Web 应用程序报告

该报告包含有关 web 应用程序的重要安全信息。

安全报告

该报告由 IBM Security AppScan Standard 创建 9.0.3.13, 规则： 18533
扫描开始时间： 2019/11/14 16:23:33

目录

- 除去 Web 站点中的电子邮件地址
- 除去 Web 站点中的信用卡号
- 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去
- 将“autocomplete”属性正确设置为“off”
- 将服务器配置为使用安全策略的“Content-Security-Policy”头
- 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头
- 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头
- 为 Web 服务器或 Web 应用程序下载相关的安全补丁

咨询

- 已解密的登录请求
- “Content-Security-Policy”头缺失或不安全
- “X-Content-Type-Options”头缺失或不安全
- “X-XSS-Protection”报头缺失或不安全
- 检测到隐藏目录
- 在未加密连接中发现信用卡号模式 (Visa)
- 自动填写未对密码字段禁用的 HTML 属性
- HTML 注释敏感信息泄露
- 发现电子邮件地址模式
- 发现可能的服务器路径泄露模式

介绍

该报告包含由 IBM Security AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题：	1
低严重性问题：	19
参考严重性问题：	6
报告中包含的严重性问题总数：	26
扫描中发现的严重性问题总数：	26

常规信息

扫描文件名称： 111

扫描开始时间： 2019/11/14 16:23:33

测试策略： Web Services

主机 124.254.61.27

端口 9090

操作系统： 未知

Web 服务器： 未知

应用程序服务器： JavaAppServer

登陆设置

登陆方法： 记录的登录

并发登陆： 已启用

JavaScript 执行文件： 已禁用

会话中检测： 已启用

会话中模式：

跟踪或会话标识 cookie： JSESSIONID

跟踪或会话标识参数：

登陆序列：

```
http://124.254.61.27:9090/web/desktop
http://124.254.61.27:9090/web/desktop
http://124.254.61.27:9090/web/desktop
```

http://124.254.61.27:9090/web/desktop
http://124.254.61.27:9090/web/desktop
http://124.254.61.27:9090/web/desktop
http://124.254.61.27:9090/web/desktop
http://124.254.61.27:9090/web/desktop
http://124.254.61.27:9090/web/sysmenu/licenseCheck.sp
http://124.254.61.27:9090/web/logomanager/getLoginInfo.do

摘要

问题类型 10

TOC

	问题类型	问题的数量
高	已解密的登录请求	1
低	“Content-Security-Policy”头缺失或不安全	5
低	“X-Content-Type-Options”头缺失或不安全	5
低	“X-XSS-Protection”头缺失或不安全	5
低	检测到隐藏目录	1
低	在未加密连接中发现信用卡号模式 (Visa)	1
低	自动填写未对密码字段禁用的 HTML 属性	2
参	HTML 注释敏感信息泄露	1
参	发现电子邮件地址模式	4
参	发现可能的服务器路径泄露模式	1

有漏洞的 URL 12

TOC

	URL	问题的数量
高	http://124.254.61.27:9090/web/desktop	5
低	http://124.254.61.27:9090/web/resource/EHM/itime.ext.js	3
低	http://124.254.61.27:9090/web/resource/EHM/itime.js;jsessionid=2AD69A46E20F35E8C98AB6912F83C7FE	3
低	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js	4
低	http://124.254.61.27:9090/web/resource/Inspinia/js/popper.min.js	3
低	http://124.254.61.27:9090/web/	1
低	http://124.254.61.27:9090/web/resource/bootstrap/fontIcon/iconFont/iconfont.js	1
低	http://124.254.61.27:9090/web/staff/initChangePwd.do	2
参	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-control.min.js	1

参	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-zh-CN.min.js	1
参	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.js	1
参	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/validate/jquery.validate.min.js	1

修复方式描述

TOC

	修复任务	问题的数量
高	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	1
低	除去 HTML 注释中的敏感信息	1
低	除去 Web 站点中的电子邮件地址	4
低	除去 Web 站点中的信用卡号	1
低	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去	1
低	将“autocomplete”属性正确设置为“off”	2
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	5
低	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	5
低	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	5
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	1

安全风险 6

TOC

	风险	问题的数量
高	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	1
低	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	21
低	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	15
低	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点	1
低	可能会绕开 Web 应用程序的认证机制	2
参	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	1

原因 5

TOC

	原因	问题的数量
高	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	1
低	Web 应用程序编程或配置不安全	22
低	Web 服务器或应用程序服务器是以不安全的方式配置的	1
参	程序员在 Web 页面上留下调试信息	1
参	未安装第三方产品的最新补丁或最新修补程序	1

WASC 威胁分类

TOC

威胁	问题的数量
传输层保护不足	1
信息泄露	25

按问题类型分类的问题

高 已解密的登录请求 TOC

问题 1 / 1 TOC

已解密的登录请求

严重性：	高
CVSS 分数：	8.5
URL：	http://124.254.61.27:9090/web/desktop
实体：	j_password (Parameter)
风险：	可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息
原因：	诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递
固定值：	发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异：

推理： AppScan 识别了不是通过 SSL 发送的密码参数。
修复状态： 已修复
修复方式： 发送敏感信息时，始终使用 SSL 和 POST（主体）参数
测试请求和响应：

```
POST /web/desktop HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=A72CAE1053AD4117FBBAA02396A61DEF
Connection: Keep-Alive
Host: 124.254.61.27:9090
Content-Length: 41
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

j_username=&j_password=&logintype=default

HTTP/1.1 200
Transfer-Encoding: chunked
Vary: Accept-Encoding
Date: Thu, 14 Nov 2019 08:24:31 GMT
Content-Type: text/html;charset=UTF-8
```

```
<!Doctype html>
<html>
<head>



<script>
  Ext_BLANK_IMAGE_URL = "";
</script>

    <title></title>
    <script type="text/javascript" src="/web/resource/EHM/itime.js"></script> <meta
    name="viewport" content="width=device-width, initial-scale=0.9">
<script>
    EHM.ImportToastr();
</script>
</head>



<script type="text/javascript">

    //EHM.Cache["LOGIN_SAVE_PASS"] = false;

    function failAction(msg) {
        if (msg == "用户密码过期，请重新设置密码")
          window.open('staff/initChangePwd.do', 'popUpWin',
'scrollbars=0,toolbar=0,status=1,width=543,height=354,left=300,
top=200,screenX=200,screenY=200');
    }

    function IsPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone",
          "SymbianOS", "Windows Phone",
          "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
          if (userAgentInfo.indexOf(Agents[v]) > 0) {
          flag = false;
          break;
          }
        }
        return flag;
    }

    $(function () {
        var authMsg = "";

        if(null!=authMsg && ""!=authMsg){
          toastr["error"](authMsg);
        }else{
          $.post(EHM.rootPath+"/sysmenu/licenseCheck.sp",function(data){
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-full-width",
          "onclick": null,
          "showDuration": "400",
          "hideDuration": "1000",
          "timeOut": "10000",
          "extendedTimeOut": "1000",
          "showEasing": "swing",
          "hideEasing": "linear",
          "showMethod": "fadeIn",
          "hideMethod": "fadeOut"
          };
          if(data["flag"]==1){

          toastr["warning"](data["authMsg"]);
          }else if(data["flag"]==0){
          toastr["error"](data["authMsg"]);
          }

          },"json");
        }
```

```
        if(!IsPC()){
          $("#showDiv").attr("style","width:500px;margin-top:25%")
        }
        var url="/web/logomanager/getLoginInfo.do";
        $.post(url,function(data){
          data=JSON.parse(data);
          var src1="resource/images/"+data.LOGIN_LOGO;
          var src2="resource/images/"+data.LOGIN_QRCODE;
          $("#logoimg").attr("src",src1);
          $("#qrimg").attr("src",src2);
        });

        $("#loginForm").submit(function (e) {
          updateCookie();
        });

        $("#loginBt").on("click",function(){
          if($("#savePassImg").is(':checked'))
          {
          cookie.set("LOGIN_SAVE_PASS",true) ;
          }else{
          cookie.set("LOGIN_SAVE_PASS",false) ;
          }
          var isUnionYW = 0;
          var yw_url = 'null';

          if(isUnionYW==1){
          var userNameValue = $("#j_username").val().trim();
          var passWordValue = $("#j_password").val().trim();
          yw_url = yw_url+"?j_username="+userNameValue+"&j_password="+passWordValue;
          $("#iframeVar").load(function(){
          $("#loginForm").submit();
          });
          $('#iframeVar').attr('src', yw_url);
          }else{
          $("#loginForm").submit();
          }


          //
        });

        var jsonStr = '{"success":"false","message":"登陆失败:用户不存在或密码错误
        "}'; if (jsonStr != null && jsonStr != "") {
          var jsonObj = JSON.parse(jsonStr);
          if (jsonObj && jsonObj != undefined) {
          if (jsonObj.success == "false") {
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-center",
          "onclick": null,
          "showDuration": "400",

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

问题 1 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/desktop
实体：	desktop (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

修复状态： 已修复

修复方式： 将服务器配置为使用安全策略的“Content-Security-Policy”头

测试请求和响应：

```
GET /web/desktop 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: 124.254.61.27:9090
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip
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
Transfer-Encoding: chunked
Content-Length: 8495
Vary: Accept-Encoding
Set-Cookie: JSESSIONID=49AB80D2E6EBA2F0E59E63E86F0DCFAA; Path=/web; HttpOnly
Date: Thu, 14 Nov 2019 08:25:41 GMT
Content-Type: text/html;charset=UTF-8



<!Doctype html>
<html>
<head>



<script>
  Ext_BLANK_IMAGE_URL = "";
</script>
```

```
    <title></title>
    <script type="text/javascript"
src="/web/resource/EHM/itime.js;jsessionid=49AB80D2E6EBA2F0E59E63E86F0DCFAA"></script>
    <meta name="viewport" content="width=device-width, initial-
scale=0.9"> <script>
    EHM.ImportToastr();
</script>
</head>



<script type="text/javascript">

    //EHM.Cache["LOGIN_SAVE_PASS"] = false;

    function failAction(msg) {
        if (msg == "用户密码过期，请重新设置密码")
          window.open('staff/initChangePwd.do', 'popUpWin',
'scrollbars=0,toolbar=0,status=1,width=543,height=354,left=300,
top=200,screenX=200,screenY=200');
    }

    function IsPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone",
          "SymbianOS", "Windows Phone",
          "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
          if (userAgentInfo.indexOf(Agents[v]) > 0) {
          flag = false;
          break;
          }
        }
        return flag;
    }

    $(function () {
        var authMsg = "";

        if(null!=authMsg && ""!=authMsg){
          toastr["error"](authMsg);
        }else{
          $.post(EHM.rootPath+"/sysmenu/licenseCheck.sp",function(data){
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-full-width",
          "onclick": null,
          "showDuration": "400",
          "hideDuration": "1000",
          "timeOut": "10000",
          "extendedTimeOut": "1000",
          "showEasing": "swing",
          "hideEasing": "linear",
          "showMethod": "fadeIn",
          "hideMethod": "fadeOut"
          };
          if(data["flag"]==1){

          toastr["warning"](data["authMsg"]);
          }else if(data["flag"]==0){
          toastr["error"](data["authMsg"]);
          }

          },"json");
        }

        if(!IsPC()){
          $("#showDiv").attr("style","width:500px;margin-top:25%")
        }
        var url="/web/logomanager/getLoginInfo.do;jsessionid=49AB80D2E6EBA2F0E59E63E86F0DCFAA";
        $.post(url,function(data){
          data=JSON.parse(data);
          var src1="resource/images/"+data.LOGIN_LOGO;
```

```
          var src2="resource/images/"+data.LOGIN_QRCODE;
          $("#logoimg").attr("src",src1);
          $("#qrimg").attr("src",src2);
        });

        $("#loginForm").submit(function (e) {
          updateCookie();
        });

        $("#loginBt").on("click",function(){
          if($("#savePassImg").is(':checked'))
          {
          cookie.set("LOGIN_SAVE_PASS",true) ;
          }else{
          cookie.set("LOGIN_SAVE_PASS",false) ;
          }
          var isUnionYW = 0;
          var yw_url = 'null';

          if(isUnionYW==1){
          var userNameValue = $("#j_username").val().trim();
          var passWordValue = $("#j_password").val().trim();
          yw_url = yw_url+"?j_username="+userNameValue+"&j_password="+passWordValue;
          $("#iframeVar").load(function(){
          $("#loginForm").submit();
          });
          $('#iframeVar').attr('src', yw_url);
          }else{
          $("#loginForm").submit();
          }


          //
        });

        var jsonStr = '{"success":"false","message":"登陆失败:用户不存在或密码错误
        "}'; if (jsonStr != null && jsonStr != "") {
          var jsonObj = JSON.parse(jsonStr);
          if (jsonObj && jsonObj != undefined) {
          if (jsonObj.success == "false") {
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-center",
          "onclick": null,

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

问题 2 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/EHM/itime.js;jsessionid=2AD69A46E20F35E8C98AB6912F83C7FE
实体：	itime.js;jsessionid=2AD69A46E20F35E8C98AB6912F83C7FE (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下
修复状态： 已修复
修复方式： 将服务器配置为使用安全策略的“Content-Security-Policy”头
测试请求和响应：

```
GET /web/resource/EHM/itime.js;jsessionid=7C15879B0ED11B9A08F98F109DD4C897 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: Keep-Alive
Host: 124.254.61.27:9090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:20 GMT
Accept-Ranges: bytes
Content-Length: 6725
ETag: W/"6725-1571017700350"
Date: Thu, 14 Nov 2019 08:25:41 GMT
Content-Type: application/javascript

window["undefined"] = window["undefined"];
var EHM = {
    Cache: {},
    rootPath: (function () {
        if (window["ROOT_PATH"]) {
          window["ROOT_PATH"] = "/" + window["ROOT_PATH"].split("\/")[1];
        }

        return window["ROOT_PATH"] || (function () {

          var L = window.location;
          var SR = L.pathname;
          if (SR.indexOf("/") > 0) SR = "/" + SR;
          return "/" + SR.split("\/")[1];
        })();
    })(),
    ImportScript: function (url) {
        document.writeln("<script type='text/javascript' src='" + EHM.rootPath + url +
"' ><" + "/scr" + "ipt>");
    },
    ImportCss: function (url) {
        document.writeln("<link href=\"" + EHM.rootPath + url + "\" rel=\"stylesheet\"
type=\"text/css\" />");
    },
    ImportWebIcon: function (url) {

        if (url.indexOf(EHM.rootPath) < 0) {
          url = EHM.rootPath + ((url.indexOf("EHM") == 0) ? EHM.appPath : "") + url;
        }
```

```
        try {
          document.writeln("<link href=\"" + url + "\" rel=\"Bookmark\"
type=\"image/x-icon\"/>");
          document.writeln("<link href=\"" + url + "\" rel=\"Shortcut Icon\"
type=\"image/x-icon\"/>");
        }
        catch (e) {
          var linksBookmark = document.createElement("link");
          linksBookmark.href = url;
          linksBookmark.rel = "Bookmark";

          var linksShortcut = document.createElement("link");
          linksShortcut.href = url;
          linksShortcut.rel = "Shortcut Icon";

          document.getElementsByTagName("head")[0].appendChild(links);
        }

        return EHM;
    },
    //根据指标值返回呈现颜色,数值从低到高为绿色,黄色,红色
    getAlarmColor:function(kpiValue){
        if(!isNaN(kpiValue)){
          if(kpiValue<70){
          return "#1ab394";
          }else if(kpiValue>=70 && kpiValue<90){
          return "#f8ac59";
          }else{
          return "#ed5565";
          }
        }else{
          return "#23c6c8";
        }
    },

    //根据指标值返回呈现颜色,数值从低到高为红色,黄色,绿色
    getAlarmReverseColor:function(kpiValue){
        if(!isNaN(kpiValue)){
          if(kpiValue<70){
          return "#ed5565";
          }else if(kpiValue>=70 && kpiValue<85){
          return "#f8ac59";
          }else{
          return "#1ab394";
          }
        }else{
          return "#23c6c8";
        }
    },

    getInspiniaAlarmColor:function(kpiValue){

        if(!isNaN(kpiValue)){
          if(kpiValue>=90){
          return '<div class="progress progress-itime "><div style="width: '+ kpiValue +
'%;"     class="progress-bar     progress-bar-danger"></div><div     class="progress-itime-
text">'+kpiValue+' % </div></div>';
          }else if(kpiValue>=75 && kpiValue<90){
          return '<div class="progress progress-itime "><div style="width: '+ kpiValue +
'%;"     class="progress-bar     progress-bar-warning"></div><div     class="progress-itime-
text">'+kpiValue+' % </div></div>';
          }else{
          return '<div class="progress progress-itime"><div style="width: '+ kpiValue + '%;"
class="progress-bar"></div><div class="progress-itime-text">'+kpiValue+' %</div></div>';
          }
        }else{
          return "#23c6c8";
        }
    },

    //根据告警级别返回颜色，包含轻微、重要、严重、正常、未管理
    getAlarmLevelColor:function(alarmLevel){
        //告警级别及设备管理状态
        if(alarmLevel=='10'){
          //轻微
          return "#f3f315";
        }else if(alarmLevel=='15'){
          //重要
```

```
            return "#f8ac59";
          }else if(alarmLevel=='20'){
            //严重
            return "#ed5565";
          }else if(alarmLevel=='1'){
            //未管理
            return "#f3f3f4";
          }else{
            //正常
            return "#1ab394";
          }
      },


}

//inspinaia 基础组件
EHM.ImportInspinia = function () {
    EHM.ImportCss("/resource/Inspinia/css/bootstrap.min.css");
    //font-awesome 字体库
    EHM.ImportCss("/resource/Inspinia/font-awesome/css/font-awesome.css");



    EHM.ImportScript("/resource/Inspinia/js/jquery-3.1.1.min.js");

    EHM.ImportScript("/resource/Inspinia/js/popper.min.js");
    EHM.ImportScript("/resource/Inspinia/js/bootstrap.min.js");

    EHM.ImportScript("/resourc
...
...
...
```

问题 3 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js
实体：	jquery.metisMenu.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下
修复状态： 已修复
修复方式： 将服务器配置为使用安全策略的“Content-Security-Policy”头
测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko Referer: http://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
```

```
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:59 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 13431
Vary: Accept-Encoding
ETag: W/"13431-1571017739982"
Date: Thu, 14 Nov 2019 08:27:25 GMT
Content-Type: application/javascript

/*!
 * metismenu - v2.7.7
 * A jQuery menu plugin
 * https://github.com/onokumus/metismenu#readme
*
 * Made by Osman Nuri Okumus <onokumus@gmail.com> (https://github.com/onokumus)
 * Under MIT License
 */
(function (global, factory) {
    typeof exports === 'object' && typeof module !== 'undefined' ?
module.exports = factory(require('jquery')) :
        typeof define === 'function' && define.amd ? define(['jquery'], factory) :
          (global.metisMenu = factory(global.jQuery));
}(this, (function ($) { 'use strict';

    $ = $ && $.hasOwnProperty('default') ? $['default'] : $;

    function _defineProperty(obj, key, value) {
        if (key in obj) {
          Object.defineProperty(obj, key, {
          value: value,
          enumerable: true,
          configurable: true,
          writable: true
          });
        } else { obj[key]
          = value;
        }

        return obj;
    }

    function _objectSpread(target) {
        for (var i = 1; i < arguments.length; i++) {
          var source = arguments[i] != null ? arguments[i] : {};
          var ownKeys = Object.keys(source);

          if (typeof Object.getOwnPropertySymbols === 'function') {
          ownKeys = ownKeys.concat(Object.getOwnPropertySymbols(source).filter(function (sym)
          { return Object.getOwnPropertyDescriptor(source, sym).enumerable; }));

          }

          ownKeys.forEach(function (key) {
          _defineProperty(target, key, source[key]);
          });
        }

        return target;
    }

    var Util = function ($$$1) {
        // eslint-disable-line no-shadow
        var TRANSITION_END = 'transitionend';
        var Util = {
          // eslint-disable-line no-shadow
          TRANSITION_END: 'mmTransitionEnd',
          triggerTransitionEnd: function triggerTransitionEnd(element) {
          $$$1(element).trigger(TRANSITION_END); },

          supportsTransitionEnd: function supportsTransitionEnd() { return

          Boolean(TRANSITION_END);
```

```
          }
        };

        function getSpecialTransitionEndEvent() {
          return {
          bindType: TRANSITION_END,
          delegateType: TRANSITION_END,
          handle: function handle(event) {
          if ($$$1(event.target).is(this)) {
          return event.handleObj.handler.apply(this, arguments); // eslint-disable-line
prefer-rest-params
          }

          return undefined;
          }
          };
        }

        function transitionEndEmulator(duration) {
          var _this = this;

          var called = false;
          $$$1(this).one(Util.TRANSITION_END, function () {
          called = true;
          });
          setTimeout(function () {
          if (!called) {
          Util.triggerTransitionEnd(_this);
          }
          }, duration);
          return this;
        }

        function setTransitionEndSupport() {
          $$$1.fn.mmEmulateTransitionEnd = transitionEndEmulator; // eslint-disable-line
no-param-reassign
          // eslint-disable-next-line no-param-reassign

          $$$1.event.special[Util.TRANSITION_END] = getSpecialTransitionEndEvent();
        }

        setTransitionEndSupport();
        return Util;
    }($);

    var MetisMenu = function ($$$1) {
        // eslint-disable-line no-
        shadow var NAME = 'metisMenu';
        var DATA_KEY = 'metisMenu'; var
        EVENT_KEY = "." + DATA_KEY; var
        DATA_API_KEY = '.data-api';
        var JQUERY_NO_CONFLICT = $$$1.fn[NAME]; var
        TRANSITION_DURATION = 350;
        var Default = { toggle: true,
          preventDefault: true,
          activeClass: 'active',
          collapseClass: 'collapse',
          collapseInClass: 'in',
          collapsingClass: 'collapsing',
          triggerElement: 'a',
          parentTrigger: 'li', subMenu:
          'ul'

        };
        var Event = {
          SHOW: "show" + EVENT_KEY,
          SHOWN: "shown" + EVENT_KEY,
          HIDE
...
...
...
```

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/EHM/itime.ext.js
实体：	itime.ext.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下
修复状态： 已修复
修复方式： 将服务器配置为使用安全策略的“Content-Security-Policy”头
测试请求和响应：

```
GET /web/resource/EHM/itime.ext.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:20 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 14237
Vary: Accept-Encoding
ETag: W/"14237-1571017700341"
Date: Thu, 14 Nov 2019 08:27:23 GMT
Content-Type: application/javascript

/**
 * ----------------  自动引入的插件 -----------------
 * @constructor
 */
EHM.ImportBootstrapTable = function () {
    EHM.ImportCss("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.css");
    EHM.ImportCss("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-
control.min.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-
control.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-zh-
CN.min.js");

};
//选择框插件
EHM.ImportSelect2 = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/select2/select2.min.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/select2/select2.full.min.js");
};

EHM.ImportChosen = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/chosen/bootstrap-chosen.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/chosen/chosen.jquery.js");
};
```

```
//checkbox 插件
EHM.ImportICheck = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/iCheck/custom.css");
    EHM.ImportCss("/resource/Inspinia/css/plugins/awesome-bootstrap-checkbox/awesome-bootstrap-
checkbox.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/iCheck/icheck.min.js");
};
EHM.ImportValidate = function () {
    EHM.ImportScript("/resource/Inspinia/js/plugins/validate/jquery.validate.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/validate/messages_zh.min.js");
};

EHM.ImportItimeCommon = function(){

    EHM.ImportScript("/resource/js/itimecommon.js");
};
//日期选择插件
EHM.ImportDatapicker = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/datapicker/datepicker3.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/datapicker/bootstrap-datepicker.js");
};
EHM.ImportDataRangePicker = function(){

EHM.ImportScript("/resource/bootstrap/AdminLTE/plugins/daterangepicker/ext/moment.min.itim.js");
    EHM.ImportScript("/resource/bootstrap/AdminLTE/plugins/daterangepicker/daterangepicker.js");
    EHM.ImportCss("/resource/bootstrap/AdminLTE/plugins/daterangepicker/daterangepicker-
bs3.css");
}
//alert 窗口插件
EHM.ImportSweetalert = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/sweetalert/sweetalert.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/sweetalert/sweetalert.min.js");
}
EHM.ImportBasePlugins = function(){
    EHM.ImportValidate();


    EHM.ImportSelect2();

    EHM.ImportICheck();

    EHM.ImportDatapicker();

    EHM.ImportDataRangePicker();
    //弹窗
    EHM.ImportScript("/resource/EHM/Toolkit/PopWin/InspiniaPopWin.js");
    //全屏
    EHM.ImportScript("/resource/jquery/jquery.fullscreenITIME.js");

    EHM.ImportScript("/resource/EHM/util/cookie/cookieITIME.js");
   //json 工具
    EHM.ImportScript("/resource/js/json2.js");

    EHM.ImportSweetalert();
    EHM.ImportBootstrapTable();
    EHM.ImportItimeCommon();
};

//自动引入相关组件
EHM.ImportBasePlugins();

/**
 * ---------- 需手工引入的插件 ------
 * @constructor
 */
//瀑布流布局
EHM.ImportMasonary = function () {
    EHM.ImportScript("/resource/Inspinia/js/plugins/masonary/masonry.pkgd.min.js");
};

//highchart 图表插件
EHM.ImportHighcharts = function () {
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-3d.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-more.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/exporting.js");
//EHM.Import("/resource/pluginsWithDhtmlx/highchart/js/offline-exporting.js");
```

```
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/sankey.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/oldie.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/heatmap.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/tilemap.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/organization.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/no-data-to-display.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-zh_CN.js");
    EHM.ImportScript("/resource/plugi
...
...
...
```

问题 5 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/popper.min.js
实体：	popper.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

修复状态： 已修复

修复方式： 将服务器配置为使用安全策略的“Content-Security-Policy”头

测试请求和响应：

```
GET /web/resource/Inspinia/js/popper.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://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:49:27 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 19191
Vary: Accept-Encoding
ETag: W/"19191-1571017767939"
Date: Thu, 14 Nov 2019 08:27:25 GMT
Content-Type: application/javascript

/*
 Copyright (C) Federico Zivolo 2017
 Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).
 */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?
module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function()
{'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t)
```

```
{if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e)
{return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return
document.body;switch(e.nodeName){case'HTML':case'BODY':return
e.ownerDocument.body;case'#document':return e.body;}var
i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?
e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?
-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?
e.ownerDocument.documentElement:document.documentElement}function p(e){var
t=e.nodeName;return'BODY'!==t&&('HTML'===t||r(e.firstElementChild)===e)}function s(e){return
null===e.parentNode?e:s(e.parentNode)}function d(e,t){if(!e||!e.nodeType||!t||!t.nodeType)return
document.documentElement;var o=e.compareDocumentPosition(t)&Node.DOCUMENT_POSITION_FOLLOWING,i=o?
e:t,n=o?t:e,a=document.createRange();a.setStart(i,0),a.setEnd(n,0);var
l=a.commonAncestorContainer;if(e!==l&&t!==l||i.contains(n))return p(l)?l:r(l);var f=s(e);return
f.host?d(f.host,t):d(e,s(t).host)}function a(e){var t=1<arguments.length&&void 0!==arguments[1]?
arguments[1]:'top',o='top'===t?'scrollTop':'scrollLeft',i=e.nodeName;if('BODY'===i||'HTML'===i)
{var n=e.ownerDocument.documentElement,r=e.ownerDocument.scrollingElement||n;return r[o]}return
e[o]}function l(e,t){var o=2<arguments.length&&void
0!==arguments[2]&&arguments[2],i=a(t,'top'),n=a(t,'left'),r=o?-1:1;return
e.top+=i*r,e.bottom+=i*r,e.left+=n*r,e.right+=n*r,e}function f(e,t){var
o='x'===t?'Left':'Top',i='Left'==o?'Right':'Bottom';return
parseFloat(e['border'+o+'Width'],10)+parseFloat(e['border'+i+'Width'],10)}function m(e,t,o,i)
{return J(t['offset'+e],t['scroll'+e],o['client'+e],o['offset'+e],o['scroll'+e],ie()?
o['offset'+e]+i['margin'+('Height'===e?'Top':'Left')]+i['margin'+
('Height'===e?'Bottom':'Right')]:0)}function h(){var
e=document.body,t=document.documentElement,o=ie()&&getComputedStyle(t);return{height:m('Height',e
,t,o),width:m('Width',e,t,o)}}function c(e){return se({},e,
{right:e.left+e.width,bottom:e.top+e.height})}function g(e){var o=
{};if(ie())try{o=e.getBoundingClientRect();var
i=a(e,'top'),n=a(e,'left');o.top+=i,o.left+=n,o.bottom+=i,o.right+=n}catch(e){}else
o=e.getBoundingClientRect();var r={left:o.left,top:o.top,width:o.right-o.left,height:o.bottom-
o.top},p='HTML'===e.nodeName?h():{},s=p.width||e.clientWidth||r.right-
r.left,d=p.height||e.clientHeight||r.bottom-r.top,l=e.offsetWidth-s,m=e.offsetHeight-d;if(l||m)
{var g=t(e);l-=f(g,'x'),m-=f(g,'y'),r.width-=l,r.height-=m}return c(r)}function u(e,o){var
i=ie(),r='HTML'===o.nodeName,p=g(e),s=g(o),d=n(e),a=t(o),f=parseFloat(a.borderTopWidth,10),m=pars
eFloat(a.borderLeftWidth,10),h=c({top:p.top-s.top-f,left:p.left-s.left-
m,width:p.width,height:p.height});if(h.marginTop=0,h.marginLeft=0,!i&&r){var
u=parseFloat(a.marginTop,10),b=parseFloat(a.marginLeft,10);h.top-=f-u,h.bottom-=f-u,h.left-=m-
b,h.right-=m-b,h.marginTop=u,h.marginLeft=b}return(i?o.contains(d):o===d&&'BODY'!==d.nodeName)&&
(h=l(h,o)),h}function b(e){var
t=e.ownerDocument.documentElement,o=u(e,t),i=J(t.clientWidth,window.innerWidth||0),n=J(t.clientHe
ight,window.innerHeight||0),r=a(t),p=a(t,'left'),s={top:r-o.top+o.marginTop,left:p-
o.left+o.marginLeft,width:i,height:n};return c(s)}function w(e){var
i=e.nodeName;return'BODY'===i||'HTML'===i?!1:'fixed'===t(e,'position')||w(o(e))}function
y(e,t,i,r){var p={top:0,left:0},s=d(e,t);if('viewport'===r)p=b(s);else{var a;'scrollParent'===r?
(a=n(o(t)),'BODY'===a.nodeName&&(a=e.ownerDocument.documentElement)):'window'===r?
a=e.ownerDocument.documentElement:a=r;var l=u(a,s);if('HTML'===a.nodeName&&!w(s)){var
f=h(),m=f.height,c=f.width;p.top+=l.top-l.marginTop,p.bottom=m+l.top,p.left+=l.left-
l.marginLeft,p.right=c+l.left}else p=l}return p.left+=i,p.top+=i,p.right-=i,p.bottom-
=i,p}function E(e){var t=e.width,o=e.height;return t*o}function v(e,t,o,i,n){var r=5<
...
...
...
```


低 “X-Content-Type-Options”头缺失或不安全 5 TOC

问题 1 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/desktop
实体：	desktop (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

修复状态： 已修复

修复方式： 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

测试请求和响应：

```
GET /web/desktop 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: 124.254.61.27:9090
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip
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
Transfer-Encoding: chunked
Content-Length: 8495
Vary: Accept-Encoding
Set-Cookie: JSESSIONID=49AB80D2E6EBA2F0E59E63E86F0DCFAA; Path=/web; HttpOnly
Date: Thu, 14 Nov 2019 08:25:41 GMT
Content-Type: text/html;charset=UTF-8



<!Doctype html>
<html>
<head>



<script>
  Ext_BLANK_IMAGE_URL = "";
</script>

    <title></title>
    <script type="text/javascript"
src="/web/resource/EHM/itime.js;jsessionid=49AB80D2E6EBA2F0E59E63E86F0DCFAA"></script>
    <meta name="viewport" content="width=device-width, initial-
scale=0.9"> <script>
    EHM.ImportToastr();
</script>
</head>



<script type="text/javascript">

    //EHM.Cache["LOGIN_SAVE_PASS"] = false;

    function failAction(msg) {
        if (msg == "用户密码过期，请重新设置密码")
          window.open('staff/initChangePwd.do', 'popUpWin',
'scrollbars=0,toolbar=0,status=1,width=543,height=354,left=300,
```

```
top=200,screenX=200,screenY=200');
    }

    function IsPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone",
          "SymbianOS", "Windows Phone",
          "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
          if (userAgentInfo.indexOf(Agents[v]) > 0) {
          flag = false;
          break;
          }
        }
        return flag;
    }

    $(function () {
        var authMsg = "";

        if(null!=authMsg && ""!=authMsg){
          toastr["error"](authMsg);
        }else{
          $.post(EHM.rootPath+"/sysmenu/licenseCheck.sp",function(data){
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-full-width",
          "onclick": null,
          "showDuration": "400",
          "hideDuration": "1000",
          "timeOut": "10000",
          "extendedTimeOut": "1000",
          "showEasing": "swing",
          "hideEasing": "linear",
          "showMethod": "fadeIn",
          "hideMethod": "fadeOut"
          };
          if(data["flag"]==1){

          toastr["warning"](data["authMsg"]);
          }else if(data["flag"]==0){
          toastr["error"](data["authMsg"]);
          }

          },"json");
        }

        if(!IsPC()){
          $("#showDiv").attr("style","width:500px;margin-top:25%")
        }
        var url="/web/logomanager/getLoginInfo.do;jsessionid=49AB80D2E6EBA2F0E59E63E86F0DCFAA";
        $.post(url,function(data){
          data=JSON.parse(data);
          var src1="resource/images/"+data.LOGIN_LOGO;
          var src2="resource/images/"+data.LOGIN_QRCODE;
          $("#logoimg").attr("src",src1);
          $("#qrimg").attr("src",src2);
        });

        $("#loginForm").submit(function (e) {
          updateCookie();
        });

        $("#loginBt").on("click",function(){
          if($("#savePassImg").is(':checked'))
          {
          cookie.set("LOGIN_SAVE_PASS",true) ;
          }else{
          cookie.set("LOGIN_SAVE_PASS",false) ;
          }
          var isUnionYW = 0;
          var yw_url = 'null';

          if(isUnionYW==1){
```

```
          var userNameValue = $("#j_username").val().trim();
          var passWordValue = $("#j_password").val().trim();
          yw_url = yw_url+"?j_username="+userNameValue+"&j_password="+passWordValue;
          $("#iframeVar").load(function(){
          $("#loginForm").submit();
          });
          $('#iframeVar').attr('src', yw_url);
          }else{
          $("#loginForm").submit();
          }


          //
        });

        var jsonStr = '{"success":"false","message":"登陆失败:用户不存在或密码错误
        "}'; if (jsonStr != null && jsonStr != "") {
          var jsonObj = JSON.parse(jsonStr);
          if (jsonObj && jsonObj != undefined) {
          if (jsonObj.success == "false") {
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-center",
          "onclick": null,

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

问题 2 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/EHM/itime.ext.js
实体：	itime.ext.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

修复状态： 已修复

修复方式： 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

测试请求和响应：

```
GET /web/resource/EHM/itime.ext.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
```

```
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:20 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 14237
Vary: Accept-Encoding
ETag: W/"14237-1571017700341"
Date: Thu, 14 Nov 2019 08:27:23 GMT
Content-Type: application/javascript

/**
 * ----------------  自动引入的插件 -----------------
 * @constructor
 */
EHM.ImportBootstrapTable = function () {
    EHM.ImportCss("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.css");
    EHM.ImportCss("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-
control.min.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-
control.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-zh-
CN.min.js");

};
//选择框插件
EHM.ImportSelect2 = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/select2/select2.min.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/select2/select2.full.min.js");
};

EHM.ImportChosen = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/chosen/bootstrap-chosen.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/chosen/chosen.jquery.js");
};

//checkbox 插件
EHM.ImportICheck = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/iCheck/custom.css");
    EHM.ImportCss("/resource/Inspinia/css/plugins/awesome-bootstrap-checkbox/awesome-bootstrap-
checkbox.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/iCheck/icheck.min.js");
};
EHM.ImportValidate = function () {
    EHM.ImportScript("/resource/Inspinia/js/plugins/validate/jquery.validate.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/validate/messages_zh.min.js");
};

EHM.ImportItimeCommon = function(){

    EHM.ImportScript("/resource/js/itimecommon.js");
};
//日期选择插件
EHM.ImportDatapicker = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/datapicker/datepicker3.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/datapicker/bootstrap-datepicker.js");
};
EHM.ImportDataRangePicker = function(){

EHM.ImportScript("/resource/bootstrap/AdminLTE/plugins/daterangepicker/ext/moment.min.itim.js");
    EHM.ImportScript("/resource/bootstrap/AdminLTE/plugins/daterangepicker/daterangepicker.js");
    EHM.ImportCss("/resource/bootstrap/AdminLTE/plugins/daterangepicker/daterangepicker-
bs3.css");
}
//alert 窗口插件
EHM.ImportSweetalert = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/sweetalert/sweetalert.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/sweetalert/sweetalert.min.js");
}
EHM.ImportBasePlugins = function(){
    EHM.ImportValidate();


    EHM.ImportSelect2();
```

```
    EHM.ImportICheck();

    EHM.ImportDatapicker();

    EHM.ImportDataRangePicker();
    //弹窗
    EHM.ImportScript("/resource/EHM/Toolkit/PopWin/InspiniaPopWin.js");
    //全屏
    EHM.ImportScript("/resource/jquery/jquery.fullscreenITIME.js");

    EHM.ImportScript("/resource/EHM/util/cookie/cookieITIME.js");
   //json 工具
    EHM.ImportScript("/resource/js/json2.js");

    EHM.ImportSweetalert();
    EHM.ImportBootstrapTable();
    EHM.ImportItimeCommon();
};

//自动引入相关组件
EHM.ImportBasePlugins();

/**
 * ---------- 需手工引入的插件 ------
 * @constructor
 */
//瀑布流布局
EHM.ImportMasonary = function () {
    EHM.ImportScript("/resource/Inspinia/js/plugins/masonary/masonry.pkgd.min.js");
};

//highchart 图表插件
EHM.ImportHighcharts = function () {
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-3d.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-more.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/exporting.js");
//EHM.Import("/resource/pluginsWithDhtmlx/highchart/js/offline-exporting.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/sankey.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/oldie.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/heatmap.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/tilemap.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/organization.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/no-data-to-display.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-zh_CN.js");
    EHM.ImportScript("/resource/plugi
...
...
...
```

问题 3 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/EHM/itime.js;jsessionid=2AD69A46E20F35E8C98AB6912F83C7FE
实体：	itime.js;jsessionid=2AD69A46E20F35E8C98AB6912F83C7FE (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

修复状态： 已修复

修复方式： 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

测试请求和响应：

```
GET /web/resource/EHM/itime.js;jsessionid=7C15879B0ED11B9A08F98F109DD4C897 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: Keep-Alive
Host: 124.254.61.27:9090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:20 GMT
Accept-Ranges: bytes
Content-Length: 6725
ETag: W/"6725-1571017700350"
Date: Thu, 14 Nov 2019 08:25:41 GMT
Content-Type: application/javascript

window["undefined"] = window["undefined"];
var EHM = {
    Cache: {},
    rootPath: (function () {
        if (window["ROOT_PATH"]) {
          window["ROOT_PATH"] = "/" + window["ROOT_PATH"].split("\/")[1];
        }

        return window["ROOT_PATH"] || (function () {

          var L = window.location;
          var SR = L.pathname;
          if (SR.indexOf("/") > 0) SR = "/" + SR;
          return "/" + SR.split("\/")[1];
        })();
    })(),
    ImportScript: function (url) {
        document.writeln("<script type='text/javascript' src='" + EHM.rootPath + url +
"' ><" + "/scr" + "ipt>");
    },
    ImportCss: function (url) {
        document.writeln("<link href=\"" + EHM.rootPath + url + "\" rel=\"stylesheet\"
type=\"text/css\" />");
    },
    ImportWebIcon: function (url) {

        if (url.indexOf(EHM.rootPath) < 0) {
          url = EHM.rootPath + ((url.indexOf("EHM") == 0) ? EHM.appPath : "") + url;
        }
```

```
        try {
          document.writeln("<link href=\"" + url + "\" rel=\"Bookmark\"
type=\"image/x-icon\"/>");
          document.writeln("<link href=\"" + url + "\" rel=\"Shortcut Icon\"
type=\"image/x-icon\"/>");
        }
        catch (e) {
          var linksBookmark = document.createElement("link");
          linksBookmark.href = url;
          linksBookmark.rel = "Bookmark";

          var linksShortcut = document.createElement("link");
          linksShortcut.href = url;
          linksShortcut.rel = "Shortcut Icon";

          document.getElementsByTagName("head")[0].appendChild(links);
        }

        return EHM;
    },
    //根据指标值返回呈现颜色,数值从低到高为绿色,黄色,红色
    getAlarmColor:function(kpiValue){
        if(!isNaN(kpiValue)){
          if(kpiValue<70){
          return "#1ab394";
          }else if(kpiValue>=70 && kpiValue<90){
          return "#f8ac59";
          }else{
          return "#ed5565";
          }
        }else{
          return "#23c6c8";
        }
    },

    //根据指标值返回呈现颜色,数值从低到高为红色,黄色,绿色
    getAlarmReverseColor:function(kpiValue){
        if(!isNaN(kpiValue)){
          if(kpiValue<70){
          return "#ed5565";
          }else if(kpiValue>=70 && kpiValue<85){
          return "#f8ac59";
          }else{
          return "#1ab394";
          }
        }else{
          return "#23c6c8";
        }
    },

    getInspiniaAlarmColor:function(kpiValue){

        if(!isNaN(kpiValue)){
          if(kpiValue>=90){
          return '<div class="progress progress-itime "><div style="width: '+ kpiValue +
'%;"     class="progress-bar     progress-bar-danger"></div><div     class="progress-itime-
text">'+kpiValue+' % </div></div>';
          }else if(kpiValue>=75 && kpiValue<90){
          return '<div class="progress progress-itime "><div style="width: '+ kpiValue +
'%;"     class="progress-bar     progress-bar-warning"></div><div     class="progress-itime-
text">'+kpiValue+' % </div></div>';
          }else{
          return '<div class="progress progress-itime"><div style="width: '+ kpiValue + '%;"
class="progress-bar"></div><div class="progress-itime-text">'+kpiValue+' %</div></div>';
          }
        }else{
          return "#23c6c8";
        }
    },

    //根据告警级别返回颜色，包含轻微、重要、严重、正常、未管理
    getAlarmLevelColor:function(alarmLevel){
        //告警级别及设备管理状态
        if(alarmLevel=='10'){
          //轻微
          return "#f3f315";
        }else if(alarmLevel=='15'){
          //重要
```

```
            return "#f8ac59";
          }else if(alarmLevel=='20'){
            //严重
            return "#ed5565";
          }else if(alarmLevel=='1'){
            //未管理
            return "#f3f3f4";
          }else{
            //正常
            return "#1ab394";
          }
      },


}

//inspinaia 基础组件
EHM.ImportInspinia = function () {
    EHM.ImportCss("/resource/Inspinia/css/bootstrap.min.css");
    //font-awesome 字体库
    EHM.ImportCss("/resource/Inspinia/font-awesome/css/font-awesome.css");



    EHM.ImportScript("/resource/Inspinia/js/jquery-3.1.1.min.js");

    EHM.ImportScript("/resource/Inspinia/js/popper.min.js");
    EHM.ImportScript("/resource/Inspinia/js/bootstrap.min.js");

    EHM.ImportScript("/resourc
...
...
...
```

问题 4 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js
实体：	jquery.metisMenu.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

修复状态： 已修复

修复方式： 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko Referer: http://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897 Connection: keep-alive
```

```
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:59 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 13431
Vary: Accept-Encoding
ETag: W/"13431-1571017739982"
Date: Thu, 14 Nov 2019 08:27:25 GMT
Content-Type: application/javascript

/*!
 * metismenu - v2.7.7
 * A jQuery menu plugin
 * https://github.com/onokumus/metismenu#readme
*
 * Made by Osman Nuri Okumus <onokumus@gmail.com> (https://github.com/onokumus)
 * Under MIT License
 */
(function (global, factory) {
    typeof exports === 'object' && typeof module !== 'undefined' ?
module.exports = factory(require('jquery')) :
        typeof define === 'function' && define.amd ? define(['jquery'], factory) :
          (global.metisMenu = factory(global.jQuery));
}(this, (function ($) { 'use strict';

    $ = $ && $.hasOwnProperty('default') ? $['default'] : $;

    function _defineProperty(obj, key, value) {
        if (key in obj) {
          Object.defineProperty(obj, key, {
          value: value,
          enumerable: true,
          configurable: true,
          writable: true
          });
        } else { obj[key]
          = value;
        }

        return obj;
    }

    function _objectSpread(target) {
        for (var i = 1; i < arguments.length; i++) {
          var source = arguments[i] != null ? arguments[i] : {};
          var ownKeys = Object.keys(source);

          if (typeof Object.getOwnPropertySymbols === 'function') {
          ownKeys = ownKeys.concat(Object.getOwnPropertySymbols(source).filter(function (sym)
          { return Object.getOwnPropertyDescriptor(source, sym).enumerable; }));

          }

          ownKeys.forEach(function (key) {
          _defineProperty(target, key, source[key]);
          });
        }

        return target;
    }

    var Util = function ($$$1) {
        // eslint-disable-line no-shadow
        var TRANSITION_END = 'transitionend';
        var Util = {
          // eslint-disable-line no-shadow
          TRANSITION_END: 'mmTransitionEnd',
          triggerTransitionEnd: function triggerTransitionEnd(element) {
          $$$1(element).trigger(TRANSITION_END); },

          supportsTransitionEnd: function supportsTransitionEnd() { return

          Boolean(TRANSITION_END);
```

```
          }
        };

        function getSpecialTransitionEndEvent() {
          return {
          bindType: TRANSITION_END,
          delegateType: TRANSITION_END,
          handle: function handle(event) {
          if ($$$1(event.target).is(this)) {
          return event.handleObj.handler.apply(this, arguments); // eslint-disable-line
prefer-rest-params
          }

          return undefined;
          }
          };
        }

        function transitionEndEmulator(duration) {
          var _this = this;

          var called = false;
          $$$1(this).one(Util.TRANSITION_END, function () {
          called = true;
          });
          setTimeout(function () {
          if (!called) {
          Util.triggerTransitionEnd(_this);
          }
          }, duration);
          return this;
        }

        function setTransitionEndSupport() {
          $$$1.fn.mmEmulateTransitionEnd = transitionEndEmulator; // eslint-disable-line
no-param-reassign
          // eslint-disable-next-line no-param-reassign

          $$$1.event.special[Util.TRANSITION_END] = getSpecialTransitionEndEvent();
        }

        setTransitionEndSupport();
        return Util;
    }($);

    var MetisMenu = function ($$$1) {
        // eslint-disable-line no-
        shadow var NAME = 'metisMenu';
        var DATA_KEY = 'metisMenu'; var
        EVENT_KEY = "." + DATA_KEY; var
        DATA_API_KEY = '.data-api';
        var JQUERY_NO_CONFLICT = $$$1.fn[NAME]; var
        TRANSITION_DURATION = 350;
        var Default = { toggle: true,
          preventDefault: true,
          activeClass: 'active',
          collapseClass: 'collapse',
          collapseInClass: 'in',
          collapsingClass: 'collapsing',
          triggerElement: 'a',
          parentTrigger: 'li', subMenu:
          'ul'

        };
        var Event = {
          SHOW: "show" + EVENT_KEY,
          SHOWN: "shown" + EVENT_KEY,
          HIDE
...
...
...
```

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/popper.min.js
实体：	popper.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

差异：

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

修复状态： 已修复

修复方式： 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

测试请求和响应：

```
GET /web/resource/Inspinia/js/popper.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://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:49:27 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 19191
Vary: Accept-Encoding
ETag: W/"19191-1571017767939"
Date: Thu, 14 Nov 2019 08:27:25 GMT
Content-Type: application/javascript

/*
 Copyright (C) Federico Zivolo 2017
 Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).
 */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module? module.exports=t():'function'==typeof
define&&define.amd?define(t):e.Popper=t()})(this,function() {'use strict';function e(e){return e&&'[object
Function]'==={}.toString.call(e)}function t(e,t) {if(1!==e.nodeType)return[];var
o=getComputedStyle(e,null);return t?o[t]:o}function o(e)
{return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return
document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return
e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?
e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i? -
1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?
e.ownerDocument.documentElement:document.documentElement}function p(e){var
t=e.nodeName;return'BODY'!==t&&('HTML'===t||r(e.firstElementChild)===e)}function s(e){return
null===e.parentNode?e:s(e.parentNode)}function d(e,t){if(!e||!e.nodeType||!t||!t.nodeType)return
document.documentElement;var o=e.compareDocumentPosition(t)&Node.DOCUMENT_POSITION_FOLLOWING,i=o?
e:t,n=o?t:e,a=document.createRange();a.setStart(i,0),a.setEnd(n,0);var
l=a.commonAncestorContainer;if(e!==l&&t!==l||i.contains(n))return p(l)?l:r(l);var f=s(e);return
f.host?d(f.host,t):d(e,s(t).host)}function a(e){var t=1<arguments.length&&void 0!==arguments[1]?
arguments[1]:'top',o='top'===t?'scrollTop':'scrollLeft',i=e.nodeName;if('BODY'===i||'HTML'===i) {var
n=e.ownerDocument.documentElement,r=e.ownerDocument.scrollingElement||n;return r[o]}return e[o]}function
l(e,t){var o=2<arguments.length&&void 0!==arguments[2]&&arguments[2],i=a(t,'top'),n=a(t,'left'),r=o?-
1:1;return e.top+=i*r,e.bottom+=i*r,e.left+=n*r,e.right+=n*r,e}function f(e,t){var
```

```
o='x'===t?'Left':'Top',i='Left'==o?'Right':'Bottom';return
parseFloat(e['border'+o+'Width'],10)+parseFloat(e['border'+i+'Width'],10)}function m(e,t,o,i)
{return J(t['offset'+e],t['scroll'+e],o['client'+e],o['offset'+e],o['scroll'+e],ie()?
o['offset'+e]+i['margin'+('Height'===e?'Top':'Left')]+i['margin'+
('Height'===e?'Bottom':'Right')]:0)}function h(){var
e=document.body,t=document.documentElement,o=ie()&&getComputedStyle(t);return{height:m('Height',e
,t,o),width:m('Width',e,t,o)}}function c(e){return se({},e,
{right:e.left+e.width,bottom:e.top+e.height})}function g(e){var o=
{};if(ie())try{o=e.getBoundingClientRect();var
i=a(e,'top'),n=a(e,'left');o.top+=i,o.left+=n,o.bottom+=i,o.right+=n}catch(e){}else
o=e.getBoundingClientRect();var r={left:o.left,top:o.top,width:o.right-o.left,height:o.bottom-
o.top},p='HTML'===e.nodeName?h():{},s=p.width||e.clientWidth||r.right-
r.left,d=p.height||e.clientHeight||r.bottom-r.top,l=e.offsetWidth-s,m=e.offsetHeight-d;if(l||m)
{var g=t(e);l-=f(g,'x'),m-=f(g,'y'),r.width-=l,r.height-=m}return c(r)}function u(e,o){var
i=ie(),r='HTML'===o.nodeName,p=g(e),s=g(o),d=n(e),a=t(o),f=parseFloat(a.borderTopWidth,10),m=pars
eFloat(a.borderLeftWidth,10),h=c({top:p.top-s.top-f,left:p.left-s.left-
m,width:p.width,height:p.height});if(h.marginTop=0,h.marginLeft=0,!i&&r){var
u=parseFloat(a.marginTop,10),b=parseFloat(a.marginLeft,10);h.top-=f-u,h.bottom-=f-u,h.left-=m-
b,h.right-=m-b,h.marginTop=u,h.marginLeft=b}return(i?o.contains(d):o===d&&'BODY'!==d.nodeName)&&
(h=l(h,o)),h}function b(e){var
t=e.ownerDocument.documentElement,o=u(e,t),i=J(t.clientWidth,window.innerWidth||0),n=J(t.clientHe
ight,window.innerHeight||0),r=a(t),p=a(t,'left'),s={top:r-o.top+o.marginTop,left:p-
o.left+o.marginLeft,width:i,height:n};return c(s)}function w(e){var
i=e.nodeName;return'BODY'===i||'HTML'===i?!1:'fixed'===t(e,'position')||w(o(e))}function
y(e,t,i,r){var p={top:0,left:0},s=d(e,t);if('viewport'===r)p=b(s);else{var a;'scrollParent'===r?
(a=n(o(t)),'BODY'===a.nodeName&&(a=e.ownerDocument.documentElement)):'window'===r?
a=e.ownerDocument.documentElement:a=r;var l=u(a,s);if('HTML'===a.nodeName&&!w(s)){var
f=h(),m=f.height,c=f.width;p.top+=l.top-l.marginTop,p.bottom=m+l.top,p.left+=l.left-
l.marginLeft,p.right=c+l.left}else p=l}return p.left+=i,p.top+=i,p.right-=i,p.bottom-
=i,p}function E(e){var t=e.width,o=e.height;return t*o}function v(e,t,o,i,n){var r=5<
...
...
...
```


低 “X-XSS-Protection”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js
实体：	jquery.metisMenu.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

修复状态： 已修复

修复方式： 在 HTTP 响应报文的头部增加一个 X-XSS-Protection 字段，设置 XSS-Protection: 1; mode=block

测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko Referer: http://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:59 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 13431
Vary: Accept-Encoding
ETag: W/"13431-1571017739982"
Date: Thu, 14 Nov 2019 08:27:25 GMT
Content-Type: application/javascript

/*!
 * metismenu - v2.7.7
 * A jQuery menu plugin
 * https://github.com/onokumus/metismenu#readme
*
 * Made by Osman Nuri Okumus <onokumus@gmail.com> (https://github.com/onokumus)
 * Under MIT License
 */
(function (global, factory) {
    typeof exports === 'object' && typeof module !== 'undefined' ?
module.exports = factory(require('jquery')) :
        typeof define === 'function' && define.amd ? define(['jquery'], factory) :
          (global.metisMenu = factory(global.jQuery));
}(this, (function ($) { 'use strict';

    $ = $ && $.hasOwnProperty('default') ? $['default'] : $;

    function _defineProperty(obj, key, value) {
        if (key in obj) {
          Object.defineProperty(obj, key, {
          value: value,
          enumerable: true,
          configurable: true,
          writable: true
          });
        } else { obj[key]
          = value;
        }

        return obj;
    }

    function _objectSpread(target) {
        for (var i = 1; i < arguments.length; i++) {
          var source = arguments[i] != null ? arguments[i] : {};
          var ownKeys = Object.keys(source);

          if (typeof Object.getOwnPropertySymbols === 'function') {
          ownKeys = ownKeys.concat(Object.getOwnPropertySymbols(source).filter(function (sym)
          { return Object.getOwnPropertyDescriptor(source, sym).enumerable; }));

          }

          ownKeys.forEach(function (key) {
          _defineProperty(target, key, source[key]);
          });
        }

        return target;
    }

    var Util = function ($$$1) {
        // eslint-disable-line no-shadow
        var TRANSITION_END = 'transitionend';
```

```
        var Util = {
          // eslint-disable-line no-shadow
          TRANSITION_END: 'mmTransitionEnd',
          triggerTransitionEnd: function triggerTransitionEnd(element) {
          $$$1(element).trigger(TRANSITION_END); },

          supportsTransitionEnd: function supportsTransitionEnd() { return
          Boolean(TRANSITION_END);
          }
        };

        function getSpecialTransitionEndEvent() {
          return {
          bindType: TRANSITION_END,
          delegateType: TRANSITION_END,
          handle: function handle(event) {
          if ($$$1(event.target).is(this)) {
          return event.handleObj.handler.apply(this, arguments); // eslint-disable-line
prefer-rest-params
          }

          return undefined;
          }
          };
        }

        function transitionEndEmulator(duration) {
          var _this = this;

          var called = false;
          $$$1(this).one(Util.TRANSITION_END, function () {
          called = true;
          });
          setTimeout(function () {
          if (!called) {
          Util.triggerTransitionEnd(_this);
          }
          }, duration);
          return this;
        }

        function setTransitionEndSupport() {
          $$$1.fn.mmEmulateTransitionEnd = transitionEndEmulator; // eslint-disable-line
no-param-reassign
          // eslint-disable-next-line no-param-reassign

          $$$1.event.special[Util.TRANSITION_END] = getSpecialTransitionEndEvent();
        }

        setTransitionEndSupport();
        return Util;
    }($);

    var MetisMenu = function ($$$1) {
        // eslint-disable-line no-
        shadow var NAME = 'metisMenu';
        var DATA_KEY = 'metisMenu'; var
        EVENT_KEY = "." + DATA_KEY; var
        DATA_API_KEY = '.data-api';
        var JQUERY_NO_CONFLICT = $$$1.fn[NAME]; var
        TRANSITION_DURATION = 350;
        var Default = { toggle: true,
          preventDefault: true,
          activeClass: 'active',
          collapseClass: 'collapse',
          collapseInClass: 'in',
          collapsingClass: 'collapsing',
          triggerElement: 'a',
          parentTrigger: 'li', subMenu:
          'ul'

        };
        var Event = {
          SHOW: "show" + EVENT_KEY,
          SHOWN: "shown" + EVENT_KEY,
          HIDE
...
...
```

```
...
```

问题 2 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/desktop
实体：	desktop (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

修复状态： 已修复

修复方式： 在 HTTP 响应报文的头部增加一个 X-XSS-Protection 字段，设置 XSS-Protection: 1; mode=block

测试请求和响应：

```
GET /web/desktop 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: 124.254.61.27:9090
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip
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
Transfer-Encoding: chunked
Content-Length: 8495
Vary: Accept-Encoding
Set-Cookie: JSESSIONID=49AB80D2E6EBA2F0E59E63E86F0DCFAA; Path=/web; HttpOnly
Date: Thu, 14 Nov 2019 08:25:41 GMT
Content-Type: text/html;charset=UTF-8



<!Doctype html>
<html>
<head>



<script>
  Ext_BLANK_IMAGE_URL = "";
</script>

    <title></title>
    <script type="text/javascript"
src="/web/resource/EHM/itime.js;jsessionid=49AB80D2E6EBA2F0E59E63E86F0DCFAA"></script>
    <meta name="viewport" content="width=device-width, initial-
scale=0.9"> <script>
    EHM.ImportToastr();
</script>
```

```
</head>


<script type="text/javascript">

    //EHM.Cache["LOGIN_SAVE_PASS"] = false;

    function failAction(msg) {
        if (msg == "用户密码过期，请重新设置密码")
          window.open('staff/initChangePwd.do', 'popUpWin',
'scrollbars=0,toolbar=0,status=1,width=543,height=354,left=300,
top=200,screenX=200,screenY=200');
    }

    function IsPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone",
          "SymbianOS", "Windows Phone",
          "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
          if (userAgentInfo.indexOf(Agents[v]) > 0) {
          flag = false;
          break;
          }
        }
        return flag;
    }

    $(function () {
        var authMsg = "";

        if(null!=authMsg && ""!=authMsg){
          toastr["error"](authMsg);
        }else{
          $.post(EHM.rootPath+"/sysmenu/licenseCheck.sp",function(data){
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-full-width",
          "onclick": null,
          "showDuration": "400",
          "hideDuration": "1000",
          "timeOut": "10000",
          "extendedTimeOut": "1000",
          "showEasing": "swing",
          "hideEasing": "linear",
          "showMethod": "fadeIn",
          "hideMethod": "fadeOut"
          };
          if(data["flag"]==1){

          toastr["warning"](data["authMsg"]);
          }else if(data["flag"]==0){
          toastr["error"](data["authMsg"]);
          }

          },"json");
        }

        if(!IsPC()){
          $("#showDiv").attr("style","width:500px;margin-top:25%")
        }
        var url="/web/logomanager/getLoginInfo.do;jsessionid=49AB80D2E6EBA2F0E59E63E86F0DCFAA";
        $.post(url,function(data){
          data=JSON.parse(data);
          var src1="resource/images/"+data.LOGIN_LOGO;
          var src2="resource/images/"+data.LOGIN_QRCODE;
          $("#logoimg").attr("src",src1);
          $("#qrimg").attr("src",src2);
        });

        $("#loginForm").submit(function (e) {
          updateCookie();
        });
```

```
        $("#loginBt").on("click",function(){
          if($("#savePassImg").is(':checked'))
          {
          cookie.set("LOGIN_SAVE_PASS",true) ;
          }else{
          cookie.set("LOGIN_SAVE_PASS",false) ;
          }
          var isUnionYW = 0;
          var yw_url = 'null';

          if(isUnionYW==1){
          var userNameValue = $("#j_username").val().trim();
          var passWordValue = $("#j_password").val().trim();
          yw_url = yw_url+"?j_username="+userNameValue+"&j_password="+passWordValue;
          $("#iframeVar").load(function(){
          $("#loginForm").submit();
          });
          $('#iframeVar').attr('src', yw_url);
          }else{
          $("#loginForm").submit();
          }


          //
        });

        var jsonStr = '{"success":"false","message":"登陆失败:用户不存在或密码错误
        "}'; if (jsonStr != null && jsonStr != "") {
          var jsonObj = JSON.parse(jsonStr);
          if (jsonObj && jsonObj != undefined) {
          if (jsonObj.success == "false") {
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-center",
          "onclick": null,

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

问题 3 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/EHM/itime.js;jsessionid=2AD69A46E20F35E8C98AB6912F83C7FE
实体：	itime.js;jsessionid=2AD69A46E20F35E8C98AB6912F83C7FE (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

修复状态：已修复

修复方式：在 HTTP 响应报文的头部增加一个 X-XSS-Protection 字段，设置 XSS-Protection: 1; mode=block

测试请求和响应：

```
GET /web/resource/EHM/itime.js;jsessionid=7C15879B0ED11B9A08F98F109DD4C897
HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0)
like Gecko Referer: http://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: Keep-Alive
Host: 124.254.61.27:9090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:20 GMT
Accept-Ranges: bytes
Content-Length: 6725
ETag: W/"6725-1571017700350"
Date: Thu, 14 Nov 2019 08:25:41 GMT
Content-Type: application/javascript

window["undefined"] = window["undefined"];
var EHM = {
    Cache: {},
    rootPath: (function () {
        if (window["ROOT_PATH"]) {
          window["ROOT_PATH"] = "/" + window["ROOT_PATH"].split("\/")[1];
        }

        return window["ROOT_PATH"] || (function () {

          var L = window.location;
          var SR = L.pathname;
          if (SR.indexOf("/") > 0) SR = "/" + SR;
          return "/" + SR.split("\/")[1];
        })();
    })(),
    ImportScript: function (url) {
        document.writeln("<script type='text/javascript' src='" + EHM.rootPath + url +
"' ><" + "/scr" + "ipt>");
    },
    ImportCss: function (url) {
        document.writeln("<link href=\"" + EHM.rootPath + url + "\" rel=\"stylesheet\"
type=\"text/css\" />");
    },
    ImportWebIcon: function (url) {

        if (url.indexOf(EHM.rootPath) < 0) {
          url = EHM.rootPath + ((url.indexOf("EHM") == 0) ? EHM.appPath : "") + url;
        }

        try {
          document.writeln("<link href=\"" + url + "\" rel=\"Bookmark\"
type=\"image/x-icon\"/>");
          document.writeln("<link href=\"" + url + "\" rel=\"Shortcut Icon\"
type=\"image/x-icon\"/>");
        }
        catch (e) {
          var linksBookmark = document.createElement("link");
          linksBookmark.href = url;
          linksBookmark.rel = "Bookmark";

          var linksShortcut = document.createElement("link");
          linksShortcut.href = url;
          linksShortcut.rel = "Shortcut Icon";

          document.getElementsByTagName("head")[0].appendChild(links);
        }

        return EHM;
    },
    //根据指标值返回呈现颜色,数值从低到高为绿色,黄色,红色
    getAlarmColor:function(kpiValue){
        if(!isNaN(kpiValue)){
          if(kpiValue<70){
```

```
          return "#1ab394";
          }else if(kpiValue>=70 && kpiValue<90){
          return "#f8ac59";
          }else{
          return "#ed5565";
          }
        }else{
          return "#23c6c8";
        }
    },

    //根据指标值返回呈现颜色,数值从低到高为红色,黄色,绿色
    getAlarmReverseColor:function(kpiValue){
        if(!isNaN(kpiValue)){
          if(kpiValue<70){
          return "#ed5565";
          }else if(kpiValue>=70 && kpiValue<85){
          return "#f8ac59";
          }else{
          return "#1ab394";
          }
        }else{
          return "#23c6c8";
        }
    },

    getInspiniaAlarmColor:function(kpiValue){

        if(!isNaN(kpiValue)){
          if(kpiValue>=90){
          return '<div class="progress progress-itime "><div style="width: '+ kpiValue +
'%;"     class="progress-bar     progress-bar-danger"></div><div     class="progress-itime-
text">'+kpiValue+' % </div></div>';
          }else if(kpiValue>=75 && kpiValue<90){
          return '<div class="progress progress-itime "><div style="width: '+ kpiValue +
'%;"     class="progress-bar     progress-bar-warning"></div><div     class="progress-itime-
text">'+kpiValue+' % </div></div>';
          }else{
          return '<div class="progress progress-itime"><div style="width: '+ kpiValue + '%;"
class="progress-bar"></div><div class="progress-itime-text">'+kpiValue+' %</div></div>';
          }
        }else{
          return "#23c6c8";
        }
    },

    //根据告警级别返回颜色，包含轻微、重要、严重、正常、未管理
    getAlarmLevelColor:function(alarmLevel){
        //告警级别及设备管理状态
        if(alarmLevel=='10'){
          //轻微
          return "#f3f315";
        }else if(alarmLevel=='15'){
          //重要
          return "#f8ac59";
        }else if(alarmLevel=='20'){
          //严重
          return "#ed5565";
        }else if(alarmLevel=='1'){
          //未管理
          return "#f3f3f4";
        }else{
          //正常
          return "#1ab394";
        }
    },


}

//inspinaia 基础组件
EHM.ImportInspinia = function () {
    EHM.ImportCss("/resource/Inspinia/css/bootstrap.min.css");
    //font-awesome 字体库
    EHM.ImportCss("/resource/Inspinia/font-awesome/css/font-awesome.css");
```

```
    EHM.ImportScript("/resource/Inspinia/js/jquery-3.1.1.min.js");

    EHM.ImportScript("/resource/Inspinia/js/popper.min.js");
    EHM.ImportScript("/resource/Inspinia/js/bootstrap.min.js");

    EHM.ImportScript("/resourc
...
...
...
```

问题 4 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/EHM/itime.ext.js
实体：	itime.ext.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

修复状态： 已修复

修复方式： 在 HTTP 响应报文的头部增加一个 X-XSS-Protection 字段，设置 XSS-Protection: 1; mode=block

测试请求和响应：

```
GET /web/resource/EHM/itime.ext.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:20 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 14237
Vary: Accept-Encoding
ETag: W/"14237-1571017700341"
Date: Thu, 14 Nov 2019 08:27:23 GMT
Content-Type: application/javascript

/**
 * ----------------  自动引入的插件 -----------------
 * @constructor
 */
EHM.ImportBootstrapTable = function () {
    EHM.ImportCss("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.css");
    EHM.ImportCss("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-
control.min.css");
```

```
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-
control.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-zh-
CN.min.js");

};
//选择框插件
EHM.ImportSelect2 = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/select2/select2.min.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/select2/select2.full.min.js");
};

EHM.ImportChosen = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/chosen/bootstrap-chosen.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/chosen/chosen.jquery.js");
};

//checkbox 插件
EHM.ImportICheck = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/iCheck/custom.css");
    EHM.ImportCss("/resource/Inspinia/css/plugins/awesome-bootstrap-checkbox/awesome-bootstrap-
checkbox.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/iCheck/icheck.min.js");
};
EHM.ImportValidate = function () {
    EHM.ImportScript("/resource/Inspinia/js/plugins/validate/jquery.validate.min.js");
    EHM.ImportScript("/resource/Inspinia/js/plugins/validate/messages_zh.min.js");
};

EHM.ImportItimeCommon = function(){

    EHM.ImportScript("/resource/js/itimecommon.js");
};
//日期选择插件
EHM.ImportDatapicker = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/datapicker/datepicker3.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/datapicker/bootstrap-datepicker.js");
};
EHM.ImportDataRangePicker = function(){

EHM.ImportScript("/resource/bootstrap/AdminLTE/plugins/daterangepicker/ext/moment.min.itim.js");
    EHM.ImportScript("/resource/bootstrap/AdminLTE/plugins/daterangepicker/daterangepicker.js");
    EHM.ImportCss("/resource/bootstrap/AdminLTE/plugins/daterangepicker/daterangepicker-
bs3.css");
}
//alert 窗口插件
EHM.ImportSweetalert = function () {
    EHM.ImportCss("/resource/Inspinia/css/plugins/sweetalert/sweetalert.css");
    EHM.ImportScript("/resource/Inspinia/js/plugins/sweetalert/sweetalert.min.js");
}
EHM.ImportBasePlugins = function(){
    EHM.ImportValidate();


    EHM.ImportSelect2();

    EHM.ImportICheck();

    EHM.ImportDatapicker();

    EHM.ImportDataRangePicker();
    //弹窗
    EHM.ImportScript("/resource/EHM/Toolkit/PopWin/InspiniaPopWin.js");
    //全屏
    EHM.ImportScript("/resource/jquery/jquery.fullscreenITIME.js");

    EHM.ImportScript("/resource/EHM/util/cookie/cookieITIME.js");
   //json 工具
    EHM.ImportScript("/resource/js/json2.js");

    EHM.ImportSweetalert();
    EHM.ImportBootstrapTable();
    EHM.ImportItimeCommon();
};

//自动引入相关组件
EHM.ImportBasePlugins();
```

```
/**
 * ---------- 需手工引入的插件 ------
 * @constructor
 */
//瀑布流布局
EHM.ImportMasonary = function () {
    EHM.ImportScript("/resource/Inspinia/js/plugins/masonary/masonry.pkgd.min.js");
};

//highchart 图表插件
EHM.ImportHighcharts = function () {
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-3d.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-more.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/exporting.js");
//EHM.Import("/resource/pluginsWithDhtmlx/highchart/js/offline-exporting.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/sankey.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/oldie.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/heatmap.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/tilemap.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/organization.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/no-data-to-display.js");
    EHM.ImportScript("/resource/pluginsWithDhtmlx/highchart/js/highcharts-zh_CN.js");
    EHM.ImportScript("/resource/plugi
...
...
...
```

问题 5 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/popper.min.js
实体：	popper.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

差异：

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

修复状态： 已修复

修复方式： 在 HTTP 响应报文的头部增加一个 X-XSS-Protection 字段，设置 XSS-Protection: 1; mode=block

测试请求和响应：

```
GET /web/resource/Inspinia/js/popper.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://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:49:27 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 19191
Vary: Accept-Encoding
ETag: W/"19191-1571017767939"
Date: Thu, 14 Nov 2019 08:27:25 GMT
Content-Type: application/javascript

/*
 Copyright (C) Federico Zivolo 2017
 Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).
 */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?
module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function()
{'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t)
{if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e)
{return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return
document.body;switch(e.nodeName){case'HTML':case'BODY':return
e.ownerDocument.body;case'#document':return e.body;}var
i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?
e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?
-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?
e.ownerDocument.documentElement:document.documentElement}function p(e){var
t=e.nodeName;return'BODY'!==t&&('HTML'===t||r(e.firstElementChild)===e)}function s(e){return
null===e.parentNode?e:s(e.parentNode)}function d(e,t){if(!e||!e.nodeType||!t||!t.nodeType)return
document.documentElement;var o=e.compareDocumentPosition(t)&Node.DOCUMENT_POSITION_FOLLOWING,i=o?
e:t,n=o?t:e,a=document.createRange();a.setStart(i,0),a.setEnd(n,0);var
l=a.commonAncestorContainer;if(e!==l&&t!==l||i.contains(n))return p(l)?l:r(l);var f=s(e);return
f.host?d(f.host,t):d(e,s(t).host)}function a(e){var t=1<arguments.length&&void 0!==arguments[1]?
arguments[1]:'top',o='top'===t?'scrollTop':'scrollLeft',i=e.nodeName;if('BODY'===i||'HTML'===i)
{var n=e.ownerDocument.documentElement,r=e.ownerDocument.scrollingElement||n;return r[o]}return
e[o]}function l(e,t){var o=2<arguments.length&&void
0!==arguments[2]&&arguments[2],i=a(t,'top'),n=a(t,'left'),r=o?-1:1;return
e.top+=i*r,e.bottom+=i*r,e.left+=n*r,e.right+=n*r,e}function f(e,t){var
o='x'===t?'Left':'Top',i='Left'==o?'Right':'Bottom';return
parseFloat(e['border'+o+'Width'],10)+parseFloat(e['border'+i+'Width'],10)}function m(e,t,o,i)
{return J(t['offset'+e],t['scroll'+e],o['client'+e],o['offset'+e],o['scroll'+e],ie()?
o['offset'+e]+i['margin'+('Height'===e?'Top':'Left')]+i['margin'+
('Height'===e?'Bottom':'Right')]:0)}function h(){var
e=document.body,t=document.documentElement,o=ie()&&getComputedStyle(t);return{height:m('Height',e
,t,o),width:m('Width',e,t,o)}}function c(e){return se({},e,
{right:e.left+e.width,bottom:e.top+e.height})}function g(e){var o=
{};if(ie())try{o=e.getBoundingClientRect();var
i=a(e,'top'),n=a(e,'left');o.top+=i,o.left+=n,o.bottom+=i,o.right+=n}catch(e){}else
o=e.getBoundingClientRect();var r={left:o.left,top:o.top,width:o.right-o.left,height:o.bottom-
o.top},p='HTML'===e.nodeName?h():{},s=p.width||e.clientWidth||r.right-
r.left,d=p.height||e.clientHeight||r.bottom-r.top,l=e.offsetWidth-s,m=e.offsetHeight-d;if(l||m)
{var g=t(e);l-=f(g,'x'),m-=f(g,'y'),r.width-=l,r.height-=m}return c(r)}function u(e,o){var
i=ie(),r='HTML'===o.nodeName,p=g(e),s=g(o),d=n(e),a=t(o),f=parseFloat(a.borderTopWidth,10),m=pars
eFloat(a.borderLeftWidth,10),h=c({top:p.top-s.top-f,left:p.left-s.left-
m,width:p.width,height:p.height});if(h.marginTop=0,h.marginLeft=0,!i&&r){var
u=parseFloat(a.marginTop,10),b=parseFloat(a.marginLeft,10);h.top-=f-u,h.bottom-=f-u,h.left-=m-
b,h.right-=m-b,h.marginTop=u,h.marginLeft=b}return(i?o.contains(d):o===d&&'BODY'!==d.nodeName)&&
(h=l(h,o)),h}function b(e){var
t=e.ownerDocument.documentElement,o=u(e,t),i=J(t.clientWidth,window.innerWidth||0),n=J(t.clientHe
ight,window.innerHeight||0),r=a(t),p=a(t,'left'),s={top:r-o.top+o.marginTop,left:p-
o.left+o.marginLeft,width:i,height:n};return c(s)}function w(e){var
i=e.nodeName;return'BODY'===i||'HTML'===i?!1:'fixed'===t(e,'position')||w(o(e))}function
y(e,t,i,r){var p={top:0,left:0},s=d(e,t);if('viewport'===r)p=b(s);else{var a;'scrollParent'===r?
(a=n(o(t)),'BODY'===a.nodeName&&(a=e.ownerDocument.documentElement)):'window'===r?
a=e.ownerDocument.documentElement:a=r;var l=u(a,s);if('HTML'===a.nodeName&&!w(s)){var
f=h(),m=f.height,c=f.width;p.top+=l.top-l.marginTop,p.bottom=m+l.top,p.left+=l.left-
l.marginLeft,p.right=c+l.left}else p=l}return p.left+=i,p.top+=i,p.right-=i,p.bottom-
=i,p}function E(e){var t=e.width,o=e.height;return t*o}function v(e,t,o,i,n){var r=5<
...
...
...
```

低 检测到隐藏目录 1 TOC

问题 1 / 1 TOC

检测到隐藏目录

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/
实体：	web/ (Page)
风险：	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

差异： **路径** 从以下位置进行控制：
`/web/resource/EHM/itime.js;jsessionid=7C15879B0ED11B9A08F98F109DD4C897` 至：`/web/`

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。
修复状态： 已修复
修复方式： 对禁止的资源发布“404 - Not Found”响应状态代码
测试请求和响应：

```
GET /web/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Transfer-Encoding: chunked
Content-Length: 8332
Vary: Accept-Encoding
Date: Thu, 14 Nov 2019 08:29:56 GMT
Content-Type: text/html;charset=UTF-8



<!Doctype html>
<html>
<head>



<script>
  Ext_BLANK_IMAGE_URL = "";
</script>

    <title></title>
    <script type="text/javascript" src="/web/resource/EHM/itime.js"></script> <meta
    name="viewport" content="width=device-width, initial-scale=0.9">
<script>
    EHM.ImportToastr();
</script>
```

```
</head>


<script type="text/javascript">

    //EHM.Cache["LOGIN_SAVE_PASS"] = false;

    function failAction(msg) {
        if (msg == "用户密码过期，请重新设置密码")
          window.open('staff/initChangePwd.do', 'popUpWin',
'scrollbars=0,toolbar=0,status=1,width=543,height=354,left=300,
top=200,screenX=200,screenY=200');
    }

    function IsPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone",
          "SymbianOS", "Windows Phone",
          "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
          if (userAgentInfo.indexOf(Agents[v]) > 0) {
          flag = false;
          break;
          }
        }
        return flag;
    }

    $(function () {
        var authMsg = "";

        if(null!=authMsg && ""!=authMsg){
          toastr["error"](authMsg);
        }else{
          $.post(EHM.rootPath+"/sysmenu/licenseCheck.sp",function(data){
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-full-width",
          "onclick": null,
          "showDuration": "400",
          "hideDuration": "1000",
          "timeOut": "10000",
          "extendedTimeOut": "1000",
          "showEasing": "swing",
          "hideEasing": "linear",
          "showMethod": "fadeIn",
          "hideMethod": "fadeOut"
          };
          if(data["flag"]==1){

          toastr["warning"](data["authMsg"]);
          }else if(data["flag"]==0){
          toastr["error"](data["authMsg"]);
          }

          },"json");
        }

        if(!IsPC()){
          $("#showDiv").attr("style","width:500px;margin-top:25%")
        }
        var url="/web/logomanager/getLoginInfo.do";
        $.post(url,function(data){
          data=JSON.parse(data);
          var src1="resource/images/"+data.LOGIN_LOGO;
          var src2="resource/images/"+data.LOGIN_QRCODE;
          $("#logoimg").attr("src",src1);
          $("#qrimg").attr("src",src2);
        });

        $("#loginForm").submit(function (e) {
          updateCookie();
        });
```

```
        $("#loginBt").on("click",function(){
          if($("#savePassImg").is(':checked'))
          {
          cookie.set("LOGIN_SAVE_PASS",true) ;
          }else{
          cookie.set("LOGIN_SAVE_PASS",false) ;
          }
          var isUnionYW = 0;
          var yw_url = 'null';

          if(isUnionYW==1){
          var userNameValue = $("#j_username").val().trim();
          var passWordValue = $("#j_password").val().trim();
          yw_url = yw_url+"?j_username="+userNameValue+"&j_password="+passWordValue;
          $("#iframeVar").load(function(){
          $("#loginForm").submit();
          });
          $('#iframeVar').attr('src', yw_url);
          }else{
          $("#loginForm").submit();
          }


          //
        });

        var jsonStr = '';
        if (jsonStr != null && jsonStr != "") {
          var jsonObj = JSON.parse(jsonStr);
          if (jsonObj && jsonObj != undefined) {
          if (jsonObj.success == "false") {
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-center",
          "onclick": null,
          "showDuration": "400",
          "hideDuration": "1000",
          "timeOut": "3000",
          "extendedTimeOut": "1000",

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

低 在未加密连接中发现信用卡号模式 (Visa) TOC

问题 1 / 1 TOC

在未加密连接中发现信用卡号模式 (Visa)

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/resource/bootstrap/fontIcon/iconFont/iconfont.js
实体：	iconfont.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的信用卡号

差异：

推理： 响应包含完整的 Visa 信用卡号。
修复状态： 已修复
修复方式： 除去 Web 站点中的信用卡号
测试请求和响应：

```
GET /web/resource/bootstrap/fontIcon/iconFont/iconfont.js HTTP/1.1 User-Agent:
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Referer:
http://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:50:24 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 697199
Vary: Accept-Encoding
ETag: W/"697199-1571017824135"
Date: Thu, 14 Nov 2019 08:27:59 GMT
Content-Type: application/javascript

!function(p){var c,h='<svg><symbol id="icon-yingpan" viewBox="0 0 1024 1024"><path d="M719.872
153.6q34.816 0 53.248 9.728t31.744 37.376q5.12 11.264 16.384 34.816t25.6 53.248 29.696 62.976
29.184 62.976 24.576 52.736 14.848 33.28q5.12 11.264 8.704 16.896t6.144 12.288 3.584 15.872 1.024
25.6q0 12.288-0.512 37.888t-0.512 54.272l0 57.344 0 39.936q0 28.672-16.896 48.64t-48.64 19.968l-
786.432 0q-29.696 0-45.056-18.944t-16.384-48.64l0-35.84q0-23.552 0.512-50.176t0.512-53.248l0-
43.008q0-17.408 0.512-27.648t2.56-17.92 4.608-15.872 7.68-20.48q3.072-8.192 13.312-31.232t24.576-
52.736 31.232-63.488 31.744-64 27.136-53.76l16.384-33.792q13.312-26.624 32.768-35.84t46.08-
9.216l430.08 0zM897.024 589.824q0-30.72-28.672-30.72l-724.992 1.024q-17.408 0-26.624 9.728t-9.216
25.088l0 145.408q0 12.288 6.656 20.48t20.992 8.192l729.088 1.024q20.48 0 26.624-9.728t6.144-
24.064l0-146.432zM293.888 206.848q-14.336 0-24.064 9.728t-9.728 24.064 9.728 24.064 24.064 9.728
23.552-9.728 9.216-24.064-9.216-24.064-23.552-9.728zM215.04 391.168q-14.336 0-24.064 9.728t-9.728
24.064 9.728 24.064 24.064 9.728 24.064-9.728 9.728-24.064-9.728-24.064-24.064-9.728zM686.08
240.64q0 14.336 9.216 24.064t23.552 9.728 24.064-9.728 9.728-24.064-9.728-24.064-24.064-9.728-
23.552 9.728-9.216 24.064zM763.904 424.96q0 14.336 9.728 24.064t24.064 9.728 23.552-9.728 9.216-
24.064-9.216-24.064-23.552-9.728-24.064 9.728-9.728 24.064zM233.472 740.352l-30.72 0 0-145.408
30.72 0 0 145.408zM326.656 740.352l-30.72 0 0-145.408 30.72 0 0 145.408zM420.864 740.352l-30.72 0
0-145.408 30.72 0 0 145.408zM514.048 740.352l-30.72 0 0-145.408 30.72 0 0 145.408zM610.304
740.352l-30.72 0 0-145.408 30.72 0 0 145.408zM705.536 740.352l-30.72 0 0-145.408 30.72 0 0
145.408zM795.648 740.352l-30.72 0 0-145.408 30.72 0 0 145.408z" ></path></symbol><symbol id="icon-
bangzhu" viewBox="0 0 1000 1000"><path d="M895.8893 317.4907c-22.011-52.0407-53.5179-98.774-93.6463-
138.9018-40.1274-40.1268-86.8627-71.6334-138.9055-93.6435-53.8907-22.7925-
111.1282-34.3487-170.1216-34.3487-58.9934 0-116.231 11.5562-170.1216 34.3487-52.0438 22.0101-
98.7791 53.5167-138.9065 93.6435-40.1284 40.1268-71.6354 86.8601-93.6463 138.9018-22.7915
53.8885-34.3481 111.1227-34.3481 170.1117 0 58.99 11.5566 116.2232 34.3481 170.1127 22.011
52.0417 53.5179 98.776 93.6463 138.9038 40.1284 40.1278 86.8637 71.6354 138.9065 93.6465 53.8917
22.7935 1
...
...
...
75-8.207812500000001-7.9875-17.4965625-19.310624999999998-20.510625-23.083125-7.732499999999999
4.498125-12.3553125 6.5625-12.3553125 6.5625-64.141875-37.996875-110.240625000000001-81.3225-
```

```
143.13093750000002-125.98124999999999h-
56.5725V519.8000000000001h49.089375000000004a388.24312499999996 388.24312499999996 0 0 1-
12.350624999999999-19.113750000000003h-36.729375v-10.5075H555.21875a385.2909375 385.2909375 0 0
1-24.1725-51.335625c-7.305-0.375-15.600000000000001 2.7075-25.185000000000002 10.2909375-2.990625
2.3765625000000004-7.1184375 2.9090625-10.815 3.7303125-19.0275 4.16625-25.2375
13.646249999999998-17.049375 32.9371875 6.834375 16.0753125 10.69875 33.417187500000004
16.655624999999997 52.7090625-39.508125-4.6846875-57.868125-48.163125-100.905-43.08121.7584375
48.355312500000004c-26.2903125-7.070625-48.523125-19.713749999999997-68.67375-16.96875-
36.389062499999994 4.9303125-9.1875 37.051874999999995-16.483125 58.92-9.518437500000001-5.64375-
17.00625-11.3709375-25.4503125-14.683125-6.4359375000000005-2.5003124999999997-16.621875-5.29875-
20.754375000000003-2.184375-18.956249999999997 14.34375-36.609375 30.4715625-54.058125 46.685625-
2.48625 2.29875-3.4125 10.497187499999999-1.44 12.676875 11.3521875 12.5184375 22.6125 32.2265625
36.12 34.185 27.489375 3.975 56.4675-1.1325 84.6-4.483125 3.2690625-0.37875000000000003
5.7215625-13.108125 7.3875-20.390625 2.9615625-13.003124999999999 3.705-26.6634375
8.040000000000001-39.114375 2.2218750000000003-6.4078125 10.190624999999999-10.8046875
15.5615625-16.1090625 2.6062499999999997 6.8062499999999995 7.555312499999999 13.69875 7.3246875
20.418750000000003-0.4171875 12.2690625-3.975 24.412499999999998-6.08625 36.644062500000004-
3.058125 17.71125 0.6140625000000001 26.71125 22.2234375 30.0525 50.765625 7.847812500000001
101.5059375 17.683124999999997 151.095 31.040625 113.9615625 30.706874999999997 220.276875
80.731875 324.4125 135.3515625 30.307500000000005 15.887812499999999 60.6187
...
...
...
```

低 自动填写未对密码字段禁用的 HTML 属性 2 TOC

问题 1 / 2 TOC

自动填写未对密码字段禁用的 HTML 属性

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/desktop
实体：	desktop (Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

差异：

推理： AppScan 发现密码字段没有强制禁用自动填写功能。
修复状态： 已修复
修复方式： 将“autocomplete”属性正确设置为“off”
测试请求和响应：

```
GET /web/desktop 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: 124.254.61.27:9090
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip
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
Transfer-Encoding: chunked
Content-Length: 8495
Vary: Accept-Encoding
Set-Cookie: JSESSIONID=FCE4645D4C54811E4B64C2326C4CFEED; Path=/web; HttpOnly
Date: Thu, 14 Nov 2019 08:25:46 GMT
Content-Type: text/html;charset=UTF-8



<!Doctype html>
<html>
<head>



<script>
  Ext_BLANK_IMAGE_URL = "";
</script>

    <title></title>
    <script type="text/javascript"
src="/web/resource/EHM/itime.js;jsessionid=FCE4645D4C54811E4B64C2326C4CFEED"></script>
    <meta name="viewport" content="width=device-width, initial-
scale=0.9"> <script>
    EHM.ImportToastr();
</script>
</head>



<script type="text/javascript">

    //EHM.Cache["LOGIN_SAVE_PASS"] = false;

    function failAction(msg) {
        if (msg == "用户密码过期，请重新设置密码")
          window.open('staff/initChangePwd.do', 'popUpWin',
'scrollbars=0,toolbar=0,status=1,width=543,height=354,left=300,
top=200,screenX=200,screenY=200');
    }

    function IsPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone",
          "SymbianOS", "Windows Phone",
          "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
          if (userAgentInfo.indexOf(Agents[v]) > 0) {
          flag = false;
          break;
          }
        }
        return flag;
    }

    $(function () {
        var authMsg = "";

        if(null!=authMsg && ""!=authMsg){
          toastr["error"](authMsg);
        }else{
          $.post(EHM.rootPath+"/sysmenu/licenseCheck.sp",function(data){
          toastr.options = {
          "closeButton": true,
          "debug": false,
          "progressBar": true,
          "preventDuplicates": false,
          "positionClass": "toast-top-full-width",
          "onclick": null,
          "showDuration": "400",
          "hideDuration": "1000",
          "timeOut": "10000",
          "extendedTimeOut": "1000",
          "showEasing": "swing",
          "hideEasing": "linear",
```

```
          "showMethod": "fadeIn",
          "hideMethod": "fadeOut"
          };
          if(data["flag"]==1){

          toastr["warning"](data["authMsg"]);
          }else if(data["flag"]==0){
          toastr["error"](data["authMsg"]);
          }

          },"json");
        }

        if(!IsPC()){
          $("#showDiv").attr("style","width:500px;margin-top:25%")
        }
        var url="/web/logomanager/getLoginInfo.do;jsessionid=FCE4645D4C54811E4B64C2326C4CFEED";
        $.post(url,function(data){
          data=JSON.parse(data);
          var src1="resource/images/"+data.LOGIN_LOGO;
          var src2="resource/images/"+data.LOGIN_QRCODE;
          $("#logoimg").attr("src",src1);
          $("#qrimg").attr("src",src2);
        });

        $("#loginForm").submit(function (e) {
          updateCookie();
        });

        $("#loginBt").on("click",function(){
          if($("#savePassImg").is(':checked'))
          {
          cookie.set("LOGIN_SAVE_PASS",true) ;
          }else{
          cookie.set("LOGIN_SAVE_PASS",false) ;
          }
          var isUnionYW = 0;
          var yw_url = 'null';

          if(isUnionYW==1){
          var userNameValue = $("#j_username").val().trim();
          var passWordValue = $("#j_password").val().trim();
          yw_url = yw_url+"?j_username="+userNameValue+"&j_password="+passWordValue;
          $("#iframeVar").load(function(){
          $("#loginForm").submit();
          });
          $('#iframeVar').attr('src', yw_url);
          }else{
          $("#loginForm").submit();

...
...
...

          <div class="form-group">
          <input type="text" class="form-control" id="j_username" name="j_username"
placeholder="用户名" required="">
          </div>
          <div class="form-group">
          <input type="password" class="form-control" id="j_password" name="j_password"
placeholder="密码" required="">
          </div>
          <div class="form-group pull-left">
          <input type="hidden" name="logintype" value="default"/>
          <input id="savePassImg" type="checkbox" class="i-checks">  <label
style="font-size: 14px;font-weight: normal" for="savePassImg">记住用户名&密码</label>
...
...
...
```

自动填写未对密码字段禁用的 HTML 属性

严重性：	低
CVSS 分数：	5.0
URL：	http://124.254.61.27:9090/web/staff/initChangePwd.do
实体：	initChangePwd.do (Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

差异：

推理： AppScan 发现密码字段没有强制禁用自动填写功能。
修复状态： 已修复
修复方式： 将“autocomplete”属性正确设置为“off”
测试请求和响应：

```
GET /web/staff/initChangePwd.do HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: Keep-Alive
Host: 124.254.61.27:9090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 4030
Date: Thu, 14 Nov 2019 08:28:31 GMT
Content-Type: text/html;charset=GBK

<!--author lixin/web/staff/first_change_password.jsp -->



<script>
  Ext_BLANK_IMAGE_URL = "";
</script>
<html>
<head>
    <title>密码修改</title>
 <script type="text/javascript" src="/web/resource/EHM/Base.js"></script> <script
    type="text/javascript">
          ChangeSkinAPP.Register(function() {
          ChangeSkin.Import("style.css")
        });
        ChangeSkinAPP.init();
    </script>
    <style type="text/css">
        <!--
        .STYLE1 {
          color: #FF0000
        }

        -->
    </style>
</head>

<body>


<script type="text/javascript">
    function validate() {
        var loginID = $("loginID").value;
        if (loginID.trim() == "") {
```

```
          alert("请输入工号!");
          $("loginID").focus();
          return false;
        }
        var oldPwd = $("oldPwd").value;
        if (oldPwd == "") {
          alert("输入的旧密码不能为空!");
          return false;
        }
        var newPwd = $("newPwd").value;
        if (newPwd == "") {
          alert("输入的新密码不能为空!");
          return false;
        }
        var confirmPwd = $("confirmPwd").value;
        if (confirmPwd == "") {
          alert("输入的确认密码不能为空!");
          return false;
        }
        if (oldPwd == newPwd) {
          alert("新密码不能跟原密码相同，请从新输入！");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }
        var str = /^[A-Za-z0-9]+$/;
        if (newPwd.length < 8 || confirmPwd.length < 8) {
          alert("密码长度必须大于 8 位！");
          return false;
        }
        if (!str.test(newPwd))
        {
          alert("口令只允许输入数字或字母!!");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }
        var str1 = /([a-zA-Z][0-9]|[0-9][a-zA-Z])+/;
        if (!str1.test(newPwd))
        {
          alert("口令请输入数字和字母的组合!!");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }
        if (newPwd != confirmPwd) {
          alert("输入的新密码不一致!");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }

        disableAllBts();
        return true;
    }
</script>
<br>
<form name="changePwdForm" method="post" action="/web/staff/firstChangePwd.do"
onsubmit="return validate()">
    <table border=0 cellpadding=1 cellspacing=1 class="form_table" width="95%"
        align="center"> <tr>
          <th width="30%" scope="row">工号
          </th>
          <td width="70%"><input type="text" name="loginID" maxlength="24"
          value=""> </td>
        </tr>
        <tr>
          <th scope="row"><font color="#FF0000">*</font>原口令
          </th>
          <td><input type="password" name="oldPwd" maxlength="24" value="">
          </td>
        </tr>
        <tr>
          <th scope="row"><font color="#FF0000">*</font>新口令
```

```
          </th>
          <td><input type="password" name="newPwd" maxlength="24" value="">
          </td>
        </tr>
        <tr>
          <th scope="row"><font color="#FF0000">*</font>确认口令
          </th>
          <td><input type="password" name="confirmPwd" maxlength="24"
          value=""> </td>
        </tr>


    </table>

    <p align="center">
        <input type="submit" value="确  定" class="btn4">
        <input type="button" value="取  消" class="btn4" onClick="window.close();"/>
    </p>

</form>
<br><br>
<center><font size="2" color="red">提示：为了保证密码的安全性更高，密码用 字母+数字 组合</font></center>

<script language="javascript">

</script>
</body>
</html>
```

问题 1 / 1

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://124.254.61.27:9090/web/staff/initChangePwd.do
实体：	author lixin/web/staff/first_change_password.jsp (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。
修复状态： 已修复
修复方式： 删除注释信息
测试请求和响应：

```
GET /web/staff/initChangePwd.do HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: Keep-Alive
Host: 124.254.61.27:9090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 4030
Date: Thu, 14 Nov 2019 08:28:31 GMT
Content-Type: text/html;charset=GBK

<!--author lixin/web/staff/first_change_password.jsp -->




<script>
  Ext_BLANK_IMAGE_URL = "";
</script>
<html>
<head>
    <title>密码修改</title>
 <script type="text/javascript" src="/web/resource/EHM/Base.js"></script> <script
    type="text/javascript">
          ChangeSkinAPP.Register(function() {
          ChangeSkin.Import("style.css")
        });
        ChangeSkinAPP.init();
```

```
    </script>
    <style type="text/css">
        <!--
        .STYLE1 {
          color: #FF0000
        }

        -->
    </style>
</head>

<body>


<script type="text/javascript">
    function validate() {
        var loginID = $("loginID").value;
        if (loginID.trim() == "") {
          alert("请输入工号!");
          $("loginID").focus();
          return false;
        }
        var oldPwd = $("oldPwd").value;
        if (oldPwd == "") {
          alert("输入的旧密码不能为空!");
          return false;
        }
        var newPwd = $("newPwd").value;
        if (newPwd == "") {
          alert("输入的新密码不能为空!");
          return false;
        }
        var confirmPwd = $("confirmPwd").value;
        if (confirmPwd == "") {
          alert("输入的确认密码不能为空!");
          return false;
        }
        if (oldPwd == newPwd) {
          alert("新密码不能跟原密码相同，请从新输入！");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }
        var str = /^[A-Za-z0-9]+$/;
        if (newPwd.length < 8 || confirmPwd.length < 8) {
          alert("密码长度必须大于 8 位！");
          return false;
        }
        if (!str.test(newPwd))
        {
          alert("口令只允许输入数字或字母!!");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }
        var str1 = /([a-zA-Z][0-9]|[0-9][a-zA-Z])+/;
        if (!str1.test(newPwd))
        {
          alert("口令请输入数字和字母的组合!!");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }
        if (newPwd != confirmPwd) {
          alert("输入的新密码不一致!");
          $("newPwd").value = "";
          $("confirmPwd").value = "";
          $("newPwd").focus();
          return false;
        }

        disableAllBts();
        return true;
    }
</script>
```

```
<br>
<form name="changePwdForm" method="post" action="/web/staff/firstChangePwd.do"
onsubmit="return validate()">
    <table border=0 cellpadding=1 cellspacing=1 class="form_table" width="95%"
        align="center"> <tr>
          <th width="30%" scope="row">工号
          </th>
          <td width="70%"><input type="text" name="loginID" maxlength="24"
          value=""> </td>
        </tr>
        <tr>
          <th scope="row"><font color="#FF0000">*</font>原口令
          </th>
          <td><input type="password" name="oldPwd" maxlength="24" value="">
          </td>
        </tr>
        <tr>
          <th scope="row"><font color="#FF0000">*</font>新口令
          </th>
          <td><input type="password" name="newPwd" maxlength="24" value="">
          </td>
        </tr>
        <tr>
          <th scope="row"><font color="#FF0000">*</font>确认口令
          </th>
          <td><input type="password" name="confirmPwd" maxlength="24"
          value=""> </td>
        </tr>


    </table>

    <p align="center">
        <input type="submit" value="确  定" class="btn4">
        <input type="button" value="取  消" class="btn4" onClick="window.close();"/>
    </p>

</form>
<br><br>
<center><font size="2" color="red">提示：为了保证密码的安全性更高，密码用 字母+数字 组合</font></center>

<script language="javascript">

</script>
</body>
</html>
```

参 发现电子邮件地址模式 4 TOC

问题 1 / 4 TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js
实体：	jquery.metisMenu.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。
修复状态： 已修复
修复方式： 根据扫描建议删除注释中出现 email 地址信息
测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/metisMenu/jquery.metisMenu.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko Referer: http://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:59 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 13431
Vary: Accept-Encoding
ETag: W/"13431-1571017739982"
Date: Thu, 14 Nov 2019 08:27:25 GMT
Content-Type: application/javascript

/*!
 * metismenu - v2.7.7
 * A jQuery menu plugin
 * https://github.com/onokumus/metismenu#readme

 * Made by Osman Nuri Okumus <onokumus@gmail.com> (https://github.com/onokumus)
 * Under MIT License
 */
(function (global, factory) {
    typeof exports === 'object' && typeof module !== 'undefined' ?
module.exports = factory(require('jquery')) :
        typeof define === 'function' && define.amd ? define(['jquery'], factory) :
          (global.metisMenu = factory(global.jQuery));
}(this, (function ($) { 'use strict';

    $ = $ && $.hasOwnProperty('default') ? $['default'] : $;

    function _defineProperty(obj, key, value) {
        if (key in obj) {
          Object.defineProperty(obj, key, {
          value: value,
          enumerable: true,
          configurable: true,
          writable: true
          });
        } else { obj[key]
          = value;
        }

        return obj;
    }
```

*

```
    function _objectSpread(target) {
        for (var i = 1; i < arguments.length; i++) {
          var source = arguments[i] != null ? arguments[i] : {};
          var ownKeys = Object.keys(source);

          if (typeof Object.getOwnPropertySymbols === 'function') {
          ownKeys = ownKeys.concat(Object.getOwnPropertySymbols(source).filter(function (sym)
          { return Object.getOwnPropertyDescriptor(source, sym).enumerable; }));

          }

          ownKeys.forEach(function (key) {
          _defineProperty(target, key, source[key]);
          });
        }

        return target;
    }

    var Util = function ($$$1) {
        // eslint-disable-line no-shadow
        var TRANSITION_END = 'transitionend';
        var Util = {
          // eslint-disable-line no-shadow
          TRANSITION_END: 'mmTransitionEnd',
          triggerTransitionEnd: function triggerTransitionEnd(element) {
          $$$1(element).trigger(TRANSITION_END); },

          supportsTransitionEnd: function supportsTransitionEnd() { return
          Boolean(TRANSITION_END);
          }
        };

        function getSpecialTransitionEndEvent() {
          return {
          bindType: TRANSITION_END,
          delegateType: TRANSITION_END,
          handle: function handle(event) {
          if ($$$1(event.target).is(this)) {
          return event.handleObj.handler.apply(this, arguments); // eslint-disable-line
prefer-rest-params
          }

          return undefined;
          }
          };
        }

        function transitionEndEmulator(duration) {
          var _this = this;

          var called = false;
          $$$1(this).one(Util.TRANSITION_END, function () {
          called = true;
          });
          setTimeout(function () {
          if (!called) {
          Util.triggerTransitionEnd(_this);
          }
          }, duration);
          return this;
        }

        function setTransitionEndSupport() {
          $$$1.fn.mmEmulateTransitionEnd = transitionEndEmulator; // eslint-disable-line
no-param-reassign
          // eslint-disable-next-line no-param-reassign

          $$$1.event.special[Util.TRANSITION_END] = getSpecialTransitionEndEvent();
        }

        setTransitionEndSupport();
        return Util;
    }($);

    var MetisMenu = function ($$$1) {
        // eslint-disable-line no-shadow
```

```
        var NAME = 'metisMenu';
        var DATA_KEY = 'metisMenu';
        var EVENT_KEY = "." + DATA_KEY;
        var DATA_API_KEY = '.data-api';
        var JQUERY_NO_CONFLICT = $$$1.fn[NAME];
        var TRANSITION_DURATION = 350;
        var Default = {
          toggle: true,
          preventDefault: true,
          activeClass: 'active',
          collapseClass: 'collapse',
          collapseInClass: 'in',
          collapsingClass: 'collapsing',
          triggerElement: 'a',
          parentTrigger: 'li',
          subMenu: 'ul'
        };
        var Event = {
          SHOW: "show" + EVENT_KEY,
          SHOWN: "shown" + EVENT_KEY,
          HIDE
...
...
...
```

问题 2 / 4

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-zh-CN.min.js
实体：	bootstrap-table-zh-CN.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。
修复状态： 已修复
修复方式： 根据扫描建议删除注释中出现 email 地址信息
测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-zh-CN.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://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:42 GMT
Accept-Ranges: bytes
Content-Length: 9617
```

```
ETag: W/"9617-1571017722396"
Date: Thu, 14 Nov 2019 08:28:16 GMT
Content-Type: application/javascript

/**
  * bootstrap-table - An extended table to integration with some of the most widely used
CSS frameworks. (Supports Bootstrap, Semantic UI, Bulma, Material Design, Foundation)

  * @version v1.15.4
  * @homepage https://bootstrap-table.com
  * @author wenzhixin <wenzhixin2010@gmail.com> (http://wenzhixin.net.cn/)
  * @license MIT
  */

(function(a,b){"object"==typeof exports&&"undefined"!=typeof module?
b(require("jquery")):"function"==typeof define&&define.amd?define(["jquery"],b):
(a=a||self,b(a.jQuery))})(this,function(a){'use strict';var c=Math.min;function b(a,b){return b=
{exports:{}},a(b,b.exports),b.exports}a=a&&a.hasOwnProperty("default")?a["default"]:a;var
d,e,g,h="undefined"==typeof globalThis?"undefined"==typeof window?"undefined"==typeof
global?"undefined"==typeof self?{}:self:global:window:globalThis,i="object",j=function(a){return
a&&a.Math==Math&&a},k=j(typeof globalThis==i&&globalThis)||j(typeof window==i&&window)||j(typeof
self==i&&self)||j(typeof h==i&&h)||Function("return this")(),l=function(a)
{try{return!!a()}catch(a){return!0}},m=!l(function(){return 7!=Object.defineProperty({},"a",
{get:function(){return 7}}).a}),n=
{}.propertyIsEnumerable,o=Object.getOwnPropertyDescriptor,p=o&&!n.call({1:2},1),q=p?function(a)
{var b=o(this,a);return!!b&&b.enumerable}:n,f={f:q},r=function(a,b){return{enumerable:!
(1&a),configurable:!(2&a),writable:!(4&a),value:b}},s={}.toString,t=function(a){return
s.call(a).slice(8,-1)},u="".split,v=l(function(){return!Object("z").propertyIsEnumerable(0)})?
function(a){return"String"==t(a)?u.call(a,""):Object(a)}:Object,w=function(a){if(a==null)throw
TypeError("Can't call method on "+a);return a},x=function(a){return v(w(a))},y=function(a)
{return"object"==typeof a?null!==a:"function"==typeof a},z=function(a,b){if(!y(a))return a;var
c,d;if(b&&"function"==typeof(c=a.toString)&&!y(d=c.call(a)))return
d;if("function"==typeof(c=a.valueOf)&&!y(d=c.call(a)))return
d;if(!b&&"function"==typeof(c=a.toString)&&!y(d=c.call(a)))return d;throw TypeError("Can't
convert object to primitive value")},A={}.hasOwnProperty,B=function(a,b){return
A.call(a,b)},C=k.document,D=y(C)&&y(C.createElement),E=function(a){return D?C.createElement(a):
{}},F=!m&&!l(function(){return 7!=Object.defineProperty(E("div"),"a",{get:function(){return
7}}).a}),G=Object.getOwnPropertyDescriptor,H=m?G:function(a,b){if(a=x(a),b=z(b,!0),F)try{return
G(a,b)}catch(a){}return B(a,b)?r(!f.f.call(a,b),a[b]):void 0},I={f:H},J=function(a)
{if(!y(a))throw TypeError(a+" is not an object");return a},K=Object.defineProperty,L=m?
K:function(a,b,c){if(J(a),b=z(b,!0),J(c),F)try{return K(a,b,c)}catch(a){}if("get"in c||"set"in
c)throw TypeError("Accessors not supported");return"value"in c&&(a[b]=c.value),a},M={f:L},N=m?
function(a,b,c){return M.f(a,b,r(1,c))}:function(a,b,c){return a[b]=c,a},P=function(a,b)
{try{N(k,a,b)}catch(c){k[a]=b}return b},Q=b(function(a){var b=k["__core-js_shared__"]||P("__core-
js_shared__",{});(a.exports=function(a,c){return b[a]||(b[a]=c===void 0?{}:c)})("versions",
[]).push({version:"3.1.3",mode:"global",copyright:"\xA9 2019 Denis Pushkarev
(zloirock.ru)"})}),R=Q("native-function-to-
string",Function.toString),S=k.WeakMap,T="function"==typeof S&&/native
code/.test(R.call(S)),U=0,O=Math.random(),V=function(a){return"Symbol("+((a===void
0?"":a)+"")+")_"+(++U+O).toString(36)},W=Q("keys"),X=function(a){return W[a]||(W[a]=V(a))},Y=
{},Z=k.WeakMap,_=function(a){return g(a)?e(a):d(a,{})};if(T){var aa=new
Z,ba=aa.get,ca=aa.has,da=aa.set;d=function(a,b){return da.call(aa,a,b),b},e=function(a){return
ba.call(aa,a)||{}},g=function(a){return ca.call(aa,a)}}else{var
ea=X("state");Y[ea]=!0,d=function(a,b){return N(a,ea,b),b},e=function(a){return B(a,ea)?a[ea]:
{}},g=function(a){return B(a,ea)}}var fa={set:d,get:e,has:g,enforce:_,getterFor:function(a)
{return function(b){var c;if(!y(b)||(c=e(b)).type!==a)throw TypeError("Incompatible receiver,
"+a+" required");return c}}},ga=b(function(a){var b=fa.get,c=fa.enforce,d=
(R+"").split("toString");Q("inspectSource",function(a){return R.call(a)}),
(a.exports=function(a,b,e,f){var
g=!!f&&!!f.unsafe,h=!!f&&!!f.enumerable,i=!!f&&!!f.noTargetGet;return("function"==typeof e&&
("string"==typeof b&&!B(e,"name")&&N(e,"name",b),c(e).source=d.join("string"==typeof b?
b:"")),a===k)?void(h?a[b]=e:P(b,e)):void(g?!i&&a[b]&&(h=!0):delete a[b],h?a[b]=e:N
...
...
...
```

*

问题 3 / 4

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-control.min.js
实体：	bootstrap-table-filter-control.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。
修复状态： 已修复
修复方式： 根据扫描建议删除注释中出现 email 地址信息
测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table-filter-control.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://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:42 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 34052
Vary: Accept-Encoding
ETag: W/"34052-1571017722340"
Date: Thu, 14 Nov 2019 08:27:59 GMT
Content-Type: application/javascript

/**
  * bootstrap-table - An extended table to integration with some of the most widely used
CSS frameworks. (Supports Bootstrap, Semantic UI, Bulma, Material Design, Foundation)

  * @version v1.15.4
  * @homepage https://bootstrap-table.com
  * @author wenzhixin <wenzhixin2010@gmail.com> (http://wenzhixin.net.cn/)
  * @license MIT
  */

(function(e,t){"object"==typeof exports&&"undefined"!=typeof module? t(require("jquery")):"function"==typeof
define&&define.amd?define(["jquery"],t): (e=e||self,t(e.jQuery))})(this,function(e){'use strict';var
h=Math.max,g=Math.min,C=Math.floor;function t(e,t){return t={exports: {}},e(t,t.exports),t.exports}function
o(e){return o="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof
e}:function(e){return e&&"function"==typeof
Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof e},o(e)}function l(e,t){if(! (e
instanceof t))throw new TypeError("Cannot call a class as a function")}function n(e,t){for(var
o,l=0;l<t.length;l++)o=t[l],o.enumerable=o.enumerable||!1,o.configurable=!0,"value"in o&&
(o.writable=!0),Object.defineProperty(e,o.key,o)}function r(e,t,o){return
t&&n(e.prototype,t),o&&n(e,o),e}function a(e,t){if("function"!=typeof t&&null!==t)throw new TypeError("Super
expression must either be null or a function");e.prototype=Object.create(t&&t.prototype,{constructor:
{value:e,writable:!0,configurable:!0}}),t&&s(e,t)}function i(e){return i=Object.setPrototypeOf?
Object.getPrototypeOf:function(e){return e.__proto__||Object.getPrototypeOf(e)},i(e)}function s(e,t){return
s=Object.setPrototypeOf||function(e,t){return e.__proto__=t,e},s(e,t)}function c(e) {if(void 0===e)throw new
ReferenceError("this hasn't been initialised - super() hasn't been called");return e}function d(e,t){return
t&&("object"==typeof t||"function"==typeof t)?
```

```
t:c(e)}function u(e,t){for(;!Object.prototype.hasOwnProperty.call(e,t)&&
(e=i(e),null!==e););return e}function p(e,t,o){return p="undefined"!=typeof Reflect&&Reflect.get?
Reflect.get:function(e,t,o){var l=u(e,t);if(l){var n=Object.getOwnPropertyDescriptor(l,t);return
n.get?n.get.call(o):n.value}},p(e,t,o||e)}e=e&&e.hasOwnProperty("default")?e["default"]:e;var
y,m,b,S="undefined"==typeof globalThis?"undefined"==typeof window?"undefined"==typeof
global?"undefined"==typeof self?{}:self:global:window:globalThis,T="object",O=function(e){return
e&&e.Math==Math&&e},v=O(typeof globalThis==T&&globalThis)||O(typeof window==T&&window)||O(typeof
self==T&&self)||O(typeof S==T&&S)||Function("return this")(),x=function(e)
{try{return!!e()}catch(e){return!0}},k=!x(function(){return 7!=Object.defineProperty({},"a",
{get:function(){return 7}}).a}),E=
{}.propertyIsEnumerable,P=Object.getOwnPropertyDescriptor,D=P&&!E.call({1:2},1),L=D?function(e)
{var t=P(this,e);return!!t&&t.enumerable}:E,f={f:L},I=function(e,t){return{enumerable:!
(1&e),configurable:!(2&e),writable:!(4&e),value:t}},A={}.toString,w=function(e){return
A.call(e).slice(8,-1)},j="".split,M=x(function(){return!Object("z").propertyIsEnumerable(0)})?
function(e){return"String"==w(e)?j.call(e,""):Object(e)}:Object,_=function(e){if(e==null)throw
TypeError("Can't call method on "+e);return e},N=function(e){return M(_(e))},H=function(e)
{return"object"==typeof e?null!==e:"function"==typeof e},F=function(e,t){if(!H(e))return e;var
o,l;if(t&&"function"==typeof(o=e.toString)&&!H(l=o.call(e)))return
l;if("function"==typeof(o=e.valueOf)&&!H(l=o.call(e)))return
l;if(!t&&"function"==typeof(o=e.toString)&&!H(l=o.call(e)))return l;throw TypeError("Can't
convert object to primitive value")},R={}.hasOwnProperty,B=function(e,t){return
R.call(e,t)},V=v.document,G=H(V)&&H(V.createElement),Y=function(e){return G?V.createElement(e):
{}},U=!k&&!x(function(){return 7!=Object.defineProperty(Y("div"),"a",{get:function(){return
7}}).a}),W=Object.getOwnPropertyDescriptor,K=k?W:function(e,t){if(e=N(e),t=F(t,!0),U)try{return
W(e,t)}catch(e){}return B(e,t)?I(!f.f.call(e,t),e[t]):void 0},z={f:K},Q=function(e)
{if(!H(e))throw TypeError(e+" is not an object");return e},J=Object.defineProperty,X=k?
J:function(e,t,o){if(Q(e),t=F(t,!0),Q(o),U)try{return J(e,t,o)}catch(e){}if("get"in o||"set"in
o)throw TypeError("Accessors not supported");return"value"in o&&(e[t]=o.value),e},Z={f:X},ee=k?
function(e,t,o
...
...
...
```

问题 4 / 4

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.min.js
实体：	bootstrap-table.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。
修复状态： 已修复
修复方式： 根据扫描建议删除注释中出现 email 地址信息
测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/bootstrap-table/bootstrap-table.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://124.254.61.27:9090/web/desktop Cookie:
JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9
```

```
HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:48:42 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 110693
Vary: Accept-Encoding
ETag: W/"110693-1571017722601"
Date: Thu, 14 Nov 2019 08:28:26 GMT
Content-Type: application/javascript

/**
  * bootstrap-table - An extended table to integration with some of the most widely used
CSS frameworks. (Supports Bootstrap, Semantic UI, Bulma, Material Design, Foundation)
*
  * @version v1.15.4
  * @homepage https://bootstrap-table.com
  * @author wenzhixin <wenzhixin2010@gmail.com> (http://wenzhixin.net.cn/)
  * @license MIT
  */

(function(e,t){"object"==typeof exports&&"undefined"!=typeof module?
module.exports=t(require("jquery")):"function"==typeof define&&define.amd?define(["jquery"],t):
(e=e||self,e.BootstrapTable=t(e.jQuery))})(this,function(t){'use strict';var
m=String.prototype,b=Math.max,y=Math.min,w=Math.floor,v=Math.ceil;function e(e,t){return t=
{exports:{}},e(t,t.exports),t.exports}function n(e){return n="function"==typeof
Symbol&&"symbol"==typeof Symbol.iterator?function(e){return typeof e}:function(e){return
e&&"function"==typeof Symbol&&e.constructor===Symbol&&e!==Symbol.prototype?"symbol":typeof
e},n(e)}function a(e,t){if(!(e instanceof t))throw new TypeError("Cannot call a class as a
function")}function i(e,t){for(var
o,n=0;n<t.length;n++)o=t[n],o.enumerable=o.enumerable||!1,o.configurable=!0,"value"in o&&
(o.writable=!0),Object.defineProperty(e,o.key,o)}function s(e,t,o){return
t&&i(e.prototype,t),o&&i(e,o),e}function l(e,t){return d(e)||u(e,t)||g()}function r(e){return
c(e)||p(e)||h()}function c(e){if(Array.isArray(e)){for(var
t=0,o=Array(e.length);t<e.length;t++)o[t]=e[t];return o}}function d(e){if(Array.isArray(e))return
e}function p(e){if(Symbol.iterator in Object(e)||"[object
Arguments]"===Object.prototype.toString.call(e))return Array.from(e)}function u(e,t){var o=
[],n=!0,a=!1,i=void 0;try{for(var s,l=e[Symbol.iterator]();!(n=(s=l.next()).done)&&
(o.push(s.value),!(t&&o.length===t));n=!0);}catch(e)
{a=!0,i=e}finally{try{n||null==l["return"]||l["return"]()}finally{if(a)throw i}}return o}function
h(){throw new TypeError("Invalid attempt to spread non-iterable instance")}function g(){throw new
TypeError("Invalid attempt to destructure non-iterable
instance")}t=t&&t.hasOwnProperty("default")?t["default"]:t;var S,x,k,T="undefined"==typeof
globalThis?"undefined"==typeof window?"undefined"==typeof global?"undefined"==typeof self?
{}:self:global:window:globalThis,P="object",o=function(e){return e&&e.Math==Math&&e},C=o(typeof
globalThis==P&&globalThis)||o(typeof window==P&&window)||o(typeof self==P&&self)||o(typeof
T==P&&T)||Function("return this")(),I=function(e){try{return!!e()}catch(e)
{return!0}},A=!I(function(){return 7!=Object.defineProperty({},"a",{get:function(){return
7}}).a}),E={}.propertyIsEnumerable,R=Object.getOwnPropertyDescriptor,_=R&&!E.call({1:2},1),N=_?
function(e){var t=R(this,e);return!!t&&t.enumerable}:E,f={f:N},F=function(e,t)
{return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}},D=
{}.toString,L=function(e){return D.call(e).slice(8,-1)},B="".split,V=I(function()
{return!Object("z").propertyIsEnumerable(0)})?function(e){return"String"==L(e)?
B.call(e,""):Object(e)}:Object,H=function(e){if(null==e)throw TypeError("Can't call method on
"+e);return e},M=function(e){return V(H(e))},U=function(e){return"object"==typeof e?
null!==e:"function"==typeof e},q=function(e,t){if(!U(e))return e;var
o,n;if(t&&"function"==typeof(o=e.toString)&&!U(n=o.call(e)))return
n;if("function"==typeof(o=e.valueOf)&&!U(n=o.call(e)))return
n;if(!t&&"function"==typeof(o=e.toString)&&!U(n=o.call(e)))return n;throw TypeError("Can't
convert object to primitive value")},z={}.hasOwnProperty,G=function(e,t){return
z.call(e,t)},W=C.document,Y=U(W)&&U(W.createElement),K=function(e){return Y?W.createElement(e):
{}},X=!A&&!I(function(){return 7!=Object.defineProperty(K("div"),"a",{get:function(){return
7}}).a}),Q=Object.getOwnPropertyDescriptor,J=A?Q:function(e,t){if(e=M(e),t=q(t,!0),X)try{return
Q(e,t)}catch(e){}return G(e,t)?F(!f.f.call(e,t),e[t]):void 0},Z={f:J},ee=function(e)
{if(!U(e))throw TypeError(e+" is not an object");return e},te=Object.defineProperty,oe=A?
te:function(e,t,o){if(ee(e),t=q(t,!0),ee(o),X)try{return te(e,t,o)}catch(e){}if("get"in
o||"set"in o)throw TypeError("Accessors not supported");return"value"in o&&(e[t]=o.value),e},ne=
{f:oe},ae=A?function(e,t,o){return ne.f(e,t,F(1,o))}:function(e,t,o){return
e[t]=o,e},ie=function(e,t){try{ae(C,e,t)}catch(o){C[e]=t}return t},se=e(funct
...
...
...
```

问题 1 / 1 TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://124.254.61.27:9090/web/resource/Inspinia/js/plugins/validate/jquery.validate.min.js
实体：	jquery.validate.min.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。
修复状态： 已修复
修复方式： 为 Web 服务器或 Web 应用程序下载相关的安全补丁
测试请求和响应：

```
GET /web/resource/Inspinia/js/plugins/validate/jquery.validate.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://124.254.61.27:9090/web/desktop
Cookie: JSESSIONID=7C15879B0ED11B9A08F98F109DD4C897
Connection: keep-alive
Host: 124.254.61.27:9090
Accept-Encoding: gzip
Accept: */*
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200
Last-Modified: Mon, 14 Oct 2019 01:49:27 GMT
Transfer-Encoding: chunked
Accept-Ranges: bytes
Content-Length: 23027
Vary: Accept-Encoding
ETag: W/"23027-1571017767868"
Date: Thu, 14 Nov 2019 08:27:44 GMT
Content-Type: application/javascript

/*! jQuery Validation Plugin - v1.15.1 - 7/22/2016
 * http://jqueryvalidation.org/
 * Copyright (c) 2016 Jörn Zaefferer; Licensed MIT */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof
module&&module.exports?module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,
{validate:function(b){if(!this.length)return
void(b&&b.debug&&window.console&&console.warn("Nothing selected, can't validate, returning
nothing."));var c=a.data(this[0],"validator");return c?c:
(this.attr("novalidate","novalidate"),c=new
a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&&
(this.on("click.validate",":submit",function(b){c.settings.submitHandler&&
(c.submitButton=b.target),a(this).hasClass("cancel")&&(c.cancelSubmit=!0),void
0!==a(this).attr("formnovalidate")&&(c.cancelSubmit=!0)}),this.on("submit.validate",function(b)
{function d(){var d,e;return!c.settings.submitHandler||(c.submitButton&&(d=a("<input
type='hidden'/>").attr("name",c.submitButton.name).val(a(c.submitButton).val()).appendTo(c.curren
```

```
tForm)),e=c.settings.submitHandler.call(c,c.currentForm,b),c.submitButton&&d.remove(),void
0!==e&&e)}return c.settings.debug&&b.preventDefault(),c.cancelSubmit?
(c.cancelSubmit=!1,d()):c.form()?c.pendingRequest?(c.formSubmitted=!0,!1):d():
(c.focusInvalid(),!1)})),c)},valid:function(){var b,c,d;return a(this[0]).is("form")?
b=this.validate().form():(d=[],b=!0,c=a(this[0].form).validate(),this.each(function()
{b=c.element(this)&&b,b||(d=d.concat(c.errorList))}),c.errorList=d),b},rules:function(b,c){var
d,e,f,g,h,i,j=this[0];if(null!=j&&null!=j.form)
{if(b)switch(d=a.data(j.form,"validator").settings,e=d.rules,f=a.validator.staticRules(j),b)
{case"add":a.extend(f,a.validator.normalizeRule(c)),delete f.messages,e[j.name]=f,c.messages&&
(d.messages[j.name]=a.extend(d.messages[j.name],c.messages));break;case"remove":return c?(i=
{},a.each(c.split(/\s/),function(b,c){i[c]=f[c],delete
f[c],"required"===c&&a(j).removeAttr("aria-required")}),i):(delete e[j.name],f)}return
g=a.validator.normalizeRules(a.extend({},a.validator.classRules(j),a.validator.attributeRules(j),
a.validator.dataRules(j),a.validator.staticRules(j)),j),g.required&&(h=g.required,delete
g.required,g=a.extend({required:h},g),a(j).attr("aria-required","true")),g.remote&&
(h=g.remote,delete g.remote,g=a.extend(g,{rem
...
...
...
b.settings.debug&&window.console&&console.error("%o has no name
assigned",this),this.hasAttribute("contenteditable")&&(this.form=a(this).closest("form")[0]),!(d
in c||!b.objectLength(a(this).rules()))&&(c[d]=!0,!0)})},clean:function(b){return a(b)
[0]},errors:function(){var b=this.settings.errorClass.split(" ").join(".");return
a(this.settings.errorElement+"."+b,this.errorContext)},resetInternals:function()
{this.successList=[],this.errorList=[],this.errorMap=
{},this.toShow=a([]),this.toHide=a([])},reset:function()
{this.resetInternals(),this.currentElements=a([])},prepareForm:function()
{this.reset(),this.toHide=this.errors().add(this.containers)},prepareElement:function(a)
{this.reset(),this.toHide=this.errorsFor(a)},elementValue:function(b){var
c,d,e=a(b),f=b.type;return"radio"===f||"checkbox"===f?
this.findByName(b.name).filter(":checked").val():"number"===f&&"undefined"!=typeof b.validity?
b.validity.badInput?"NaN":e.val():(c=b.hasAttribute("contenteditable")?
e.text():e.val(),"file"===f?"C:\\fakepath\\"===c.substr(0,12)?c.substr(12):
(d=c.lastIndexOf("/"),d>=0?c.substr(d+1):(d=c.lastIndexOf("\\"),d>=0?
c.substr(d+1):c)):"string"==typeof c?c.replace(/\r/g,""):c)},check:function(b)
{b=this.validationTargetFor(this.clean(b));var c,d,e,f=a(b).rules(),g=a.map(f,function(a,b)
{return b}).length,h=!1,i=this.elementValue(b);if("function"==typeof f.normalizer)
{if(i=f.normalizer.call(b,i),"string"!=typeof i)throw new TypeError("The normalizer should return
a string value.");delete f.normalizer}for(d in f){e=
{method:d,parameters:f[d]};try{if(c=a.validator.methods[d].call(this,i,b,e.parameters),"dependenc
y-mismatch"===c&&1===g){h=!0;continue}if(h=!1,"pending"===c)return
void(this.toHide=this.toHide.not(this.errorsFor(b)));if(!c)return
this.formatAndAdd(b,e),!1}catch(a){throw
this.settings.debug&&window.console&&console.log("Exception occurred when checking element
"+b.id+", check the '"+e.method+"' method.",a),a instanceof TypeError&&(a.mes
...
...
...
```

修复方式描述

高 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。 TOC

该任务修复的问题类型

- 已解密的登录请求

常规

1. 确保所有登录请求都以加密方式发送到服务器。
2. 请确保敏感信息，例如：
   - 用户名
   - 密码
   - 社会保险号码
   - 信用卡号码
   - 驾照号码
   - 电子邮件地址
   - 电话号码
   - 邮政编码

一律以加密方式传给服务器。

低 除去 HTML 注释中的敏感信息 TOC

该任务修复的问题类型

- HTML 注释敏感信息泄露

常规

[1] 请勿在 HTML 注释中遗留任何重要信息（如文件名或文件路径）。
[2] 从生产站点注释中除去以前（或未来）站点链接的跟踪信息。

[3] 避免在 HTML 注释中放置敏感信息。
[4] 确保 HTML 注释不包括源代码片段。
[5] 确保程序员没有遗留重要信息。

低 除去 Web 站点中的电子邮件地址 TOC

该任务修复的问题类型

- 发现电子邮件地址模式

常规

从 Web 站点中除去任何电子邮件地址，以便其不会被恶意用户利用。

低 除去 Web 站点中的信用卡号 TOC

该任务修复的问题类型

- 在未加密连接中发现信用卡号模式 (Visa)

常规

请克制，避免将信用卡号码包含在 web 站点中。

低 对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去 TOC

该任务修复的问题类型

- 检测到隐藏目录

常规

如果不需要禁止的资源，请将其从站点中除去。
可能的话，请发出改用“404 — 找不到”响应状态代码，而不是“403 — 禁止”。这项更改会将站点的目录模糊化，可以防止泄漏站点结构。

低 将“autocomplete”属性正确设置为“off” TOC

该任务修复的问题类型

- 自动填写未对密码字段禁用的 HTML 属性

常规

如果“input”元素的“password”字段中缺失“autocomplete”属性，请进行添加并将其设置为“off“。
如果“autocomplete”属性设置为“on”，请将其更改为“off”。
例如：易受攻击站点：

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" />
    <input type="submit" value="Submit" />
<form>
```

非易受攻击站点：

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname"
    autocomplete="off"/> <input type="submit" value="Submit" />
<form>
```

低 将服务器配置为使用安全策略的“Content-Security-Policy”头 TOC

该任务修复的问题类型

- “Content-Security-Policy”头缺失或不安全

常规

将服务器配置为发送“Content-Security-Policy”头。
关于 Apache，请参阅： link:http://httpd.apache.org/docs/2.2/mod/mod_headers.html 关于 IIS，请参阅：
link:https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx 关于 nginx，请参阅：
link:http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头 TOC

该任务修复的问题类型

- “X-XSS-Protection”头缺失或不安全

常规

配置您的服务器，以确保在所有传出请求上发送值为“1”（即已启用）的“X-XSS-Protection”报头。

关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头 TOC

该任务修复的问题类型

- “X-Content-Type-Options”头缺失或不安全

常规

将服务器配置为针对所有外发请求发送具有值“nosniff”的“X-Content-Type-Options”头。

关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

该任务修复的问题类型

- 发现可能的服务器路径泄露模式

常规

咨询

已解密的登录请求

TOC

测试类型：
应用程序级别测试

威胁分类：
传输层保护不足

原因：
诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

安全性风险：
可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

受影响产品：

CWE:
523

X-Force：
52471

引用：
金融隐私权：格拉斯-斯蒂格尔法案
健康保险可移植性和责任法案 (HIPAA)
萨班斯法案
加利福尼亚州 SB1386

技术描述：
在应用程序测试过程中，检测到将未加密的登录请求发送到服务器。由于登录过程中所使用的部分输入字段（例如：用户名、密码、电子邮件地址、社会安全号等）是个人敏感信息，因此建议通过加密连接（例如 SSL）将其发送到服务器。
任何以明文传给服务器的信息都可能被窃，稍后可用来电子欺骗身份或伪装用户。

此外，若干隐私权法规指出，用户凭证之类的敏感信息一律以加密方式传给 Web 站点。

“Content-Security-Policy”头缺失或不安全

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:

200

引用：

有用 HTTP 头列表
内容安全策略简介
MDN Web 文档 - 内容安全策略

技术描述：

“内容安全策略”标头旨在修改浏览器呈现页面的方式，从而防止各种跨站点注入，包括跨站点脚本。以不妨碍网站正常运行的方式正确设置标头值非常重要。例如，如果将标头设置为阻止执行内联 JavaScript，则网站不得在其页面中使用内联 JavaScript。 为了防止跨站点脚本、跨框架脚本和点击劫持，使用适当的值设置以下策略非常重要： 'default-src' 和 'frame-ancestors'策略、*或*所有 'script-src'、'object-src' 和 'frame-ancestors' 策略。 对于 'default-src'、'script-src' 和 'object-src'，应避免使用不安全的值，例如 '*'、'data:'、'unsafe-inline' 或 'unsafe-eval'。 对于 'frame-ancestors'，应避免使用不安全的值，例如 '*' 或 'data:'。 有关更多信息，请参阅以下链接。

“X-Content-Type-Options”头缺失或不安全

TOC

测试类型：

应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:
200

引用：
有用 HTTP 头列表
减少 MIME 类型安全风险

技术描述：
“X-Content-Type-Options”头（具有“nosniff”值）防止 IE 和 Chrome 忽略响应的内容类型。
此操作可能防止不可信内容（例如，用户上载内容）在用户浏览器上执行（例如，在恶意命名之后）。

“X-XSS-Protection”报头缺失或不安全

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:
200

引用：
有用 HTTP 头列表
IE XSS 过滤器

技术描述：
值为‘1’的“X-XSS-Protection”报头强制跨站点脚本编制过滤器进入启用模式，即使用户已禁用。
此过滤器内置于最新版本的 Web 浏览器（IE 8 +、Chrome 4+）中，在缺省情况下通常为已启用状态。虽然此过滤器不是第一个也不是唯一一个针对跨站点脚本编制的防御程序，但它可以作为额外保护层。

检测到隐藏目录

TOC

测试类型：
基础结构测试

威胁分类：
信息泄露

原因：
Web 服务器或应用程序服务器是以不安全的方式配置的

安全性风险：
可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点

受影响产品：

CWE:
200

X-Force：
52599

技术描述：
Web 应用程序显现了站点中的目录。虽然目录并没有列出其内容，但此信息可以帮助攻击者发展对站点进一步的攻击。例如，知道目录名称之后，攻击者便可以猜测它的内容类型，也许还能猜出其中的文件名或子目录，并尝试访问它们。内容的敏感度越高，此问题也可能越严重。

在未加密连接中发现信用卡号模式 (Visa)

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:
200

X-Force：
87836

技术描述：
AppScan 检测到包含完整 Visa 信用卡号码的响应。
基于安全和隐私权考虑，信用卡号码不应出现在 web 页面中。

自动填写未对密码字段禁用的 HTML 属性

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
Web 应用程序编程或配置不安全

安全性风险：
可能会绕开 Web 应用程序的认证机制

受影响产品：

CWE:
522

X-Force：
85989

技术描述：
“autocomplete”属性已在 HTML5 标准中进行规范。W3C 的站点声明该属性有两种状态：“on”和“off”，完全忽略时等同于设置为“on”。
该页面易受攻击，因为“input”元素的“password”字段中的“autocomplete”属性没有设置为“off”。
这可能会使未授权用户（具有授权客户机的本地访问权）能够自动填写用户名和密码字段，并因此登录站点。

HTML 注释敏感信息泄露

TOC

测试类型：
应用程序级别测试

威胁分类：
信息泄露

原因：
程序员在 Web 页面上留下调试信息

安全性风险：
可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:
615

X-Force：
52601

引用：
WASC 威胁分类：信息泄露

技术描述：
很多 Web 应用程序程序员使用 HTML 注释，以在需要时帮助调试应用程序。尽管添加常规注释有助于调试应用程序，

但一些程序员往往会遗留重要数据（例如：与 Web 应用程序相关的文件名、旧的链接或原非供用户浏览的链接、旧的代码片段等）。

发现电子邮件地址模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:

359

X-Force：

52584

引用：

Spambot 的定义（维基百科）

技术描述：

Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。
AppScan 检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。
而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。

发现可能的服务器路径泄露模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

未安装第三方产品的最新补丁或最新修补程序

安全性风险：

可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

受影响产品：

CWE:

200

X-Force：

52839

技术描述：

AppScan 检测到包含文件绝对路径的响应（例如，Windows 中的 c:\dir\file，或 Unix 中的 /dir/file）。 攻击者可能能够利用这一信息访问服务器机器目录结构上的敏感信息，进而对站点发起进一步攻击。