Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 9.0.3.13, Rules: 18533
Scan started: 10/20/2019 3:02:20 PM

Table of Contents

Introduction

Summary

Issues Sorted by Issue Type

Fix Recommendations

Advisories

- Link to Non-Existing Domain Found
- Unencrypted Login Request
- Body Parameters Accepted in Query
- Missing or insecure "Content-Security-Policy" header
- Missing or insecure "X-Content-Type-Options" header
- Missing or insecure "X-XSS-Protection" header

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.

High severity issues:	2
Low severity issues:	10
Total security issues included in the report:	12
Total security issues discovered in the scan:	12

General Information

Scan file name:	MohanLal_201019
Scan started:	10/20/2019 3:02:20 PM
Test policy:	Default

Host	10.90.171.82
Port	8080
Operating system:	Unknown
Web server:	Apache
Application server:	Tomcat

Login Settings

Login method:	Recorded login
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:	`http://10.90.171.82:8080/hpcl_grp1/Event/`

Summary

Issue Types 6

TOC

	Issue Type	Number of Issues
H	Link to Non-Existing Domain Found	1
H	Unencrypted Login Request	1
L	Body Parameters Accepted in Query	1
L	Missing or insecure "Content-Security-Policy" header	3
L	Missing or insecure "X-Content-Type-Options" header	3
L	Missing or insecure "X-XSS-Protection" header	3

Vulnerable URLs 4

TOC

	URL	Number of Issues
H	http://10.90.171.82:8080/hpcl_grp1/Event/	1
H	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp	5
L	http://10.90.171.82:8080/hpcl_grp1/Event/js/jquery-1.11.1.min.js	3
L	http://10.90.171.82:8080/hpcl_grp1/Event/js/snow.js	3

Fix Recommendations 6

TOC

	Remediation Task	Number of Issues
H	Always use SSL and POST (body) parameters when sending sensitive information.	1
H	Remove the non-existing domain from the web site	1
L	Config your server to use the "Content-Security-Policy" header with secure policies	3
L	Config your server to use the "X-Content-Type-Options" header with	3

	"nosniff" value	
L	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)	3
L	Do not accept body parameters that are sent in the query string	1

Security Risks 3

TOC

	Risk	Number of Issues
H	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	11
H	It may be possible to steal user login information such as usernames and passwords that are sent unencrypted	1
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	10

Causes 3

TOC

	Cause	Number of Issues
H	The web application contains a link to a non-existing domain	1
H	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted	1
L	Insecure web application programming or configuration	10

WASC Threat Classification

TOC

Threat	Number of Issues
Information Leakage	10
Insufficient Transport Layer Protection	1
URL Redirector Abuse	1

Issues Sorted by Issue Type

H Link to Non-Existing Domain Found 1

TOC

Issue 1 of 1

TOC

Link to Non-Existing Domain Found

Severity:	High
CVSS Score:	8.5
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/
Entity:	https://maxcdn.bootstrapcdn.com/font-awesome/4.4.0/css/font-awesome.min.css (Link)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The web application contains a link to a non-existing domain
Fix:	Remove the non-existing domain from the web site

Difference:

Reasoning: AppScan found a link to an external site, and was not able to resolve it

Test Requests and Responses:

```
GET /hpcl_grp1/Event/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 2678
Date: Sun, 20 Oct 2019 10:02:38 GMT
Content-Type: text/html;charset=ISO-8859-1

<html>
<head>

<title>Event Nomination</title>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.4.0/css/font-
awesome.min.css">
  <link rel="stylesheet" href="css/style1.css">
<link rel="stylesheet" href="css/styles.css">
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<script src="js/jquery-1.11.1.min.js" type="text/javascript"></script>
<script type="text/javascript" src="js/snow.js"></script>
<style>
.listTh{
    background-color: #297DB5;
   --- opacity: .4;

}
</style>
<script type="text/javascript">
$(function() {
 //$(document).snow({ SnowImage:
["images/star1.png","images/star2.png","images/star3.jpg","images/star4.gif"], Quantity: 20 });
});
</script>
<style>
.indexForm {background-color: #cef6f5; background: url("images/bgGif1.gif");}
</style>
</head>
<body>
<table class="listTable1" style="width:100%;background-color:"><tr><th style="width:70px;"><img
src="images/logo3.png" style="height:90px;float:left;"></img></th>
<th class="listTh">
<label id ="masterheader"><font color="white" style= "bold">Event Nomination </font></label>
<div style='color:white; font-size:24px; margin-top:10px;'>Employee Connect / Reboot35+ /
Yuvantage / Sampark</div>
</th>
</tr></table>
<div class = "indexForm">
<form id="login" action="login.jsp" autocomplete="off"  method="POST"  onsubmit="return
FrontPage_Form1_Validator(this)"  name="FrontPage_Form1" >
<!--<div class="masthead">
<div style="width:10%"><img src="logo.png" style="height:auto;width:100px"></img></div>
<div ><h1 class="site-title" style="margin-left:30%" >Intimation under CDA rule</h1></div>
</div>-->
<br><br><br><br><br>
    <div class="login">
      <h1>Login</h1>
        <p><input type="text" name="t1" id="t1" MAXLENGTH="8"  placeholder="Employe No."></p>
        <p><input type="password" name="t2" id="t2"  placeholder="Password"></p>
        <p class="submit"><input type="submit" name="commit" value="Login"></p>
 </div><br/><br/>

 </form>
 <div style="width: 490px; margin-left: auto; margin-right: auto; margin-top: 20%;"
align="center">
         <div style="margin-bottom: 10%;">'

                 <a href="winner.jsp" style="text-decoration: none;">
                         <!--<div style="background: url('images/ribbon.png') no-repeat
scroll 0px 0px transparent; height: 170px; padding-top: 28px; font-size: 25px; font-weight: bold;
font-family: arial; color: white;">
                                 <!--<span style="margin-left: 10px; margin-right:
250px;">Click</span>
                                 <span>Here</span
                         </div>>-->
                 </a>
         </div>
 </div>
</div>
</body>
</html>
```

H Unencrypted Login Request 1

TOC

Issue 1 of 1

TOC

Unencrypted Login Request

Severity:	High
CVSS Score:	8.5
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp
Entity:	t2 (Parameter)
Risk:	It may be possible to steal user login information such as usernames and passwords that are sent unencrypted
Causes:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Difference:

Reasoning: AppScan identified a password parameter that was not sent over SSL.

Test Requests and Responses:

```
POST /hpcl_grp1/Event/login.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Content-Length: 28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

t1=1234&t2=1234&commit=Login

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 472
Date: Sun, 20 Oct 2019 10:02:44 GMT
Content-Type: text/html;charset=ISO-8859-1









<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">







<HTML>

<form method="POST" action="" name="FrontPage_Form1">

 <script language="Javascript">
```

```
                 alert("User not found.");
                 document.location.href = "index.jsp";
 </script>

         <script language="Javascript">
                 alert("Please enter Proper Credentials.");
                 document.location.href = "index.jsp";
         </script>


</form>
</HTML>
</html>
```

L Body Parameters Accepted in Query 1 TOC

Issue 1 of 1 TOC

Body Parameters Accepted in Query

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp
Entity:	login.jsp (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Do not accept body parameters that are sent in the query string

Difference: **Body Parameter** removed from request: `1234`
Query Parameter added to request: `1234`
Body Parameter removed from request: `1234`
Query Parameter added to request: `1234`
Body Parameter removed from request: `Login`
Query Parameter added to request: `Login`
Method manipulated from: `POST` to: `GET`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Test Requests and Responses:

```
GET /hpcl_grp1/Event/login.jsp?t1=1234&t2=1234&commit=Login HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 472
Date: Sun, 20 Oct 2019 10:03:20 GMT
Content-Type: text/html;charset=ISO-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">




<HTML>

<form method="POST" action="" name="FrontPage_Form1">

 <script language="Javascript">
                alert("User not found.");
                document.location.href = "index.jsp";
 </script>

         <script language="Javascript">
                alert("Please enter Proper Credentials.");
                document.location.href = "index.jsp";
         </script>


</form>
</HTML>
</html>
```

Original Response

≈

Test Response

L Missing or insecure "Content-Security-Policy" header 3 TOC

Issue 1 of 3

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/js/snow.js
Entity:	snow.js (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

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

Test Requests and Responses:

```
GET /hpcl_grp1/Event/js/snow.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Mon, 24 Nov 2014 12:00:26 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 2651
ETag: W/"2651-1416830426758"
Date: Sun, 20 Oct 2019 10:03:16 GMT
Content-Type: application/javascript

/**
 * jQuery snow effects.
 *
 * This is a heavily modified, jQuery-adapted, browser-agnostic version of
 * "Snow Effect Script" by Altan d.o.o. (http://www.altan.hr/snow/index.html).
 *
 * Dustin Oprea (2011)
 */

function __ShowSnow(settings)
{

    var snowsrc = settings.SnowImage;
    var no = settings.Quantity;

    var dx, xp, yp;    // coordinate and position variables
    var am, stx, sty;  // amplitude and step variables
    var i;

    var doc_width = $(window).width() - 10;
    var doc_height = $(window).height();

    dx = [];
    xp = [];
    yp = [];
    am = [];
    stx = [];
    sty = [];
    flakes = [];
    for (i = 0; i < no; ++i)
    {
        dx[i] = 0;          // set coordinate variables
        xp[i] = Math.random()*(doc_width-50);  // set position variables
        yp[i] = Math.random()*doc_height;
        am[i] = Math.random()*20;         // set amplitude variables
        stx[i] = 0.02 + Math.random()/10; // set step variables
        sty[i] = 0.7 + Math.random();     // set step variables

        var flake = $("<div />");

        var id = ("dot" + i);
        flake.attr("id", id);
        flake.css({
          position: "absolute",
          zIndex: i,
          top: "15px",
          left: "15px"
          });

        flake.append("<img src='" + snowsrc[i%4] + "'>");
        flake.appendTo("body");

        flakes[i] = $("#" + id);
    }

    var animateSnow;
    animateSnow = function()
    {
        for (i = 0; i < no; ++ i)
        {
          // iterate for every dot
          yp[i] += sty[i];
          if (yp[i] > doc_height - 50)
          {
          xp[i] = Math.random() * (doc_width - am[i] - 30);
          yp[i] = 0;
          stx[i] = 0.02 + Math.random() / 10;
          sty[i] = 0.7 + Math.random();
          }

          dx[i] += stx[i];
          flakes[i].css("top", yp[i] + "px");
          flakes[i].css("left", (xp[i] + am[i] * Math.sin(dx[i])) + "px");
        }

        snowtimer = setTimeout(animateSnow, 10);
    };

 function hidesnow()
    {
         if(window.snowtimer)
          clearTimeout(snowtimer)

        for (i = 0; i < no; i++)
          flakes[i].hide();
        }

    animateSnow();
 if (settings.HideSnowTime > 0)
        setTimeout(hidesnow, settings.HideSnowTime * 1000)
}

(function($) {
    $.fn.snow = function(options) {

    var settings = $.extend({
          SnowImage:      undefined,
          Quantity:       7,
          HideSnowTime:   0
        }, options);

    __ShowSnow(settings);

    return this;
  }
})(jQuery);
```

Issue 2 of 3

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp
Entity:	login.jsp (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

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

Test Requests and Responses:

```
POST /hpcl_grp1/Event/login.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Content-Length: 28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

t1=1234&t2=1234&commit=Login

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 472
Date: Sun, 20 Oct 2019 10:03:20 GMT
Content-Type: text/html;charset=ISO-8859-1









<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
```

```
<HTML>

<form method="POST" action="" name="FrontPage_Form1">

 <script language="Javascript">
                 alert("User not found.");
                 document.location.href = "index.jsp";
 </script>

         <script language="Javascript">
                 alert("Please enter Proper Credentials.");
                 document.location.href = "index.jsp";
         </script>


</form>
</HTML>
</html>
```

Issue 3 of 3

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/js/jquery-1.11.1.min.js
Entity:	jquery-1.11.1.min.js (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

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

Test Requests and Responses:

```
GET /hpcl_grp1/Event/js/jquery-1.11.1.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 19 Aug 2014 05:12:15 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 95786
ETag: W/"95786-1408425135754"
```

```
Date: Sun, 20 Oct 2019 10:03:19 GMT
Content-Type: application/javascript

/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?
module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a
window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b)
{var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k=
{},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|
[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return
b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function()
{return d.call(this)},get:function(a){return null!=a?0>a?
this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var
b=m.merge(this.constructor(),a);return
b.prevObject=this,b.context=this.context,b},each:function(a,b){return
m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return
this.pushStack(d.apply(this,arguments))},first:function(){return this.eq(0)},last:function()
{return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor(null)},push:f,sort:c.sort,splice:c.splice},m.extend=m.fn.extend
=function(){var a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof
g&&(j=g,g=arguments[h]||{},h++),"object"==typeof g||m.isFunction(g)||(g={}),h===i&&(g=this,h--
);i>h;h++)if(null!=(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(m.isPlainObject(c)||
(b=m.isArray(c)))?(b?(b=!1,f=a&&m.isArray(a)?a:[]):f=a&&m.isPlainObject(a)?a:
{},g[d]=m.extend(j,f,c)):void 0!==c&&(g[d]=c));return g},m.extend({expando:"jQuery"+
(l+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new
Error(a)},noop:function(){},isFunction:function(a)
{return"function"===m.type(a)},isArray:Array.isArray||function(a)
{return"array"===m.type(a)},isWindow:function(a){return
null!=a&&a==a.window},isNumeric:function(a){return!m.isArray(a)&&a-
parseFloat(a)>=0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==m.type(a)||a.nodeType||m.isWindow(a))return!1;try{if(a.constructor&&!j.call(a
,"constructor")&&!j.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c)
{return!1}if(k.ownLast)for(b in a)return j.call(a,b);for(b in a);return void
0===b||j.call(a,b)},type:function(a){return null==a?a+"":"object"==typeof a||"function"==typeof
a?h[i.call(a)]||"object":typeof a},globalEval:function(b){b&&m.trim(b)&&
(a.execScript||function(b){a.eval.call(a,b)})(b)},camelCase:function(a){return a.replace(o,"ms-
").replace(p,q)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b,c){var
d,e=0,f=a.length,g=r(a);if(c){if(g){for(;f>e;e++)if(d=b.apply(a[e],c),d===!1)break}else for(e in
a)if(d=b.apply(a[e],c),d===!1)break}else if(g)
{for(;f>e;e++)if(d=b.call(a[e],e,a[e]),d===!1)break}else for(e in
a)if(d=b.call(a[e],e,a[e]),d===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(n,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(r(Object(a))?
m.merge(c,"string"==typeof a?[a]:a):f.call(c,a)),c},inArray:function(a,b,c){var d;if(b)
{if(g)return g.call(b,a,c);for(d=b.length,c=c?0>c?Math.max(0,d+c):c:0;d>c;c++)if(c in
b&&b[c]===a)return c}return-1},merge:function(a,b){var
c=+b.length,d=0,e=a.length;while(c>d)a[e++]=b[d++];if(c!==c)while(void
0!==b[d])a[e++]=b[d++];return a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var
d,f=0,g=a.length,h=r(a),i=[];if(h)for(;g>f;f++)d=b(a[f],f,c),null!=d&&i.push(d);else for(f in
a)d=b(a[f],f,c),null!=d&&i.push(d);return e.apply([],i)},guid:1,proxy:function(a,b){var
c,e,f;return"string"==typeof b&&(f=a[b],b=a,a=f),m.isFunction(a)?
(c=d.call(arguments,2),e=function(){return
a.apply(b||this,c.concat(d.call(arguments)))},e.guid=a.guid=a.guid||m.guid++,e):void
0},now:function(){return+new Date},support:k}),m.each("Boolean Number String Function Array Date
RegExp Object Error".split(" "),function(a,b){h["[object "+b+"]"]=b.toLowerCase()});function r(a)
{var
...
...
...
```

L Missing or insecure "X-Content-Type-Options" header 3

TOC

Issue 1 of 3

TOC

Missing or insecure "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/js/jquery-1.11.1.min.js
Entity:	jquery-1.11.1.min.js (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Difference:

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

Test Requests and Responses:

```
GET /hpcl_grp1/Event/js/jquery-1.11.1.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 19 Aug 2014 05:12:15 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 95786
ETag: W/"95786-1408425135754"
Date: Sun, 20 Oct 2019 10:03:19 GMT
Content-Type: application/javascript

/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?
module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a
window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b)
{var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k=
{},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|
[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return
b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function()
{return d.call(this)},get:function(a){return null!=a?0>a?
this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var
b=m.merge(this.constructor(),a);return
b.prevObject=this,b.context=this.context,b},each:function(a,b){return
m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return
this.pushStack(d.apply(this,arguments))},first:function(){return this.eq(0)},last:function()
{return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor(null)},push:f,sort:c.sort,splice:c.splice},m.extend=m.fn.extend
=function(){var a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof
g&&(j=g,g=arguments[h]||{},h++),"object"==typeof g||m.isFunction(g)||(g={}),h===i&&(g=this,h--
);i>h;h++)if(null!=(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(m.isPlainObject(c)||
(b=m.isArray(c)))?(b?(b=!1,f=a&&m.isArray(a)?a:[]):f=a&&m.isPlainObject(a)?a:
{},g[d]=m.extend(j,f,c)):void 0!==c&&(g[d]=c));return g},m.extend({expando:"jQuery"+
(1+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new
Error(a)},noop:function(){},isFunction:function(a)
{return"function"===m.type(a)},isArray:Array.isArray||function(a)
{return"array"===m.type(a)},isWindow:function(a){return
null!=a&&a==a.window},isNumeric:function(a){return!m.isArray(a)&&a-
parseFloat(a)>=0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==m.type(a)||a.nodeType||m.isWindow(a))return!1;try{if(a.constructor&&!j.call(a
,"constructor")&&!j.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c)
{return!1}if(k.ownLast)for(b in a)return j.call(a,b);for(b in a);return void
0===b||j.call(a,b)},type:function(a){return null==a?a+"":"object"==typeof a||"function"==typeof
a?h[i.call(a)]||"object":typeof a},globalEval:function(b){b&&m.trim(b)&&
(a.execScript||function(b){a.eval.call(a,b)})(b)},camelCase:function(a){return a.replace(o,"ms-
").replace(p,q)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b,c){var
d,e=0,f=a.length,g=r(a);if(c){if(g){for(;f>e;e++)if(d=b.apply(a[e],c),d===!1)break}else for(e in
a)if(d=b.apply(a[e],c),d===!1)break}else if(g)
{for(;f>e;e++)if(d=b.call(a[e],e,a[e]),d===!1)break}else for(e in
a)if(d=b.call(a[e],e,a[e]),d===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(n,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(r(Object(a))?
m.merge(c,"string"==typeof a?[a]:a):f.call(c,a)),c},inArray:function(a,b,c){var d;if(b)
{if(g)return g.call(b,a,c);for(d=b.length,c=c?0>c?Math.max(0,d+c):c:0;d>c;c++)if(c in
b&&b[c]===a)return c}return-1},merge:function(a,b){var
c=+b.length,d=0,e=a.length;while(c>d)a[e++]=b[d++];if(c!==c)while(void
0!==b[d])a[e++]=b[d++];return a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var
d,f=0,g=a.length,h=r(a),i=[];if(h)for(;g>f;f++)d=b(a[f],f,c),null!=d&&i.push(d);else for(f in
a)d=b(a[f],f,c),null!=d&&i.push(d);return e.apply([],i)},guid:1,proxy:function(a,b){var
c,e,f;return"string"==typeof b&&(f=a[b],b=a,a=f),m.isFunction(a)?
(c=d.call(arguments,2),e=function(){return
a.apply(b||this,c.concat(d.call(arguments)))},e.guid=a.guid=a.guid||m.guid++,e):void
0},now:function(){return+new Date},support:k}),m.each("Boolean Number String Function Array Date
RegExp Object Error".split(" "),function(a,b){h["[object "+b+"]"]=b.toLowerCase()});function r(a)
{var
...
...
...
```

Issue 2 of 3

TOC

Missing or insecure "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/js/snow.js
Entity:	snow.js (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Difference:

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

Test Requests and Responses:

```
GET /hpcl_grp1/Event/js/snow.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Mon, 24 Nov 2014 12:00:26 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 2651
ETag: W/"2651-1416830426758"
Date: Sun, 20 Oct 2019 10:03:16 GMT
Content-Type: application/javascript

/**
 * jQuery snow effects.
 *
 * This is a heavily modified, jQuery-adapted, browser-agnostic version of
 * "Snow Effect Script" by Altan d.o.o. (http://www.altan.hr/snow/index.html).
 *
 * Dustin Oprea (2011)
 */

function __ShowSnow(settings)
{

    var snowsrc = settings.SnowImage;
    var no = settings.Quantity;

    var dx, xp, yp;    // coordinate and position variables
    var am, stx, sty;  // amplitude and step variables
    var i;

    var doc_width = $(window).width() - 10;
    var doc_height = $(window).height();

    dx = [];
    xp = [];
    yp = [];
    am = [];
    stx = [];
    sty = [];
    flakes = [];
    for (i = 0; i < no; ++i)
    {
        dx[i] = 0;          // set coordinate variables
        xp[i] = Math.random()*(doc_width-50);  // set position variables
        yp[i] = Math.random()*doc_height;
        am[i] = Math.random()*20;         // set amplitude variables
        stx[i] = 0.02 + Math.random()/10; // set step variables
        sty[i] = 0.7 + Math.random();     // set step variables

        var flake = $("<div />");

        var id = ("dot" + i);
        flake.attr("id", id);
        flake.css({
          position: "absolute",
          zIndex: i,
          top: "15px",
          left: "15px"
          });

        flake.append("<img src='" + snowsrc[i%4] + "'>");
        flake.appendTo("body");

        flakes[i] = $("#" + id);
    }

    var animateSnow;
    animateSnow = function()
    {
        for (i = 0; i < no; ++ i)
        {
          // iterate for every dot
          yp[i] += sty[i];
          if (yp[i] > doc_height - 50)
          {
          xp[i] = Math.random() * (doc_width - am[i] - 30);
          yp[i] = 0;
          stx[i] = 0.02 + Math.random() / 10;
          sty[i] = 0.7 + Math.random();
          }

          dx[i] += stx[i];
          flakes[i].css("top", yp[i] + "px");
          flakes[i].css("left", (xp[i] + am[i] * Math.sin(dx[i])) + "px");
        }

        snowtimer = setTimeout(animateSnow, 10);
    };

 function hidesnow()
    {
         if(window.snowtimer)
          clearTimeout(snowtimer)

        for (i = 0; i < no; i++)
          flakes[i].hide();
        }

    animateSnow();
 if (settings.HideSnowTime > 0)
        setTimeout(hidesnow, settings.HideSnowTime * 1000)
}

(function($) {
    $.fn.snow = function(options) {

    var settings = $.extend({
          SnowImage:      undefined,
          Quantity:       7,
          HideSnowTime:   0
        }, options);

    __ShowSnow(settings);

    return this;
  }

})(jQuery);
```

Issue 3 of 3

TOC

Missing or insecure "X-Content-Type-Options" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp
Entity:	login.jsp (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Difference:

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

Test Requests and Responses:

```
POST /hpcl_grp1/Event/login.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Content-Length: 28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

t1=1234&t2=1234&commit=Login

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 472
Date: Sun, 20 Oct 2019 10:03:20 GMT
Content-Type: text/html;charset=ISO-8859-1









<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">







<HTML>

<form method="POST" action="" name="FrontPage_Form1">

 <script language="Javascript">
                 alert("User not found.");
                 document.location.href = "index.jsp";
 </script>

         <script language="Javascript">
                 alert("Please enter Proper Credentials.");
```

```
                document.location.href = "index.jsp";
        </script>


</form>
</HTML>
</html>
```

L Missing or insecure "X-XSS-Protection" header 3 TOC

Issue 1 of 3 TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/js/jquery-1.11.1.min.js
Entity:	jquery-1.11.1.min.js (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Difference:

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

Test Requests and Responses:

```
GET /hpcl_grp1/Event/js/jquery-1.11.1.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 19 Aug 2014 05:12:15 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 95786
ETag: W/"95786-1408425135754"
Date: Sun, 20 Oct 2019 10:03:19 GMT
Content-Type: application/javascript

/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
```

```
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?
module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a
window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b)
{var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k=
{},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|
[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return
b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function()
{return d.call(this)},get:function(a){return null!=a?0>a?
this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var
b=m.merge(this.constructor(),a);return
b.prevObject=this,b.context=this.context,b},each:function(a,b){return
m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return
this.pushStack(d.apply(this,arguments))},first:function(){return this.eq(0)},last:function()
{return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor(null)},push:f,sort:c.sort,splice:c.splice},m.extend=m.fn.extend
=function(){var a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof
g&&(j=g,g=arguments[h]||{},h++),"object"==typeof g||m.isFunction(g)||(g={}),h===i&&(g=this,h--
);i>h;h++)if(null!=(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(m.isPlainObject(c)||
(b=m.isArray(c)))?(b?(b=!1,f=a&&m.isArray(a)?a:[]):f=a&&m.isPlainObject(a)?a:
{},g[d]=m.extend(j,f,c)):void 0!==c&&(g[d]=c));return g},m.extend({expando:"jQuery"+
(l+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new
Error(a)},noop:function(){},isFunction:function(a)
{return"function"===m.type(a)},isArray:Array.isArray||function(a)
{return"array"===m.type(a)},isWindow:function(a){return
null!=a&&a==a.window},isNumeric:function(a){return!m.isArray(a)&&a-
parseFloat(a)>=0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==m.type(a)||a.nodeType||m.isWindow(a))return!1;try{if(a.constructor&&!j.call(a
,"constructor")&&!j.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c)
{return!1}if(k.ownLast)for(b in a)return j.call(a,b);for(b in a);return void
0===b||j.call(a,b)},type:function(a){return null==a?a+"":"object"==typeof a||"function"==typeof
a?h[i.call(a)]||"object":typeof a},globalEval:function(b){b&&m.trim(b)&&
(a.execScript||function(b){a.eval.call(a,b)})(b)},camelCase:function(a){return a.replace(o,"ms-
").replace(p,q)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b,c){var
d,e=0,f=a.length,g=r(a);if(c){if(g){for(;f>e;e++)if(d=b.apply(a[e],c),d===!1)break}else for(e in
a)if(d=b.apply(a[e],c),d===!1)break}else if(g)
{for(;f>e;e++)if(d=b.call(a[e],e,a[e]),d===!1)break}else for(e in
a)if(d=b.call(a[e],e,a[e]),d===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(n,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(r(Object(a))?
m.merge(c,"string"==typeof a?[a]:a):f.call(c,a)),c},inArray:function(a,b,c){var d;if(b)
{if(g)return g.call(b,a,c);for(d=b.length,c=c?0>c?Math.max(0,d+c):c:0;d>c;c++)if(c in
b&&b[c]===a)return c}return-1},merge:function(a,b){var
c=+b.length,d=0,e=a.length;while(c>d)a[e++]=b[d++];if(c!==c)while(void
0!==b[d])a[e++]=b[d++];return a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var
d,f=0,g=a.length,h=r(a),i=[];if(h)for(;g>f;f++)d=b(a[f],f,c),null!=d&&i.push(d);else for(f in
a)d=b(a[f],f,c),null!=d&&i.push(d);return e.apply([],i)},guid:1,proxy:function(a,b){var
c,e,f;return"string"==typeof b&&(f=a[b],b=a,a=f),m.isFunction(a)?
(c=d.call(arguments,2),e=function(){return
a.apply(b||this,c.concat(d.call(arguments)))},e.guid=a.guid=a.guid||m.guid++,e):void
0},now:function(){return+new Date},support:k}),m.each("Boolean Number String Function Array Date
RegExp Object Error".split(" "),function(a,b){h["[object "+b+"]"]=b.toLowerCase()});function r(a)
{var
...
...
...
```

Issue 2 of 3

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/js/snow.js
Entity:	snow.js (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Difference:

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

Test Requests and Responses:

```
GET /hpcl_grp1/Event/js/snow.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Mon, 24 Nov 2014 12:00:26 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 2651
ETag: W/"2651-1416830426758"
Date: Sun, 20 Oct 2019 10:03:16 GMT
Content-Type: application/javascript

/**
 * jQuery snow effects.
 *
 * This is a heavily modified, jQuery-adapted, browser-agnostic version of
 * "Snow Effect Script" by Altan d.o.o. (http://www.altan.hr/snow/index.html).
 *
 * Dustin Oprea (2011)
 */

function __ShowSnow(settings)
{

    var snowsrc = settings.SnowImage;
    var no = settings.Quantity;

    var dx, xp, yp;    // coordinate and position variables
    var am, stx, sty;  // amplitude and step variables
    var i;

    var doc_width = $(window).width() - 10;
    var doc_height = $(window).height();

    dx = [];
    xp = [];
    yp = [];
    am = [];
    stx = [];
    sty = [];
    flakes = [];
    for (i = 0; i < no; ++i)
    {
        dx[i] = 0;          // set coordinate variables
        xp[i] = Math.random()*(doc_width-50);  // set position variables
        yp[i] = Math.random()*doc_height;
        am[i] = Math.random()*20;         // set amplitude variables
        stx[i] = 0.02 + Math.random()/10; // set step variables
        sty[i] = 0.7 + Math.random();     // set step variables

        var flake = $("<div />");

        var id = ("dot" + i);
        flake.attr("id", id);
        flake.css({
          position: "absolute",
          zIndex: i,
          top: "15px",
          left: "15px"
          });

        flake.append("<img src='" + snowsrc[i%4] + "'>");
        flake.appendTo("body");

        flakes[i] = $("#" + id);
    }

    var animateSnow;
    animateSnow = function()
    {
        for (i = 0; i < no; ++ i)
        {
          // iterate for every dot
          yp[i] += sty[i];
          if (yp[i] > doc_height - 50)
          {
          xp[i] = Math.random() * (doc_width - am[i] - 30);
          yp[i] = 0;
          stx[i] = 0.02 + Math.random() / 10;
          sty[i] = 0.7 + Math.random();
          }

          dx[i] += stx[i];
          flakes[i].css("top", yp[i] + "px");
          flakes[i].css("left", (xp[i] + am[i] * Math.sin(dx[i])) + "px");
        }

        snowtimer = setTimeout(animateSnow, 10);
    };

 function hidesnow()
    {
         if(window.snowtimer)
          clearTimeout(snowtimer)

        for (i = 0; i < no; i++)
          flakes[i].hide();
        }

    animateSnow();
 if (settings.HideSnowTime > 0)
        setTimeout(hidesnow, settings.HideSnowTime * 1000)
}

(function($) {
    $.fn.snow = function(options) {

    var settings = $.extend({
          SnowImage:      undefined,
          Quantity:       7,
          HideSnowTime:   0
        }, options);

    __ShowSnow(settings);

    return this;
  }
})(jQuery);
```

Issue 3 of 3

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp
Entity:	login.jsp (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to 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:	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)

Difference:

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

Test Requests and Responses:

```
POST /hpcl_grp1/Event/login.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.90.171.82:8080/hpcl_grp1/Event/
Cookie: JSESSIONID=53BFA9957EA077ECA63B790E527D2A08
Connection: Keep-Alive
Host: 10.90.171.82:8080
Content-Length: 28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded

t1=1234&t2=1234&commit=Login

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 472
Date: Sun, 20 Oct 2019 10:03:20 GMT
Content-Type: text/html;charset=ISO-8859-1








<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
```

```
<HTML>

<form method="POST" action="" name="FrontPage_Form1">

 <script language="Javascript">
                alert("User not found.");
                document.location.href = "index.jsp";
 </script>

         <script language="Javascript">
                 alert("Please enter Proper Credentials.");
                 document.location.href = "index.jsp";
         </script>


</form>
</HTML>
</html>
```

Fix Recommendations

H Always use SSL and POST (body) parameters when sending sensitive information. TOC

Issue Types that this task fixes

- Unencrypted Login Request

General

1. Make sure that all login requests are sent encrypted to the server.
2. 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 encrypted to the server.

H Remove the non-existing domain from the web site TOC

Issue Types that this task fixes

- Link to Non-Existing Domain Found

General

It is advised to remove all links to non-existent domains.

In addition, periodically check the validity of links to external sites.

L Config your server to use the "Content-Security-Policy" header with secure policies TOC

Issue Types that this task fixes

- Missing or insecure "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 with "nosniff" value TOC

Issue Types that this task fixes

- Missing or insecure "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-XSS-Protection" header with value '1' (enabled) TOC

Issue Types that this task fixes

- Missing or insecure "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 Do not accept body parameters that are sent in the query string TOC

Issue Types that this task fixes

- Body Parameters Accepted in Query

General

Re-program the application to disallow handling of POST parameters that were listed in the Query

Advisories

Link to Non-Existing Domain Found

TOC

Test Type:

Application-level test

Threat Classification:

URL Redirector Abuse

Causes:

The web application contains a link to a non-existing domain

Security Risks:

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:

601

Technical Description:

The web site contains a link to a non-existent domain.
An attacker can exploit this scenario to launch a phishing attack by registering the non-existent domain.
A naive user may browse to that link, thinking that he is within the original site, while in fact he is browsing the attacker site.
This situation may lead to sensitive information leakage, because the user trusts the malicious site.

Unencrypted Login Request

TOC

Test Type:

Application-level test

Threat Classification:

Insufficient Transport Layer Protection

Causes:

Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Security Risks:

It may be possible to steal user login information such as usernames and passwords that are sent unencrypted

Affected Products:

CWE:

523

X-Force:

52471

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 an unencrypted login request was sent to the server. Since some of the input fields used in a login process (for example: usernames, passwords, e-mail addresses, social security number, etc.) are personal and sensitive, it is recommended that they will be sent to the server over an encrypted connection (e.g. SSL).
Any information 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.

Body Parameters Accepted in Query

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:

200

References:

Hypertext Transfer Protocol (HTTP/1.1) Semantics and Content:
GET
POST

Technical Description:

GET requests are designed to query the server, while POST requests are for submitting data.
However, aside from the technical purpose, attacking query parameters is easier than body parameters, because sending a link to the original site, or posting it in a blog or comment, is easier and has better results than the alternative - in order to attack a request with body parameters, an attacker would need to create a page containing a form that will be submitted when visited by the victim.
It is a lot harder to convince the victim to visit a page that he doesn't know, than letting him visit the original site. It it therefore not recommended to support body parameters that arrive in the query string.

Missing or insecure "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:

CWE:

200

References:

List of useful HTTP headers
An Introduction to Content Security Policy
MDN web docs - 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.
To protect against Cross-Site Scripting, Cross-Frame Scripting and clickjacking, it is important to set the following policies with proper values:
Both of 'default-src' and 'frame-ancestors' policies, *OR* all of 'script-src', 'object-src' and 'frame-ancestors' policies.
For 'default-src', 'script-src' and 'object-src', insecure values such as '*', 'data:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
For 'frame-ancestors', insecure values such as '*' or 'data:' should be avoided.
Please refer the following links for more information.

Missing or insecure "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:

CWE:

200

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 or insecure "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:

CWE:

200

References:

List of useful HTTP headers
IE XSS Filter

Technical Description:

The "X-XSS-Protection" header with value '1' 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 defense against Cross-Site Scripting, it acts as an additional layer of protection.

Application Data

Visited URLs 5

TOC

URL
http://10.90.171.82:8080/hpcl_grp1/Event/
http://10.90.171.82:8080/hpcl_grp1/Event/js/jquery-1.11.1.min.js
http://10.90.171.82:8080/hpcl_grp1/Event/js/snow.js
http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp
http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp

Parameters 3

TOC

Name	Value	URL	Type
t1	1234	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp	Text
t2	1234	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp	Password
commit	Login	http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp	Submit

Failed Requests 2

TOC

URL	Reason
http://10.90.171.82:8080/hpcl_grp1/Event/winner.jsp	Response Status '404' - Not Found
http://10.90.171.82:8080/a	Response Status '404' - Not Found

Filtered URLs 10

TOC

URL	Reason

https://maxcdn.bootstrapcdn.com/font-awesome/4.4.0/css/font-awesome.min.css	Untested Web Server
http://10.90.171.82:8080/hpcl_grp1/Event/css/style1.css	File Extension
http://10.90.171.82:8080/hpcl_grp1/Event/css/styles.css	File Extension
http://10.90.171.82:8080/hpcl_grp1/Event/images/logo3.png	File Extension
http://10.90.171.82:8080/hpcl_grp1/Event/images/star2.png	File Extension
http://10.90.171.82:8080/hpcl_grp1/Event/images/star4.gif	File Extension
http://10.90.171.82:8080/hpcl_grp1/Event/images/bgGif1.gif	File Extension
http://10.90.171.82:8080/hpcl_grp1/Event/	Similar DOM
http://10.90.171.82:8080/hpcl_grp1/Event/index.jsp	Similar DOM
http://10.90.171.82:8080/hpcl_grp1/Event/	Similar Body

Comments 3

TOC

URL	Comment
http://10.90.171.82:8080/hpcl_grp1/Event/	<div class="masthead"> <div style="width:10%"><img src="logo.png" style="height:auto;width:100px"></img> </div> <div ><h1 class="site-title" style="margin-left:30%" >Intimation under CDA rule</h1></div> </div>
http://10.90.171.82:8080/hpcl_grp1/Event/	<div style="background: url('images/ribbon.png') no-repeat scroll 0px 0px transparent; height: 170px; padding-top: 28px; font-size: 25px; font-weight: bold; font-family: arial; color: white;"> <!--<span style="margin-left: 10px; margin-right: 250px;">Click</span> <span>Here</span </div>>
http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

JavaScripts 6

TOC

URL / Code

http://10.90.171.82:8080/hpcl_grp1/Event/

```
$(function() {//$(document).snow({ SnowImage:
["images/star1.png","images/star2.png","images/star3.jpg","images/star4.gif"], Quantity: 20 });});
```

http://10.90.171.82:8080/hpcl_grp1/Event/

```
return FrontPage_Form1_Validator(this)
```

http://10.90.171.82:8080/hpcl_grp1/Event/js/snow.js

```
/**
 * jQuery snow effects.
 *
 * This is a heavily modified, jQuery-adapted, browser-agnostic version of
 * "Snow Effect Script" by Altan d.o.o. (http://www.altan.hr/snow/index.html).
 *
 * Dustin Oprea (2011)
 */

function __ShowSnow(settings)
{

    var snowsrc = settings.SnowImage;
    var no = settings.Quantity;

    var dx, xp, yp;    // coordinate and position variables
    var am, stx, sty;  // amplitude and step variables
    var i;

    var doc_width = $(window).width() - 10;
    var doc_height = $(window).height();

    dx = [];
    xp = [];
    yp = [];
    am = [];
    stx = [];
    sty = [];
    flakes = [];
    for (i = 0; i < no; ++i)
    {
        dx[i] = 0;          // set coordinate variables
        xp[i] = Math.random()*(doc_width-50);  // set position variables
        yp[i] = Math.random()*doc_height;
        am[i] = Math.random()*20;         // set amplitude variables
        stx[i] = 0.02 + Math.random()/10; // set step variables
        sty[i] = 0.7 + Math.random();     // set step variables

        var flake = $("<div />");

        var id = ("dot" + i);
        flake.attr("id", id);
        flake.css({
          position: "absolute",
          zIndex: i,
          top: "15px",
          left: "15px"
          });

        flake.append("<img src='" + snowsrc[i%4] + "'>");
        flake.appendTo("body");

        flakes[i] = $("#" + id);
    }

    var animateSnow;
    animateSnow = function()
    {
        for (i = 0; i < no; ++ i)
        {
          // iterate for every dot
          yp[i] += sty[i];
          if (yp[i] > doc_height - 50)
          {
          xp[i] = Math.random() * (doc_width - am[i] - 30);
          yp[i] = 0;
          stx[i] = 0.02 + Math.random() / 10;
          sty[i] = 0.7 + Math.random();
          }
          dx[i] += stx[i];
          flakes[i].css("top", yp[i] + "px");
          flakes[i].css("left", (xp[i] + am[i] * Math.sin(dx[i])) + "px");
        }

        snowtimer = setTimeout(animateSnow, 10);
    };

 function hidesnow()
    {
         if(window.snowtimer)
          clearTimeout(snowtimer)

        for (i = 0; i < no; i++)
          flakes[i].hide();
        }

    animateSnow();
 if (settings.HideSnowTime > 0)
        setTimeout(hidesnow, settings.HideSnowTime * 1000)
}

(function($) {
    $.fn.snow = function(options) {

    var settings = $.extend({
          SnowImage:      undefined,
          Quantity:       7,
          HideSnowTime:   0
        }, options);

    __ShowSnow(settings);

    return this;
  }

})(jQuery);
```

http://10.90.171.82:8080/hpcl_grp1/Event/js/jquery-1.11.1.min.js

```
/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?
b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return
b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=
[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k=
{},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-
/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype=
{jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return
null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var
b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return
m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return this.pushStack(d.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor(null)},push:f,sort:c.sort,splice:c.splice},m.extend=m.fn.extend=function()
{var a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof g&&
(j=g,g=arguments[h]||{},h++),"object"==typeof g||m.isFunction(g)||(g={}),h===i&&(g=this,h--
);i>h;h++)if(null!=(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(m.isPlainObject(c)||
(b=m.isArray(c)))?(b?(b=!1,f=a&&m.isArray(a)?a:[]):f=a&&m.isPlainObject(a)?a:{},g[d]=m.extend(j,f,c)):void
0!==c&&(g[d]=c));return g},m.extend({expando:"jQuery"+
(l+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new Error(a)},noop:function()
{},isFunction:function(a){return"function"===m.type(a)},isArray:Array.isArray||function(a)
{return"array"===m.type(a)},isWindow:function(a){return null!=a&&a==a.window},isNumeric:function(a)
{return!m.isArray(a)&&a-parseFloat(a)>=0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==m.type(a)||a.nodeType||m.isWindow(a))return!1;try{if(a.constructor&&!j.call(a,"constructo
r")&&!j.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c){return!1}if(k.ownLast)for(b in
a)return j.call(a,b);for(b in a);return void 0===b||j.call(a,b)},type:function(a){return null==a?
a+"":"object"==typeof a||"function"==typeof a?h[i.call(a)]||"object":typeof a},globalEval:function(b)
{b&&m.trim(b)&&(a.execScript||function(b){a.eval.call(a,b)})(b)},camelCase:function(a){return
a.replace(o,"ms-").replace(p,q)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b,c){var
d,e=0,f=a.length,g=r(a);if(c){if(g){for(;f>e;e++)if(d=b.apply(a[e],c),d===!1)break}else for(e in
a)if(d=b.apply(a[e],c),d===!1)break}else if(g){for(;f>e;e++)if(d=b.call(a[e],e,a[e]),d===!1)break}else for(e
in a)if(d=b.call(a[e],e,a[e]),d===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(n,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(r(Object(a))?
m.merge(c,"string"==typeof a?[a]:a):f.call(c,a)),c},inArray:function(a,b,c){var d;if(b){if(g)return
g.call(b,a,c);for(d=b.length,c=c?0>c?Math.max(0,d+c):c:0;d>c;c++)if(c in b&&b[c]===a)return c}return-
1},merge:function(a,b){var c=+b.length,d=0,e=a.length;while(c>d)a[e++]=b[d++];if(c!==c)while(void
0!==b[d])a[e++]=b[d++];return a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var
d,f=0,g=a.length,h=r(a),i=[];if(h)for(;g>f;f++)d=b(a[f],f,c),null!=d&&i.push(d);else for(f in
a)d=b(a[f],f,c),null!=d&&i.push(d);return e.apply([],i)},guid:1,proxy:function(a,b){var
c,e,f;return"string"==typeof b&&(f=a[b],b=a,a=f),m.isFunction(a)?(c=d.call(arguments,2),e=function(){return
a.apply(b||this,c.concat(d.call(arguments)))},e.guid=a.guid=a.guid||m.guid++,e):void 0},now:function()
{return+new Date},support:k}),m.each("Boolean Number String Function Array Date RegExp Object Error".split("
"),function(a,b){h["[object "+b+"]"]=b.toLowerCase()});function r(a){var
b=a.length,c=m.type(a);return"function"===c||m.isWindow(a)?!1:1===a.nodeType&&b?!0:"array"===c||0===b||"numbe
r"==typeof b&&b>0&&b-1 in a}var s=function(a){var b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u="sizzle"+-new
Date,v=a.document,w=0,x=0,y=gb(),z=gb(),A=gb(),B=function(a,b){return a===b&&
(l=!0),0},C="undefined",D=1<<31,E={}.hasOwnProperty,F=
[],G=F.pop,H=F.push,I=F.push,J=F.slice,K=F.indexOf||function(a){for(var
b=0,c=this.length;c>b;b++)if(this[b]===a)return b;return-
1},L="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",M="[\\x20\\t\\r\\n\\f]",N="(?:\\\\.|[\\w-]|[^\\x00-\\xa0])+",O=N.replace("w...
```

http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp

```
alert("User not found.");document.location.href = "index.jsp";
```

http://10.90.171.82:8080/hpcl_grp1/Event/login.jsp

```
alert("Please enter Proper Credentials.");document.location.href = "index.jsp";
```

Cookies 1

TOC

Name	First Set	Domain	Secure
Value	**Requested URL**		**Expires**
JSESSIONID	http://10.90.171.82:8080/hpcl_grp1/Event/	10.90.171.82	False
05781F2D4F1DC2E50B86E76AAA45B9D6	http://10.90.171.82:8080/hpcl_grp1/Event/		