                                                    <td>
                                                                        <img
src="images/RedPrairie_logo.png" />
                                                                    </td>
                                                                    <td>

...
...
...
```

Issue 8 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	login.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
```

```
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:51 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
```

```
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;padding-bottom:10px;">
                    <table border="0" cellpadding="0" cellspacing="0">
                        <tr>
                            <td height="100%" align
...
...
...
```

Issue 9 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin/scriptresource.axd
Entity:	ScriptResource.axd (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEK... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:38:29 GMT
Content-Length: 177

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd">here</a>.</h2>
</body></html>


GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

```
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></sc
...
...
...
```

Issue 10 of 11 TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin.aspx
Entity:	admin.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /admin.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:36:55 GMT
Content-Length: 128
Set-Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi; path=/; HttpOnly

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=2wi0z5rr2gnuyi2xtk4wixco
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
```

```
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">
```

```
         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>

...
...
...
```

Issue 11 of 11

TOC

Missing HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/logout.aspx
Entity:	logout.aspx (Page)
Risk:	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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /logout.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=ixcfxi4mglaic0chaaoicodl
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Referer: https://md1npdvpadss02.dev.corp.local/logout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
```

```
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-t
...
...
...
```

L Query Parameter in SSL Request 8 TOC

Issue 1 of 8 TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/webresource.axd
Entity:	t (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
GET /WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m1BKCj... HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript
Expires: Thu, 16 Aug 2018 11:27:34 GMT
Last-Modified: Wed, 30 Nov 2016 06:34:16 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:54 GMT
Content-Length: 23063

function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup,
actionUrl, trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) &&
(active.id.length > 0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback,
useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" +
WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
        var action = theForm.action || document.location.pathname, fragmentIndex =
action.indexOf('#');
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                if (/^https?\:\/\/.*$/gi.test(path)) {

...
...
...
```

Issue 2 of 8

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/webresource.axd
Entity:	d (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
GET /WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m1BKCj... HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript
Expires: Thu, 16 Aug 2018 11:27:34 GMT
Last-Modified: Wed, 30 Nov 2016 06:34:16 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:54 GMT
Content-Length: 23063

function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup,
actionUrl, trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) &&
(active.id.length > 0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback,
useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" +
WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
        var action = theForm.action || document.location.pathname, fragmentIndex =
action.indexOf('#');
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                    if (/^https?\:\/\/.*$/gi.test(path)) {

...
...
...
```

Issue 3 of 8

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	r (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 4 of 8

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	t (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
GET /ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexx... HTTP/1.1
Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript; charset=utf-8
Expires: Thu, 16 Aug 2018 11:49:51 GMT
Last-Modified: Wed, 16 Aug 2017 11:49:51 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:08 GMT
Content-Length: 319864

// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
```

```
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters,
expectedParameters, validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams,
validateParameterCount) {
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) ===
"undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params,
expectedParams, validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }

...
...
...
```

Issue 5 of 8

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/scriptresource.axd
Entity:	d (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
GET /ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexx... HTTP/1.1
Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public
Content-Type: application/x-javascript; charset=utf-8
Expires: Thu, 16 Aug 2018 11:49:51 GMT
Last-Modified: Wed, 16 Aug 2017 11:49:51 GMT
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:37:08 GMT
Content-Length: 319864

// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//------------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//------------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters,
expectedParameters, validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams,
validateParameterCount) {
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) ===
"undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params,
expectedParams, validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }
```

```
...
...
...
```

Issue 6 of 8

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/error_handling.aspx
Entity:	aspxerrorpath (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
```

```
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Bl
...
...
...
```

Issue 7 of 8

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin/scriptresource.axd
Entity:	t (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
GET /admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEK... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:38:29 GMT
```

```
Content-Length: 177

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd">here</a>.</h2>
</body></html>


GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
```

```
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></sc
...
...
...
```

Issue 8 of 8

TOC

Query Parameter in SSL Request

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/admin/scriptresource.axd
Entity:	d (Parameter)
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

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

Test Requests and Responses:

```
GET /admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEK... HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:38:29 GMT
Content-Length: 177

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd">here</a>.</h2>
</body></html>


GET /Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?
d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK...
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /login.aspx
Server: Microsoft-IIS/8.5
refresh: 645;url=timeout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 128

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


GET /login.aspx HTTP/1.1
Cookie: ASP.NET_SessionId=b1clbhhs02ic5oznljbyww1p
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?
aspxerrorpath=/admin/ScriptResource.axd
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:08 GMT
Content-Length: 36506
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></sc
...
...
...
```

L Temporary File Download 1 TOC

Issue 1 of 1 TOC

Temporary File Download

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	DXR.axd (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Difference: **Path** manipulated from: `/DXR.axd` to: `/Copy%20of%20DXR.axd`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /Copy%20of%20DXR.axd?r=1_155-i3tS8 HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:14:09 GMT
Content-Length: 111531

var ASPx = {};
ASPx.SSLSecureBlankUrl = "/DXR.axd?r=1_0-i3tS8";
ASPx.EmptyImageUrl = "/DXR.axd?r=1_11-i3tS8";
var __aspxVersionInfo = "Version='13.2.5.0', File Version='13.2.5.0', Date Modified='6/5/2014
5:18:54 AM'";
var __aspxStyleSheet = null;
var __aspxInvalidDimension = -10000;
var __aspxInvalidPosition = -10000;
var __aspxAbsoluteLeftPosition = -10000;
var __aspxAbsoluteRightPosition = 10000;
var __aspxMenuZIndex = 21998;
var __aspxPopupControlZIndex = 11998;
var __aspxPopupShadowWidth = 5;
var __aspxPopupShadowHeight = 5;
var __aspxCallbackSeparator = ":";
var __aspxItemIndexSeparator = "i";
var __aspxCallbackResultPrefix = "/*DX*/";
var __aspxItemClassName = "dxi";
var __aspxAccessibilityEmptyUrl = "javascript:;";
var __aspxAccessibilityMarkerClass = "dxalink";
var __aspxEmptyAttributeValue = { };
var __aspxEmptyCachedValue = { };
var __aspxCachedRules = { };
var __aspxStyleCount = 0;
var __aspxStyleNameCache = { };
var __aspxPossibleNumberDecimalSeparators = [",", "."];
var __aspxAdaptiveClass = "dx-adaptive";
var __aspxCultureInfo = {
 twoDigitYearMax: 2029,
 ts: ":",
 ds: "/",
 am: "AM",
 pm: "PM",
 monthNames: ["January", "February", "March", "April", "May", "June", "July", "August",
"September", "October", "November", "December", ""],
 genMonthNames: null,
 abbrMonthNames: ["Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov",
"Dec", ""],
 abbrDayNames: ["Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"],
 dayNames: ["Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday"],
 numDecimalPoint: ".",
 numPrec: 2,
 numGroupSeparator: ",",
 numGroups: [ 3 ],
 numNegPattern: 1,
 numPosInf: "Infinity",
 numNegInf: "-Infinity",
 numNan: "NaN",
 currency: "$",
 currDecimalPoint: ".",
 currPrec: 2,
 currGroupSeparator: ",",
 currGroups: [ 3 ],
 currPosPattern: 0,
 currNegPattern: 0,
 percentPattern: 0,
 shortTime: "h:mm tt",
 longTime: "h:mm:ss tt",
 shortDate: "M/d/yyyy",
 longDate: "dddd, MMMM dd, yyyy",
 monthDay: "MMMM dd",
 yearMonth: "MMMM, yyyy"
};
__aspxCultureInfo.genMonthNames = __aspxCultureInfo.monthNames;
function _aspxGetInvariantDateString(date) {
 if(!date)
  return "01/01/0001";
 var day = date.getDate();
 var month = date.getMonth() + 1;
 var year = date.getFullYear();
 var result = "";
 if(month < 10)
  result += "0";
 result += month.toString() + "/";
 if(day < 10)
  result += "0";
 result += day.toString() + "/";
 if(year < 1000)
  result += "0";
 result += year.toString();
 return result;
}
function _aspxGetInvariantDateTimeString(date) {
 var dateTimeString = _aspxGetInvariantDateString(date);
 var time = {
  h: date.getHours(),
  m: date.getMinutes(),
  s: date.getSeconds()
 };
 for(var key in time) {
  var str = time[key].toString();
  if(str.length < 2)
   str = "0" + str;
  time[key] = str;
 }
 dateTimeString += " " + time.h + ":" + time.m + ":" + time.s;
 var msec = date.getMilliseconds();
 if(msec > 0)
  dateTimeString += "." + msec.toString();
 return dateTimeString;
}
function _aspxExpandTwoDigitYear(value) {
 value += 1900;
 if(value + 99 < __aspxCultureInfo.twoDigitYearMax)
  value += 100;
 return value;
}
function _aspxToUtcTime(date) {
 var result = new Date();
 result.setTime(date.valueOf() + 60000 * date.getTimezoneOffset());
 return result;
}
function _aspxToLocalTime(date) {
 var result = new Date();
 result.setTime(date.valueOf() - 60000 * date.getTimezoneOffset());
 return result;
}
function _aspxAreDatesEqualExact(date1, date2) {
 if(date1 == null && date2 == null)
  return true;
 if(date1 == null || date2 == null)
  return false;
 return date1.getTime() == date2.getTime();
}
function _aspxFixTimezoneGap(oldDate, newDate) {
 var diff = newDate.getHours() - oldDate.getHours();
 if(diff == 0)
  return;
 var sign = (diff == 1 || diff == -23) ? -1 : 1;
 var trial = new Date(newDate.getTime() + sign * 3600000);
 if(sign > 0 || trial.getDate() == newDate.getDate())
  newDate.setTime(trial.getTime());
}
var ASPxKey = {
 F1     : 112,
 F2     : 113,
 F3     : 114,
 F4     : 115,
 F5     : 116,
 F6     : 117,
 F7     : 118,
 F8     : 119,
 F9     : 120,
 F1
...
...
...
```

L Unencrypted __VIEWSTATE Parameter 2 TOC

Issue 1 of 2 TOC

Unencrypted __VIEWSTATE Parameter

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/login.aspx
Entity:	__VIEWSTATE (Parameter)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Modify your Web.Config file to encrypt the VIEWSTATE parameter

Difference:

Reasoning: AppScan decoded the __VIEWSTATE parameter value and found it to be unencrypted.

Test Requests and Responses:

```
POST /Login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 2612

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:57 GMT
Content-Length: 38205


<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3172-iW248" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3174-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3027-
iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3025-iW248" /><title>
 LOGIN TEMPLATE
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <style type="text/css">
        .style1
        {
            width: 251px;
        }
    </style>
</head>
<body>
    <form name="frmLogin" method="post" action="./Login.aspx" id="frmLogin">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD.
.. />
</div>

<script type="text/javascript">
```

```
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
</script>


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="C2EE9ABB" />
</div>
    <div align="center">
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <br />
        <input type="hidden"/><script id="dxis_369557409" src="/DXR.axd?r=1_155-i3tS8"
type="text/javascript"></script><script id="dxis_1899118280" src="/DXR.axd?r=1_87-i3tS8"
type="text/javascript"></script><script id="dxis_1345508920" src="/DXR.axd?r=1_106-i3tS8"
type="text/javascript"></script><script id="dxis_2035228747" src="/DXR.axd?r=1_113-i3tS8"
type="text/javascript"></script><script id="dxis_867212604" src="/DXR.axd?r=1_147-i3tS8"
type="text/javascript"></script><script id="dxis_1861735992" src="/DXR.axd?r=1_105-i3tS8"
type="text/javascript"></script><script id="dxis_1159806369" src="/DXR.axd?r=1_84-i3tS8"
type="text/javascript"></script><script id="dxis_226041151" src="/DXR.axd?r=1_139-i3tS8"
type="text/javascript"></script><script id="dxis_1881873727" src="/DXR.axd?r=1_137-i3tS8"
type="text/javascript"></script><script id="dxis_1677252152" src="/DXR.axd?r=1_108-i3tS8"
type="text/javascript"></script><script id="dxis_1756385571" src="/DXR.axd?r=1_98-i3tS8"
type="text/javascript"></script><table class="dxrpControl_Office2010Black" cellspacing="0"
cellpadding="0" id="ASPxRoundPanel1" border="0" style="width:517px;border-
collapse:collapse;border-collapse:separate;">
 <tr>
         <td><img class="dxWeb_rpHeaderTopLeftCorner_Office2010Black" src="/DXR.axd?
r=1_11-i3tS8" alt="" /></td><td class="dxrpTE"><div
style="height:1px;width:1px;overflow:hidden;font-size:1px;">

         </div></td><td><img class="dxWeb_rpHeaderTopRightCorner_Office2010Black"
src="/DXR.axd?r=1_11-i3tS8" alt="" /></td>
 </tr><tr>
         <td class="dxrpHLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td class="dxrpHeader_Office2010Black" style="padding-
left:9px;padding-right:11px;padding-top:3px;padding-bottom:6px;">
                <div style="padding-left: 13px; padding-top: 2px">
                    <strong>
                        <span class="dxeBase_Office2010Black"
id="ASPxRoundPanel1_HTC_ASPxLabel1">Welcome...Please login below</span>
                    </strong>
                </div>
            </td><td class="dxrpHRE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td>
 </tr><tr>
         <td class="dxrpLE"><div style="height:1px;width:1px;overflow:hidden;font-
size:1px;">

         </div></td><td id="ASPxRoundPanel1_RPC" class="dxrp dxrpcontent"
style="width:100%;padding-left:9px;padding-right:11px;padding-top:10px;paddin
...
...
...
```

Issue 2 of 2

TOC

Unencrypted __VIEWSTATE Parameter

Severity:	Low
CVSS Score:	5.0
URL:	https://md1npdvpadss02.dev.corp.local/timeout.aspx
Entity:	__VIEWSTATE (Parameter)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Modify your Web.Config file to encrypt the VIEWSTATE parameter

Difference:

Reasoning: AppScan decoded the __VIEWSTATE parameter value and found it to be unencrypted.

Test Requests and Responses:

```
POST /timeout.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: ASP.NET_SessionId=anb24vgkocow4szzzqtqbybi
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/timeout.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 571

__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFg.
..

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
refresh: 120;url=logout.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:16:10 GMT
Content-Length: 15661


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><link rel="stylesheet" type="text/css" href="/DXR.axd?r=1_8-i3tS8" /><link
rel="stylesheet" type="text/css" href="/DXR.axd?r=1_4-i3tS8" /><link rel="stylesheet"
type="text/css" href="/DXR.axd?r=0_3027-iW248" /><link rel="stylesheet" type="text/css"
href="/DXR.axd?r=0_3172-iW248" /><link rel="stylesheet" type="text/css" href="/DXR.axd?r=0_3174-
iW248" />
    <style type="text/css">
   #progressBackgroundFilter {
    position:fixed;
    top:0px;
    bottom:0px;
    left:0px;
    right:0px;
    overflow:hidden;
    padding:0;
    margin:0;
    background-color:#000;
    filter:alpha(opacity=50);
    opacity:0.5;
    z-index:1000;
}#processMessage {
    position:fixed;
    top:30%;
    left:30%;
    padding:10px;
    width:14%;
    z-index:1001;
    background-color:#fff;
    border:solid 1px #000;
}
 </style>
    <title>

</title></head>
<body>
    <form name="form1" method="post" action="./timeout.aspx" id="form1">
<div>
<input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
<input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFgYCAw88KwAJAQAPFgIeDl8hVXNlVmlld1N0YXRlZ.
.. />
</div>

<script type="text/javascript">
//<![CDATA[
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();
    }
}
//]]>
</script>


<script src="/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-
iWCQbDJTd7nCCwzp1m... type="text/javascript"></script>


<script src="/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-
j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQ... type="text/javascript"></script>
<script type="text/javascript">
//<![CDATA[
if (typeof(Sys) === 'undefined') throw new Error('ASP.NET Ajax client-side framework failed to
load.');
//]]>
</script>

<script src="/ScriptResource.axd?d=QboLriYDP1ZrRrfi-
wRmZTLBi570ymPqHln8bdyGSIUmxlNthrWBsBbCYpnaGowWCBQ_2... type="text/javascript"></script>
<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="4D335315" />
</div>
        <script type="text/javascript">
//<![CDATA[
Sys.WebForms.PageRequestManager._initialize('Scriptmanager1', 'form1', ['tUpdatePanel1',''], [],
[], 0, '');
//]]>
</script>

        <div id="UpdatePanel1">

                <div style="padding-left: 0px; padding-top: 3px">
                    <table width="100%" border="0" cellspacing="0" cellpadding="0">
                        <tr>
                            <td>&nbsp;</td>
                            <td width="810px" align="left" valign="middle">
                                <table width="810px" border="1" cellspacing="0" cellpadding="0"
bgcolor="White">
                                    <tr>
                                        <td height="56">
                                            <table width="100%">
                                                <tr>
                                                    <td align="left" valign="top" width="60%">
                                                        <div style="padding-left: 8px;">
                                                            <table cellpadding="0"
cellspacing="0" border="0">
                                                                <tr>
                                                                    <td>
                                                                        <img
src="images/RedPrairie_logo.png" />
                                                                    </td>
                                                                    <td>

...
...
...
```

I Application Test Script Detected 2 TOC

Issue 1 of 2 TOC

Application Test Script Detected

Severity:	Informational
CVSS Score:	0.0
URL:	https://md1npdvpadss02.dev.corp.local/
Entity:	test.aspx (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove test scripts from the server

Difference: **Path** manipulated from: `/Login.aspx` to: `/test.aspx`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /test.aspx HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:32:30 GMT
Content-Length: 612
Set-Cookie: ASP.NET_SessionId=43n1001f1oq5cjya11lzkhvp; path=/; HttpOnly



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
<head><title>
 Untitled Page
</title></head>
<body>
    <form name="form1" method="post" action="./test.aspx" id="form1">
```

```
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUJNzgzNDMwNTMzZGQyMef9v4mVmuClA1XDzWEapK2qZbVcBnjYlgIdPcGoMw==" />
</div>

<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR"
value="75BBA7D6" />
</div>

    </form>
</body>
</html>
```

Issue 2 of 2

TOC

Application Test Script Detected

Severity:	Informational
CVSS Score:	0.0
URL:	https://md1npdvpadss02.dev.corp.local/help/
Entity:	test.html (Page)
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove test scripts from the server

Difference: **Path** manipulated from: `/help/` to: `/help/test.html`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /help/test.html HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Fri, 05 Mar 2010 17:01:06 GMT
Accept-Ranges: bytes
ETag: "0f5d57185bcca1:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:44:20 GMT
Content-Length: 719

<table>
    <tr>
        <td valign="top">
            <img src="images/help/customer_lookup.jpg"></td>
    </tr>
    <tr>
```

```
        <td>
            Enter lookup information for your customer. Wild card can be used to expand your
            searches. For example, entering JO% in the first name field will return results
            such as ""JOE"", ""JOHN"", ""JOCELYN"". Placing a % sign anywhere within your search
            criteria will act as a wild card. If your customer is new and does not have an
existing
            customer code, enternig their data and doing a search will automatically populate
            their new customer file with the search data.
        </td>
    </tr>
</table>
```

I Client-Side (JavaScript) Cookie References 1 TOC

Issue 1 of 1 TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://md1npdvpadss02.dev.corp.local/dxr.axd
Entity:	var ASPx = {}; (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Causes:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Difference:

Reasoning: AppScan found a reference to cookies in the JavaScript.

Test Requests and Responses:

```
GET /DXR.axd?r=1_155-i3tS8 HTTP/1.1
Cookie: ASP.NET_SessionId=2tayzw3g1nhtsf00fxfxc512
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://md1npdvpadss02.dev.corp.local/Login.aspx
Host: md1npdvpadss02.dev.corp.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko


HTTP/1.1 200 OK
Cache-Control: public, max-age=31536000
Content-Type: text/javascript
Expires: Fri, 05 Jun 2015 05:18:54 GMT
Last-Modified: Thu, 05 Jun 2014 05:18:54 GMT
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 16 Aug 2017 12:12:48 GMT
Content-Length: 111531
```

```
var ASPx = {};
ASPx.SSLSecureBlankUrl = "/DXR.axd?r=1_0-i3tS8";
ASPx.EmptyImageUrl = "/DXR.axd?r=1_11-i3tS8";
var __aspxVersionInfo = "Version='13.2.5.0', File Version='13.2.5.0', Date Modified='6/5/2014
5:18:54 AM'";
var __aspxStyleSheet = null;
var __aspxInvalidDimension = -10000;
var __aspxInvalidPosition = -10000;
var __aspxAbsoluteLeftPosition = -10000;
var __aspxAbsoluteRightPosition = 10000;
var __aspxMenuZIndex = 21998;
var __aspxPopupControlZIndex = 11998;
var __aspxPopupShadowWidth = 5;
var __aspxPopupShadowHeight = 5;
var __aspxCallbackSeparator = ":";
var __aspxItemIndexSeparator = "i";
var __aspxCallbackResultPrefix = "/*DX*/";
var __aspxItemClassName = "dxi";
var __aspxAccessibilityEmptyUrl = "javascript:;";
var __aspxAccessibilityMarkerClass = "dxalink";
var __aspxEmptyAttributeValue = { };
var __aspxEmptyCachedValue = { };
var __aspxCachedRules = { };
var __aspxStyleCount = 0;
var __aspxStyleNameCache = { };
var __aspxPossibleNumberDecimalSeparators = [",", "."];
var __aspxAdaptiveClass = "dx-adaptive";
var __aspxCultureInfo = {
 twoDigitYearMax: 2029,
 ts: ":",
 ds: "/",
 am: "AM",
 pm: "PM",
 monthNames: ["January", "February", "March", "April", "May", "June", "July", "August",
"September", "October", "November", "December", ""],
 genMonthNames: null,
 abbrMonthNames: ["Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov",
"Dec", ""],
 abbrDayNames: ["Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"],
 dayNames: ["Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday"],
 numDecimalPoint: ".",
 numPrec: 2,
 numGroupSeparator: ",",
 numGroups: [ 3 ],
 numNegPattern: 1,
 numPosInf: "Infinity",
 numNegInf: "-Infinity",
 numNan: "NaN",
 currency: "$",
 currDecimalPoint: ".",
 currPrec: 2,
 currGroupSeparator: ",",
 currGroups: [ 3 ],
 currPosPattern: 0,
 currNegPattern: 0,
 percentPattern: 0,
 shortTime: "h:mm tt",
 longTime: "h:mm:ss tt",
 shortDate: "M/d/yyyy",
 longDate: "dddd, MMMM dd, yyyy",
 monthDay: "MMMM dd",
 yearMonth: "MMMM, yyyy"
};
__aspxCultureInfo.genMonthNames = __aspxCultureInfo.monthNames;
function _aspxGetInvariantDateString(date) {
 if(!date)
  return "01/01/0001";
 var day = date.getDate();
 var month = date.getMonth() + 1;
 var year = date.getFullYear();
 var result = "";
 if(month < 10)
  result += "0";
 result += month.toString() + "/";
 if(day < 10)
  result += "0";
 result += day.toString() + "/";
 if(year < 1000)
```

```
  result += "0";
 result += year.toString();
 return result;
}
function _aspxGetInvariantDateTimeString(date) {
 var dateTimeString = _aspxGetInvariantDateString(date);
 var time = {
  h: date.getHours(),
  m: date.getMinutes(),
  s: date.getSeconds()
 };
 for(var key in time) {
  var str = time[key].toString();
  if(str.length < 2)
   str = "0" + str;
  time[key] = str;
 }
 dateTimeString += " " + time.h + ":" + time.m + ":" + time.s;
 var msec = date.getMilliseconds();
 if(msec > 0)
  dateTimeString += "." + msec.toString();
 return dateTimeString;
}
function _aspxExpandTwoDigitYear(value) {
 value += 1900;
 if(value + 99 < __aspxCultureInfo.twoDigitYearMax)
  value += 100;
 return value;
}
function _aspxToUtcTime(date) {
 var result = new Date();
 result.setTime(date.valueOf() + 60000 * date.getTimezoneOffset());
 return result;
}
function _aspxToLocalTime(date) {
 var result = new Date();
 result.setTime(date.valueOf() - 60000 * date.getTimezoneOffset());
 return result;
}
function _aspxAreDatesEqualExact(date1, date2) {
 if(date1 == null && date2 == null)
  return true;
 if(date1 == null || date2 == null)
  return false;
 return date1.getTime() == date2.getTime();
}
function _aspxFixTimezoneGap(oldDate, newDate) {
 var diff = newDate.getHours() - oldDate.getHours();
 if(diff == 0)
  return;
 var sign = (diff == 1 || diff == -23) ? -1 : 1;
 var trial = new Date(newDate.getTime() + sign * 3600000);
 if(sign > 0 || trial.getDate() == newDate.getDate())
  newDate.setTime(trial.getTime());
}
var ASPxKey = {
 F1     : 112,
 F2     : 113,
 F3     : 114,
 F4     : 115,
 F5     : 116,
 F6     : 117,
 F7     : 118,
 F8     : 119,
 F9     : 120,
 F10    : 121,
 F11    : 122,
 F12    : 123,
 Ctrl   : 17,
 Shift  : 16,
 Alt    : 18,

...
...
...
```

Fix Recommendations

M Add the 'Secure' attribute to all sensitive cookies TOC

Issue Types that this task fixes

- Missing Secure Attribute in Encrypted Session (SSL) Cookie

General

Basically the only required attribute for the cookie is the "name" field. Common optional attributes are: "comment", "domain", "path", etc.
The "secure" attribute must be set accordingly in order to prevent to cookie from being sent unencrypted.
For more information on how to set the secure flag, see OWASP "SecureFlag" at
https://www.owasp.org/index.php/SecureFlag

RFC 2965 states:
"The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin server whenever it sends back this cookie, to protect the confidentially and authenticity of the information in the cookie."
For further reference please see the HTTP State Management Mechanism RFC 2965 at:
http://www.ietf.org/rfc/rfc2965.txt
and for "Best current practice" for use of HTTP State Management please see
http://tools.ietf.org/html/rfc2964

M Change session identifier values after login TOC

Issue Types that this task fixes

- Session Identifier Not Updated

General

Prevent user ability to manipulate session ID. Do not accept session IDs provided by the user's browser at login; always generate a new session to which the user will log in if successfully authenticated.
Invalidate any existing session identifiers prior to authorizing a new user session.
For platforms such as ASP that do not generate new values for sessionid cookies, utilize a secondary cookie. In this approach, set a secondary cookie on the user's browser to a random value and set a session variable to the same value. If the session variable and the cookie value ever don't match, invalidate the session, and force the user to log on again.

M Configure your server to allow only required HTTP methods TOC

Issue Types that this task fixes

- Authentication Bypass Using HTTP Verb Tampering

General

If you use HTTP Method based access control, configure your web server to allow only required HTTP methods.

Make sure that the configuration indeed limits the non-listed methods:

In Apache .htaccess file: avoid using the problematic "LIMIT" directive. Use "LimitExcept" directive instead.
In JAVA EE: avoid using the <http-method> elements in access control policy.
In ASP.NET Authorization: use <deny verbs="*" users="*" /> after allowing a white list of required verbs.

M Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form TOC

Issue Types that this task fixes

- Cross-Site Request Forgery

General

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.

L Always use SSL and POST (body) parameters when sending sensitive information.

TOC

Issue Types that this task fixes

- Query Parameter in SSL Request

General

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.

L Apply proper authorization to administration scripts TOC

Issue Types that this task fixes

- Direct Access to Administration Pages

General

Do not allow access to administration scripts without proper authorization, as it may allow an attacker to gain privileged rights.

L Config your server to use the "Content-Security-Policy" header TOC

Issue Types that this task fixes

- Missing "Content-Security-Policy" header

General

Configure your server to send the "Content-Security-Policy" header.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

L Config your server to use the "X-Content-Type-Options" header TOC

Issue Types that this task fixes

- Missing "X-Content-Type-Options" header

General

Configure your server to send the "X-Content-Type-Options" header with value "nosniff" on all outgoing requests.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

L Config your server to use the "X-Frame-Options" header TOC

Issue Types that this task fixes

- Missing Cross-Frame Scripting Defence

General

Use the X-Frame-Options to prevent (or limit) pages from being embedded in iFrames. For older browser, include a "frame-breaker" script in each page that should not be framed.

L Config your server to use the "X-XSS-Protection" header TOC

Issue Types that this task fixes

- Missing "X-XSS-Protection" header

General

Configure your server to send the "X-XSS-Protection" header with value "1" (i.e. Enabled) on all outgoing requests.

For Apache, see:

http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

L Correctly set the "autocomplete" attribute to "off"

TOC

Issue Types that this task fixes

- Autocomplete HTML Attribute Not Disabled for Password Field

General

If the "autocomplete" attribute is missing in the "password" field of the "input" element, add it and set it to "off".
If the "autocomplete" attribute is set to "on", change it to "off".

For example:

Vulnerable site:

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" />
    <input type="submit" value="Submit" />
<form>
```

Non-vulnerable site:

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" autocomplete="off"/>
    <input type="submit" value="Submit" />
<form>
```

L Disable Debugging on Microsoft ASP.NET

TOC

Issue Types that this task fixes

- Microsoft ASP.NET Debugging Enabled

General

In order to disable debugging in ASP.NET, edit your web.config file to contain the following:

```
<compilation
    debug="false"
/>
```

L Implement the HTTP Strict-Transport-Security policy TOC

Issue Types that this task fixes

- Missing HTTP Strict-Transport-Security Header

General

Implement the The HTTP Strict Transport Security policy by adding the "Strict-Transport-Security" response header to the web application responses.
For more information please see
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

L Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely TOC

Issue Types that this task fixes

- Hidden Directory Detected

General

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.

L Modify your Web.Config file to encrypt the VIEWSTATE parameter TOC

Issue Types that this task fixes

- Unencrypted __VIEWSTATE Parameter

General

Add the following line to your Web.Config file, under the <system.web> element:

<machineKey validation="3DES" />

L Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses. TOC

Issue Types that this task fixes

- Cacheable SSL Page Found

General

Disable caching on all SSL pages or all pages that contain sensitive data.
This can be achieved by using "Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache" response directives in your SSL page headers.

Cache-Control: private - This directive instructs proxies that the page contains private information, and therefore should not be cached by a shared cache. However, it does not instruct browsers to refrain from caching the pages.

Cache-Control: no-cache - This directive also instructs proxies that the page contains private information, and therefore should not be cached. It also instructs the browser to revalidate with the server to check if a new version is available. This means that the browser may store sensitive pages or information to be used in the revalidation. Certain browsers do not necessarily follow the RFC and may treat no-cache as no-store.

Cache-Control: no-store - This is the most secure directive. It instructs both the proxy and the browser not to cache the page or store it in its cache folders.

Pragma: no-cache - This directive is required for older browsers, that do not support the Cache-Control header.

L Remove business and security logic from the client side TOC

Issue Types that this task fixes

- Client-Side (JavaScript) Cookie References

General

[1] Avoid placing business/security logic at the client side.
[2] Find and remove insecure client-side Javascript code which may pose a security threat to the site.

L Remove old versions of files from the virtual directory TOC

Issue Types that this task fixes

- Temporary File Download

General

Do not keep backup/temporary versions of files underneath the virtual web server root. This usually happens when editing these files "in place" by editors. Instead, when updating the site, move or copy the files to a directory outside the virtual root, edit them there, and move (or copy) the files back to the virtual root. Make sure that only the files that are actually in use reside under the virtual root.

L Remove test scripts from the server TOC

Issue Types that this task fixes

- Application Test Script Detected

General

Do not leave test/temporary scripts on the server and avoid doing so in the future.
Make sure there are no other scripts on the server that are not essential for its normal operation.

Advisories

Authentication Bypass Using HTTP Verb Tampering

TOC

Test Type:

Application-level test

Threat Classification:

Insufficient Authentication

Causes:

Insecure web application programming or configuration

Security Risks:

- It might be possible to escalate user privileges and gain administrative permissions over the web application
- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

References:

Bypassing VBAAC with HTTP Verb Tampering
Http Verb Tempering - Bypassing Web Authentication and Authorization

Technical Description:

Many web servers allow configuring access control using HTTP Methods (a.k.a Verbs), enabling access using one or more methods.
The problem is that many of those configuration implementations ALLOW access to methods that were not listed in the access control rule, resulting in access control breach.

Sample Exploit:

```
BOGUS /some_protected_resource.html HTTP/1.1
host: www.vulnerable_site.com
```

Cross-Site Request Forgery

TOC

Test Type:

Application-level test

Threat Classification:

Cross-site Request Forgery

Causes:

Insufficient authentication method was used by the application

Security Risks:

It may be 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

Affected Products:

CWE:

352

X-Force:

6784

References:

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

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.

Missing Secure Attribute in Encrypted Session (SSL) Cookie

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

The web application sends non-secure cookies over SSL

Security Risks:

It may be possible to steal user and session information (cookies) that was sent during an encrypted session

Affected Products:

CWE:

614

X-Force:

52696

References:

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

Technical Description:

During the application test, it was detected that the tested web application set a cookie without the "secure" attribute, during an encrypted session. Since this cookie does not contain the "secure" attribute, it might also be sent to the site during an unencrypted session. Any information such as cookies, session tokens or user credentials that are sent to the server as clear text, may be stolen and used later for identity theft or user impersonation.

In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site

Session Identifier Not Updated

TOC

Test Type:

Application-level test

Threat Classification:

Session Fixation

Causes:

Insecure web application programming or configuration

Security Risks:

It may be 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

Affected Products:

CWE:

304

X-Force:

52863

References:

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

Technical Description:

Authenticating a user, or otherwise establishing a new user session, without invalidating any existing session identifier, gives an attacker the opportunity to steal authenticated sessions.

Such a scenario is commonly observed when:
[1] A web application authenticates a user without first invalidating the existing session, thereby continuing to use the session already associated with the user
[2] An attacker is able to force a known session identifier on a user so that, once the user authenticates, the attacker has access to the authenticated session
[3] The application or container uses predictable session identifiers.

In the generic exploit of session fixation vulnerabilities, an attacker creates a new session on a web application and records the associated session identifier. The attacker then causes the victim to associate, and possibly authenticate, against the server using that session identifier, giving the attacker access to the user's account through the active session.

AppScan has found that the session identifiers before and after the login process were not updated, which means that user impersonation may be possible. Preliminary knowledge of the session identifier value may enable a remote attacker to pose as a logged-in legitimate user.
The flow of attack:
a) An attacker uses the victim's browser to open the login form of the vulnerable site.
b) Once the form is open, the attacker writes down the session identifier value, and waits.
c) When the victim logs into the vulnerable site, his session identifier is not updated.
d) The attacker can then use the session identifier value to impersonate the victim user, and operate on his behalf.

The session identifier value can be obtained by utilizing a Cross-Site Scripting vulnerability, causing the victim's browser to use a predefined session identifier when contacting the vulnerable site, or by launching a Session Fixation attack that will cause the site to present a predefined session identifier to the victim's browser.

Autocomplete HTML Attribute Not Disabled for Password Field

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

It may be possible to bypass the web application's authentication mechanism

Affected Products:

CWE:

522

X-Force:

85989

Technical Description:

The "autocomplete" attribute has been standardized in the HTML5 standard. W3C's site states that the attribute has two states, "on" and "off", and that omitting it altogether is equivalent to setting it to "on".

This page is vulnerable since it does not set the "autocomplete" attribute to "off" for the "password" field in the "input" element.
This may enable an unauthorized user (with local access to an authorized client) to autofill the username and password fields, and thus log in to the site.

Cacheable SSL Page Found

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Sensitive information might have been cached by your browser

Security Risks:

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

Affected Products:

CWE:

525

X-Force:

52512

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.

Direct Access to Administration Pages

TOC

Test Type:

Application-level test

Threat Classification:

Predictable Resource Location

Causes:

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

Security Risks:

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

CWE:

306

X-Force:

52579

Technical Description:

A common user can access certain pages on a site through simple surfing (i.e. following web links). However, there might be pages and scripts that are not accessible through simple surfing, (i.e. pages and scripts that are not linked). An attacker may be able to access these pages by guessing their name, e.g. admin.php, admin.asp, admin.cgi, admin.html, etc.

Example request for a script named "admin.php":
http://[SERVER]/admin.php

Access to administration scripts should not be allowed without proper authorization, as it may allow an attacker to gain privileged rights.

Sample Exploit:
http://[SERVER]/admin.php
http://[SERVER]/admin.asp
http://[SERVER]/admin.aspx
http://[SERVER]/admin.html
http://[SERVER]/admin.cfm
http://[SERVER]/admin.cgi

Hidden Directory Detected

TOC

Test Type:

Infrastructure test

Threat Classification:

Information Leakage

Causes:

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

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

Affected Products:

X-Force:

52599

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.

Microsoft ASP.NET Debugging Enabled

TOC

Test Type:

Infrastructure test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

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

Affected Products:

X-Force:

949

References:

Vendor site
Debugging ASP.NET Web Application
HOW TO: Disable Debugging for ASP.NET Applications

Technical Description:

Microsoft ASP.NET is vulnerable to information disclosure. An attacker can send a malicious request which informs whether debugging support is enabled.
An attacker may be able to send malicious requests using the DEBUG verb.

Sample Exploit:

```
DEBUG /AppScan.aspx HTTP/1.0
Command: stop-debug
Content-Length: 0
```

Missing "Content-Security-Policy" header

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- 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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

References:

List of useful HTTP headers
An Introduction to Content Security Policy

Technical Description:

The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in it's pages.

Missing "X-Content-Type-Options" header

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- 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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

References:

List of useful HTTP headers
Reducing MIME type security risks

Technical Description:

The "X-Content-Type-Options" header (with "nosniff" value) prevents IE and Chrome from ignoring the content-type of a response.
This action may prevent untrusted content (e.g. user uploaded content) from being executed on the user browser (after a malicious naming, for example).

Missing "X-XSS-Protection" header

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- 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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

References:

List of useful HTTP headers
IE XSS Filter

Technical Description:

The "X-XSS-Protection" header forces the Cross-Site Scripting filter into Enable mode, even if disabled by the user. This filter is built into most recent web browsers (IE 8+, Chrome 4+), and is usually enabled by default. Although it is not designed as first and only defence against Cross-Site Scripting, it acts as an additional layer of protection.

Missing Cross-Frame Scripting Defence

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- 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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

CWE:

693

References:

Cross-Frame Scripting
Clickjacking

Technical Description:

Cross-Frame Scripting is an attack technique where an attacker loads a vulnerable application in an iFrame on his malicious site.
The attacker can then launch a Clickjacking attack, which may lead to Phishing, Cross-Site Request Forgery, sensitive information leakage, and more.

Sample Exploit:
Within a malicious site, it is possible to embed the vulnerable page:
<frame src="http://vulnerable.com/login.html">

Missing HTTP Strict-Transport-Security Header

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

- 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 persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

References:

OWASP "HTTP Strict Transport Security"
HSTS Spec

Technical Description:

HTTP Strict Transport Security (HSTS) is a mechanism which protects secure (HTTPS) websites from being downgraded to non-secure HTTP. This mechanism enables web servers to instuct their clients (web browsers or other user agents) to use secure HTTPS connections when interacting with the server, and never use the insecure HTTP protocol.

The HTTP Strict Transport Security policy is communicated by the server to its clients using a response header named "Strict-Transport-Security". The value of this header is a period of time during which the client should access the server in HTTPS only. Other header attributes include "includeSubDomains" and "preload".

Query Parameter in SSL Request

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

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

Security Risks:

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

Affected Products:

CWE:

598

X-Force:

52845

References:

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

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.

Temporary File Download

TOC

Test Type:

Infrastructure test

Threat Classification:

Predictable Resource Location

Causes:

Temporary files were left in production environment

Security Risks:

It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Affected Products:

X-Force:

52887

References:

WASC Threat Classification: Predictable Resource Location

Technical Description:

Web servers usually associate Common Gateway Interface (CGI) filename extensions, such as .pl, with a handler, such as Perl. When a URL path ends with .pl, the filename designated in the path is sent to Perl for execution; the file contents are not returned to the browser. However, when the script files are edited in place, the editor may save a backup copy of the edited script with a new file extension, such as .bak, .sav, .old, ~, etc. The web server usually does not have a specific handler for these extensions. If the attacker requests one of these files, the file contents are sent directly to the browser.
It is important to remove these temporary files from under the virtual directory, as they may contain sensitive information that was used for debugging purposes, or they may reveal application logic that is different than the current logic, but may still be exploited.

Unencrypted __VIEWSTATE Parameter

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Insecure web application programming or configuration

Security Risks:

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

Affected Products:

CWE:

311

X-Force:

52470

References:

Vendor site
Taking a bite out of ASP.NET ViewState

Technical Description:

An ASP.NET server control inherits a property named ViewState from Control that enables it to participate easily in state management. The type of ViewState is System.Web.UI.StateBag, which is a dictionary that stores name/value pairs. ViewState is persisted to a string variable by the ASP.NET page framework and is sent to the client and back as a hidden variable. Upon postback, the page framework parses the input string from the hidden variable and populates the ViewState property of each control. If a control uses ViewState for property data instead of a private field, that property will automatically be persisted across round trips to the client. (If a property is not persisted in ViewState, it is a good practice to return its default value on postback.)

The ViewState hidden parameter is base64-encoded to ensure that values are not altered during a roundtrip, regardless of the response/request encoding used by the application. There are three levels of ViewState security that can be applied:
1. Tamper-Proofing: You can instruct ASP.NET to append a hashcode to the ViewState field by setting the EnableViewStateMAC attribute:
<%@Page EnableViewStateMAC=true %>

EnableViewStateMAC can be set at the page or application level. Upon postback, ASP.NET will generate a hashcode for the ViewState data and compare it to the hashcode store in the posted value. If the two do not match, the ViewState data will be discarded, and the controls will revert to their original settings.

By default, ASP.NET generates the ViewState hashcode using the SHA1 algorithm. Alternatively, you can select the MD5 algorithm by setting <machineKey> in the machine.config file as follows:
<machineKey validation="MD5" />

2. Encryption: You can use encryption to protect the actual data values within the ViewState field. First, you must set EnableViewStatMAC="true", as above. Then set the machineKey validation type to 3DES. This instructs ASP.NET to encrypt the ViewState value using the Triple DES symmetric encryption algorithm.
<machineKey validation="3DES" />

3. ViewState Security on a Web Farm: By default, ASP.NET creates a random validation key and stores it in each server's Local Security Authority (LSA). In order to validate a ViewState field created on another server, the validationKey for both servers must be set to the same value. If you secure ViewState by any of the means listed above for an application running in a Web Farm configuration, you will need to provide a single, shared validation key for all of the servers.

The validation key is a string of 20 to 64 random, cryptographically-strong bytes, represented as 40 to 128 hexadecimal characters. Longer is more secure, so a 128-character key is recommended for machines that support it. For example:

<machineKey validation="SHA1" validationKey="
F3690E7A3143C185AB1089616A8B4D81FD55DD7A69EEAA3B32A6AE813ECEECD28DEA66A
23BEE42193729BD48595EBAFE2C2E765BE77E006330BC3B1392D7C73F" />
The System.Security.Cryptography namespace includes the RNGCryptoServiceProvider class that you can use to generate this string, as demonstrated in the following GenerateCryptoKey.aspx sample:

```
<%@ Page Language="c#" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<HTML>
    <body>
        <form runat="server">
        <H3>Generate Random Crypto Key</H3>
        <P>
            <asp:RadioButtonList id="RadioButtonList1"
            runat="server" RepeatDirection="Horizontal">
                <asp:ListItem Value="40">40-byte</asp:ListItem>
                <asp:ListItem Value="128" Selected="True">128-byte</asp:ListItem>
            </asp:RadioButtonList>&nbsp;
            <asp:Button id="Button1" runat="server" onclick="GenerateKey"
            Text="Generate Key">
            </asp:Button></P>
        <P>
            <asp:TextBox id="TextBox1" runat="server" TextMode="MultiLine"
            Rows="10" Columns="70" BackColor="#EEEEEE" EnableViewState="False">
            Copy and paste generated results</asp:TextBox></P>
        </form>
    </body>
</HTML>

<script runat=server>
```

```
       void GenerateKey(object sender, System.EventArgs e)
       {
           int keylength = Int32.Parse(RadioButtonList1.SelectedItem.Value);

          // Put user code to initialize the page here
            byte[] buff = new Byte[keylength/2];

            RNGCryptoServiceProvider rng = new RNGCryptoServiceProvider();

            // The array is now filled with cryptographically strong random bytes
            rng.GetBytes(buff);

            StringBuilder sb = new StringBuilder(keylength);
            int i;
            for (i = 0; i < buff.Length; i++) {
                sb.Append(String.Format("{0:X2}",buff[i]));
            }

            // paste to the textbox to the user can copy it out
            TextBox1.Text = sb.ToString();
        }

    </script>
```

By default, only the EnableViewStateMAC (Hashing) security measure is used by the .NET framework. If you do not explicitly turn on the encryption option, the ViewState information (the dictionary that stores name/value pairs) and the Controls' state are exposed to the attacker. This may help the attacker to learn the application logic, and may reveal sensitive information.

Application Test Script Detected

TOC

Test Type:

Application-level test

Threat Classification:

Predictable Resource Location

Causes:

Temporary files were left in production environment

Security Risks:

It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

CWE:

531

X-Force:

52497

Technical Description:

A common user can access certain pages on a site through simple surfing (i.e. following web links). However, there might be pages and scripts that are not accessible through simple surfing, (i.e. pages and scripts that are not linked). An attacker may be able to access these pages by guessing their name, e.g. test.php, test.asp, test.cgi, test.html, etc.

Example request for a script named "test.php":
http://[SERVER]/test.php

Sometimes developers forget to remove certain debugging or test pages from production environments. These pages may include sensitive information that should not be accessed by web users. They may also be vulnerable and/or help an attacker gain information about the server that will help leverage an attack.

Sample Exploit:
http://[SERVER]/test.php
http://[SERVER]/test.asp
http://[SERVER]/test.aspx
http://[SERVER]/test.html
http://[SERVER]/test.cfm
http://[SERVER]/test.cgi

Client-Side (JavaScript) Cookie References

TOC

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

Cookies are created at the client side

Security Risks:

The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side

Affected Products:

CWE:

602

X-Force:

52514

References:

WASC Threat Classification: Information Leakage

Technical Description:

A cookie is a piece of information usually created by the Web server and stored in the Web browser.
The cookie contains information used by web applications mainly (but not only) to identify users and maintain their state.

AppScan detected that the JavaScript code at the client side is used to manipulate (either create or modify) the site's cookies.
It is possible for an attacker to view this code, understand its logic, and use it to compose his own cookies, or modify existing ones, based on this knowledge.

The damage an attacker may cause depends on how the application uses its cookies, or what information it stores in them.
Among other things, cookie manipulation may lead to session hijacking or privilege escalation.
Other vulnerabilities caused by cookie poisoning contain SQL injection and Cross-Site scripting.

Application Data

Visited URLs 113

TOC

URL
https://md1npdvpadss02.dev.corp.local/Login.aspx
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_155-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_87-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_106-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_113-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_147-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_105-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_84-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_139-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_137-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_108-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_98-i3tS8
https://md1npdvpadss02.dev.corp.local/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-iWCQbDJTd7nCCwzp1m1BKCjyFi0Xe11j4ldudjAzkVMi1kJdSoA281&t=636160664560000000
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3172-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_8-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3174-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_4-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3027-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3025-iW248
https://md1npdvpadss02.dev.corp.local/Login.aspx
https://md1npdvpadss02.dev.corp.local/Login.aspx
https://md1npdvpadss02.dev.corp.local/Login.aspx
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_13-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_15-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_14-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_16-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3026-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3173-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3021-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3022-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3011-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3012-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3017-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3015-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3018-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3016-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3019-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3020-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3013-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3014-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_2999-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3007-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3005-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_2996-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_2998-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3002-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_2997-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3001-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3009-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3000-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3008-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3006-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3023-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3003-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3004-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3143-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3147-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3010-iW248

https://md1npdvpadss02.dev.corp.local/Login.aspx

https://md1npdvpadss02.dev.corp.local/Login.aspx

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3132-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3141-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3146-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3148-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3142-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3149-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3144-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3145-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3150-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3152-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3151-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3155-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3157-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3158-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3156-iW248

https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3154-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3153-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3167-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3175-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3176-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3178-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3179-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3180-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3181-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3182-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3171-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3169-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3170-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3136-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3139-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3137-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3138-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3159-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3164-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3166-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3165-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3168-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3161-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3162-iW248
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=0_3163-iW248
https://md1npdvpadss02.dev.corp.local/admin.aspx
https://md1npdvpadss02.dev.corp.local/login.aspx
https://md1npdvpadss02.dev.corp.local/timeout.aspx
https://md1npdvpadss02.dev.corp.local/logout.aspx
https://md1npdvpadss02.dev.corp.local/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0&t=2a48f442
https://md1npdvpadss02.dev.corp.local/ScriptResource.axd?d=QboLriYDP1ZrRrfi-wRmZTLBi570ymPqHln8bdyGSIUmxlNthrWBsBbCYpnaGowWCBQ_2B8-fWjqSoqrMavPsHiCSHUvz5TR0HV1PMmQ-5vfBAdmxms4rnUJolSGjFCK7y--6dPG2O3O2y2smVZeE_jmO-OylE4i15YuIcCYwN3kvw7yqlRFp306GxVn7qkG0&t=2a48f442
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_145-i3tS8
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_130-i3tS8
https://md1npdvpadss02.dev.corp.local/salestrends.aspx
https://md1npdvpadss02.dev.corp.local/timeout.aspx
https://md1npdvpadss02.dev.corp.local/timeout.aspx
https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0&t=2a48f442
https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd

Parameters 33

TOC

Name	Value	URL	Type
ASPxPopupControl1$txt_change_new_password2	kjp	https://md1npdvpadss02.dev.corp.local/Login.aspx	Password
__EVENTTARGET		https://md1npdvpadss02.dev.corp.local/timeout.aspx	Hidden
ASPxRoundPanel1$ImageButton1.y	0	https://md1npdvpadss02.dev.corp.local/Login.aspx	Image
t	2a48f442	https://md1npdvpadss02.dev.corp.local/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0&t=2a48f442	Simple Link
r	1_155-i3tS8 1_87-i3tS8 1_106-i3tS8 1_113-i3tS8 1_147-i3tS8 ...	https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_155-i3tS8	Simple Link
d	AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0	https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0&t=2a48f442	Simple Link
ASPxRoundPanel1$ASPxButt	Sign On	https://md1npdvpadss02.dev.corp.local/Login.aspx	Submit

on1			
__VIEWSTATEGENERATOR	4D335315	https://md1npdvpadss02.dev.corp.local/timeout.aspx	Hidden
t	636160664560000000	https://md1npdvpadss02.dev.corp.local/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-iWCQbDJTd7nCCwzp1m1BKCjyFi0Xe11j4ldudjAzkVMi1kJdSoA281&t=636160664560000000	Simple Link
t	2a48f442	https://md1npdvpadss02.dev.corp.local/admin/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0&t=2a48f442	Simple Link
ASPxRoundPanel1_cbo_co_cd_VI	SLS	https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden
__VIEWSTATE	/wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYCAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD2QWAgIBDzwrAAQBAA8WAh4PRGF0YVNvdXJjZUJvdW5kZ2RkAgIPZBYCAgEPZBYCZg9kFgQCAQ9kFgJmD2QWAgILDxQrAAYPFgIfAGdkZGQ8KwAJAQgUKwAEFggeClZhbHVlRmllbGQFBWNvX2NkHglUZXh0RmllbGQFCWZ1bGxfZGVzYx4SRW5hYmxlQ2FsbGJhY2tNb2RlaB4nRW5hYmxlU3luY2hyb25pemF0aW9uT25QZXJmb3JtQ2FsbGJhY2sgaGQPFgIeCklzU2F2ZWRBbGxnDxQrABQUKwABFggeBFRleHQFD0JaIC0gU2FuIFNpbWVvbh4FVmFsdWUFAkJaHghJbWFnZVVybGUeDlJ1bnRpbWVDcmVhdGVkZxQrAAEWCB8GBRFDMDEgLSBNYWN5J3Mg... /wEPDwULLTE1Mjk1ODY5NjYPZBYCAgMPZBYEAgEPZBYCZg9kFgJmD2QWBAIBD2QWAgIBD2QWAmYPZBYCZg9kFgJmD2QWAgIBDzwrAAQBAA8WAh4PRGF0YVNvdXJjZUJvdW5kZ2RkAgIPZBYCAgEPZBYCZg9kFgQCAQ9kFgJmD2QWCgIDDzwrAAYBAA8WAh4FVmFsdWUFA2tqcGRkAgcPPCsABgEADxYCHwEFA2tqcGRkAgsPFCsABg8WBB8AZx8BBQNTTFNkZGQ8KwAJAQgUKwAEFggeClZhbHVlRmllbGQFBWNvX2NkHglUZXh0RmllbGQFCWZ1bGxfZGVzYx4SRW5hYmxlQ2FsbGJhY2tNb2RlaB4nRW5hYmxlU3luY2hyb25pemF0aW9uT25QZXJmb3JtQ2FsbGJhY2sgaGQPFgIeCklzU2F2ZWRBbGxnDxQrABQUKwABFggeBFRleHQFD0JaIC0gU2FuIFNpbWVvbh8BBQJCWh4I...	https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden
DXScript	1_155,1_87,1_147,1_84,1_139,1_145,1_130	https://md1npdvpadss02.dev.corp.local/timeout.aspx	Hidden
ASPxRoundPanel	0:0:-1:-10000:-10000:0:-10000:-10000:1:0:0:0	https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden

1_cbo_co_cd_DDDWS			
__VIEWSTATEGENERATOR	C2EE9ABB	https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden
d	Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-iWCQbDJTd7nCCwzp1m1BKCjyFi0Xe11j4ldudjAzkVMi1kJdSoA281	https://md1npdvpadss02.dev.corp.local/WebResource.axd?d=Ymv0ijgZJnFGtWmd7XXVAt0dTbniD4WqrrEd9BEuiPqQQV5-7mu93-iWCQbDJTd7nCCwzp1m1BKCjyFi0Xe11j4ldudjAzkVMi1kJdSoA281&t=636160664560000000	Simple Link
ASPxPopupControl1$txt_change_new_password	kjp	https://md1npdvpadss02.dev.corp.local/Login.aspx	Password
d	AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0QboLriYDP1ZrRrfi-wRmZTLBi570ymPqHln8bdyGSIUmxlNthrWBsBbCYpnaGowWCBQ_2B8-fWjqSoqrMavPsHiCSHUvz5TR0HV1PMmQ-5vfBAdmxms4rnUJolSGjFCK7y--6dPG2O3O2y2smVZeE_jmO-OylE4i15YuIcCYwN3kvw7yqlRFp306GxVn7qkG0	https://md1npdvpadss02.dev.corp.local/ScriptResource.axd?d=AqRq1OiwjvWGB4ASa91DrCAyoeJjIKK4-j3e1WWagW0dm8YNfEwpTfdXOcjJK7zJzWEKQELexxvpjRUoLo9XBsV0YdgORmLKuzaMFNCveK6M5S4x35o-kPVBSUnRkOEJ7xFyztFDbUs2lJIFEl-wgIJzjeoYWxiVlC5ttjPIS-xfUtP7-uvQ2KDqxrBeIh2N0&t=2a48f442	Simple Link
__EVENTARGUMENT		https://md1npdvpadss02.dev.corp.local/timeout.aspx	Hidden
__EVENTARGUMENT		https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden
ASPxRoundPanel1$txtLogin	kjp	https://md1npdvpadss02.dev.corp.local/Login.aspx	Text
ASPxRoundPanel1$ImageButton1.x	0	https://md1npdvpadss02.dev.corp.local/Login.aspx	Image
ASPxRoundPanel	SLS	https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden

1$cbo_co_cd$DDD$L			
ASPxPopupControl1WS	0:0:-1:-10000:-10000:0:322px:-10000:1:0:0:0 1:0:-1:-10000:-10000:0:322px:-10000:1:0:0:0	https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden
ASPxRoundPanel1$cbo_co_cd	1234 SLS - SEQUEL LIVE SHOWCASE	https://md1npdvpadss02.dev.corp.local/Login.aspx	Text
DXScript	1_155,1_87,1_106,1_113,1_147,1_105,1_84,1_139,1_137,1_108,1_98	https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden
aspxerrorpath	/admin/ScriptResource.axd	https://md1npdvpadss02.dev.corp.local/Error_handling.aspx?aspxerrorpath=/admin/ScriptResource.axd	Simple Link
ASPxRoundPanel1$txt_co_password	kjp	https://md1npdvpadss02.dev.corp.local/Login.aspx	Password
ASPxRoundPanel1$txt_password	kjp	https://md1npdvpadss02.dev.corp.local/Login.aspx	Password
ASPxPopupControl1$txt_change_curr_password	kjp	https://md1npdvpadss02.dev.corp.local/Login.aspx	Password
ASPxPopupControl1$txt_change_username	kjp	https://md1npdvpadss02.dev.corp.local/Login.aspx	Text
__VIEWSTATE	/wEPDwULLTEzNDY5NjE4NTIPZBYCAgMPZBYCAgMPZBYCZg9kFgYCAw88KwAJAQAPFgIeDl8hVXNlVmlld1N0YXRlZ2RkAgQPPCsACQEADxYCHwBnZGQCBw88KwAEAQAPFgIeBVZhbHVlBXhZb3UgaGF2ZSBiZWVuIGluYWN0aXZlIGZvciAxMCBtaW51dGVzLiBZb3Ugd2lsbCBiZSBhdXRvbWF0aWNhbGx5IGxvZ2dlZCBvdXQgaW4gMiBtaW51dGVzIHVubGVzcyB5b3UgYmVnaW4gd29ya2luZyBhZ2Fpbi5kZBgBBR5fX0NvbnRyb2xzUmVxdWlyZVBvc3RCYWNrS2V5X18WAgUJQVNQeE1lbnUyBQlBU1B4TWVudTHzu2cqhvNMR1aCVUEsJFbpL/2Y6o1GTVymzqvTvV	https://md1npdvpadss02.dev.corp.local/timeout.aspx	Hidden

	gCNg==		
__EVENTTARGET		https://md1npdvpadss02.dev.corp.local/Login.aspx	Hidden

Failed Requests 18

TOC

URL	Reason
https://md1npdvpadss02.dev.corp.local/links[i].href;	Response Status '404' - Not Found
https://md1npdvpadss02.dev.corp.local/scripts[i].src;	Response Status '404' - Not Found
https://md1npdvpadss02.dev.corp.local/(this.allowLoadToHiddenIframe	Response Status '404' - Not Found
https://md1npdvpadss02.dev.corp.local/_aspxGetEventSource(evt);	Response Status '404' - Not Found
https://md1npdvpadss02.dev.corp.local/event.srcElement	Response Status '404' - Not Found
https://md1npdvpadss02.dev.corp.local/css/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/data/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/help/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/images/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/reports/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/scripts/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/services/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/templates/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/uploads/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/cvs/	Client Side Certificate Error
https://md1npdvpadss02.dev.corp.local/MicrosoftAjaxWebForms.js	Response Status '404' - Not Found
https://md1npdvpadss02.dev.corp.local/MicrosoftAjaxComponentModel.js	Response Status '404' - Not Found
https://md1npdvpadss02.dev.corp.local/MicrosoftAjaxSerialization.js	Response Status '404' - Not Found

Filtered URLs 12

TOC

URL	Reason
https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_11-i3tS8	Image Context
https://md1npdvpadss02.dev.corp.local/images/RedPrairie_logo.png	File Extension
https://md1npdvpadss02.dev.corp.local/images/login_icon.gif	File Extension
https://md1npdvpadss02.dev.corp.local/images/password.png	File Extension
https://md1npdvpadss02.dev.corp.local/Login.aspx	Similar DOM
https://md1npdvpadss02.dev.corp.local/Login.aspx	Similar DOM
https://md1npdvpadss02.dev.corp.local/images/warning.jpg	File Extension
https://md1npdvpadss02.dev.corp.local/images/spacer.gif	File Extension
http://www.redprairie.com/	Untested Web Server

https://md1npdvpadss02.dev.corp.local/newmain.aspx	Similar DOM
https://md1npdvpadss02.dev.corp.local/Reporting.aspx	Similar DOM
https://md1npdvpadss02.dev.corp.local/Utilities.aspx	Similar DOM

Comments 0

TOC

URL	Comment

JavaScripts 80

TOC

URL / Code

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<![CDATA[
var theForm = document.forms['frmLogin'];
if (!theForm) {
    theForm = document.frmLogin;
}
function __doPostBack(eventTarget, eventArgument) {
    if (!theForm.onsubmit || (theForm.onsubmit() != false)) {
        theForm.__EVENTTARGET.value = eventTarget;
        theForm.__EVENTARGUMENT.value = eventArgument;
        theForm.submit();
    }
}
//]]>
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxRoundPanel1_txtLogin');
window['ASPxRoundPanel1_txtLogin'] = dxo;
dxo.autoPostBack = true;
dxo.uniqueID = 'ASPxRoundPanel1$txtLogin';
dxo.initialFocused = true;
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxRoundPanel1_txt_password');
window['ASPxRoundPanel1_txt_password'] = dxo;
dxo.uniqueID = 'ASPxRoundPanel1$txt_password';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```


//<!--
aspxAddDisabledItems('ASPxRoundPanel1_cbo_co_cd_DDD_L',[[['dxeDisabled_Office2010Black'],[''],['']]]);

var dxo = new ASPxClientListBox('ASPxRoundPanel1_cbo_co_cd_DDD_L');
window['ASPxRoundPanel1_cbo_co_cd_DDD_L'] = dxo;
dxo.uniqueID = 'ASPxRoundPanel1$cbo_co_cd$DDD$L';
dxo.SelectedIndexChanged.AddHandler(function (s, e) {
aspxCBLBSelectedIndexChanged('ASPxRoundPanel1_cbo_co_cd', e); });
dxo.ItemClick.AddHandler(function (s, e) { aspxCBLBItemMouseUp('ASPxRoundPanel1_cbo_co_cd', e); });
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.itemsValue=
['BZ','C01','CAM','GRS','KA','KK','KPC','KZ','MAY','PIN','PSS','ROB','SAL','SLS','SQB','TSS','TST','VSJ','WWW
','ZZ'];
dxo.isComboBoxList = true;
dxo.hoverClasses=['dxeListBoxItemHover_Office2010Black'];
dxo.selectedClasses=['dxeListBoxItemSelected_Office2010Black'];
dxo.disabledClasses=['dxeDisabled_Office2010Black'];
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```


//<!--
aspxAddHoverItems('ASPxRoundPanel1_cbo_co_cd_DDD',[[['dxpc-closeBtnHover'],[''],['HCB-1']]]);

var dxo = new ASPxClientPopupControl('ASPxRoundPanel1_cbo_co_cd_DDD');
window['ASPxRoundPanel1_cbo_co_cd_DDD'] = dxo;
dxo.uniqueID = 'ASPxRoundPanel1$cbo_co_cd$DDD';
dxo.Shown.AddHandler(function (s, e) { aspxDDBPCShown('ASPxRoundPanel1_cbo_co_cd', e); });
dxo.adjustInnerControlsSizeOnShow=false;
dxo.popupAnimationType='slide';
dxo.closeAction='CloseButton';
dxo.popupHorizontalAlign='LeftSides';
dxo.popupVerticalAlign='Below';
dxo.isPopupPositionCorrectionOn=false;
dxo.width=0;
dxo.height=0;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```


//<!--
aspxAddHoverItems('ASPxRoundPanel1_cbo_co_cd',[[['dxeButtonEditButtonHover_Office2010Black'],[''],['B-1']]]);
```

```
aspxAddPressedItems('ASPxRoundPanel1_cbo_co_cd',[[['dxeButtonEditButtonPressed_Office2010Black'],[''],['B-
1']]]);
document.getElementById("ASPxRoundPanel1_cbo_co_cd_I").setAttribute("autocomplete", "off");

var dxo = new ASPxClientComboBox('ASPxRoundPanel1_cbo_co_cd');
window['ASPxRoundPanel1_cbo_co_cd'] = dxo;
dxo.autoPostBack = true;
dxo.uniqueID = 'ASPxRoundPanel1$cbo_co_cd';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.lastSuccessValue = null;
dxo.islastSuccessValueInit = true;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--
aspxAddHoverItems('ASPxRoundPanel1_ASPxButton1',[[['dxbButtonHover_Office2010Black'],[''],[''],['','TC']]]);
aspxAddPressedItems('ASPxRoundPanel1_ASPxButton1',[[['dxbButtonPressed_Office2010Black'],[''],[''],
['','TC']]]);

var dxo = new ASPxClientButton('ASPxRoundPanel1_ASPxButton1');
window['ASPxRoundPanel1_ASPxButton1'] = dxo;
dxo.autoPostBack = true;
dxo.uniqueID = 'ASPxRoundPanel1$ASPxButton1';
dxo.RegisterServerEventAssigned(['Click']);
aspxAddSelectedItems('ASPxRoundPanel1_ASPxButton1',[[['dxbf'],[''],['CD']]]);
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxPopupControl1_txt_change_username');
window['ASPxPopupControl1_txt_change_username'] = dxo;
dxo.uniqueID = 'ASPxPopupControl1$txt_change_username';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxPopupControl1_txt_change_curr_password');
window['ASPxPopupControl1_txt_change_curr_password'] = dxo;
dxo.uniqueID = 'ASPxPopupControl1$txt_change_curr_password';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxPopupControl1_txt_change_new_password');
window['ASPxPopupControl1_txt_change_new_password'] = dxo;
dxo.uniqueID = 'ASPxPopupControl1$txt_change_new_password';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxPopupControl1_txt_change_new_password2');
window['ASPxPopupControl1_txt_change_new_password2'] = dxo;
dxo.uniqueID = 'ASPxPopupControl1$txt_change_new_password2';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--
aspxAddHoverItems('ASPxPopupControl1_ASPxButton2',[[['dxbButtonHover_Office2010Black'],[''],[''],
['','TC']]]);
aspxAddPressedItems('ASPxPopupControl1_ASPxButton2',[[['dxbButtonPressed_Office2010Black'],[''],[''],
['','TC']]]);

var dxo = new ASPxClientButton('ASPxPopupControl1_ASPxButton2');
window['ASPxPopupControl1_ASPxButton2'] = dxo;
dxo.autoPostBack = true;
dxo.uniqueID = 'ASPxPopupControl1$ASPxButton2';
dxo.RegisterServerEventAssigned(['Click']);
aspxAddSelectedItems('ASPxPopupControl1_ASPxButton2',[[['dxbf'],[''],['CD']]]);
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientPopupControl('ASPxPopupControl1');
window['ASPxPopupControl1'] = dxo;
dxo.popupAnimationType='fade';
dxo.closeAction='CloseButton';
dxo.popupHorizontalAlign='WindowCenter';
dxo.popupVerticalAlign='WindowCenter';
dxo.isPopupPositionCorrectionOn=false;
dxo.width=322;
dxo.height=0;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
javascript:return WebForm_FireDefaultButton(event, 'ASPxRoundPanel1_ASPxButton1')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyUp('ASPxRoundPanel1_txtLogin', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
setTimeout('__doPostBack("ASPxRoundPanel1$txtLogin","")', 0)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxRoundPanel1_txtLogin')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxRoundPanel1_txtLogin')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxRoundPanel1_txtLogin', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxRoundPanel1_txt_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxRoundPanel1_txt_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxRoundPanel1_txt_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyUp('ASPxRoundPanel1_txt_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
return aspxDDDropDown('ASPxRoundPanel1_cbo_co_cd', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxETextChanged('ASPxRoundPanel1_cbo_co_cd')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxRoundPanel1_cbo_co_cd')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxRoundPanel1_cbo_co_cd')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxRoundPanel1_cbo_co_cd', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxBGotFocus('ASPxRoundPanel1_ASPxButton1')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyUp('ASPxPopupControl1_txt_change_username', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxPopupControl1_txt_change_username')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxPopupControl1_txt_change_username')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxPopupControl1_txt_change_username', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxPopupControl1_txt_change_curr_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxPopupControl1_txt_change_curr_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxPopupControl1_txt_change_curr_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyUp('ASPxPopupControl1_txt_change_curr_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxPopupControl1_txt_change_new_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxPopupControl1_txt_change_new_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxPopupControl1_txt_change_new_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyUp('ASPxPopupControl1_txt_change_new_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxPopupControl1_txt_change_new_password2')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxPopupControl1_txt_change_new_password2')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxPopupControl1_txt_change_new_password2', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyUp('ASPxPopupControl1_txt_change_new_password2', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxBGotFocus('ASPxPopupControl1_ASPxButton2')
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var ASPx = {};
ASPx.SSLSecureBlankUrl = "/DXR.axd?r=1_0-i3tS8";
ASPx.EmptyImageUrl = "/DXR.axd?r=1_11-i3tS8";
var __aspxVersionInfo = "Version='13.2.5.0', File Version='13.2.5.0', Date Modified='6/5/2014 5:18:54 AM'";
var __aspxStyleSheet = null;
var __aspxInvalidDimension = -10000;
var __aspxInvalidPosition = -10000;
var __aspxAbsoluteLeftPosition = -10000;
var __aspxAbsoluteRightPosition = 10000;
var __aspxMenuZIndex = 21998;
var __aspxPopupControlZIndex = 11998;
var __aspxPopupShadowWidth = 5;
var __aspxPopupShadowHeight = 5;
var __aspxCallbackSeparator = ":";
var __aspxItemIndexSeparator = "i";
var __aspxCallbackResultPrefix = "/*DX*/";
var __aspxItemClassName = "dxi";
var __aspxAccessibilityEmptyUrl = "javascript:;";
var __aspxAccessibilityMarkerClass = "dxalink";
var __aspxEmptyAttributeValue = { };
var __aspxEmptyCachedValue = { };
var __aspxCachedRules = { };
var __aspxStyleCount = 0;
var __aspxStyleNameCache = { };
var __aspxPossibleNumberDecimalSeparators = [",", "."];
var __aspxAdaptiveClass = "dx-adaptive";
var __aspxCultureInfo = {
 twoDigitYearMax: 2029,
 ts: ":",
 ds: "/",
 am: "AM",
 pm: "PM",
 monthNames: ["January", "February", "March", "April", "May", "June", "July", "August", "September",
"October", "November", "December", ""],
 genMonthNames: null,
 abbrMonthNames: ["Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec", ""],
 abbrDayNames: ["Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"],
 dayNames: ["Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday"],
 numDecimalPoint: ".",
 numPrec: 2,
 numGroupSeparator: ",",
 numGroups: [ 3 ],
 numNegPattern: 1,
 numPosInf: "Infinity",
 numNegInf: "-Infinity",
 numNan: "NaN",
 currency: "$",
 currDecimalPoint: ".",
 currPrec: 2,
 currGroupSeparator: ",",
 currGroups: [ 3 ],
 currPosPattern: 0,
 currNegPattern: 0,
 percentPattern: 0,
 shortTime: "h:mm tt",
 longTime: "h:mm:ss tt",
 shortDate: "M/d/yyyy",
 longDate: "dddd, MMMM dd, yyyy",
 monthDay: "MMMM dd",
 yearMonth: "MMMM, yyyy"
};
__aspxCultureInfo.genMonthNames = __aspxCultureInfo.monthNames;
function _aspxGetInvariantDateString(date) {
 if(!date)
  return "01/01/0001";
 var day = date.getDate();
 var month = date.getMonth() + 1;
 var year = date.getFullYear();
 var result = "";
 if(month < 10)
  result += "0";
 result += month.toString() + "/";
 if(day < 10)
  result += "0";
 result += day.toString() + "/";
 if(year < 1000)
  result += "0";
 result += year.toString();
 return result;
}
function _aspxGetInvariantDateTimeString(date) {
 var dateTimeString = _aspxGetInvariantDateString(date);
 var time = {
  h: date.getHours(),
  m: date.getMinutes(),
  s: date.getSeconds()
 };
 for(var key in time) {
  var str = time[key].toString();
  if(str.length < 2)
   str = "0" + str;
  time[key] = str;
 }
 dateTimeString += " " + time.h + ":" + time.m + ":" + time.s;
 var msec = date.getMilliseconds();
 if(msec > 0)
  dateTimeString += "." + msec.toString();
 return dateTimeString;
}
function _aspxExpandTwoDigitYear(value) {
 value += 1900;
 if(value + 99 < __aspxCultureInfo.twoDigitYearMax)
  value += 100;
 return value;
}
function _aspxToUtcTime(date) {
 var result = new Date();
 result.setTime(date.valueOf() + 60000 * date.getTimezoneOffset());
 return result;
}
function _aspxToLocalTime(date) {
 var result = new Date();
 result.setTime(date.valueOf() - 60000 * date.getTimezoneOffset());
 return result;
}
function _aspxAreDatesEqualExact(date1, date2) {
 if(date1 == null && date2 == null)
  return true;
 if(date1 == null || date2 == null)
  return false;
 return date1.getTime() == date2.getTime();
}
function _aspxFixTimezoneGap(oldDate, newDate) {
 var diff = newDate.getHours() - oldDate.getHours();
 if(diff == 0)
  return;
 var sign = (diff == 1 || diff == -23) ? -1 : 1;
 var trial = new Date(newDate.getTime() + sign * 3600000);
 if(sign > 0 || trial.getDate() == newDate.getDate())
  newDate.setTime(trial.getTime());
}
var ASPxKey = {
 F1     : 112,
 F2     : 113,
 F3     : 114,
 F4     : 115,
 F5     : 116,
 F6     : 117,
 F7     : 118,
 F8     : 119,
 F9     : 120,
 F10    : 121,
 F11    : 122,
 F12    : 123,
 Ctrl   : 17,
 Shift  : 16,
 Alt    : 18,
 Enter  : 13,
 Home   : 36,
 End    : 35,
 Left   : 37,
 Right  : 39,
 Up     : 38,
 Down   : 40,
 PageUp    : 33,
 PageDown  : 34,
 Esc    : 27,
 Space  : 32,
 Tab    : 9,
 Backspace : 8,
 Delete    : 46,
 Insert    : 45,
 ContextMenu  : 93,
 Windows   : 91,
 Decimal   : 110
};
var ASPxCallbackType = {
 Data: "d",
 Common: "c"
};
var ASPxWhiteSpaces = {
 0x0009: 1, 0x000a: 1, 0x000b: 1, 0x000c: 1, 0x000d: 1, 0x0020: 1, 0x0085: 1,
 0x00a0: 1, 0x1680: 1, 0x180e: 1, 0x2000: 1, 0x2001: 1, 0x2002: 1, 0x2003: 1,
 0x2004: 1, 0x2005: 1, 0x2006: 1, 0x2007: 1, 0x2008: 1, 0x2009: 1, 0x200a: 1,
 0x200b: 1, 0x2028: 1, 0x2029: 1,...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxClassesScriptParsed = false;
var __aspxDocumentLoaded = false;
ASPxClientEvent = _aspxCreateClass(null, {
 constructor: function() {
  this.handlerInfoList = [];
 },
 AddHandler: function(handler, executionContext) {
  if(typeof(executionContext) == "undefined")
   executionContext = null;
  var handlerInfo = ASPxClientEvent.CreateHandlerInfo(handler, executionContext);
  this.handlerInfoList.push(handlerInfo);
 },
 RemoveHandler: function(handler, executionContext) {
  this.removeHandlerByCondition(function(handlerInfo) {
   return handlerInfo.handler == handler &&
    (!executionContext || handlerInfo.executionContext == executionContext);
  });
 },
 removeHandlerByCondition: function(predicate) {
   for(var i = this.handlerInfoList.length - 1; i >= 0; i--) {
   var handlerInfo = this.handlerInfoList[i];
   if(predicate(handlerInfo))
    _aspxArrayRemoveAt(this.handlerInfoList, i);
  }
 },
 removeHandlerByControlName: function(controlName) {
  this.removeHandlerByCondition(function(handlerInfo) {
   return handlerInfo.executionContext &&
    handlerInfo.executionContext.name === controlName;
  });
 },
 ClearHandlers: function() {
  this.handlerInfoList.length = 0;
 },
 FireEvent: function(obj, args) {
  for(var i = 0; i < this.handlerInfoList.length; i++) {
   var handlerInfo = this.handlerInfoList[i];
   handlerInfo.handler.call(handlerInfo.executionContext, obj, args);
  }
 },
 InsertFirstHandler: function(handler, executionContext){
  if(typeof(executionContext) == "undefined")
   executionContext = null;
  var handlerInfo = ASPxClientEvent.CreateHandlerInfo(handler, executionContext);
  _aspxArrayInsert(this.handlerInfoList, handlerInfo, 0);
 },
 IsEmpty: function() {
  return this.handlerInfoList.length == 0;
 }
});
ASPxClientEvent.CreateHandlerInfo = function(handler, executionContext) {
 return {
  handler: handler,
  executionContext: executionContext
 };
};
```

```
ASPxClientEventArgs = _aspxCreateClass(null, {
 constructor: function() {
 }
});
ASPxClientEventArgs.Empty = new ASPxClientEventArgs();
ASPxClientCancelEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(){
  this.constructor.prototype.constructor.call(this);
  this.cancel = false;
 }
});
ASPxClientProcessingModeEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(processOnServer){
  this.constructor.prototype.constructor.call(this);
  this.processOnServer = processOnServer;
 }
});
ASPxClientProcessingModeCancelEventArgs = _aspxCreateClass(ASPxClientProcessingModeEventArgs, {
 constructor: function(processOnServer){
  this.constructor.prototype.constructor.call(this, processOnServer);
  this.cancel = false;
 }
});
ASPxClientBeginCallbackEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(command){
  this.constructor.prototype.constructor.call(this);
  this.command = command;
 }
});
ASPxClientEndCallbackEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(){
  this.constructor.prototype.constructor.call(this);
 }
});
ASPxClientCustomDataCallbackEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(result) {
  this.constructor.prototype.constructor.call(this);
  this.result = result;
 }
});
ASPxClientCallbackErrorEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(message){
  this.constructor.prototype.constructor.call(this);
  this.message = message;
  this.handled = false;
 }
});
ASPxClientControlsInitializedEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(isCallback) {
  this.isCallback = isCallback;
 }
});
ASPxClientAdaptiveLayoutChangingEventArgs = _aspxCreateClass(ASPxClientEventArgs, {
 constructor: function(){
  this.constructor.prototype.constructor.call(this);
  this.isAdaptiveView = false;
 }
});
ASPxClientControlCollection = _aspxCreateClass(null, {
 constructor: function(){
  this.elements = new Object();
  this.prevWndWidth = "";
  this.prevWndHeight = "";
  this.BeforeInitCallback = new ASPxClientEvent();
  this.ControlsInitialized = new ASPxClientEvent();
 },
 Add: function(element){
  this.elements[element.name] = element;
 },
 Remove: function(element) {
  this.elements[element.name] = null;
 },
 Get: function(name){
  return this.elements[name];
 },
 GetGlobal: function(name) {
  var result = window[name];
  return result && result.isASPxClientControl
```

```
   ? result
   : null;
 },
 GetByName: function(name){
  return this.Get(name) || this.GetGlobal(name);
 },
 ForEachControl: function(processFunc, context) {
  if(!context)
   context = this;
  for(var name in this.elements) {
   var control = this.elements[name];
   if(ASPxIdent.IsASPxClientControl(control))
    if(processFunc.call(context, control))
     return;
  }
 },
 AdjustControls: function(container) {
  if(typeof(container) == "undefined")
   containe...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxClientValidationStateNameSuffix = "$CVS";
ASPxClientEditBase = _aspxCreateClass(ASPxClientControl, {
 constructor: function(name) {
  this.constructor.prototype.constructor.call(this, name);
  this.EnabledChanged = new ASPxClientEvent();
 },
 InlineInitialize: function(){
  ASPxClientControl.prototype.InlineInitialize.call(this);
  this.InitializeEnabled();
 },
 InitializeEnabled: function() {
  this.SetEnabledInternal(this.clientEnabled, true);
 },
 GetValue: function() {
  var element = this.GetMainElement();
  if(_aspxIsExistsElement(element))
   return element.innerHTML;
  return "";
 },
 GetValueString: function(){
  var value = this.GetValue();
  return (value == null) ? null : value.toString();
 },
 SetValue: function(value) {
  if(value == null)
   value = "";
  var element = this.GetMainElement();
  if(_aspxIsExistsElement(element))
   element.innerHTML = value;
 },
 GetEnabled: function(){
  return this.enabled && this.clientEnabled;
 },
 SetEnabled: function(enabled){
  if(this.clientEnabled != enabled) {
   var errorFrameRequiresUpdate = this.GetIsValid && !this.GetIsValid();
   if(errorFrameRequiresUpdate && !enabled)
    this.UpdateErrorFrameAndFocus(false , null , true );
   this.clientEnabled = enabled;
   this.SetEnabledInternal(enabled, false);
   if(errorFrameRequiresUpdate && enabled)
    this.UpdateErrorFrameAndFocus(false );
   this.RaiseEnabledChangedEvent();
  }
 },
 SetEnabledInternal: function(enabled, initialization){
  if(!this.enabled) return;
  if(!initialization || !enabled)
   this.ChangeEnabledStateItems(enabled);
  this.ChangeEnabledAttributes(enabled);
  if(__aspxChrome) {
   var mainElement = this.GetMainElement();
   if(mainElement)
    mainElement.className = mainElement.className;
  }
 },
 ChangeEnabledAttributes: function(enabled){
 },
 ChangeEnabledStateItems: function(enabled){
 },
 RaiseEnabledChangedEvent: function(){
  if(!this.EnabledChanged.IsEmpty()){
   var args = new ASPxClientEventArgs();
   this.EnabledChanged.FireEvent(this, args);
  }
 },
 GetDecodeValue: function (value) {
  if (typeof (value) == "string" && value.length > 1)
   value = this.SimpleDecodeHtml(value);
  return value;
 },
 SimpleDecodeHtml: function (html) {
  return _aspxApplyReplacement(html, [
   [/&lt;/g, '<'],
   [/&amp;/g, '&'],
   [/&quot;/g, '"'],
   [/&#39;/g, '\'']
  ]);
 }
});
ASPxValidationPattern = _aspxCreateClass(null, {
 constructor: function(errorText) {
  this.errorText = errorText;
 }
});
ASPxRequiredFieldValidationPattern = _aspxCreateClass(ASPxValidationPattern, {
 constructor: function(errorText) {
  this.constructor.prototype.constructor.call(this, errorText);
 },
 EvaluateIsValid: function(value) {
  return value != null && (value.constructor == Array || _aspxTrim(value.toString()) != "");
 }
});
ASPxRegularExpressionValidationPattern = _aspxCreateClass(ASPxValidationPattern, {
 constructor: function(errorText, pattern) {
  this.constructor.prototype.constructor.call(this, errorText);
  this.pattern = pattern;
 },
 EvaluateIsValid: function(value) {
  if (value == null)
   return true;
  var strValue = value.toString();
  if (_aspxTrim(strValue).length == 0)
   return true;
  var regEx = new RegExp(this.pattern);
  var matches = regEx.exec(strValue);
  return matches != null && strValue == matches[0];
 }
});
function _aspxIsEditorFocusable(inputElement) {
 return _aspxIsFocusableCore(inputElement, function(container) {
  return container.getAttribute("errorFrame") == "errorFrame";
 });
}
var __aspxInvalidEditorToBeFocused = null;
ASPxValidationType = {
 PersonalOnValueChanged: "ValueChanged",
 PersonalViaScript: "CalledViaScript",
 MassValidation: "MassValidation"
};
ASPxErrorFrameDisplay = {
 None: "None",
 Static: "Static",
 Dynamic: "Dynamic"
};
ASPxEditElementSuffix = {
 ExternalTable: "_ET",
 ControlCell: "_CC",
 ErrorCell: "_EC",
 ErrorTextCell: "_ETC",
 ErrorImage: "_EI"
};
ASPxClientEdit = _aspxCreateClass(ASPxClientEditBase, {
 constructor: function(name) {
  this.constructor.prototype.constructor.call(this, name);
  this.isASPxClientEdit = true;
  this.inputElement = null;
  this.elementCache = { };
  this.convertEmptyStringToNull = true;
  this.readOnly = false;
  this.focused = false;
  this.focusEventsLocked = false;
  this.receiveGlobalMouseWheel = true;
  this.styleDecoration = null;
  this.widthCorrectionRequired = false;
  this.heightCorrectionRequired = false;
  this.customValidationEnabled = false;
  this.display = ASPxErrorFrameDisplay.Static;
  this.initialErrorText = "";
  this.causesValidation = false;
  this.validateOnLeave = true;
  this.validationGroup = "";
  this.sendPostBackWithValidation = null;
  this.validationPatterns = [];
  this.setFocusOnError = false;
  this.errorDisplayMode = "it";
  this.errorText = "";
  this.isValid = true;
  this.errorImageIsAssigned = fal...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxTEInputSuffix = "_I";
var __aspxTERawInputSuffix = "_Raw";
var __aspxPasteCheckInterval = 50;
ASPxEditorStretchedInputElementsManager = _aspxCreateClass(null, {
 constructor: function() {
  this.targetEditorNames = { };
 },
 Initialize: function() {
  this.InitializeTargetEditorsList();
 },
 InitializeTargetEditorsList: function() {
  aspxGetControlCollection().ForEachControl(function(control) {
   if(this.targetEditorNames[control.name])
    return;
   if(ASPxIdent.IsASPxClientTextEdit(control) && control.WidthCorrectionRequired()) {
    var inputElement = control.GetInputElement();
    if(inputElement && _aspxIsPercentageSize(inputElement.style.width))
     this.targetEditorNames[control.name] = true;
   }
  }, this);
 },
 HideInputElementsExceptOf: function(exceptedEditor) {
  var collection = aspxGetControlCollection();
  for(var editorName in this.targetEditorNames) {
   if(typeof(editorName) != "string")
    continue;
   var editor = collection.Get(editorName);
   if(!ASPxIdent.IsASPxClientEdit(editor)) continue;
   if(editor && editor != exceptedEditor) {
    var input = editor.GetInputElement();
    if(input) {
     var existentSavedDisplay = input._dxSavedDisplayAttr;
     if(!_aspxIsExists(existentSavedDisplay)) {
      input._dxSavedDisplayAttr = input.style.display;
      input.style.display = "none";
     }
    }
   }
  }
 },
 ShowInputElements: function() {
  var collection = aspxGetControlCollection();
  for(var editorName in this.targetEditorNames) {
   if(typeof(editorName) != "string")
    continue;
   var editor = collection.Get(editorName);
   if(!ASPxIdent.IsASPxClientEdit(editor)) continue;
   if(editor) {
    var input = editor.GetInputElement();
    if(input) {
     var savedDisplay = input._dxSavedDisplayAttr;
     if(_aspxIsExists(savedDisplay)) {
      input.style.display = savedDisplay;
      _aspxRemoveAttribute(input, "_dxSavedDisplayAttr");
     }
    }
   }
  }
 }
});
var __aspxEditorStretchedInputElementsManager = null;
function _aspxGetEditorStretchedInputElementsManager() {
 if(!__aspxEditorStretchedInputElementsManager)
  __aspxEditorStretchedInputElementsManager = new ASPxEditorStretchedInputElementsManager();
 return __aspxEditorStretchedInputElementsManager;
}
ASPxClientBrowserHelper = {
 SAFARI_SYSTEM_CLASS_NAME: "dxeSafariSys",
 MOBILE_SAFARI_SYSTEM_CLASS_NAME: "dxeIPadSys",
 GetBrowserSpecificSystemClassName: function() {
  if (__aspxSafari)
   return __aspxMacOSMobilePlatform ? this.MOBILE_SAFARI_SYSTEM_CLASS_NAME : this.SAFARI_SYSTEM_CLASS_NAME;
  return "";
 }
},
ASPxClientTextEdit = _aspxCreateClass(ASPxClientEdit, {
 constructor: function(name) {
  this.constructor.prototype.constructor.call(this, name);
  this.isASPxClientTextEdit = true;
  this.nullText = "";
  this.escCount = 0;
  this.raiseValueChangedOnEnter = true;
  this.autoResizeWithContainer = false;
  this.lastChangedValue = null;
  this.helpText = "";
  this.helpTextObj = null;
  this.helpTextStyle = [];
  this.helpTextPosition = ASPxClientTextEditHelpTextPosition.Right;
  this.helpTextMargins = null;
  this.helpTextHAlign = ASPxClientTextEditHelpTextHAlign.Left;
  this.helpTextVAlign = ASPxClientTextEditHelpTextVAlign.Top;
  this.enableHelpTextPopupAnimation = true;
  this.helpTextDisplayMode = ASPxClientTextEditHelpTextDisplayMode.Inline;
  this.maskInfo = null;
  this.maskValueBeforeUserInput = "";
  this.maskPasteTimerID = -1;
  this.maskPasteLock = false;
  this.maskPasteCounter = 0;
  this.maskTextBeforePaste = "";
  this.maskHintHtml = "";
  this.maskHintTimerID = -1;
  this.displayFormat = null;
  this.TextChanged = new ASPxClientEvent();
 },
 Initialize: function(){
  this.SaveChangedValue();
  ASPxClientEdit.prototype.Initialize.call(this);
  this.CorrectInputMaxLength();
  if(__aspxWebKitFamily)
   this.CorrectMainElementWhiteSpaceStyle();
 },
 InlineInitialize: function(){
  ASPxClientEdit.prototype.InlineInitialize.call(this);
  if(this.maskInfo != null)
   this.InitMask();
  this.ApplyBrowserSpecificClassName();
  this.helpTextInitialize();
  if(__aspxIE && __aspxBrowserVersion > 8 && !this.isNative)
```

```
   this.correctInputElementHeight();
 },
 correctInputElementHeight: function() {
  var mainElement = this.GetMainElement();
  var inputElement = this.GetInputElement();
  if (mainElement) {
   var mainElementHeight = mainElement.style.height;
   var mainElementHeightSpecified = mainElementHeight && mainElementHeight.indexOf('px') !== -1;
   if(mainElementHeightSpecified) {
    var inputElementHeight = _aspxPxToInt(mainElementHeight) -
_aspxGetTopBottomBordersAndPaddingsSummaryValue(mainElement);
    var inputElementContainer = inputElement.parentNode;
    inputElementHeight -= _aspxGetTopBottomBordersAndPaddingsSummaryValue(inputElementContainer);
    var mainElementCellspacing = _aspxGetCellSpacing(mainElement);
    if(mai...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxStateItemsExist = false;
var __aspxFocusedItemKind = "FocusedStateItem";
var __aspxHoverItemKind = "HoverStateItem";
var __aspxPressedItemKind = "PressedStateItem";
var __aspxSelectedItemKind = "SelectedStateItem";
var __aspxDisabledItemKind = "DisabledStateItem";
var __aspxCachedStatePrefix = "cached";
ASPxStateItem = _aspxCreateClass(null, {
 constructor: function(name, classNames, cssTexts, postfixes, imageObjs, imagePostfixes, kind,
disableApplyingStyleToLink){
  this.name = name;
  this.classNames = classNames;
  this.customClassNames = [];
  this.resultClassNames = [];
  this.cssTexts = cssTexts;
  this.postfixes = postfixes;
  this.imageObjs = imageObjs;
  this.imagePostfixes = imagePostfixes;
  this.kind = kind;
  this.classNamePostfix = kind.substr(0, 1).toLowerCase();
  this.enabled = true;
  this.needRefreshBetweenElements = false;
  this.elements = null;
  this.images = null;
  this.linkColor = null;
  this.lintTextDecoration = null;
  this.disableApplyingStyleToLink = !!disableApplyingStyleToLink;
 },
 GetCssText: function(index){
  if(_aspxIsExists(this.cssTexts[index]))
   return this.cssTexts[index];
  return this.cssTexts[0];
 },
 CreateStyleRule: function(index){
  if(this.GetCssText(index) == "") return "";
  var styleSheet = _aspxGetCurrentStyleSheet();
  if(styleSheet)
   return _aspxCreateImportantStyleRule(styleSheet, this.GetCssText(index), this.classNamePostfix);
  return "";
 },
 GetClassName: function(index){
  if(_aspxIsExists(this.classNames[index]))
   return this.classNames[index];
  return this.classNames[0];
 },
 GetResultClassName: function(index){
  if(!_aspxIsExists(this.resultClassNames[index])) {
   if(!_aspxIsExists(this.customClassNames[index]))
    this.customClassNames[index] = this.CreateStyleRule(index);
   if(this.GetClassName(index) != "" && this.customClassNames[index] != "")
    this.resultClassNames[index] = this.GetClassName(index) + " " + this.customClassNames[index];
   else if(this.GetClassName(index) != "")
    this.resultClassNames[index] = this.GetClassName(index);
   else if(this.customClassNames[index] != "")
    this.resultClassNames[index] = this.customClassNames[index];
   else
    this.resultClassNames[index] = "";
  }
  return this.resultClassNames[index];
 },
 GetElements: function(element){
  if(!this.elements || !_aspxIsValidElements(this.elements)){
   if(this.postfixes && this.postfixes.length > 0){
    this.elements = [ ];
    var parentNode = element.parentNode;
    if(parentNode){
     for(var i = 0; i < this.postfixes.length; i++){
      var id = this.name + this.postfixes[i];
      this.elements[i] = _aspxGetChildById(parentNode, id);
      if(!this.elements[i])
       this.elements[i] = _aspxGetElementById(id);
     }
    }
   }
   else
    this.elements = [element];
  }
  return this.elements;
 },
 GetImages: function(element){
  if(!this.images || !_aspxIsValidElements(this.images)){
   this.images = [ ];
   if(this.imagePostfixes && this.imagePostfixes.length > 0){
    var elements = this.GetElements(element);
    for(var i = 0; i < this.imagePostfixes.length; i++){
     var id = this.name + this.imagePostfixes[i];
     for(var j = 0; j < elements.length; j++){
      if(!elements[j]) continue;
      if(elements[j].id == id)
       this.images[i] = elements[j];
      else
       this.images[i] = _aspxGetChildById(elements[j], id);
      if(this.images[i])
       break;
     }
    }
   }
  }
  return this.images;
 },
 Apply: function(element){
  if(!this.enabled) return;
  try{
   this.ApplyStyle(element);
   if(this.imageObjs && this.imageObjs.length > 0)
    this.ApplyImage(element);
  }
  catch(e){
  }
 },
 ApplyStyle: function(element){
  var elements = this.GetElements(element);
  for(var i = 0; i < elements.length; i++){
   if(!elements[i]) continue;
   var className = elements[i].className.replace(this.GetResultClassName(i), "");
   elements[i].className = _aspxTrim(className) + " " + this.GetResultClassName(i);
   if(!__aspxOpera || __aspxBrowserVersion >= 9)
    this.ApplyStyleToLinks(elements, i);
  }
 },
 ApplyStyleToLinks: function(elements, index){
  if(this.disableApplyingStyleToLink)
   return;
  var linkCount = 0;
  var savedLinkCount = -1;
  if(_aspxIsExists(elements[index]["savedLinkCount"]))
   savedLinkCount = parseInt(elements[index]["savedLinkCount"]);
  do{
   if(savedLinkCount > -1 && savedLinkCount <= linkCount)
    break;
   var link = elements[index]["link" + linkCount];
   if(!link){
    link = _aspxGetChildByTagName(elements[index], "A", linkCount);
```

```
    if(!link)
     link = _aspxGetChildByTagName(elements[index], "SPAN", linkCount);
    if(link)
     elements[index]["link" + linkCount] = link;
   }
   if(link)
    this.ApplyStyleToLinkElement(link, index);
   else
    elements[index]["savedLinkCount"] = linkCount;
   linkCount++;
  }
  while(link != n...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxLoadFilteredItemsCallbackPrefix = "CBLF";
var __aspxCorrectFilterCallbackPrefix = "CBCF";
var __aspxtCurrentSelectedItemCallbackPrefix = "CBSI";
var __aspxLoadDropDownOnDemandCallbackPrefix = "CBLD";
var __aspxDropDownNameSuffix = "_DDD";
var __aspxCalendarNameSuffix = "_C";
var __aspxTimeEditNameSiffix = __aspxCalendarNameSuffix + "_TE";
var __aspxClockNameSiffix= __aspxCalendarNameSuffix + "_CL";
var __aspxListBoxNameSuffix = "_L";
var __aspxItemImageCellClassName = "dxeIIC";
var __aspxTokensHiddenFieldSuffix = "TK";
var __aspxTokenBoxTokenSuffix = "Token";
var __aspxTokenBoxTokenTextSuffix = "TokenT";
var __aspxTokenBoxTokenRemoveButtonSuffix = "TokenRB";
var __aspxTokenBoxInputMinWidth = 30;
ASPxClientDropDownEditBase = _aspxCreateClass(ASPxClientButtonEditBase, {
 constructor: function(name) {
  this.constructor.prototype.constructor.call(this, name);
  this.DropDown = new ASPxClientEvent();
  this.CloseUp = new ASPxClientEvent();
  this.ddHeightCache = __aspxInvalidDimension;
  this.ddWidthCache = __aspxInvalidDimension;
  this.mainElementWidthCache = __aspxInvalidDimension;
  this.dropDownButtonIndex = -1;
  this.droppedDown = false;
  this.ddButtonPushed = false;
  this.lastSuccessText = "";
  this.isToolbarItem = false;
  this.allowFocusDropDownWindow = false;
  this.pcIsShowingNow = false;
  this.needTimeoutForInputElementFocusEvent = false;
  aspxGetDropDownCollection().Add(this);
 },
 Initialize: function(){
  var pc = this.GetPopupControl();
  if(pc) {
   pc.allowCorrectYOffsetPosition = false;
   pc.dropDownEditName = this.name;
  }
  this.AssignClientAttributes();
  this.InitLastSuccessText();
  if(this.RefocusOnClickRequired()){
   var clickFunc = new Function("aspxDDRefocusClick('" + this.name + "', event);");
   _aspxAttachEventToElement(this.GetMainElement(), "click", clickFunc);
  }
  ASPxClientButtonEditBase.prototype.Initialize.call(this);
 },
 InitLastSuccessText: function(){
  var rawText = this.GetTextInternal();
  this.SetLastSuccessTest(rawText);
 },
 AssignClientAttributes: function(){
  var element = this.GetDropDownButton();
  if(_aspxIsExistsElement(element))
   _aspxPreventElementDragAndSelect(element, true);
 },
 RefocusOnClickRequired: function(){
  return false;
 },
 GetDropDownButton: function(){
  return this.GetButton(this.dropDownButtonIndex);
 },
 GetPopupControl: function(){
  var pc = aspxGetControlCollection().Get(this.name + __aspxDropDownNameSuffix);
  if(pc && pc.GetWindowElement(-1))
   return pc;
  else
   return null;
 },
 GetDropDownInnerControlName: function(suffix){
  var pc = this.GetPopupControl();
  if(pc)
   return this.GetPopupControl().name + suffix;
  return "";
 },
 GetDropDownItemImageCell: function() {
  return _aspxGetChildrenByPartialClassName(this.GetMainElement(), __aspxItemImageCellClassName)[0];
 },
 GetIsControlWidthWasChanged: function(){
  return this.mainElementWidthCache == __aspxInvalidDimension || this.mainElementWidthCache !=
this.GetMainElement().clientWidth;
 },
 GetDropDownHeight: function(){
  return 0;
 },
 GetDropDownWidth: function(){
  return 0;
 },
 GetDropDownIsWindowElement: function(id, pcPostfix) {
  var pos = id.lastIndexOf(pcPostfix);
  if(pos != -1) {
   var name = id.substring(0, pos);
   var pc = aspxGetPopupControlCollection().Get(name);
   if(pc && pc.dropDownEditName)
    return aspxGetDropDownCollection().Get(pc.dropDownEditName);
  }
  return null;
 },
 GetDropDownParents: function() {
  var parents = [ ];
  var mainElement = this.GetMainElement();
  var pcPostfix = __aspxPCWIdSuffix + "-1";
  var element = mainElement.parentNode;
  while(element != null){
   if(element.tagName == "BODY")
    break;
   if(element.id) {
    var dropDown = this.GetDropDownIsWindowElement(element.id, pcPostfix);
    if(dropDown != null)
     parents.push(dropDown);
   }
   element = element.parentNode;
  }
  return parents.reverse();
 },
 BeforePopupControlResizing: function() {
 },
 AfterPopupControlResizing: function() {
 },
 ShowDropDownArea: function(isRaiseEvent){
  this.SetPCIsShowingNow(true);
  aspxGetDropDownCollection().RegisterDroppedDownControl(this, this.GetDropDownParents());
  if(!this.droppedDown)
   this.lockListBoxClick = true;
  this.lockClosing = true;
  var pc = this.GetPopupControl();
  var element = this.GetMainElement();
  var pcwElement = pc.GetWindowElement(-1);
  if (!_aspxGetElementDisplay(pcwElement))
   pcwElement.style.visibility = "hidden";
  _aspxSetElementDisplay(pcwElement, true);
  var height = this.GetDropDownHeight();
  var width = this.GetDropDownWidth();
  this.BeforePopupControlResizing();
  if(this.ddHeightCache != height || this.ddWidthCache != width){
   pc.SetSize(width, height);
   this.ddHeightCache = height;
   this.ddWidthCache = width;
  }
  this.AfterPopupControlResizing();
  pc.popupVerticalOffset = - _aspxGetClientTop(element);
  ...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
_aspxEnableCssAnimation = true;
aspxAnimationTransitionBase = _aspxCreateClass(null, {
 constructor: function (element, options) {
  aspxAnimationTransitionBase.Cancel(element);
  this.element = element;
  this.element.aspxTransition = this;
  this.duration = options.duration || aspxAnimationTransitionBase.Durations.DEFAULT;
  this.transition = options.transition || aspxAnimationTransitionBase.Transitions.SINE;
  this.property = options.property;
  this.unit = options.unit || "";
  this.onComplete = options.onComplete;
  this.to = null;
  this.from = null;
 },
 Start: function (from, to) {
  if (to != undefined) {
   this.to = to;
   this.from = from;
   this.SetValue(this.from);
  }
  else
   this.to = from;
 },
 Cancel: function () {
  try {
   delete this.element.aspxTransition;
  } catch (e) {
   this.element.aspxTransition = undefined;
  }
 },
 GetValue: function () {
  return this.getValueInternal(this.element, this.property);
 },
 SetValue: function (value) {
  this.setValueInternal(this.element, this.property, this.unit, value);
 },
 setValueInternal: function (element, property, unit, value) {
  if (property == "opacity")
   ASPxAnimationHelper.setOpacity(element, value);
  else
   element.style[property] = value + unit;
 },
 getValueInternal: function (element, property) {
  if (property == "opacity")
   return _aspxGetElementOpacity(element);
  var value = parseFloat(element.style[property]);
  return isNaN(value) ? 0 : value;
 },
 performOnComplete: function () {
  if (this.onComplete)
   this.onComplete(this.element);
 },
 getTransition: function () {
  return this.transition;
 }
});
aspxAnimationTransitionBase.Cancel = function (element) {
 if (element.aspxTransition)
  element.aspxTransition.Cancel();
};
aspxAnimationTransitionBase.Durations = {
 SHORT: 200,
 DEFAULT: 400,
 LONG: 600
```

```
};
aspxAnimationTransitionBase.Transitions = {
 LINER: {
  Css: "cubic-bezier(0.250, 0.250, 0.750, 0.750)",
  Js: function (progress) { return progress; }
 },
 SINE: {
  Css: "cubic-bezier(0.470, 0.000, 0.745, 0.715)",
  Js: function (progress) { return Math.sin(progress * 1.57); }
 },
 POW: {
  Css: "cubic-bezier(0.755, 0.050, 0.855, 0.060)",
  Js: function (progress) { return Math.pow(progress, 4); }
 },
 POW_EASE_OUT: {
  Css: "cubic-bezier(0.165, 0.840, 0.440, 1.000)",
  Js: function (progress) { return 1 - aspxAnimationTransitionBase.Transitions.POW.Js(1 - progress); }
 }
};
aspxJsAnimationTransition = _aspxCreateClass(aspxAnimationTransitionBase, {
 constructor: function (element, options) {
  this.constructor.prototype.constructor.call(this, element, options);
  this.fps = 60;
  this.startTime = null;
 },
 Start: function (from, to) {
  aspxAnimationTransitionBase.prototype.Start.call(this, from, to);
  this.initTimer();
 },
 Cancel: function () {
  aspxAnimationTransitionBase.prototype.Cancel.call(this);
  if (this.timerId)
   clearInterval(this.timerId);
 },
 initTimer: function () {
  this.startTime = new Date();
  this.timerId = window.setInterval(function () { this.onTick(); }.aspxBind(this), 1000 / this.fps);
 },
 onTick: function () {
  var progress = (new Date() - this.startTime) / this.duration;
  if (progress >= 1)
   this.complete();
  else
   this.update(progress);
 },
 update: function (progress) {
  this.SetValue(this.gatCalculatedValue(this.from, this.to, progress));
 },
 complete: function () {
  this.Cancel();
  this.update(1);
  this.performOnComplete();
 },
 gatCalculatedValue: function (from, to, progress) {
  if (progress == 1)
   return to;
  return from + (to - from) * this.getTransition()(progress);
 },
 getTransition: function () {
  return this.transition.Js;
 }
});
aspxMultipleJsAnimationTransition = _aspxCreateClass(aspxJsAnimationTransition, {
 constructor: function (element, options) {
  this.constructor.prototype.constructor.call(this, element, options);
  this.properties = { };
 },
 Start: function (properties) {
  this.initProperties(properties);
  this.initTimer();
 },
 initProperties: function (properties) {
  this.properties = properties;
  for (var propName in this.properties)
   if (properties[propName].from == undefined)
    properties[propName].from = this.getValueInternal(this.element, propName);
 },
 update: function (progress) {
  for (var propName in this.properties) {
   var property = this.properties[propName];
   if (property.from != property.to)
    this.setValueInternal(this.element, propName, property.unit, this.gatCalculatedValue(property.from,
property.to, progress));
  }
 }
});
aspxCssAnimationTransition = _aspxCreateClass(aspxAnimationTransitionBase, {
 constructor: function (element, options) {
  this.constructor.prototype.constructor.call(this, element, options);
  this.transitionPropertyName = aspxCssAnimationTransition.CSS_TRANSITION.transitionPropertyName;
  this.eventName = aspxCssAnimationTransit...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxNotSetAlignIndicator = "NotSet";
var __aspxInnerAlignIndicator = "Sides";
function _aspxIsAlignNotSet(align){
 return align == __aspxNotSetAlignIndicator;
}
function _aspxIsInnerAlign(align){
 return align.indexOf(__aspxInnerAlignIndicator) != -1;
}
function _aspxIsOuterAlign(align){
 return (!this.IsInnerAlign(align)) && (!_aspxIsAlignNotSet(align));
}
function _aspxPopupPosition(position, isInverted){
 this.position = position;
 this.isInverted = isInverted;
}
function _aspxSegment(pos, len){
 this.pos = pos;
 this.len = len;
}
function _aspxRect(left, top, width, height){
 this.left = left;
 this.top = top;
 this.width = width;
 this.height = height;
}
function _aspxSize(width, height){
 this.width = width;
 this.height = height;
}
function _aspxFindPopupElementById(id){
 if(id == "") return null;
 var popupElement = _aspxGetElementById(id);
 if(!_aspxIsExistsElement(popupElement)){
  var idParts = id.split("_");
  var uniqueId = idParts.join("$");
  popupElement = _aspxGetElementById(uniqueId);
 }
 return popupElement;
}
function _aspxFindEventSourceParentByTestFunc(evt, testFunc){
 return _aspxFindParentByTestFunc(_aspxGetEventSource(evt), testFunc);
}
function _aspxPreventContextMenu(evt){
 if (__aspxWebKitFamily){
  if(evt.stopPropagation)
   evt.stopPropagation();
  evt.returnValue = false;
  if(evt.preventDefault)
   evt.preventDefault();
 } else if (__aspxNetscapeFamily || (__aspxIE && __aspxBrowserVersion > 8))
  evt.preventDefault();
}
function _aspxIsExistsAbsolutePosParent(element){
 return _aspxIsExistsParentWithSpecPosition(element, ["absolute"]);
}
function _aspxIsExistsAbsoluteOrRelativePosParent(element){
 return _aspxIsExistsParentWithSpecPosition(element, ["absolute", "relative"]);
```

```
}
function _aspxIsExistsParentWithSpecPosition(element, positions){
 var curEl = element.offsetParent;
 while(curEl != null) {
  for(var i = 0; i < positions.length; i ++){
   if (_aspxGetCurrentStyle(curEl).position == positions[i])
    return true;
  }
  curEl = curEl.offsetParent;
 }
 return false;
}
function _aspxGetDocumentClientWidthForPopup(){
 return (__aspxWebKitTouchUI ? _aspxGetDocumentWidth() : _aspxGetDocumentClientWidth());
}
function _aspxAdjustPositionToClientScreen(element, shadowSize, pos, isX){
 var min = isX ? _aspxGetDocumentScrollLeft() : _aspxGetDocumentScrollTop();
 var documentClientWidth = _aspxGetDocumentClientWidthForPopup();
 var max = min + (isX ? documentClientWidth : _aspxGetDocumentClientHeight());
 max -= (isX ? element.offsetWidth + shadowSize : element.offsetHeight + shadowSize);
 if (pos > max) pos = max;
 if (pos < min) pos = min;
 return pos;
}
function _aspxGetPopupAbsoluteX(element, shadowWidth, popupElement, hAlign, hOffset, x, left, rtl,
isPopupFullCorrectionOn){
 var width = element.offsetWidth;
 var bodyWidth = _aspxGetDocumentClientWidth();
 var elementX = _aspxGetAbsoluteX(popupElement);
 var scrollX = _aspxGetDocumentScrollLeft();
 if (hAlign == "WindowCenter"){
  var showAtPos = x != __aspxInvalidPosition && !popupElement;
  if(showAtPos)
   hAlign = "";
  else
   return new _aspxPopupPosition(Math.ceil((__aspxWebKitTouchUI ? window.innerWidth : bodyWidth) / 2 - width
/ 2) + scrollX + hOffset, false);
 }
 if (popupElement) {
  var leftX = elementX - width;
  var rightX = elementX + popupElement.offsetWidth;
  var innerLeftX = elementX;
  var innerRightX = elementX + popupElement.offsetWidth - width;
  var isMoreFreeSpaceLeft = bodyWidth - (rightX + width) < leftX - 2 * scrollX;
 }
 else
  hAlign = "";
 var isInverted = false;
 if (hAlign == "OutsideLeft"){
  isInverted = isPopupFullCorrectionOn && (!(leftX - scrollX > 0 || isMoreFreeSpaceLeft));
  if(isInverted)
   x = rightX - hOffset;
  else
   x = leftX + hOffset;
 }
 else if (hAlign == "LeftSides"){
  x =  innerLeftX + hOffset;
  if (isPopupFullCorrectionOn)
   x = _aspxAdjustPositionToClientScreen(element, shadowWidth, x, true);
 }
 else if (hAlign == "Center"){
  x =  elementX + Math.round((popupElement.offsetWidth  - width) / 2) + hOffset;
 }
 else if (hAlign == "RightSides"){
  x = innerRightX + hOffset;
  if (isPopupFullCorrectionOn)
   x = _aspxAdjustPositionToClientScreen(element, shadowWidth, x, true);
 }
 else if (hAlign == "OutsideRight"){
  isInverted = isPopupFullCorrectionOn && (!(rightX + width < bodyWidth + scrollX || !isMoreFreeSpaceLeft));
  if(isInverted)
   x = leftX - hOffset;
  else
   x = rightX + hOffset;
 }
 else{
  if(rtl){
   if(!_aspxGetIsValidPosition(x))
```

```
    x = popupElement ? innerRightX : left;
   else
    x -= width;
   isInverted = isPopupFullCorrectionOn && (x < scrollX && x - scrollX < bodyWidth / 2);
   if(isInverted)
    x = x + width + hOffset;
   else
    x = x - hOffset;
  } else {
   if (!_aspxGetIsValidPosition(x))
    x = popupElement ? elementX : left;
   isInverted = isPopupFullCorrectionOn && (x - scrollX + wi...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxPCWIdSuffix = "_PW";
function ASPxPCResizeCursorInfo(horizontalDirection, verticalDirection, horizontalOffset, verticalOffset) {
 this.horizontalDirection = horizontalDirection;
 this.verticalDirection = verticalDirection;
 this.horizontalOffset = horizontalOffset;
 this.verticalOffset = verticalOffset;
 this.course = verticalDirection + horizontalDirection;
}
ASPxClientPopupControlCssClasses = {};
ASPxClientPopupControlCssClasses.Prefix = "dxpc-";
ASPxClientPopupControlCssClasses.SizeGripLiteCssClassName = ASPxClientPopupControlCssClasses.Prefix +
"sizeGrip";
ASPxClientPopupControlCssClasses.LinkCssClassName = ASPxClientPopupControlCssClasses.Prefix + "link";
ASPxClientPopupControlCssClasses.ShadowLiteCssClassName = ASPxClientPopupControlCssClasses.Prefix + "shadow";
ASPxClientPopupControlCssClasses.MainDivLiteCssClass = ASPxClientPopupControlCssClasses.Prefix + "mainDiv";
ASPxClientPopupControl = _aspxCreateClass(ASPxClientControl, {
 constructor: function(name) {
  this.constructor.prototype.constructor.call(this, name);
  this.leadingAfterInitCall = true;
  this.adjustInnerControlsSizeOnShow = true;
  this.slideAnimationDuration = 80;
  this.appearAfter = 300;
  this.disappearAfter = 500;
  this.allowResize = false;
  this.enableAnimation = true;
  this.popupAnimationType = null;
  this.shadowVisible = true;
  this.allowCorrectYOffsetPosition = true;
  this.contentUrl = "";
  this.contentUrlArray = [];
  this.contentLoadingMode = "Default"
  this.loadingPanels = [];
  this.loadingDivs = [];
  this.lpTimers = [];
  this.windowRequestCount = [];
  this.callbackAnimationProcessings = [];
  this.savedCallbackResults = [];
  this.isCallbackFinishedStates = [];
  this.savedCallbackWindowIndex = null;
  this.cookieName = "";
  this.closeAction = "OuterMouseClick";
  this.popupAction = "LeftMouseClick";
  this.closeActionArray = [];
  this.popupActionArray = [];
  this.windowsPopupElementIDList = [];
  this.windowsPopupElementList = [];
  this.windowsLastUsedPopupElementInfoList = [];
  this.windowsIsPopupedList = [];
  this.windowsPopupReasonMouseEventList = [];
  this.defaultWindowPopupElementIDList = [];
  this.defaultWindowPopupElementList = [];
  this.defaultLastUsedPopupElementInfo = {};
  this.defaultIsPopuped = false;
  this.defaultPopupReasonMouseEvent = null;
  this.showOnPageLoad = false;
  this.showOnPageLoadArray = [];
  this.popupHorizontalAlign = __aspxNotSetAlignIndicator;
  this.popupVerticalAlign = __aspxNotSetAlignIndicator;
```

```
    this.popupHorizontalOffset = 0;
    this.popupVerticalOffset = 0;
    this.windows = [];
    this.windowCount = 0;
    this.isDragged = false;
    this.isResized = false;
    this.zIndex = -1;
    this.left = 0;
    this.top = 0;
    this.allowLoadToHiddenIframe = __aspxIE || __aspxFirefox;
    this.iframeLoading = false;
    this.isDraggedArray = [];
    this.isResizedArray = [];
    this.zIndexArray = [];
    this.leftArray = [];
    this.topArray = [];
    this.height = 0;
    this.width = 0;
    this.minHeight = null;
    this.minWidth = null;
    this.maxHeight = null;
    this.maxWidth = null;
    this.heightArray = [];
    this.widthArray = [];
    this.minHeightArray = [];
    this.minWidthArray = [];
    this.maxHeightArray = [];
    this.maxWidthArray = [];
    this.iframeLoadingArray = [];
    this.isLiveResizingMode = true;
    this.isPopupPositionCorrectionOn = true;
    this.isPopupFullCorrectionOn = true;
    this.windowElements = new Object();
    this.hideBodyScrollWhenModal = true;
    this.hideBodyScrollWhenMaximized = true;
    this.autoUpdatePosition = false;
    this.autoUpdatePositionArray = [];
    this.cachedSize = null;
    this.cachedSizeArray = [];
    this.fakeDragDiv = null;
    this.headerHeight = 0;
    this.headerHeightArray = [];
    this.footerHeight = 0;
    this.footerHeightArray = [];
    this.ResizeBorderSize = __aspxTouchUI ? 10 : 6;
    this.ResizeCornerBorderSize = 20;
    this.allowDragging = false;
    this.isWindowDragging = false;
    this.enableContentScrolling = false;
    this.contentOverflowX = "None";
    this.contentOverflowY = "None";
    this.isPinned = false;
    this.isPinnedArray = [];
    this.pinX = 0;
    this.pinXArray = [];
    this.pinY = 0;
    this.pinYArray = [];
    this.lockScroll = 0;
    this.isCollapsed = false;
    this.isCollapsedArray = [];
    this.isCollapsedInit = false;
    this.isCollapsedInitArray = [];
    this.collapseExecutingLockCount = 0;
    this.isMaximized = false;
    this.isMaximizedArray = [];
    this.isMaximizedInit = false;
    this.isMaximizedInitArray = [];
    this.maximizationExecutingLockCount = 0;
    this.restoredWindowValues = {};
    this.restoredWindowValuesArray = [];
    this.browserResizingForMaxWindowLockCount = 0;
    this.updateRestoredWindowSizeLockCount = 0;
    this.prohibitClearSelectionOnMouseDown = false;
    this.CloseButtonClick = new ASPxClientEvent();
    this.CloseUp = new ASPxClientEvent();
    this.Closing = new ASPxClientEvent();
    this.PopUp = new ASPxCl...
```

```
var __aspxLBSerializingSeparator = "|";
var __aspxLBSerializingSeparatorLength = __aspxLBSerializingSeparator.length;
var __aspxLoadRangeItemsCallbackPrefix = "LBCRI";
var __aspxLBIPostfixes = ['C', 'I', 'T'];
var __aspxLBIIdSuffix = "LBI";
var __aspxLBSIIdSuffix = __aspxLBIIdSuffix + "-1";
var __aspxLBTSIdSuffix = "_TS";
var __aspxLBBSIdSuffix = "_BS";
var __aspxLBHeaderDivIdSuffix = "_H";
var __aspxLTableIdSuffix = "_LBT";
var __aspxLEVISuffix = "_VI";
var __aspxLBDSuffix = "_D";
var __aspxEmptyItemsRange = "0:-1";
var __aspxNbsp = "&nbsp;";
var __aspxNameSeparator = "_";
var __aspxNbspChar = String.fromCharCode(160);
var ListBoxSelectionMode = { Single : 0, Multiple : 1, CheckColumn : 2 };
ASPxClientListEdit = _aspxCreateClass(ASPxClientEdit, {
 constructor: function(name) {
  this.constructor.prototype.constructor.call(this, name);
  this.SelectedIndexChanged = new ASPxClientEvent();
  this.savedSelectedIndex = -1;
 },
 FindInputElement: function() {
  return this.FindStateInputElement();
 },
 FindStateInputElement: function(){
  return document.getElementById(this.name + __aspxLEVISuffix);
 },
 GetItem: function(index) {
  throw "Not implemented";
 },
 GetItemValue: function(index) {
  throw "Not implemented";
 },
 GetValue: function(){
  return this.GetItemValue(this.GetSelectedIndex());
 },
 GetSelectedIndexInternal: function(){
  return this.savedSelectedIndex;
 },
 SetSelectedIndexInternal: function(index){
  this.savedSelectedIndex = index;
 },
 FindItemIndexByValue: function(value){
  for(var i = 0; i < this.GetItemCount(); i++){
   if(this.GetItemValue(i) == value)
    return i;
  }
  return -1;
 },
 RaiseItemClick: function() {
  var processOnServer = this.autoPostBack;
  if(!this.ItemClick.IsEmpty()){
   var args = new ASPxClientProcessingModeEventArgs(processOnServer);
   this.ItemClick.FireEvent(this, args);
   processOnServer = args.processOnServer;
  }
  return processOnServer;
 },
 RaiseItemDoubleClick: function() {
  var processOnServer = this.autoPostBack;
  if(!this.ItemDoubleClick.IsEmpty()){
   var args = new ASPxClientProcessingModeEventArgs(processOnServer);
   this.ItemDoubleClick.FireEvent(this, args);
   processOnServer = args.processOnServer;
  }
  return processOnServer;
 },
 RaiseValueChangedEvent: function() {
  if(!this.isInitialized) return false;
  var processOnServer = ASPxClientEdit.prototype.RaiseValueChangedEvent.call(this);
  processOnServer = this.RaiseValueChangedAdditionalEvents(processOnServer);
  return processOnServer;
 },
 RaiseValueChangedAdditionalEvents: function(processOnServer){
  return this.RaiseSelectedIndexChanged(processOnServer);
 },
 RaiseSelectedIndexChanged: function (processOnServer) {
  this.RaiseValidationInternal();
  if(!this.SelectedIndexChanged.IsEmpty()){
   var args = new ASPxClientProcessingModeEventArgs(processOnServer);
   this.SelectedIndexChanged.FireEvent(this, args);
   processOnServer = args.processOnServer;
  }
  return processOnServer;
 },
 UpdateHiddenInputs: function(){
  var element = this.FindStateInputElement();
  if(_aspxIsExistsElement(element)) {
   var value = this.GetValue();
   if (value == null)
    value = "";
   element.value = value;
  }
 },
 GetSelectedItem: function(){
  var index = this.GetSelectedIndexInternal();
  return this.GetItem(index);
 },
 GetSelectedIndex: function(){
  return this.GetSelectedIndexInternal();
 },
 SetSelectedItem: function(item){
  var index = (item != null) ? item.index : -1;
  this.SetSelectedIndex(index);
 },
 SetSelectedIndex: function(index){
  this.SelectIndexSilent(index);
 },
 SelectIndexSilent: function(index){
  throw "Not implemented";
 },
 OnValueChanged: function () {
  var processOnServer = this.RaiseValueChangedEvent() && this.GetIsValid();
  if (processOnServer)
   this.SendPostBackInternal("");
 }
});
ASPxClientListEditItem = _aspxCreateClass(null, {
 constructor: function(listEditBase, index, text, value, imageUrl){
  this.listEditBase = listEditBase;
  this.index = index;
  this.imageUrl = imageUrl;
  this.text = text;
  this.value = value;
 }
});
ASPxClientListBoxItem = _aspxCreateClass(ASPxClientListEditItem, {
 constructor: function(listEditBase, index, texts, value, imageUrl, selected){
  this.constructor.prototype.constructor.call(this, listEditBase, index, null, value, imageUrl);
  this.selected = selected ? selected : false;
  this.texts = texts;
  this.text = listEditBase.FormatText(texts);
 },
 GetColumnText: function(columnIndexOrFieldName){
  var columnIndex = -1;
  if(typeof(columnIndexOrFieldName) == "string")
   columnIndex = _aspxArrayIndexOf(this.listEditBase.columnFieldNames, columnIndexOrFieldName);
  else if(typeof(columnIndexOrFieldName) == "number")
   columnIndex = columnIndexOrFieldName;
  return this.GetColumnTextByIndex(columnIndex);
 },
 GetColumnTextByIndex: function(columnIndex){
  if(0 <= colu...
ASPxClientButton = _aspxCreateClass(ASPxClientControl, {
 constructor: function(name) {
  this.constructor.prototype.constructor.call(this, name);
  this.isASPxClientButton = true;
  this.allowFocus = true;
  this.autoPostBackFunction = null;
  this.causesValidation = true;
  this.checked = false;
  this.clickLocked = false;
  this.groupName = "";
  this.focusElementSelected = false;
  this.pressed = false;
  this.useSubmitBehavior = true;
  this.validationGroup = "";
  this.validationContainerID = null;
  this.validateInvisibleEditors = false;
  this.originalWidth = false;
  this.originalHeight = false;
  this.buttonCell = null;
  this.contentDiv = null;
  this.checkedInput = null;
  this.buttonImage = null;
  this.internalButton = null;
  this.textElement = null;
  this.textControl = null;
  this.textContainer = null;
  this.isTextEmpty = false;
  this.CheckedChanged = new ASPxClientEvent();
  this.GotFocus = new ASPxClientEvent();
  this.LostFocus = new ASPxClientEvent();
  this.Click = new ASPxClientEvent();
 },
 InlineInitialize: function() {
  var mainElement = this.GetMainElement();
  this.originalWidth = mainElement.style.width;
  this.originalHeight = mainElement.style.height;
  ASPxClientControl.prototype.InlineInitialize.call(this);
  this.InitializeElementIDs();
  this.InitializeEvents();
  this.InitializeEnabled();
  this.InitializeChecked();
  this.PreventButtonImageDragging();
 },
 InitializeElementIDs: function(){
  var mainElement = this.GetMainElement();
  var contentElement = _aspxGetChildByTagName(mainElement, "DIV", 0);
  if(contentElement) contentElement.id = this.name + "_CD";
  var imageElement = _aspxGetChildByTagName(mainElement, "IMG", 0);
  if(imageElement) imageElement.id = this.name + "Img";
 },
 InitializeEnabled: function(){
  this.SetEnabledInternal(this.clientEnabled, true);
 },
 InitializeChecked: function(){
  this.SetCheckedInternal(this.checked, true);
 },
 InitializeEvents: function(){
  if (!this.isNative) {
   var element = this.GetInternalButton();
   if(element)
    element.onfocus = null;
   var textControl = this.GetTextControl();
   if (textControl) {
    if (__aspxIE)
     _aspxAttachEventToElement(textControl, "mouseup", _aspxClearSelection);
    _aspxPreventElementDragAndSelect(textControl, false);
   }
  }
  var name = this.name;
  this.onClick = function() {
   var processOnServer = aspxBClick(name);
   if (!processOnServer) {
    var evt = _aspxGetEvent(arguments[0]);
    if (evt)
     _aspxPreventEvent(evt);
   }
   return processOnServer;
  };
  this.onGotFocus = function() { aspxBGotFocus(name); };
  this.onLostFocus = function() { aspxBLostFocus(name); };
  this.onKeyUp = function(evt) { aspxBKeyUp(evt, name); };
  this.onKeyDown = function(evt) { aspxBKeyDown(evt, name); };
  if(!this.isNative) {
   this.AttachNativeHandlerToMainElement("focus", "SetFocus");
   this.AttachNativeHandlerToMainElement("click", "DoClick");
  }
 },
 AdjustControlCore: function () {
  if(this.isNative) return;
  window.setTimeout(function() {
   this.UpdateWidth();
   this.UpdateHeight();
  }.aspxBind(this), 0);
 },
 UpdateHeight: function(){
  if(_aspxIsPercentageSize(this.originalHeight)) return;
  var height;
  var mainElement = this.GetMainElement();
  var borderAndPadding = _aspxGetTopBottomBordersAndPaddingsSummaryValue(mainElement);
  if(!this.originalHeight) {
   mainElement.style.height = "";
   height = mainElement.offsetHeight - borderAndPadding;
  }
  else
   height = (_aspxPxToInt(this.originalHeight) - borderAndPadding);
  if(height){
   mainElement.style.height = height + "px";
   var contentDiv = this.GetContentDiv();
   if(contentDiv && contentDiv.offsetHeight > 0){
    var contentDivCurrentStyle = _aspxGetCurrentStyle(contentDiv);
    var paddingTop = parseInt(contentDivCurrentStyle.paddingTop);
    var paddingBottom = parseInt(contentDivCurrentStyle.paddingBottom);
    var clientHeightDiff = height - contentDiv.offsetHeight;
    var verticalAlign = _aspxGetCurrentStyle(mainElement).verticalAlign;
    if(verticalAlign == "top")
     paddingBottom = paddingBottom + clientHeightDiff;
    else if(verticalAlign == "bottom")
     paddingTop = paddingTop + clientHeightDiff;
    else{
     var halfClientHeightDiff = Math.floor(clientHeightDiff / 2);
     paddingTop = paddingTop + halfClientHeightDiff;
     paddingBottom = paddingBottom + (clientHeightDiff - halfClientHeightDiff);
    }
    contentDiv.style.paddingTop = (paddingTop > 0 ? paddingTop : 0) + "px";
    contentDiv.style.paddingBottom = (paddingBottom > 0 ? paddingBottom : 0) + "px";
   }
  }
 },
 UpdateWidth: function(){
  if(_aspxIsPercentageSize(this.originalWidth)) return;
  var width;
  var mainElement = this.GetMainElement();
  var borderAndPadding = _aspxGetLeftRightBordersAndPaddingsSummaryValue(mainElement);
  if(!this.originalWidth) {
   if(__aspxIE && __...
```

https://md1npdvpadss02.dev.corp.local/webresource.axd

```
function WebForm_PostBackOptions(eventTarget, eventArgument, validation, validationGroup, actionUrl,
trackFocus, clientSubmit) {
    this.eventTarget = eventTarget;
    this.eventArgument = eventArgument;
    this.validation = validation;
    this.validationGroup = validationGroup;
    this.actionUrl = actionUrl;
    this.trackFocus = trackFocus;
    this.clientSubmit = clientSubmit;
}
```

```
function WebForm_DoPostBackWithOptions(options) {
    var validationResult = true;
    if (options.validation) {
        if (typeof(Page_ClientValidate) == 'function') {
            validationResult = Page_ClientValidate(options.validationGroup);
        }
    }
    if (validationResult) {
        if ((typeof(options.actionUrl) != "undefined") && (options.actionUrl != null) &&
(options.actionUrl.length > 0)) {
            theForm.action = options.actionUrl;
        }
        if (options.trackFocus) {
            var lastFocus = theForm.elements["__LASTFOCUS"];
            if ((typeof(lastFocus) != "undefined") && (lastFocus != null)) {
                if (typeof(document.activeElement) == "undefined") {
                    lastFocus.value = options.eventTarget;
                }
                else {
                    var active = document.activeElement;
                    if ((typeof(active) != "undefined") && (active != null)) {
                        if ((typeof(active.id) != "undefined") && (active.id != null) && (active.id.length >
0)) {
                            lastFocus.value = active.id;
                        }
                        else if (typeof(active.name) != "undefined") {
                            lastFocus.value = active.name;
                        }
                    }
                }
            }
        }
    }
    if (options.clientSubmit) {
        __doPostBack(options.eventTarget, options.eventArgument);
    }
}
var __pendingCallbacks = new Array();
var __synchronousCallBackIndex = -1;
function WebForm_DoCallback(eventTarget, eventArgument, eventCallback, context, errorCallback, useAsync) {
    var postData = __theFormPostData +
                "__CALLBACKID=" + WebForm_EncodeCallback(eventTarget) +
                "&__CALLBACKPARAM=" + WebForm_EncodeCallback(eventArgument);
    if (theForm["__EVENTVALIDATION"]) {
        postData += "&__EVENTVALIDATION=" + WebForm_EncodeCallback(theForm["__EVENTVALIDATION"].value);
    }
    var xmlRequest,e;
    try {
        xmlRequest = new XMLHttpRequest();
    }
    catch(e) {
        try {
            xmlRequest = new ActiveXObject("Microsoft.XMLHTTP");
        }
        catch(e) {
        }
    }
    var setRequestHeaderMethodExists = true;
    try {
        setRequestHeaderMethodExists = (xmlRequest && xmlRequest.setRequestHeader);
    }
    catch(e) {}
    var callback = new Object();
    callback.eventCallback = eventCallback;
    callback.context = context;
    callback.errorCallback = errorCallback;
    callback.async = useAsync;
    var callbackIndex = WebForm_FillFirstAvailableSlot(__pendingCallbacks, callback);
    if (!useAsync) {
        if (__synchronousCallBackIndex != -1) {
            __pendingCallbacks[__synchronousCallBackIndex] = null;
        }
        __synchronousCallBackIndex = callbackIndex;
    }
    if (setRequestHeaderMethodExists) {
        xmlRequest.onreadystatechange = WebForm_CallbackComplete;
        callback.xmlRequest = xmlRequest;
        // e.g. http:
```

```
        var action = theForm.action || document.location.pathname, fragmentIndex = action.indexOf('#');
        if (fragmentIndex !== -1) {
            action = action.substr(0, fragmentIndex);
        }
        if (!__nonMSDOMBrowser) {
            var domain = "";
            var path = action;
            var query = "";
            var queryIndex = action.indexOf('?');
            if (queryIndex !== -1) {
                query = action.substr(queryIndex);
                path = action.substr(0, queryIndex);
            }
            if (path.indexOf("%") === -1) {
                // domain may or may not be present (e.g. action of "foo.aspx" vs "http:
                if (/^https?\:\/\/.*$/gi.test(path)) {
                    var domainPartIndex = path.indexOf("\/\/") + 2;
                    var slashAfterDomain = path.indexOf("/", domainPartIndex);
                    if (slashAfterDomain === -1) {
                        // entire url is the domain (e.g. "http:
                        domain = path;
                        path = "";
                    }
                    else {
                        domain = path.substr(0, slashAfterDomain);
                        path = path.substr(slashAfterDomain);
                    }
                }
                action = domain + encodeURI(path) + query;
            }
        }
        xmlRequest.open("POST", action, true);
        xmlRequest.setRequestHeader("Content-Type", "application/x...
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxRoundPanel1_txtLogin');
window['ASPxRoundPanel1_txtLogin'] = dxo;
dxo.autoPostBack = true;
dxo.uniqueID = 'ASPxRoundPanel1$txtLogin';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxRoundPanel1_txt_password');
window['ASPxRoundPanel1_txt_password'] = dxo;
dxo.uniqueID = 'ASPxRoundPanel1$txt_password';
dxo.initialFocused = true;
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--
aspxAddDisabledItems('ASPxRoundPanel1_cbo_co_cd_DDD_L',[[['dxeDisabled_Office2010Black'],[''],['']]]);

var dxo = new ASPxClientListBox('ASPxRoundPanel1_cbo_co_cd_DDD_L');
window['ASPxRoundPanel1_cbo_co_cd_DDD_L'] = dxo;
dxo.uniqueID = 'ASPxRoundPanel1$cbo_co_cd$DDD$L';
dxo.SelectedIndexChanged.AddHandler(function (s, e) {
aspxCBLBSelectedIndexChanged('ASPxRoundPanel1_cbo_co_cd', e); });
dxo.ItemClick.AddHandler(function (s, e) { aspxCBLBItemMouseUp('ASPxRoundPanel1_cbo_co_cd', e); });
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.savedSelectedIndex = 13;
dxo.itemsValue=
['BZ','C01','CAM','GRS','KA','KK','KPC','KZ','MAY','PIN','PSS','ROB','SAL','SLS','SQB','TSS','TST','VSJ','WWW
','ZZ'];
dxo.isComboBoxList = true;
dxo.hoverClasses=['dxeListBoxItemHover_Office2010Black'];
dxo.selectedClasses=['dxeListBoxItemSelected_Office2010Black'];
dxo.disabledClasses=['dxeDisabled_Office2010Black'];
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--
aspxAddHoverItems('ASPxRoundPanel1_cbo_co_cd_DDD',[[['dxpc-closeBtnHover'],[''],['HCB-1']]]);

var dxo = new ASPxClientPopupControl('ASPxRoundPanel1_cbo_co_cd_DDD');
window['ASPxRoundPanel1_cbo_co_cd_DDD'] = dxo;
dxo.uniqueID = 'ASPxRoundPanel1$cbo_co_cd$DDD';
dxo.Shown.AddHandler(function (s, e) { aspxDDBPCShown('ASPxRoundPanel1_cbo_co_cd', e); });
dxo.adjustInnerControlsSizeOnShow=false;
dxo.popupAnimationType='slide';
dxo.closeAction='CloseButton';
dxo.popupHorizontalAlign='LeftSides';
dxo.popupVerticalAlign='Below';
dxo.width=0;
dxo.height=0;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--
aspxAddHoverItems('ASPxRoundPanel1_cbo_co_cd',[[['dxeButtonEditButtonHover_Office2010Black'],[''],['B-1']]]);
aspxAddPressedItems('ASPxRoundPanel1_cbo_co_cd',[[['dxeButtonEditButtonPressed_Office2010Black'],[''],['B-
1']]]);
document.getElementById("ASPxRoundPanel1_cbo_co_cd_I").setAttribute("autocomplete", "off");

var dxo = new ASPxClientComboBox('ASPxRoundPanel1_cbo_co_cd');
window['ASPxRoundPanel1_cbo_co_cd'] = dxo;
dxo.autoPostBack = true;
dxo.uniqueID = 'ASPxRoundPanel1$cbo_co_cd';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.lastSuccessValue = 'SLS';
dxo.islastSuccessValueInit = true;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientTextBox('ASPxRoundPanel1_txt_co_password');
window['ASPxRoundPanel1_txt_co_password'] = dxo;
dxo.uniqueID = 'ASPxRoundPanel1$txt_co_password';
dxo.RequireStyleDecoration();
dxo.styleDecoration.AddStyle('F','dxeFocused_Office2010Black','');
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientPopupControl('ASPxPopupControl1');
window['ASPxPopupControl1'] = dxo;
dxo.popupAnimationType='fade';
dxo.closeAction='CloseButton';
dxo.popupHorizontalAlign='WindowCenter';
dxo.popupVerticalAlign='WindowCenter';
dxo.width=322;
dxo.height=0;
dxo.showOnPageLoad=true;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEGotFocus('ASPxRoundPanel1_txt_co_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxELostFocus('ASPxRoundPanel1_txt_co_password')
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyDown('ASPxRoundPanel1_txt_co_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
aspxEKeyUp('ASPxRoundPanel1_txt_co_password', event)
```

https://md1npdvpadss02.dev.corp.local/login.aspx

```
//<!--

var dxo = new ASPxClientPopupControl('ASPxPopupControl1');
window['ASPxPopupControl1'] = dxo;
dxo.popupAnimationType='fade';
dxo.closeAction='CloseButton';
dxo.popupHorizontalAlign='WindowCenter';
dxo.popupVerticalAlign='WindowCenter';
dxo.width=322;
dxo.height=0;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/timeout.aspx

```
//<![CDATA[
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://md1npdvpadss02.dev.corp.local/timeout.aspx

```
//<![CDATA[
if (typeof(Sys) === 'undefined') throw new Error('ASP.NET Ajax client-side framework failed to load.');
//]]>
```

https://md1npdvpadss02.dev.corp.local/timeout.aspx

```
//<![CDATA[
Sys.WebForms.PageRequestManager._initialize('Scriptmanager1', 'form1', ['tUpdatePanel1',''], [], [], 0, '');
//]]>
```

https://md1npdvpadss02.dev.corp.local/timeout.aspx

```
//<!--
aspxAddHoverItems('ASPxMenu2',[[['dxm-hovered',''],['',''],['DXI0_'],['','T']]]);
```

```
var dxo = new ASPxClientMenu('ASPxMenu2');
window['ASPxMenu2'] = dxo;
dxo.renderData={'':[[0]]};
dxo.subMenuFIXOffset=2;
dxo.subMenuLIXOffset=2;
dxo.subMenuXOffset=2;
dxo.shadowVisible=false;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/timeout.aspx

```
//<!--
aspxAddHoverItems('ASPxMenu1',[[['dxm-hovered',''],['',''],['DXI0_','DXI1_','DXI2_','DXI3_','DXI4_','DXI5_'],
['','T']]]);

var dxo = new ASPxClientMenu('ASPxMenu1');
window['ASPxMenu1'] = dxo;
dxo.renderData={'':[[0],[1],[2],3,4,5]};
dxo.subMenuFIXOffset=2;
dxo.subMenuLIXOffset=2;
dxo.subMenuXOffset=2;
dxo.shadowVisible=false;
dxo.AfterCreate();

//-->
```

https://md1npdvpadss02.dev.corp.local/timeout.aspx

```
history.back();
```

https://md1npdvpadss02.dev.corp.local/scriptresource.axd

```
// Name:        MicrosoftAjax.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjax.js
// Microsoft AJAX Framework.

Function.__typeName = 'Function';
Function.__class = true;
Function.createCallback = function Function$createCallback(method, context) {
    /// <summary locid="M:J#Function.createCallback" />
    /// <param name="method" type="Function"></param>
    /// <param name="context" mayBeNull="true"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "method", type: Function},
        {name: "context", mayBeNull: true}
    ]);
    if (e) throw e;
    return function() {
        var l = arguments.length;
        if (l > 0) {
            var args = [];
            for (var i = 0; i < l; i++) {
                args[i] = arguments[i];
            }
            args[l] = context;
            return method.apply(this, args);
        }
        return method.call(this, context);
    }
}
Function.createDelegate = function Function$createDelegate(instance, method) {
    /// <summary locid="M:J#Function.createDelegate" />
    /// <param name="instance" mayBeNull="true"></param>
    /// <param name="method" type="Function"></param>
    /// <returns type="Function"></returns>
    var e = Function._validateParams(arguments, [
        {name: "instance", mayBeNull: true},
        {name: "method", type: Function}
    ]);
    if (e) throw e;
    return function() {
        return method.apply(instance, arguments);
    }
}
Function.emptyFunction = Function.emptyMethod = function Function$emptyMethod() {
    /// <summary locid="M:J#Function.emptyMethod" />
}
Function.validateParameters = function Function$validateParameters(parameters, expectedParameters,
validateParameterCount) {
    /// <summary locid="M:J#Function.validateParameters" />
    /// <param name="parameters"></param>
    /// <param name="expectedParameters"></param>
    /// <param name="validateParameterCount" type="Boolean" optional="true"></param>
    /// <returns type="Error" mayBeNull="true"></returns>
    var e = Function._validateParams(arguments, [
        {name: "parameters"},
        {name: "expectedParameters"},
        {name: "validateParameterCount", type: Boolean, optional: true}
    ]);
    if (e) throw e;
    return Function._validateParams(parameters, expectedParameters, validateParameterCount);
}
Function._validateParams = function Function$_validateParams(params, expectedParams, validateParameterCount)
{
    var e, expectedLength = expectedParams.length;
    validateParameterCount = validateParameterCount || (typeof(validateParameterCount) === "undefined");
    e = Function._validateParameterCount(params, expectedParams, validateParameterCount);
    if (e) {
        e.popStackFrame();
        return e;
    }
    for (var i = 0, l = params.length; i < l; i++) {
        var expectedParam = expectedParams[Math.min(i, expectedLength - 1)],
            paramName = expectedParam.name;
        if (expectedParam.parameterArray) {
            paramName += "[" + (i - expectedLength + 1) + "]";
        }
        else if (!validateParameterCount && (i >= expectedLength)) {
            break;
        }
        e = Function._validateParameter(params[i], expectedParam, paramName);
        if (e) {
            e.popStackFrame();
            return e;
        }
    }
    return null;
}
Function._validateParameterCount = function Function$_validateParameterCount(params, expectedParams,
validateParameterCount) {
    var i, error,
        expectedLen = expectedParams.length,
        actualLen = params.length;
    if (actualLen < expectedLen) {
        var minParams = expectedLen;
        for (i = 0; i < expectedLen; i++) {
            var param = expectedParams[i];
            if (param.optional || param.parameterArray) {
                minParams--;
            }
        }
        if (actualLen < minParams) {
            error = true;
        }
    }
    else if (validateParameterCount && (actualLen > expectedLen)) {
        error = true;
        for (i = 0; i < expectedLen; i++) {
            if (expectedParams[i].parameterArray) {
                error = false;
                break;
            }
        }
    }
    if (error) {
        var e = Error.parameterCount();
        e.popStackFrame();
        return e;
    }
    return null;
}
Function._validateParameter = function Function$_validateParameter(param, expectedParam, paramName) {
    var e,
        expectedType = expectedParam.type,
        expectedInteger = !!expectedParam.integer,
        expectedDomElement = !!expectedPar...
```

https://md1npdvpadss02.dev.corp.local/scriptresource.axd

```
// Name:        MicrosoftAjaxWebForms.debug.js
// Assembly:    System.Web.Extensions
// Version:     4.0.0.0
// FileVersion: 4.6.1087.0
//-----------------------------------------------------------------------
// Copyright (C) Microsoft Corporation. All rights reserved.
//-----------------------------------------------------------------------
// MicrosoftAjaxWebForms.js
// Microsoft AJAX ASP.NET WebForms Framework.
Type._registerScript("MicrosoftAjaxWebForms.js", [
 "MicrosoftAjaxCore.js",
 "MicrosoftAjaxSerialization.js",
 "MicrosoftAjaxNetwork.js",
 "MicrosoftAjaxComponentModel.js"]);
Type.registerNamespace('Sys.WebForms');
Sys.WebForms.BeginRequestEventArgs = function Sys$WebForms$BeginRequestEventArgs(request, postBackElement,
updatePanelsToUpdate) {
    /// <summary locid="M:J#Sys.WebForms.BeginRequestEventArgs.#ctor" />
    /// <param name="request" type="Sys.Net.WebRequest"></param>
    /// <param name="postBackElement" domElement="true" mayBeNull="true"></param>
    /// <param name="updatePanelsToUpdate" type="Array" elementType="String" mayBeNull="true"
optional="true"></param>
    var e = Function._validateParams(arguments, [
        {name: "request", type: Sys.Net.WebRequest},
        {name: "postBackElement", mayBeNull: true, domElement: true},
        {name: "updatePanelsToUpdate", type: Array, mayBeNull: true, optional: true, elementType: String}
    ]);
    if (e) throw e;
    Sys.WebForms.BeginRequestEventArgs.initializeBase(this);
    this._request = request;
    this._postBackElement = postBackElement;
    this._updatePanelsToUpdate = updatePanelsToUpdate;
}
    function Sys$WebForms$BeginRequestEventArgs$get_postBackElement() {
        /// <value domElement="true" mayBeNull="true"
locid="P:J#Sys.WebForms.BeginRequestEventArgs.postBackElement"></value>
        if (arguments.length !== 0) throw Error.parameterCount();
        return this._postBackElement;
    }
    function Sys$WebForms$BeginRequestEventArgs$get_request() {
        /// <value type="Sys.Net.WebRequest" locid="P:J#Sys.WebForms.BeginRequestEventArgs.request"></value>
        if (arguments.length !== 0) throw Error.parameterCount();
        return this._request;
    }
    function Sys$WebForms$BeginRequestEventArgs$get_updatePanelsToUpdate() {
        /// <value type="Array" elementType="String"
locid="P:J#Sys.WebForms.BeginRequestEventArgs.updatePanelsToUpdate"></value>
        if (arguments.length !== 0) throw Error.parameterCount();
        return this._updatePanelsToUpdate ? Array.clone(this._updatePanelsToUpdate) : [];
    }
Sys.WebForms.BeginRequestEventArgs.prototype = {
    get_postBackElement: Sys$WebForms$BeginRequestEventArgs$get_postBackElement,
    get_request: Sys$WebForms$BeginRequestEventArgs$get_request,
    get_updatePanelsToUpdate: Sys$WebForms$BeginRequestEventArgs$get_updatePanelsToUpdate
}
Sys.WebForms.BeginRequestEventArgs.registerClass('Sys.WebForms.BeginRequestEventArgs', Sys.EventArgs);

Sys.WebForms.EndRequestEventArgs = function Sys$WebForms$EndRequestEventArgs(error, dataItems, response) {
    /// <summary locid="M:J#Sys.WebForms.EndRequestEventArgs.#ctor" />
    /// <param name="error" type="Error" mayBeNull="true"></param>
    /// <param name="dataItems" type="Object" mayBeNull="true"></param>
    /// <param name="response" type="Sys.Net.WebRequestExecutor"></param>
    var e = Function._validateParams(arguments, [
        {name: "error", type: Error, mayBeNull: true},
        {name: "dataItems", type: Object, mayBeNull: true},
        {name: "response", type: Sys.Net.WebRequestExecutor}
    ]);
    if (e) throw e;
    Sys.WebForms.EndRequestEventArgs.initializeBase(this);
    this._errorHandled = false;
    this._error = error;
    this._dataItems = dataItems || new Object();
    this._response = response;
}
    function Sys$WebForms$EndRequestEventArgs$get_dataItems() {
        /// <value type="Object" locid="P:J#Sys.WebForms.EndRequestEventArgs.dataItems"></value>
        if (arguments.length !== 0) throw Error.parameterCount();
        return this._dataItems;
    }
    function Sys$WebForms$EndRequestEventArgs$get_error() {
        /// <value type="Error" locid="P:J#Sys.WebForms.EndRequestEventArgs.error"></value>
        if (arguments.length !== 0) throw Error.parameterCount();
        return this._error;
    }
    function Sys$WebForms$EndRequestEventArgs$get_errorHandled() {
        /// <value type="Boolean" locid="P:J#Sys.WebForms.EndRequestEventArgs.errorHandled"></value>
        if (arguments.length !== 0) throw Error.parameterCount();
        return this._errorHandled;
    }
    function Sys$WebForms$EndRequestEventArgs$set_errorHandled(value) {
        var e = Function._validateParams(arguments, [{name: "value", type: Boolean}]);
        if (e) throw e;
        this._errorHandled = value;
    }
    function Sys$WebForms$EndRequestEventArgs$get_response() {
        /// <value type="Sys.Net.WebReq...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
ASPxScrollingManager = _aspxCreateClass(null, {
 constructor: function(owner, scrollableArea, orientation, onBeforeScrolling, onAfterScrolling,
forseEmulation) {
  this.owner = owner;
  this.scrollableArea = scrollableArea;
  this.orientation = orientation;
  this.animationDelay = 1;
  this.animationStep = 2;
  this.animationOffset = 5;
  this.animationAcceleration = 0;
  this.scrollSessionInterval = 10;
  this.stopScrolling = true;
  this.busy = false;
  this.currentAcceleration = 0;
  this.startPos;
  this.onBeforeScrolling = onBeforeScrolling;
  this.onAfterScrolling = onAfterScrolling;
  this.emulationMode = forseEmulation === true || !__aspxTouchUI;
  this.Initialize();
 },
 Initialize: function(){
  if(__aspxMSTouchUI){
   this.scrollableArea.parentNode.style.overflow = "auto";
   this.scrollableArea.parentNode.style["-ms-overflow-style"] = "-ms-autohiding-scrollbar";
  }
  if(this.emulationMode){
   this.wrapper = new ASPxScrollingManager.scrollWrapper(this.scrollableArea);
  } else {
   this.wrapper = new ASPxScrollingManager.scrollWrapperTouchUI(this.scrollableArea, function(direction){
    if(this.onAfterScrolling)
     this.onAfterScrolling(this, direction);
   }.aspxBind(this));
  }
 },
 GetScrolledAreaPosition: function() {
  return this.wrapper.GetScrollLeft() * this.orientation[0]
   + this.wrapper.GetScrollTop() * this.orientation[1];
 },
 SetScrolledAreaPosition: function(pos) {
  this.wrapper.SetScrollLeft(pos * this.orientation[0]);
  this.wrapper.SetScrollTop(pos * this.orientation[1]);
 },
 PrepareForScrollAnimation: function() {
  if(!this.scrollableArea)
   return;
  this.currentAcceleration = 0;
  this.startPos = this.GetScrolledAreaPosition();
  this.busy = false;
 },
 GetAnimationStep: function(dir) {
  var step = dir * (this.animationStep + this.currentAcceleration);
  var newPos = this.GetScrolledAreaPosition() + step;
  var requiredPos = this.startPos + dir * this.animationOffset;
  if((dir == 1 && newPos >= requiredPos) || (dir == -1 && newPos <= requiredPos)) {
   step = requiredPos - this.GetScrolledAreaPosition();
  }
  return step;
 },
 DoScrollSessionAnimation: function(direction) {
  if(!this.scrollableArea)
   return;
  this.SetScrolledAreaPosition(this.GetScrolledAreaPosition() + this.GetAnimationStep(direction));
  var self = this;
  if(!this.ShouldStopScrollSessionAnimation()) {
   this.busy = true;
   this.currentAcceleration += this.animationAcceleration;
   _aspxSetTimeout(function() { self.DoScrollSessionAnimation(direction); }, this.animationDelay);
  } else {
   if(this.onAfterScrolling)
    this.onAfterScrolling(this, -direction);
   this.busy = false;
   this.currentAcceleration = 0;
   _aspxSetTimeout(function() { self.DoScroll(direction); }, this.scrollSessionInterval);
  }
 },
 ShouldStopScrollSessionAnimation: function() {
  return (Math.abs(this.GetScrolledAreaPosition() - this.startPos) >= Math.abs(this.animationOffset));
 },
 DoScroll: function(direction) {
  if(!this.scrollableArea)
   return;
  if(!this.busy && !this.stopScrolling) {
   if(this.onBeforeScrolling)
    this.onBeforeScrolling(this, -direction);
   if(this.stopScrolling) return;
   this.PrepareForScrollAnimation();
   this.DoScrollSessionAnimation(direction);
  }
 },
 StartScrolling: function(direction, delay, step) {
  this.stopScrolling = false;
  this.animationDelay = delay;
  this.animationStep = step;
  this.DoScroll(-direction);
 },
 StopScrolling: function() {
  this.stopScrolling = true;
 },
 IsStopped: function() {
  return this.stopScrolling;
 }
});
(function(){
 ASPxScrollingManager.scrollWrapper = function(scrollableArea){
  this.scrollableArea = scrollableArea;
  this.Initialize();
 };
 ASPxScrollingManager.scrollWrapper.prototype = {
  Initialize: function(){
   this.scrollableArea.style.position = "relative";
   this.scrollableArea.parentNode.style.position = "relative";
  },
  GetScrollLeft: function(){ return _aspxPxToInt(this.scrollableArea.style.left); },
  GetScrollTop:  function(){ return _aspxPxToInt(this.scrollableArea.style.top); },
  SetScrollLeft: function(value){ this.scrollableArea.style.left = value + "px"; },
  SetScrollTop:  function(value){ this.scrollableArea.style.top  = value + "px"; }
 };
 ASPxScrollingManager.scrollWrapperTouchUI = function(scrollableArea, onScroll){
  this.scrollableArea = scrollableArea;
  this.scrollTimerId = -1;
  this.onScroll = onScroll;
  this.Initialize(onScroll);
 };
 ASPxScrollingManager.scrollWrapperTouchUI.prototype = {
  Initialize: function(){
   var div = this.scrollableArea.parentNode;
   var timeout = __aspxMSTouchUI ? 500 : 1000;
   var nativeScrollSupported = __aspxMSTouchUI || ASPxClientTouchUI.nativeWebKitScrollingSupported();
   this.onScrollCore = function(){
     _aspxClearTimer(this.scrollTimerId);
     if(this.onScrollLocked) return;
     this.scrollTimerId = window.se...
```

https://md1npdvpadss02.dev.corp.local/dxr.axd

```
var __aspxMIIdSuffix = "_DXI";
var __aspxMMIdSuffix = "_DXM";
var __aspxSBIdSuffix = "_DXSB";
var __aspxSBUIdEnd = "_U";
var __aspxSBDIdEnd = "_D";
ASPxClientMenuItemInfo = _aspxCreateClass(null, {
 constructor: function(menu, indexPath){
  var itemElement = menu.GetItemElement(indexPath);
  this.clientHeight = itemElement.clientHeight;
  this.clientWidth = itemElement.clientWidth;
  this.clientTop = _aspxGetClientTop(itemElement);
  this.clientLeft = _aspxGetClientLeft(itemElement);
  this.offsetHeight = itemElement.offsetHeight;
  this.offsetWidth = itemElement.offsetWidth;
  this.offsetTop = 0;
  this.offsetLeft = 0;
 }
});
ASPxClientMenuCssClasses = {};
ASPxClientMenuCssClasses.Prefix = "dxm-";
ASPxClientMenuCssClasses.Menu = "dxmLite";
ASPxClientMenuCssClasses.BorderCorrector = "dxmBrdCor";
ASPxClientMenuCssClasses.Disabled = ASPxClientMenuCssClasses.Prefix + "disabled";
ASPxClientMenuCssClasses.MainMenu = ASPxClientMenuCssClasses.Prefix + "main";
ASPxClientMenuCssClasses.PopupMenu = ASPxClientMenuCssClasses.Prefix + "popup";
ASPxClientMenuCssClasses.IE7 = ASPxClientMenuCssClasses.Prefix + "ie7";
ASPxClientMenuCssClasses.HorizontalMenu = ASPxClientMenuCssClasses.Prefix + "horizontal";
ASPxClientMenuCssClasses.VerticalMenu = ASPxClientMenuCssClasses.Prefix + "vertical";
ASPxClientMenuCssClasses.NoWrapMenu = ASPxClientMenuCssClasses.Prefix + "noWrap";
ASPxClientMenuCssClasses.AutoWidthMenu = ASPxClientMenuCssClasses.Prefix + "autoWidth";
ASPxClientMenuCssClasses.DX = "dx";
ASPxClientMenuCssClasses.Separator = ASPxClientMenuCssClasses.Prefix + "separator";
ASPxClientMenuCssClasses.Spacing = ASPxClientMenuCssClasses.Prefix + "spacing";
ASPxClientMenuCssClasses.Gutter = ASPxClientMenuCssClasses.Prefix + "gutter";
ASPxClientMenuCssClasses.WithoutImages = ASPxClientMenuCssClasses.Prefix + "noImages";
ASPxClientMenuCssClasses.Item = ASPxClientMenuCssClasses.Prefix + "item";
ASPxClientMenuCssClasses.ItemHovered = ASPxClientMenuCssClasses.Prefix + "hovered";
ASPxClientMenuCssClasses.ItemSelected = ASPxClientMenuCssClasses.Prefix + "selected";
ASPxClientMenuCssClasses.ItemChecked = ASPxClientMenuCssClasses.Prefix + "checked";
ASPxClientMenuCssClasses.ItemWithoutImage = ASPxClientMenuCssClasses.Prefix + "noImage";
ASPxClientMenuCssClasses.ItemWithSubMenu = ASPxClientMenuCssClasses.Prefix + "subMenu";
ASPxClientMenuCssClasses.ItemDropDownMode = ASPxClientMenuCssClasses.Prefix + "dropDownMode";
ASPxClientMenuCssClasses.ItemWithoutSubMenu = ASPxClientMenuCssClasses.Prefix + "noPopOut";
ASPxClientMenuCssClasses.ContentContainer = ASPxClientMenuCssClasses.Prefix + "content";
ASPxClientMenuCssClasses.Image = ASPxClientMenuCssClasses.Prefix + "image";
ASPxClientMenuCssClasses.PopOutContainer = ASPxClientMenuCssClasses.Prefix + "popOut";
ASPxClientMenuCssClasses.PopOutImage = ASPxClientMenuCssClasses.Prefix + "pImage";
ASPxClientMenuCssClasses.ImageLeft = ASPxClientMenuCssClasses.Prefix + "image-l";
ASPxClientMenuCssClasses.ImageRight = ASPxClientMenuCssClasses.Prefix + "image-r";
ASPxClientMenuCssClasses.ImageTop = ASPxClientMenuCssClasses.Prefix + "image-t";
ASPxClientMenuCssClasses.ImageBottom = ASPxClientMenuCssClasses.Prefix + "image-b";
ASPxClientMenuCssClasses.ScrollArea = ASPxClientMenuCssClasses.Prefix + "scrollArea";
ASPxClientMenuCssClasses.ScrollUpButton = ASPxClientMenuCssClasses.Prefix + "scrollUpBtn";
ASPxClientMenuCssClasses.ScrollDownButton = ASPxClientMenuCssClasses.Prefix + "scrollDownBtn";
ASPxClientMenuLiteRenderHelper = {};
ASPxClientMenuLiteRenderHelper.InlineInitializeElements = function(menu) {
 if(!menu.isPopupMenu)
  this.InlineInitializeMainMenuElements(menu, menu.GetMainElement());
 var commonContainer = menu.GetMainElement().parentNode;
 var subMenuElements = this.GetNodesByTagName(commonContainer, "DIV");
 for(var i = 0; i < subMenuElements.length; i++) {
  if(!menu.isPopupMenu && subMenuElements[i] == menu.GetMainElement())
   continue;
  this.InlineInitializeSubMenuElements(menu, subMenuElements[i]);
 }
};
ASPxClientMenuLiteRenderHelper.FindNodes = function(node, match) {
 var result = [];
 for(var i = 0; i < node.childNodes.length; i++) {
  var childNode = node.childNodes[i];
  if(!childNode.tagName)
   continue;
  if(match(childNode))
   result.push(childNode);
 }
 return result;
};
ASPxClientMenuLiteRenderHelper.GetNodesByTagName = function(node, tagName) {
 return this.FindNodes(node, function(childNode) {
  return childNode.tagName == tagName;
 });
};
ASPxClientMenuLiteRenderHelper.GetNodesByClassName = function(node, className) {
 return this.FindNodes(node, function(childNode) {
  return _aspxElementCssClassContains(childNode, className);
 });
};
ASPxClientMenuLiteRenderHelper.GetNodeByClassName = function(node, childNodeClassName) {
 var nodes = this.GetNodesByClassName(node, childNodeClassName);
 return nodes.length > 0 ? nodes[0] : null;
};
ASPxClientMenuLiteRenderHelper.InlineInitializeScr...
```

Cookies 1

TOC

Name	First Set	Domain	Secure
Value	Requested URL		Expires
ASP.NET_SessionId	https://md1npdvpadss02.dev.corp.local/Login.aspx	md1npdvpadss02.dev.corp.local	False

anb24vgkocow4szzzqtqbybi	https://md1npdvpadss02.dev.corp.local/DXR.axd?r=1_155-i3tS8