Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by IBM Security AppScan Standard 9.0.3.12, Rules: 17339
Scan started: 9/11/2019 10:41:13 AM

Table of Contents

Introduction

Summary

Issues Sorted by Issue Type

Introduction

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

High severity issues:	1
Medium severity issues:	2
Low severity issues:	21
Informational severity issues:	9
Total security issues included in the report:	33
Total security issues discovered in the scan:	33

General Information

Scan file name:	Event
Scan started:	9/11/2019 10:41:13 AM
Test policy:	Default(Modified)

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:	`>Logout`
Tracked or session ID cookies:	`JSESSIONID`
Tracked or session ID parameters:	

Login sequence:	`http://10.90.171.82:8080/hpcl_grp1/Event_ui/`
	`http://10.90.171.82:8080/hpcl_grp1/Event_ui/login.jsp`
	`http://10.90.171.82:8080/hpcl_grp1/Event_ui/login.jsp`
	`http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp`

Summary

Issue Types 12

TOC

	Issue Type	Number of Issues
H	Link to Non-Existing Domain Found	1
M	MacOS X Finder Apache Directory Contents Disclosure	2
L	Body Parameters Accepted in Query	1
L	Check for SRI (Subresource Integrity) support	1
L	Insecure "OPTIONS" HTTP Method Enabled	1
L	Missing or insecure "Content-Security-Policy" header	5
L	Missing or insecure "X-Content-Type-Options" header	5
L	Missing or insecure "X-XSS-Protection" header	5
L	Temporary File Download	2
L	Unsafe third-party link (target="_blank")	1
I	Client-Side (JavaScript) Cookie References	1
I	HTML Comments Sensitive Information Disclosure	8

Vulnerable URLs 10

TOC

	URL	Number of Issues
H	http://10.90.171.82:8080/hpcl_grp1/Event_ui/	9
M	http://10.90.171.82:8080/	1
M	http://10.90.171.82:8080/hpcl_grp1/	2
L	http://10.90.171.82:8080/hpcl_grp1/Event_ui/login.jsp	2
L	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/bootstrap.min.js	3
L	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/jquery.magnific-popup .min.js	3
L	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/popper.js	3
L	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/validate.js	3
L	http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp	6

I	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/common.js	1

Fix Recommendations 12

TOC

	Remediation Task	Number of Issues
H	Remove the non-existing domain from the web site	1
M	Upgrade to the latest version of Mac OS X	2
L	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"	1
L	Add to each third-party script/link element support to SRI(Subresource Integrity).	1
L	Config your server to use the "Content-Security-Policy" header with secure policies	5
L	Config your server to use the "X-Content-Type-Options" header with "nosniff" value	5
L	Config your server to use the "X-XSS-Protection" header with value '1' (enabled)	5
L	Disable WebDAV, or disallow unneeded HTTP methods	1
L	Do not accept body parameters that are sent in the query string	1
L	Remove business and security logic from the client side	1
L	Remove old versions of files from the virtual directory	2
L	Remove sensitive information from HTML comments	8

Security Risks 7

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.	18
M	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files	2
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	24
L	In case the third-party server is compromised, the content/behavior of the site will change	1
L	It is possible to upload, modify or delete web pages, scripts and files on the web server	1
L	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords	2
I	The worst case scenario for this attack depends on the context and	1

	role of the cookies that are created at the client side

Causes 9

TOC

	Cause	Number of Issues
H	The web application contains a link to a non-existing domain	1
M	Latest patches or hotfixes for 3rd. party products were not installed	2
L	Insecure web application programming or configuration	16
L	There is no support to Subresource Integrity.	1
L	The web server or application server are configured in an insecure way	1
L	Temporary files were left in production environment	2
L	The rel attribute in the link element is not set to "noopener noreferrer".	1
I	Cookies are created at the client side	1
I	Debugging information was left by the programmer in web pages	8

WASC Threat Classification

TOC

Threat	Number of Issues
Abuse of Functionality	1
Content Spoofing	1
Directory Indexing	2
Information Leakage	25
Predictable Resource Location	2
Remote File Inclusion	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_ui/
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

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

Raw Test Response:

```
...

Date: Wed, 11 Sep 2019 05:11:24 GMT
Content-Type: text/html;charset=ISO-8859-1

<html>
<head>

<title>Event Nomination</title>
  <meta charset="utf-8">
  <meta http-equiv="--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">
<link rel="stylesheet" type="text/css" href="css/main22.css">
<meta http-equiv="--UA-Compatible" content="IE=edge" />
<script src="js/jquery-3.2.1.min.js"></script>
<!--<script src="js/jquery-1.10.2.js"></script>-->
<!--<script src="js/jquery-1.11.1.min.js" type="text/javascript"></script>-->
<script src="js/jquery-ui.min.js" type="text/javascript"></script>
<script src="js/menu_script.js" type="text/javascript"></script>
```

```
...
```

M MacOS X Finder Apache Directory Contents Disclosure 2

TOC

Issue 1 of 2

TOC

MacOS X Finder Apache Directory Contents Disclosure	
Severity:	Medium
CVSS Score:	6.4
URL:	http://10.90.171.82:8080/hpcl_grp1/
Entity:	.DS_Store (Page)
Risk:	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Upgrade to the latest version of Mac OS X

Reasoning: The test successfully retrieved the contents of a Mac OS X finder directory.

Issue 2 of 2

TOC

MacOS X Finder Apache Directory Contents Disclosure	
Severity:	Medium
CVSS Score:	6.4
URL:	http://10.90.171.82:8080/
Entity:	.DS_Store (Page)
Risk:	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Upgrade to the latest version of Mac OS X

Reasoning: The test successfully retrieved the contents of a Mac OS X finder directory.

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_ui/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

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

Original Response ≈ **Test Response**

L Check for SRI (Subresource Integrity) support 1

TOC

Issue 1 of 1

TOC

Check for SRI (Subresource Integrity) support	
Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/
Entity:	(Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Causes:	There is no support to Subresource Integrity.
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Raw Test Response:

```
...

Date: Wed, 11 Sep 2019 05:16:06 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">
<link rel="stylesheet" type="text/css" href="css/main22.css">
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<script src="js/jquery-3.2.1.min.js"></script>
<!--<script src="js/jquery-1.10.2.js"></script>-->
<!--<script src="js/jquery-1.11.1.min.js" type="text/javascript"></script>-->
<script src="js/jquery-ui.min.js" type="text/javascript"></script>
<script src="js/menu_script.js" type="text/javascript"></script>

...
```

L Insecure "OPTIONS" HTTP Method Enabled 1

TOC

Issue 1 of 1

TOC

Insecure "OPTIONS" HTTP Method Enabled

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/
Entity:	hpcl_grp1/ (Page)
Risk:	It is possible to upload, modify or delete web pages, scripts and files on the web server
Causes:	The web server or application server are configured in an insecure way
Fix:	Disable WebDAV, or disallow unneeded HTTP methods

Reasoning: The Allow header revealed that hazardous HTTP Options are allowed, indicating that WebDAV is enabled on the server.

Raw Test Response:

```
...

Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Wed, 11 Sep 2019 05:17:04 GMT
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS


...
```

L Missing or insecure "Content-Security-Policy" header 5 TOC

Issue 1 of 5 TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/
Entity:	(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

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

Raw Test Response:

```
...
GET /hpcl_grp1/Event_ui/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 10.90.171.82:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
x-ua-compatible: IE=edge
Server: Apache-Coyote/1.1
Content-Length: 4918
Set-Cookie: JSESSIONID=A23CBA5455A9131C49B478F8A8C91892; Path=/; HttpOnly
Date: Wed, 11 Sep 2019 05:16:06 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">
<link rel="stylesheet" type="text/css" href="css/main22.css">

...
```

Issue 2 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/jquery.magnific-popup.min.js
Entity:	jquery.magnific-popup.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Mon, 06 Oct 2014 05:49:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 20932
ETag: W/"20932-1412574540000"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/*! Magnific Popup - v0.9.9 - 2014-09-06
* http://dimsemenov.com/plugins/magnific-popup/
* Copyright (c) 2014 Dmitry Semenov; */
(function(e){var t,n,i,o,r,...

...
```

Issue 3 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/validate.js
Entity:	validate.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Wed, 04 May 2016 06:11:20 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 1497
ETag: W/"1497-1462342280017"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

function isNumeric(evt)
      {
         var charCode = (evt.which) ? evt.which : event.keyCode
         if ((charCode > 31 && charCode !=46 )  && ((charCode < 48 || charCode > 57) &&
charCode!=190))
          {
        alert("Enter Numeric value only");
        return false;
       }
         return true;
      }

...
```

Issue 4 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/bootstrap.min.js
Entity:	bootstrap.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Fri, 16 Nov 2018 03:36:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 51143
ETag: W/"51143-1542339360840"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/*!
 * Bootstrap v4.0.0-beta (https://getbootstrap.com)
 * Copyright 2011-2017 The Bootstrap Authors
(https://github.com/twbs/bootstrap/graphs/contributors)
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery. jQuery
must be included before Bootstrap's JavaScript.");!function(t){var e=jQuery.fn.jquery.split(" ")
[0].split(".");if(e[0]<2&&e[1]<9||1==e[0]&&9==e[1]&&e[2]<1||e[0]>=4)throw new Error("Bootstrap's
JavaScript requires at least jQuery v1.9.1 but less than v4.0.0")}(),function(){function t(t,e)
{if(!t)throw new ReferenceError("this hasn't been initialised - super() hasn't been
called");return!e||"object"!=typeof e&&"function"!=typeof e?t:e}function e(t,e)
{if("function"!=typeof e&&null!==e)throw new TypeError("Super expression must either be null or a
function, not "+typeof e);t.prototype=Object.create(e&&e.prototype,{constructor:
{value:t,enumerable:!1,writable:!0,configurable:!0}}),e&&(Object.setPrototypeOf?
Object.setPrototypeOf(t,e):t.__proto__=e)}function n(t,e){if(!(t instanceof e))throw new
TypeError("Cannot call a class as a function")}var i="function"==typeof Symbol&&"symbol"==typeof
Symbol.iterator
...
```

Issue 5 of 5

TOC

Missing or insecure "Content-Security-Policy" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/popper.js
Entity:	popper.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Fri, 16 Nov 2018 03:36:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 81670
ETag: W/"81670-1542339360642"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/**!
 * @fileOverview Kickass library to create and place poppers near their reference elements.
 * @version 1.12.5
 * @license
 * Copyright (c) 2016 Federico Zivolo and contributors
 *
 * Permission is hereby granted, free of charge, to any person obtaining a copy
 * of this software and associated documentation files (the "Software"), to deal
 * in the Software without restriction, including without limitation the rights
 * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
...
```

L Missing or insecure "X-Content-Type-Options" header 5

TOC

Issue 1 of 5

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_ui/js/jquery.magnific-popup.min.js
Entity:	jquery.magnific-popup.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Mon, 06 Oct 2014 05:49:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 20932
ETag: W/"20932-1412574540000"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/*! Magnific Popup - v0.9.9 - 2014-09-06
* http://dimsemenov.com/plugins/magnific-popup/
* Copyright (c) 2014 Dmitry Semenov; */
(function(e){var t,n,i,o,r,...

...
```

Issue 2 of 5

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_ui/
Entity:	(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

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

Raw Test Response:

```
...
GET /hpcl_grp1/Event_ui/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 10.90.171.82:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
x-ua-compatible: IE=edge
Server: Apache-Coyote/1.1
Content-Length: 4918
Set-Cookie: JSESSIONID=A23CBA5455A9131C49B478F8A8C91892; Path=/; HttpOnly
Date: Wed, 11 Sep 2019 05:16:06 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">
<link rel="stylesheet" type="text/css" href="css/main22.css">

...
```

Issue 3 of 5

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_ui/js/validate.js
Entity:	validate.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Wed, 04 May 2016 06:11:20 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 1497
ETag: W/"1497-1462342280017"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

function isNumeric(evt)
      {
         var charCode = (evt.which) ? evt.which : event.keyCode
         if ((charCode > 31 && charCode !=46 )  && ((charCode < 48 || charCode > 57) &&
charCode!=190))
          {
        alert("Enter Numeric value only");
        return false;
       }
         return true;
      }

...
```

Issue 4 of 5

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_ui/js/bootstrap.min.js
Entity:	bootstrap.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Fri, 16 Nov 2018 03:36:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 51143
ETag: W/"51143-1542339360840"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/*!
 * Bootstrap v4.0.0-beta (https://getbootstrap.com)
 * Copyright 2011-2017 The Bootstrap Authors
(https://github.com/twbs/bootstrap/graphs/contributors)
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery. jQuery
must be included before Bootstrap's JavaScript.");!function(t){var e=jQuery.fn.jquery.split(" ")
[0].split(".");if(e[0]<2&&e[1]<9||1==e[0]&&9==e[1]&&e[2]<1||e[0]>=4)throw new Error("Bootstrap's
JavaScript requires at least jQuery v1.9.1 but less than v4.0.0")}(),function(){function t(t,e)
{if(!t)throw new ReferenceError("this hasn't been initialised - super() hasn't been
called");return!e||"object"!=typeof e&&"function"!=typeof e?t:e}function e(t,e)
{if("function"!=typeof e&&null!==e)throw new TypeError("Super expression must either be null or a
function, not "+typeof e);t.prototype=Object.create(e&&e.prototype,{constructor:
{value:t,enumerable:!1,writable:!0,configurable:!0}}),e&&(Object.setPrototypeOf?
Object.setPrototypeOf(t,e):t.__proto__=e)}function n(t,e){if(!(t instanceof e))throw new
TypeError("Cannot call a class as a function")}var i="function"==typeof Symbol&&"symbol"==typeof
Symbol.iterator
...
```

Issue 5 of 5

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_ui/js/popper.js
Entity:	popper.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

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Fri, 16 Nov 2018 03:36:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 81670
ETag: W/"81670-1542339360642"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/**!
 * @fileOverview Kickass library to create and place poppers near their reference elements.
 * @version 1.12.5
 * @license
 * Copyright (c) 2016 Federico Zivolo and contributors
 *
 * Permission is hereby granted, free of charge, to any person obtaining a copy
 * of this software and associated documentation files (the "Software"), to deal
 * in the Software without restriction, including without limitation the rights
 * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
...
```

L Missing or insecure "X-XSS-Protection" header 5

TOC

Issue 1 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/jquery.magnific-popup.min.js
Entity:	jquery.magnific-popup.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)

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Mon, 06 Oct 2014 05:49:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 20932
ETag: W/"20932-1412574540000"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/*! Magnific Popup - v0.9.9 - 2014-09-06
* http://dimsemenov.com/plugins/magnific-popup/
* Copyright (c) 2014 Dmitry Semenov; */
(function(e){var t,n,i,o,r,...

...
```

Issue 2 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/
Entity:	(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)

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

Raw Test Response:

```
...
GET /hpcl_grp1/Event_ui/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: 10.90.171.82:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
x-ua-compatible: IE=edge
Server: Apache-Coyote/1.1
Content-Length: 4918
Set-Cookie: JSESSIONID=A23CBA5455A9131C49B478F8A8C91892; Path=/; HttpOnly
Date: Wed, 11 Sep 2019 05:16:06 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">
<link rel="stylesheet" type="text/css" href="css/main22.css">

...
```

Issue 3 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/validate.js
Entity:	validate.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)

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Wed, 04 May 2016 06:11:20 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 1497
ETag: W/"1497-1462342280017"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

function isNumeric(evt)
      {
         var charCode = (evt.which) ? evt.which : event.keyCode
         if ((charCode > 31 && charCode !=46 )  && ((charCode < 48 || charCode > 57) &&
charCode!=190))
          {
        alert("Enter Numeric value only");
        return false;
       }
         return true;
      }

...
```

Issue 4 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/bootstrap.min.js
Entity:	bootstrap.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)

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Fri, 16 Nov 2018 03:36:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 51143
ETag: W/"51143-1542339360840"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/*!
 * Bootstrap v4.0.0-beta (https://getbootstrap.com)
 * Copyright 2011-2017 The Bootstrap Authors
(https://github.com/twbs/bootstrap/graphs/contributors)
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery. jQuery
must be included before Bootstrap's JavaScript.");!function(t){var e=jQuery.fn.jquery.split(" ")
[0].split(".");if(e[0]<2&&e[1]<9||1==e[0]&&9==e[1]&&e[2]<1||e[0]>=4)throw new Error("Bootstrap's
JavaScript requires at least jQuery v1.9.1 but less than v4.0.0")}(),function(){function t(t,e)
{if(!t)throw new ReferenceError("this hasn't been initialised - super() hasn't been
called");return!e||"object"!=typeof e&&"function"!=typeof e?t:e}function e(t,e)
{if("function"!=typeof e&&null!==e)throw new TypeError("Super expression must either be null or a
function, not "+typeof e);t.prototype=Object.create(e&&e.prototype,{constructor:
{value:t,enumerable:!1,writable:!0,configurable:!0}}),e&&(Object.setPrototypeOf?
Object.setPrototypeOf(t,e):t.__proto__=e)}function n(t,e){if(!(t instanceof e))throw new
TypeError("Cannot call a class as a function")}var i="function"==typeof Symbol&&"symbol"==typeof
Symbol.iterator
...
```

Issue 5 of 5

TOC

Missing or insecure "X-XSS-Protection" header

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/popper.js
Entity:	popper.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)

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

Raw Test Response:

```
...

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_ui/home.jsp
Cookie: JSESSIONID=25ADB8DF127DDD4B85C16D1983279C1B
Connection: keep-alive
Host: 10.90.171.82:8080
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Last-Modified: Fri, 16 Nov 2018 03:36:00 GMT
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
Content-Length: 81670
ETag: W/"81670-1542339360642"
Date: Wed, 11 Sep 2019 05:16:29 GMT
Content-Type: application/javascript

/**!
 * @fileOverview Kickass library to create and place poppers near their reference elements.
 * @version 1.12.5
 * @license
 * Copyright (c) 2016 Federico Zivolo and contributors
 *
 * Permission is hereby granted, free of charge, to any person obtaining a copy
 * of this software and associated documentation files (the "Software"), to deal
 * in the Software without restriction, including without limitation the rights
 * to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
...
```

L Temporary File Download 2

TOC

Issue 1 of 2

TOC

Temporary File Download

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp
Entity:	home.jsp (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

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 Request:

Test Response

```
GET /hpcl_grp1/Event_ui/home%20-
%20Copy.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: http://10.90.171.82:808
0/hpcl_grp1/Event_ui/login.jsp
Connection: keep-alive
Host: 10.90.171.82:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xh
tml+xml,application/xml;q=0.9,im
age/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
...

User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: http://10.90.171.82:808
0/hpcl_grp1/Event_ui/login.jsp
Connection: keep-alive
Host: 10.90.171.82:8080
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xh
tml+xml,application/xml;q=0.9,im
age/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
x-ua-compatible: IE=edge
Transfer-Encoding: chunked
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=432F4D3D6
F34D59588EC174A40309E32; Path=/;
HttpOnly
Date: Wed, 11 Sep 2019 05:17:59
GMT
Content-Type: text/html;charset=
ISO-8859-1

<!DOCTYPE html PUBLIC "-//W3C//D
TD XHTML 1.0 Transitional//EN" "
http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<HTML>
<!--[if lt IE 7 ]><html class="i
e ie6" lang="en"> <![endif]-->
<!--[if IE 7 ]><html class="ie i
e7" lang="en"> <![endif]-->
<!--[if IE 8 ]><html class="ie i
e8" lang="en"> <![endif]-->
<!--[if (gte IE 9)|!(IE)]><!--><
html lang="en"> <!--<![endif]-->
<head>



...
```

Issue 2 of 2

TOC

Temporary File Download

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/login.jsp
Entity:	login.jsp (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

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 Request:

Test Response

```
GET /hpcl_grp1/Event_ui/login%20
-%20Copy.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows
NT 6.1; WOW64; Trident/7.0; rv:1
1.0) like Gecko
Referer: http://10.90.171.82:808
0/hpcl_grp1/Event_ui/
Connection: keep-alive
Host: 10.90.171.82:8080
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Origin: http://10.90.171.82:8080
Accept: text/html,application/xh
tml+xml,application/xml;q=0.9,im
age/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
```

```
...

Connection: keep-alive
Host: 10.90.171.82:8080
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Origin: http://10.90.171.82:8080
Accept: text/html,application/xh
tml+xml,application/xml;q=0.9,im
age/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 473
Set-Cookie: JSESSIONID=94E293BB6
A8EFAF806AD278398CEA064; Path=/;
HttpOnly
Date: Wed, 11 Sep 2019 05:17:52
GMT
Content-Type: text/html;charset=
ISO-8859-1



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


...
```

L Unsafe third-party link (target="_blank") 1

TOC

Issue 1 of 1

TOC

Unsafe third-party link (target="_blank")

Severity:	Low
CVSS Score:	5.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp
Entity:	home.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.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Raw Test Response:

```
...

    <a class="nav-link style-text-black" href="mainSubmit.jsp">New Nomination</a>
    <a class="nav-link style-text-black" href="mynomination1.jsp">My Nominations</a>
    <a class="nav-link style-text-black" href="mycancnomination.jsp">My Cancelled Nominations</a>
    <!--<a class="nav-link style-text-black" href="fitFeedBack.jsp">Feedback for Hum Fit Toh HP
Fit</a>-->


   </div></div>
  </li>
  <li class="nav-item">
          <a class="nav-link style-text-white" 
href="https://team.hpcl.in/sites/NIGall/_layouts/pictlib/Menu.aspx" target="_blank">Gallery</a>
        </li>



<li class="nav-item">
          <a href="logout.jsp" class="nav-link style-text-white">Logout
&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</a>
          </li>
  <!--<li class="nav-item dropdown">-->


...
```

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:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/js/common.js
Entity:	function isNumber(n) { (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

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```
...

    var expires;
    if (days) {
        var date = new Date();
        date.setTime(date.getTime() + (days * 24 * 60 * 60 * 1000));
        expires = "; expires=" + date.toGMTString();
    }
    else {
        expires = "";
    }
    document.cookie = name + "=" + value + expires + "; path=/";
}

function getCookie(c_name) {
    if (document.cookie.length > 0) {
        c_start = document.cookie.indexOf(c_name + "=");
        if (c_start != -1) {
          c_start = c_start + c_name.length + 1;
          c_end = document.cookie.indexOf(";", c_start);
          if (c_end == -1) {

...
```

I HTML Comments Sensitive Information Disclosure 8 TOC

Issue 1 of 8

TOC

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/
Entity:	<link rel="stylesheet" href="css/style1.css"> (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...

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">
<link rel="stylesheet" type="text/css" href="css/main22.css">
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<script src="js/jquery-3.2.1.min.js"></script>
<!--<script src="js/jquery-1.10.2.js"></script>-->
<!--<script src="js/jquery-1.11.1.min.js" type="text/javascript"></script>-->
<script src="js/jquery-ui.min.js" type="text/javascript"></script>
<script src="js/menu_script.js" type="text/javascript"></script>
<script src="js/common.js" type="text/javascript"></script>

...
```

Issue 2 of 8

TOC

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/
Entity:	<table class="listTable1" style="width:100%;background-color:"><tr><th style="width:70px;"><img src=... (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...

</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" >

<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;">


...
```

Issue 3 of 8

TOC

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/
Entity:	<img src="images/login.jpg" style="/*height: 660px;*/width: 100%"> (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...

      <button class="login100-form-btn" style="background-color: #010269!important;">
       Login
      </button>
     </div>


    </form>

    <div class="login100-more" style="background-image: url('images/222.jpg'); background-size:
cover; background-position: top!important; width: 70%;">
     <!--<img src="images/login.jpg" style="/*height: 660px;*/width: 100%">-->

    </div>
   </div>
  </div>
 </div>



<!--<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>

...
```

Issue 4 of 8

TOC

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/
Entity:	<script type="text/javascript" src="js/snow.js"></script> (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...

<link rel="stylesheet" href="css/styles.css">
<link rel="stylesheet" type="text/css" href="css/main22.css">
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<script src="js/jquery-3.2.1.min.js"></script>
<!--<script src="js/jquery-1.10.2.js"></script>-->
<!--<script src="js/jquery-1.11.1.min.js" type="text/javascript"></script>-->
<script src="js/jquery-ui.min.js" type="text/javascript"></script>
<script src="js/menu_script.js" type="text/javascript"></script>
<script src="js/common.js" type="text/javascript"></script>
<!--<script type="text/javascript" src="js/snow.js"></script>-->
<style>
.listTh{
    background-color: #297DB5;
   --- opacity: .4;

}
</style>
<style type="text/css">


...
```

Issue 5 of 8

TOC

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp
Entity:	<link rel="stylesheet" type="text/css" href="css/menu.css" /> (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...

    background-color: rgba(0,0,0,.03);
    border-bottom: 1px solid rgba(0,0,0,.125);
    padding: 0px 0px 0px 10px;
}
</style>


<!--<link rel="stylesheet" href="css/customcss.css">-->

<!--<link rel="stylesheet" type="text/css" href="css/menu.css" />-->
</head>
<body>

   <script>
   alert("Invalid User");
   location.href="index.jsp";
   </script>



...
```

Issue 6 of 8

TOC

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp
Entity:	<a class="nav-link style-text-black" href="fitFeedBack.jsp">Feedback for Hum Fit Toh HP Fit</a> (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...

          <a>Nomination</a>
          <div class="dropdown-content">


   <!--<a class="nav-link dropdown-toggle" style="cursor:pointer;" id="dropdown01" data-
toggle="dropdown" aria-haspopup="true" aria-expanded="false">Nomination</a>-->
   <!--<div class="dropdown-menu" aria-labelledby="dropdown01">-->
    <a class="nav-link style-text-black" href="mainSubmit.jsp">New Nomination</a>
    <a class="nav-link style-text-black" href="mynomination1.jsp">My Nominations</a>
    <a class="nav-link style-text-black" href="mycancnomination.jsp">My Cancelled Nominations</a>
    <!--<a class="nav-link style-text-black" href="fitFeedBack.jsp">Feedback for Hum Fit Toh HP
Fit</a>-->


   </div></div>
  </li>
  <li class="nav-item">
          <a class="nav-link style-text-white"
href="https://team.hpcl.in/sites/NIGall/_layouts/pictlib/Menu.aspx" target="_blank">Gallery</a>
        </li>



...
```

Issue 7 of 8

TOC

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp
Entity:	<link rel="stylesheet" href="css/customcss.css"> (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...

    /* padding: .75rem 1.25rem; */
    margin-bottom: 0;
    background-color: rgba(0,0,0,.03);
    border-bottom: 1px solid rgba(0,0,0,.125);
    padding: 0px 0px 0px 10px;
}
</style>


<!--<link rel="stylesheet" href="css/customcss.css">-->

<!--<link rel="stylesheet" type="text/css" href="css/menu.css" />-->
</head>
<body>

   <script>
   alert("Invalid User");
   location.href="index.jsp";
   </script>

...

...

    </div>
   </div>
  </div>
</section>


</body>

</html>
<!--<link rel="stylesheet" href="css/customcss.css">-->


...
```

HTML Comments Sensitive Information Disclosure

Severity:	Informational
CVSS Score:	0.0
URL:	http://10.90.171.82:8080/hpcl_grp1/Event_ui/home.jsp
Entity:	<nav class="navbar navbar-expand-lg navbar-dark bg-info"> (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:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Original Response

```
...


<div class="row subBar" style="border-bottom: 2px solid white; background-color: #000d39; z-
index: 999999;">
  <div class="col-sm-12" style="padding: 0px;">
  <nav class="navbar navbar-expand-md navbar-dark navbar-fixed-top" >
  &nbsp;&nbsp;
    <span class="style-right"><button class="navbar-toggler style-text-white style-grey style-
right" type="button" data-toggle="collapse" data-target="#collapsibleNavbar">
          <span class="navbar-toggler-icon style-grey"></span>
        </button></span>
   <!--<nav class="navbar navbar-expand-lg navbar-dark bg-info">
    <a class="navbar-brand" href="home.jsp" ><img src="images/logo3.png" class="d-inline-block
align-top" alt="" width="40"><font size="5" face="algerian">Event Nomination</font></a>
    <button class="navbar-toggler" type="button" data-toggle="collapse" data-
target="#navbarColor02" aria-controls="navbarColor02" aria-expanded="false" aria-label="Toggle
navigation">
      <span class="navbar-toggler-icon"></span>
    </button>-->


    <div class="collapse navbar-collapse" id="collapsibleNavbar">
      <ul class="navbar-nav ml-auto ">

        <li class="nav-item active">

...
```