



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 9.0.2.1, 规则: 1932
扫描开始时间: 2016/1/8 15:57:56

目录

介绍

- 一般信息
- 登陆设置

管理综合报告

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- 在降级的旧加密上填充 Oracle（也称为 POODLE）^①
- 发现可能的服务器路径泄露模式^①
- 客户端（JavaScript）Cookie 引用^②
- 应用程序错误^①

修订建议

- 实施 TLS_FALLBACK_SCSV。此外，要么完全禁用 SSLv3，要么禁用以通过 SSLv3 的 CBC 模式操作的所有密码套件。
- 除去客户端中的业务逻辑和安全逻辑
- 为 Web 服务器或 Web 应用程序下载相关的安全补丁
- 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

咨询

- 在降级的旧加密上填充 Oracle（也称为 POODLE）
- 发现可能的服务器路径泄露模式
- 客户端（JavaScript）Cookie 引用
- 应用程序错误

应用程序数据

- cookie
- JavaScript
- 参数
- 注释
- 已访问的 URL
- 失败的请求
- 已过滤的 URL

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。

中等严重性问题: 1
低严重性问题: 4
报告中包含的严重性问题总数: 5
扫描中发现的严重性问题总数: 5

一般信息

扫描文件名称: 未命名
扫描开始时间: 2016/1/8 15:57:56
测试策略: Default
主机: 192.168.22.60
操作系统: Unknown
Web 服务器: Apache
应用程序服务器: Any

登陆设置

登陆方法: 提示
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:
跟踪或会话标识参数:
登陆序列:

管理综合报告

问题类型 4

TOC

问题类型		问题的数量
中	在降级的旧加密上填充 Oracle（也称为 POODLE）	1
低	发现可能的服务器路径泄露模式	1
低	客户端（JavaScript）Cookie 引用	2
低	应用程序错误	1

有漏洞的 URL 4

TOC

URL		问题的数量
中	http://192.168.22.60:23080/MktSystem/page/index	2
低	http://192.168.22.60:23080/MktSystem/js/echarts/dist/echarts-all.js	1
低	http://192.168.22.60:23080/MktSystem/js/angular/1.1.5/angular.js	1
低	http://192.168.22.60:23080/MktSystem/js/jquery/jquery-cookie-1.4.1/jquery.cookie.js	1





修订建议 4

TOC

修复任务		问题的数量
中	实施 TLS_FALLBACK_SCSV。此外，要么完全禁用 SSLv3，要么禁用以通过 SSLv3 的 CBC 模式操作的所有密码套件。	1
低	除去客户端中的业务逻辑和安全逻辑	2
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	1
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	1

安全风险 4

TOC

风险	问题的数量
中 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	1 
低 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 
低 此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色	2 
低 可能会收集敏感的调试信息	1 

原因 5

TOC

原因	问题的数量
中 Web 服务器或应用程序服务器是以不安全的方式配置的	1 
低 未安装第三方产品的最新补丁或最新修订程序	1 
低 Cookie 是在客户端创建的	2 
低 未对入局参数值执行适当的边界检查	1 
低 未执行验证以确保用户输入与预期的数据类型匹配	1 

WASC 威胁分类

TOC

威胁	问题的数量
信息泄露	5 

按问题类型分类的问题

中

在降级的旧加密上填充 Oracle（也称为 POODLE） 1

TOC

问题 1 / 1

TOC

在降级的旧加密上填充 Oracle（也称为 POODLE）	
严重性:	中
CVSS 分数:	6.7
URL:	http://192.168.22.60:23080/MktSystem/page/index
实体:	192.168.22.60 (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 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:	实施 TLS_FALLBACK_SCSV。此外，要么完全禁用 SSLv3，要么禁用以通过 SSLv3 的 CBC 模式操作的所有密码套件。

差异:

推理: 对于 AppScan 使用包含 TLS_FALLBACK_SCSV 的 CBC 密码套件进行的 SSLv3 客户机问候，服务器以握手进行了响应

未经处理的测试响应:

```
GET /MktSystem/page/index HTTP/1.1
Cookie: WAF_mktinfoName=69; WAF_reportPlatform=-1; WAF_scopeId=5;
JSESSIONID=F31EAB515978E52BF505CB5062AD255C
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: 192.168.22.60:23080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: DENY
Content-Security-Policy: img-src 'self'
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Expires: Tue, 22 Dec 2015 14:40:33 CST
Content-Type: text/html; charset=UTF-8
```

Transfer-Encoding: chunked
Date: Fri, 08 Jan 2016 07:57:46 GMT
...

发现可能的服务器路径泄露模式

严重性: 低

CVSS 分数: 3.8

URL: http://192.168.22.60:23080/MktSystem/js/echarts/dist/echarts-all.js

实体: echarts-all.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订程序

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: 响应应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应:

```
...
if(r.show){var
m=e.style;m.text=this._getLabelText(t,i,n,"normal"),m.textPosition=null==r.position?"horizontal".
.. V=e.highlightStyle;V.text=this._getLabelText(t,i,n,"emphasis"),V.textPosition=r.show?
e.style.tex... e),_getLabelText:function(e,t,i,n){var
a=this.deepQuery([t,e],"itemStyle."+n+".label.formatter");a||"emphasis"!==n||
(a=this.deepQuery([... o=this.getDataFromOption(t,"-");return a?"function"===typeof a?
a.call(this.myChart,{seriesName:e.name,series:e,name:i,value:o,data:t,status:n}):"string"===typeof
a?a.replace("{a}","{a0}") .replace("{b}","{b0}") .replace("{c}","{c0}") .replace("
{a0}",e.name).r... 0:o instanceof Array?null!=o[2]?this.numAddCommas(o[2]):o[0]+" ,
"+o[1]:this.numAddCommas(o)},buildMark:function(e){var
t=this.series[e];this.selectedMap[t.name]&&
(t.markLine&&this._buildMarkLine(e),t.markPoint&&this... t,i,n=(this.markAttachStyle||{}))
[e],a=this.series[e],o=u.clone(a.markPoint),r=0,s=o.data.length;...
l=this._markPoint(e,o),r=0,s=l.length;s>r;r++){var m=l[r];m.zlevel=a.zlevel,m.z=a.z+1;for(var V
in
n)m[V]=u.clone(n[V]);this.shapeList.push(m)}if(this.type===h.CHART_TYPE_FORCE||this.type===h.CHA.
.. r=0,s=l.length;s>r;r++)this.zr.addShape(l[r]),_buildMarkLine:function(e){for(var t,i=
(this.markAttachStyle||{})) [e],n=this.series[e],a=u.clone(n.markLine),o=0,r=a.data.length;r>o...
s=a.data[o];!s.type||"max"!==s.type&&"min"!==s.type&&"average"!==s.type?t=
[this.getMarkCoord(e,s... m=this._markLine(e,a),V=a.large;if(V){var U=new l({style:
{shapeList:m}}),d=m[0];if(d){u.merge(U.style,d.style),u.merge(U.highlightStyle={},d.hig... p in
i)U[p]=u.clone(i[p]);this.shapeList.push(U),this.zr.addShape(U),U._mark="largeLine";var
c=a.effect;c.show&&(U.effect=c)}else{for(var o=0,r=m.length;r>o;o++){var
y=m[o];y.zlevel=n.zlevel,y.z=n.z+1;for(var p in
i)y[p]=u.clone(i[p]);this.shapeList.push(y)}if(this.type===h.CHART_TYPE_FORCE||this.type===h.CHA.
.. o=0,r=m.length;r>o;o++)this.zr.addShape(m[o])},_markPoint:function(e,t){var
i=this.series[e],n=this.component;u.merge(u.merge(t,u.clone(this.ecTheme.markPoint||
{})),u.clone... a,o,r,s,l,V,U,d=
[],p=t.data,c=n.dataRange,y=n.legend,g=this.zr.getWidth(),b=this.zr.getHeight();... for(var
```

```
f=0,k=p.length;k>f;f++)null!=p[f].x&&null!=p[f].y&&(r=null!=p[f].value?p[f].value:" ",y&&(o=y.get... d),_markLine:function(){function e(e,t){e[t]=e[t]instanceof Array?e[t].length>1?e[t]:[e[t][0],e[t][0]]:[e[t],e[t]]}return function(i,n){var a=this.series[i],o=this.component,r=o.dataRange,s=o.legend;u.merge(u.merge(n,u.clone(this.ecThem... l=s?s.getColor(a.name):this.zr.getColor(i);e(n,"symbol"),e(n,"symbolSize"),e(n,"symbolRotate");f... V=n.data,U=[],d=this.zr.getWidth(),p=this.zr.getHeight(),y=0;y<V.length;y++){var g=V[y];if(t(g[0])&&t(g[1])){var b=this.deepMerge(g),f=[b,n],k=l,x=null!=b.value?b.value:"";if(r){k=isNaN(x)?k:r.getColor(x);var _=this.deepQuery(f,"itemStyle.normal.color")||k,L=this.deepQuery(f,"itemStyle.emphasis.color")||...
...
```

低

客户端（JavaScript）Cookie 引用 2

TOC

问题 1 / 2

TOC

客户端（JavaScript）Cookie 引用

严重性: 低

CVSS 分数: 3.8

URL: http://192.168.22.60:23080/MktSystem/js/angular/1.1.5/angular.js

实体: /* (Page)

风险: 此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色

原因: Cookie 是在客户端创建的

固定值: 除去客户端中的业务逻辑和安全逻辑

差异:

推理: AppScan 在 JavaScript 中找到对 cookie 的引用。

原始响应

```
GET /MktSystem/js/angular/1.1.5/angular.js HTTP/1.1
Cookie: JSESSIONID=F31EAB515978E52BF505CB5062AD255C
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://192.168.22.60:23080/MktSystem/page/index
Host: 192.168.22.60:23080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: DENY
Content-Security-Policy: img-src 'self'
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Accept-Ranges: bytes
ETag: W/"88910-1452237466000"
Last-Modified: Fri, 08 Jan 2016 07:17:46 GMT
Content-Type: application/javascript
Content-Length: 88910
...
```

客户端（JavaScript）Cookie 引用	
严重性:	低
CVSS 分数:	3.8
URL:	http://192.168.22.60:23080/MktSystem/js/jquery/jquery-cookie-1.4.1/jquery.cookie.js
实体:	/*! (Page)
风险:	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因:	Cookie 是在客户端创建的
固定值:	除去客户端中的业务逻辑和安全逻辑

差异:

推理: AppScan 在 JavaScript 中找到对 cookie 的引用。

原始响应

```
...

var config = $.cookie = function (key, value, options) {

    // Write

    if (value !== undefined && !$.isFunction(value)) {
        options = $.extend({}, config.defaults, options);

        if (typeof options.expires === 'number') {
            var days = options.expires, t = options.expires = new Date();
            t.setTime(+t + days * 864e+5);
        }

        return (document.cookie = [
            encode(key), '=', stringifyCookieValue(value),
            options.expires ? '; expires=' + options.expires.toUTCString() : '', // use expires
            attribute, max-age is not supported by IE
            options.path ? '; path=' + options.path : '',
            options.domain ? '; domain=' + options.domain : '',
            options.secure ? '; secure' : ''
        ].join(''));
    }

    ...
}
```

应用程序错误

严重性: 低

CVSS 分数: 3.8

URL: http://192.168.22.60:23080/MktSystem/page/index

实体: ticket (Parameter)

风险: 可能会收集敏感的调试信息

原因: 未对入局参数值执行适当的边界检查
未执行验证以确保用户输入与预期的数据类型匹配

固定值: 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

差异: 参数 从以下位置进行控制: ST-2889-BaItDLYlBAN22CpnYRGy-BIPortal 至: %27

推理: 应用程序以错误消息响应, 表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应:

```

...
GET /MktSystem/page/index?ticket=%27 HTTP/1.1
Host: 192.168.22.60:23080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Connection: keep-alive

HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 2235
Date: Fri, 08 Jan 2016 08:08:26 GMT
Connection: close

<html><head><title>Apache Tomcat/7.0.19 - Error report</title><style><!--H1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-
family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-
family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color :
black;}A.name {color : black;}HR {color : #525D76;}--></style> </head><body><h1>HTTP Status 500 -
</h1><HR size="1" noshade="noshade"><p><b>type</b> Exception report</p><p><b>message</b> <u></u>
</p><p><b>description</b> <u>The server encountered an internal error () that prevented it from
fulfilling this request.</u></p><p><b>exception</b> <pre>javax.servlet.ServletException:
org.jasig.cas.client.validation.TicketValidationException: CAS Server could not validate ticket.
    org.jasig.cas.client.validation.AbstractTicketValidationFilter.doFilter(AbstractTicketValidation
    ...
    org.jasig.cas.client.authentication.AuthenticationFilter.doFilter(AuthenticationFilter.java:116)
    ...

```

修订建议

中

实施 TLS_FALLBACK_SCSV。此外，要么完全禁用 SSLv3，要么禁用以通过 SSLv3 的 CBC 模式操作的所有密码套件。

TOC

该任务修复的问题类型

- 在降级的旧加密上填充 Oracle（也称为 POODLE）

一般

实施针对 TLS_FALLBACK_SCSV 的支持。

此外，禁用 SSLv3 支持。

如果需要 SSLv3，请在 SSLv3 上禁用 CBC 密码套件（请参阅“参考”和“相关链接”以了解更多详细信息）。

如果需要 CBC 密码套件，请将服务器设置为在 SSLv3 中首选 RC4 密码套件，而不是 CBC 密码套件。

低

除去客户端中的业务逻辑和安全逻辑

TOC

该任务修复的问题类型

- 客户端（JavaScript）Cookie 引用

一般

[1] 避免在客户端放置业务/安全逻辑。

[2] 查找并除去客户端不安全的 JavaScript 代码，该代码可能会对站点造成安全威胁。

低

为 Web 服务器或 Web 应用程序下载相关的安全补丁

TOC

该任务修复的问题类型

- 发现可能的服务器路径泄露模式

一般

下载相关的安全补丁，这会随着 Web 服务器或 Web 应用程序上现有的问题而不同。

低

验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

TOC

该任务修复的问题类型

- 应用程序错误

一般

- [1] 检查入局请求，以了解所有预期的参数和值是否存在。当参数缺失时，发出适当的错误消息，或使用缺省值。
- [2] 应用程序应验证其输入是否由有效字符组成（解码后）。例如，应拒绝包含空字节（编码为 %00）、单引号、引号等的输入值。
- [3] 确保值符合预期范围和类型。如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。例如，如果应用程序预期值在 10..99 范围内，那么就该确保该值确实是数字，且在 10..99 范围内。
- [4] 验证数据是否属于提供给客户端的集合。
- [5] 请勿在生产环境中输出调试错误消息和异常。

.Net

要在 ASP.NET 中禁用调试，请编辑 web.config 文件，使其包含以下属性：

```
<compilation
  debug="false"
/>
```

要获取更多信息，请参阅“HOW TO: Disable Debugging for ASP.NET Applications”，位置如下：

<http://support.microsoft.com/default.aspx?scid=kb;en-us;815157>

您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于所有常见类型的标准验证的易用机制（例如，测试验证日期是否有效，或验证值是否在范围内），以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。

要确保所有的必需参数都存在于请求中，请使用“RequiredFieldValidator”验证控件。该控件确保用户不会跳过 web 表单中的任何条目。

要确保用户输入仅包含有效值，您可以使用以下验证控件中的一种：

- [1] “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。您可以检查配对数字、字母字符和日期内的范围。

[2] “**RegularExpressionValidator**”：检查条目是否与正则表达式定义的模式相匹配。此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。
重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。
有两种方法可检查用户输入的有效性：

1. 测试常规错误状态：

在您的代码中，测试页面的 **IsValid** 属性。该属性会将页面上所有验证控件的 **IsValid** 属性值汇总（使用逻辑 **AND**）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 **false**。

2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 **IsValid** 属性。

J2EE

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 **Servlet** 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。
一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：

- [1] 必需字段
- [2] 字段数据类型（缺省情况下，所有 **HTTP** 请求参数都是“字符串”）
- [3] 字段长度
- [4] 字段范围
- [5] 字段选项
- [6] 字段模式
- [7] **cookie** 值
- [8] **HTTP** 响应

好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。

如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}

...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 **Web** 应用程序中的字段数据类型和输入参数欠佳。例如，所有 **HTTP** 请求参数或 **cookie** 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 **Java** 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（**int** 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
```

```

        boolean isFieldValid = false;
        try {
            Integer.parseInt(value);
            isFieldValid = true;
        } catch (Exception e) {
            isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}

```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```

// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...

```

应用程序应处理的主要 Java 数据类型：

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 userName 字段的长度是否在 8 至 20 个字符之间：

```

// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
            validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");

```



```

if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}

```

[4] 字段范围

始终确保输入参数是在由功能需求定义的范围之内。

以下示例验证输入 **numberOfChoices** 是否在 10 至 20 之间：

```

// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
}

```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```

// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3"};
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
}

```

[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 `userName` 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]*$`

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“Apache 正则表达式包”（请参阅以下“资源”）与 Java 1.3 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包 (`java.util.regex`)。以下是使用新的 Java 1.4 正则表达式包的 `Validator.matchPattern` 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regex.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 `javax.servlet.http.Cookie` 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
```

```

        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue())) {
            // valid cookie value, continue processing request
            ...
        }
    }
}

```

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：<>"'%;)(& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```

// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
            return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
                case '<':
                    result.append("&lt;");
                    break;
                case '>':
                    result.append("&gt;");
                    break;
                case '"':
                    result.append("&quot;");
                    break;
                case '\'':
                    result.append("&#39;");
                    break;
                case '%':
                    result.append("&#37;");
                    break;
                case ';':
                    result.append("&#59;");
                    break;
                case '(':
                    result.append("&#40;");
                    break;
                case ')':
                    result.append("&#41;");
                    break;
                case '&':
                    result.append("&amp;");
                    break;
                case '+':
                    result.append("&#43;");
                    break;
                default:
                    result.append(value.charAt(i));
                    break;
            }
        }
        return result;
    }
    ...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();

```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。以下示例使用 `Validator.filter` 来用“Servlet 过滤器”清理响应：

```
// Example to filter all sensitive characters in the HTTP response using a Java Filter.
// This example is for illustration purposes since it will filter all content in the response, including
// HTML tags!
public class SensitiveCharsFilter implements Filter {
    ...
    public void doFilter(ServletRequest request,
                        ServletResponse response,
                        FilterChain chain)
        throws IOException, ServletException {

        PrintWriter out = response.getWriter();
        ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
        chain.doFilter(request, wrapper);

        CharArrayWriter caw = new CharArrayWriter();
        caw.write(Validator.filter(wrapper.toString()));

        response.setContentType("text/html");
        response.setContentLength(caw.toString().length());
        out.write(caw.toString());
        out.close();
    }
    ...
    public class CharResponseWrapper extends HttpServletResponseWrapper {
        private CharArrayWriter output;

        public String toString() {
            return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response) {
            super(response);
            output = new CharArrayWriter();
        }

        public PrintWriter getWriter(){
            return new PrintWriter(output);
        }
    }
}
```

[8-2] 保护 cookie

在 cookie 中存储敏感数据时，确保使用 `Cookie.setSecure`（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。

保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 实施所有以上数据验证需求，是强大的框架。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用

Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。

Struts 定义以下基本输入验证器，但也可定义定制的验证器：

required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。

range：如果值在 **min** 和 **max** 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。

maxLength：如果字段长度小于或等于 **max** 属性，便告成功。

minLength：如果字段长度大于或等于 **min** 属性，便告成功。

byte、**short**、**integer**、**long**、**float**、**double**：如果可将值转换为对应的基本类型，便告成功。

date：如果值代表有效日期，便告成功。可能会提供日期模式。

creditCard：如果值可以是有效的信用卡号码，便告成功。

e-mail：如果值可以是有效的电子邮件地址，便告成功。

使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
  <global>
    ...
    <validator name="required"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateRequired"
      msg="errors.required">
    </validator>
    <validator name="mask"
      classname="org.apache.struts.validator.FieldChecks"
      method="validateMask"
      msg="errors.invalid">
    </validator>
    ...
  </global>
  <formset>
    <form name="loginForm">
      <!-- userName is required and is alpha-numeric case insensitive -->
      <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayName"/>
        <var>
          <var-name>mask</var-name>
          <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
      </field>
      ...
    </form>
    ...
  </formset>
</form-validation>
```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。

JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器：**validate_doublerange**：在组件上注册 DoubleRangeValidator

validate_length：在组件上注册 LengthValidator

validate_longrange：在组件上注册 LongRangeValidator

validate_required：在组件上注册 RequiredValidator

validate_stringrange：在组件上注册 StringRangeValidator

validator：在组件上注册定制的 Validator

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：

input_date：接受以 java.text.Date 实例格式化的 java.util.Date

output_date：显示以 java.text.Date 实例格式化的 java.util.Date

input_datetime：接受以 java.text.DateTime 实例格式化的 java.util.Date

output_datetime：显示以 java.text.DateTime 实例格式化的 java.util.Date

input_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）

output_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）

input_text: 接受单行文本字符串。
output_text: 显示单行文本字符串。
input_time: 接受以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`
output_time: 显示以 `java.text.DateFormat` 时间实例格式化的 `java.util.Date`
input_hidden: 允许页面作者在页面中包括隐藏变量
input_secret: 接受不含空格的单行文本, 并在输入时, 将其显示为一组星号
input_textarea: 接受多行文本
output_errors: 显示整个页面的错误消息, 或与指定的客户端标识相关联的错误消息
output_label: 将嵌套的组件显示为指定输入字段的标签
output_message: 显示本地化消息

使用 `JavaServer Faces` 来验证 `loginForm` 的 `userName` 字段的示例:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 -

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 -

<http://java.sun.com/j2ee/jvaserverfaces/>

**** 错误处理:**

许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器 (MVC)”模式。在该模式中, `Servlet` 扮演“控制器”的角色。`Servlet` 将应用程序处理委派给 `EJB` 会话 `Bean` (模型) 之类的 `JavaBean`。然后, `Servlet` 再将请求转发给 `JSP` (视图), 以呈现处理结果。`Servlet` 应检查所有的输入、输出、返回码、错误代码和已知的异常, 以确保实际处理按预期进行。

数据验证可保护应用程序免遭恶意数据篡改, 而有效的错误处理策略则是防止应用程序意外泄露内部错误消息 (如异常堆栈跟踪) 所不可或缺的。好的错误处理策略会处理以下项:

[1] 定义错误

[2] 报告错误

[3] 呈现错误

[4] 错误映射

[1] 定义错误

应避免在应用程序层 (如 `Servlet`) 中硬编码错误消息。相反地, 应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥, 且该错误密钥映射到 `HTML` 表单字段或其他 `Bean` 属性的验证规则。例如, 如果需要“`user_name`”字段, 其内容为字母数字, 并且必须在数据库中是唯一的, 那么就应定义以下错误密钥:

- (a) **ERROR_USERNAME_REQUIRED**: 该错误密钥用于显示消息，以通知用户需要“user_name”字段；
 (b) **ERROR_USERNAME_ALPHANUMERIC**: 该错误密钥用于显示消息，以通知用户“user_name”字段应该是字母数字；
 (c) **ERROR_USERNAME_DUPLICATE**: 该错误密钥用于显示消息，以通知用户“user_name”值在数据库中重复；
 (d) **ERROR_USERNAME_INVALID**: 该错误密钥用于显示一般消息，以通知用户“user_name”值无效；
 好的做法是定义用于存储和报告应用程序错误的以下框架 **Java** 类：
 - **ErrorKeys**: 定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
// - ERROR_USERNAME_REQUIRED
// - ERROR_USERNAME_ALPHANUMERIC
// - ERROR_USERNAME_DUPLICATE
// - ERROR_USERNAME_INVALID
// ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- **Error**: 封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
        this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
    }

    // Returns the error key
    public String getKey() {
        return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
        return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- **Errors**: 封装错误的集合

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
```

```

    public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
        return (errors.size > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}

```

以下是使用上述框架类来处理“user_name”字段验证错误的示例:

```

// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...

```

[2] 报告错误

有两种方法可报告 web 层应用程序错误:

(a) Servlet 错误机制

(b) JSP 错误机制

[2-a] Servlet 错误机制

Servlet 可通过以下方式报告错误:

- 转发给输入 JSP (已将错误存储在请求属性中), 或
- 使用 HTTP 错误代码参数来调用 `response.sendError`, 或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（userInput.jsp）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 `response.sendError` 方法，将 `HttpServletResponse.SC_INTERNAL_SERVER_ERROR`（状态码 500）作为参数，来报告错误。请参阅 `javax.servlet.http.HttpServletResponse` 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。

返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类：- `RuntimeException` - `ServletException` - `IOException`

[2-b] JSP 错误机制

JSP 页面通过定义 `errorPage` 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 `errorPage`，并且原始异常设置在名称为 `javax.servlet.jsp.jspException` 的请求参数中。错误页面必须包括 `isErrorPage` 伪指令，如下所示：

```
<%@ page isErrorPage="true" %>
```

`isErrorPage` 伪指令导致“exception”变量初始化为所抛出的异常对象。

[3] 呈现错误

J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束

(b) 消息格式化

[3-a] 资源束

资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。

`java.util.PropertyResourceBundle` 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
#####
```

```
# ErrorMessages.properties
#####
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 `ErrorMessages_fr.properties` 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 `ErrorMessages.properties`。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 `java.util.MessageFormat` 提供使用替换占位符来创建消息的常规方法。`MessageFormat` 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 `ResourceBundle` 和 `MessageFormat` 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
        } else {
            return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}

...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
```

```

Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}

```

建议定义定制 JSP 标记（如 `displayErrors`），以迭代处理并呈现错误消息，如以上示例所示。

[4] 错误映射

通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如下示例所指定：

```

<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
    <exception-type>UserValidationException</exception-type>
    <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
    <error-code>500</error-code>
    <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
    ...
</error-page>
...

```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：

[1] Jakarta Commons Validator（与 Struts 1.1 集成）**Jakarta Commons Validator**是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。**Struts** 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。使用“**Struts 验证器**”来验证 `loginForm` 的 `userName` 字段的示例：

```

<form-validation>
    <global>
        ...
        <validator name="required"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateRequired"
            msg="errors.required">
        </validator>
        <validator name="mask"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateMask"
            msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
            <!-- userName is required and is alpha-numeric case insensitive -->
            <field property="userName" depends="required,mask">
                <!-- message resource key to display if validation fails -->
                <msg name="mask" key="login.userName.maskmsg"/>
                <arg0 key="login.userName.displayName"/>
            </var>

```

```

        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
    </var>
</field>
...
</form>
...
</formset>
</form-validation>

```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如下示例所示：

```

<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
        <table border="0" width="100%">
            <tr>
                <th align="right">
                    <html:errors property="username"/>
                    <bean:message key="prompt.username"/>
                </th>
                <td align="left">
                    <html:text property="username" size="16"/>
                </td>
            </tr>
            <tr>
                <td align="right">
                    <html:submit><bean:message key="button.submit"/></html:submit>
                </td>
                <td align="right">
                    <html:reset><bean:message key="button.reset"/></html:reset>
                </td>
            </tr>
        </table>
    </html:form>
</body>
</html:html>

```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```

<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
    <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>

```

```
</h:form>
</f:use_faces>
```

引用

Java API 1.3 -

<http://java.sun.com/j2se/1.3/docs/api/>

Java API 1.4 -

<http://java.sun.com/j2se/1.4/docs/api/>

Java Servlet API 2.3 -

<http://java.sun.com/products/servlet/2.3/javadoc/>

Java 正则表达式包 —

<http://jakarta.apache.org/regexp/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/javaxserverfaces/>

PHP

**** 输入数据验证：**虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 **Javascript**。

一份好的设计通常需要 **Web** 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：

- [1] 必需字段
- [2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）
- [3] 字段长度
- [4] 字段范围
- [5] 字段选项
- [6] 字段模式
- [7] cookie 值
- [8] HTTP 响应

好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 **Web** 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 **cookie** 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 **cookie** 值）有最小长度和/或最大长度的限制。[4] 字段范围

始终确保输入参数是在由功能需求定义的范围内的。

[5] 字段选项 **Web** 应用程序通常会为用户显示一组可供选择的选项（例如，使用 **SELECT HTML** 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式

始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 `userName` 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：`^[a-zA-Z0-9]+$`

[7] cookie 值

适用于 `cookie` 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。

[8] HTTP 响应

[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：`< > ' ' % ;) (& +`

PHP 包含一些自动化清理实用程序函数，如 `htmlspecialchars()`：

```
$input = htmlspecialchars($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 `Content-Type` 头，例如：

```
<?php
header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie

在 `cookie` 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 `cookie` 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 `cookie`。

为了保护 `cookie`，您可以使用以下代码示例：

```
<?php
$value = "some_value";
$time = time()+3600;
$path = "/application/";
$domain = ".example.com";
$secure = 1;

setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);

?>
```

此外，我们建议您使用 `HttpOnly` 标志。当 `HttpOnly` 标志设置为 `TRUE` 时，将只能通过 HTTP 协议来访问 `cookie`。这意味着无法用脚本语言（如 JavaScript）来访问 `cookie`。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。

在 PHP 5.2.0 中添加了 `HttpOnly` 标志。

引用[1] 使用 HTTP 专用 `cookie` 来减轻“跨站点脚本编制”的影响：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] PHP 安全协会：

<http://phpsec.org/>

[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：

<http://shiflett.org/>

咨询

在降级的旧加密上填充 Oracle（也称为 POODLE）

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：

CVE:

CVE-2014-3566

X-Force:

97013

引用：

利用 SSL 3.0 回退

Redhat 建议

如何修复 POODLE（以及为什么您可能仍然易受攻击）

技术描述：

如果将使用 CBC 模式（密码分组链接）加密的文本解密，SSL 3.0 在处理填充字节时有一个缺陷。利用此缺陷，中间人只需针对每个字节发送至多 256 个请求就可以一次解密一个字节。

遇到连接失败时，大多数浏览器会使用更旧的协议版本（包括 SSL 3.0）重试连接服务器。这使网络攻击者可以触发 SSL 3.0 的使用，然后通过故意导致连接失败来利用此问题。

利用的样本：

易受攻击的服务器在收到带有 CBC 密码套件和 TLS_FALLBACK_SCSV 的 SSLv3 客户机问候时会以握手进行响应

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订程序

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

引用：

CWE-200: 信息泄露（信息披露）

技术描述：

AppScan 检测到含有文件绝对路径（例如：Windows 的 c:\dir\file，Unix 的 /dir/file）的响应。
攻击者也许能够利用这项信息，从而访问到关于服务器机器目录结构的敏感信息，因而能够进一步攻击站点。

客户端（JavaScript）Cookie 引用

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因:

Cookie 是在客户端创建的

安全性风险:

此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色

受影响产品:

CWE:

602

X-Force:

52514

引用:

WASC 威胁分类: 信息泄露

技术描述:

cookie 是一则信息，通常由 Web 服务器创建并存储在 Web 浏览器中。

web 应用程序主要（但不只是）使用 cookie 包含的信息来识别用户并维护用户的状态。

AppScan 检测到客户端上的 JavaScript 代码用于操控（创建或修改）站点的 cookie。

攻击者有可能查看此代码、了解其逻辑并根据所了解的知识将其用于组成自己的 cookie，或修改现有 cookie。

攻击者可能导致的损坏取决于应用程序使用其 cookie 的方式或应用程序存储在这些 cookie 中的信息内容。

此外，cookie 操控还可能导致会话劫持或特权升级。

由 cookie 毒害导致的其他漏洞包含 SQL 注入和跨站点脚本编制。

应用程序错误

TOC

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

- 未对入局参数值执行适当的边界检查
- 未执行验证以确保用户输入与预期的数据类型匹配

安全性风险:

可能会收集敏感的调试信息

受影响产品：

CWE:

550

X-Force:

52502

引用：

使用单引号入侵站点的示例，可参阅[“How I hacked PacketStorm \(by Rain Forest Puppy\), RFP's site”](#)

[“Web Application Disassembly with ODBC Error Messages”](#)（作者：David Litchfield）

CERT 咨询（CA-1997-25）：清理 CGI 脚本中用户提供的数据

技术描述：

如果攻击者通过伪造包含非应用程序预期的参数或参数值的请求，来探测应用程序（如下示例所示），那么应用程序可能会进入易受攻击的未定义状态。攻击者可以从应用程序对该请求的响应中获取有用的信息，且可利用该信息，以找出应用程序的弱点。

例如，如果参数字段是单引号括起来的字符串（如在 ASP 脚本或 SQL 查询中），那么注入的单引号将会提前终止字符串流，从而更改脚本的正常流程/语法。

错误消息中泄露重要信息的另一个原因，是脚本编制引擎、Web 服务器或数据库配置错误。

以下是一些不同的变体：

- [1] 除去参数
- [2] 除去参数值
- [3] 将参数值设置为空值
- [4] 将参数值设置为数字溢出（+/- 99999999）
- [5] 将参数值设置为危险字符，如 `'"\'\"`）；
- [6] 将某字符串附加到数字参数值
- [7] 在参数名称后追加“.”（点）或“[]”（尖括号）

应用程序数据

已访问的 URL 26

TOC

URL
http://192.168.22.60:23080/MktSystem/page/index
http://192.168.22.60:23080/MktSystem/js/angular/1.1.5/angular.js
http://192.168.22.60:23080/MktSystem/js/jquery/jquery/2.1.3/jquery.js
http://192.168.22.60:23080/MktSystem/js/local/util.js
http://192.168.22.60:23080/MktSystem/js/seajs/2.2.3/sea.js
http://192.168.22.60:23080/MktSystem/js/modules/base/mms.js
http://192.168.22.60:23080/MktSystem/js/modules/base/chart.js
http://192.168.22.60:23080/MktSystem/js/modules/base/meta/meta.js
http://192.168.22.60:23080/MktSystem/js/echarts/dist/echarts-all.js
http://192.168.22.60:23080/MktSystem/js/jquery/jquery-ui/jquery-ui.min.js
http://192.168.22.60:23080/MktSystem/js/jquery/jquery-ui/jquery-ui-timepicker-addon.min.js
http://192.168.22.60:23080/MktSystem/js/jquery/jquery-cookie-1.4.1/jquery.cookie.js
http://192.168.22.60:23080/MktSystem/js/bootstrap-3.3.5-dist/js/bootstrap.min.js
http://192.168.22.60:23080/MktSystem/page/index
http://192.168.22.60:23080/MktSystem/page/index
http://192.168.22.60:23080/MktSystem/page/index?ticket=ST-2889-BaltdLYIBAN22CpnYRGy-BIPortal
http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6
http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicList
http://192.168.22.60:23080/MktSystem/api/user/login
http://192.168.22.60:23080/MktSystem/page/index
http://192.168.22.60:23080/MktSystem/api/meta/query
http://192.168.22.60:23080/MktSystem/api/admin/models?__userKey=4kuX-L8macLkENvRXy6uTC
http://192.168.22.60:23080/MktSystem/page/mktInfo
http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicCommonList
http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicCommonList
http://192.168.22.60:23080/MktSystem/api/mktInfo/query

参数 15

TOC

名称	值	URL	类型
->"__userKey"	4kuX-L8macLkENvRXy6uTC	http://192.168.22.60:23080/MktSystem/api/mktInfo/query	JSON
->"__userKey"	4kuX-L8macLkENvRXy6uTC	http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicCommo nList	JSON
	FD4D8A3F19C87ED208A38B3CDE3511E6	http://192.168.22.60:23080/MktSystem/page/index.jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6	定制
->"type"	product	http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicList	JSON
->"__userKey"	4kuX-L8macLkENvRXy6uTC	http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicList	JSON
->"meta"	mktInfo	http://192.168.22.60:23080/MktSystem/api/mktInfo/query	JSON
__userKey	4kuX-L8macLkENvRXy6uTC	http://192.168.22.60:23080/MktSystem/api/admin/models?__userKey=4kuX-L8macLkENvRXy6uTC	简单链接
__userKey	4kuX-L8macLkENvRXy6uTC	http://192.168.22.60:23080/MktSystem/page/mktInfo	主体
id	13	http://192.168.22.60:23080/MktSystem/page/mktInfo	主体
ticket	ST-2889-BaltdLYIBAN22CpnYRGy-BIPortal	http://192.168.22.60:23080/MktSystem/page/index?ticket=ST-2889-BaltdLYIBAN22CpnYRGy-BIPortal	简单链接
->"id"	13	http://192.168.22.60:23080/MktSystem/api/mktInfo/query	JSON
->"type"	platform purchase_method	http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicCommo nList	JSON
->"from"	0	http://192.168.22.60:23080/MktSystem/api/mktInfo/query	JSON
meta	mktInfo	http://192.168.22.60:23080/MktSystem/page/mktInfo	主体
->"perPage"	15	http://192.168.22.60:23080/MktSystem/api/mktInfo/query	JSON

失败的请求 2

TOC

URL
http://192.168.22.60:23080/MktSystem/js/local/en_US.js
http://192.168.22.60:23080/MktSystem/js/jquery/jquery/2.1.3/target[

已过滤的 URL 29

TOC

URL	原因
http://192.168.22.60:23080/MktSystem/js/jquery/jqui/jquery-ui.min.css	文件扩展名
http://192.168.22.60:23080/MktSystem/js/bootstrap-3.3.5-dist/css/bootstrap.min.css	文件扩展名
http://192.168.22.60:23080/MktSystem/js/jquery/jqui/jquery-ui-timepicker-addon.min.css	文件扩展名
http://192.168.22.60:23080/MktSystem/css/common.css	文件扩展名

http://192.168.22.60:23080/MktSystem/css/mms.css	文件扩展名
https://biportal/BIPortal/login?service=http:%2F%2F192.168.22.60:23080%2FMktSystem%2Fpage%2Findex	未测试的 Web Server
https://biportal/BIPortal/login?service=http://192.168.22.60:23080/MktSystem/page/index	未测试的 Web Server
https://biportal/BIPortal/images/bg2.png	未测试的 Web Server
https://biportal/BIPortal/images/bg3.png	未测试的 Web Server
https://biportal/BIPortal/images/bg6.png	未测试的 Web Server
https://biportal/BIPortal/login	未测试的 Web Server
https://biportal/BIPortal/images/icon5.png	未测试的 Web Server
http://192.168.22.60:23080/MktSystem/imgs/logo.gif	文件扩展名
http://192.168.22.60:23080/MktSystem/page/verifyCode	图像上下文
http://192.168.22.60:23080/MktSystem/imgs/login/refresh.gif	文件扩展名
https://biportal/BIPortal/noprivilege.jsp	未测试的 Web Server
https://biportal/BIPortal/login	未测试的 Web Server
https://biportal/BIPortal/js/jquery/jquery/1.11.1/jquery-1.11.1.js	未测试的 Web Server
https://biportal/BIPortal/js/common.js	未测试的 Web Server
https://biportal/BIPortal/images/logo.png	未测试的 Web Server
https://biportal/BIPortal/verifycode.servlet	未测试的 Web Server
https://biportal/BIPortal/images/icon6.png	未测试的 Web Server
https://biportal/BIPortal/images/bg1.png	未测试的 Web Server
http://fr:8086/WebReport7/ReportServer?op=fs	未测试的 Web Server
http://userinsight:8082/UserInsightSystem/index.jsp	未测试的 Web Server
http://adhoc:8083/AdHoc/adhoc.jsp	未测试的 Web Server
https://biportal/BIPortal/images/bg_login.png	未测试的 Web Server
https://biportal/BIPortal/images/icon4.png	未测试的 Web Server
https://biportal/BIPortal/images/bg4.png	未测试的 Web Server

URL	注释
http://192.168.22.60:23080/MktSystem/page/index	新 Bootstrap 核心 CSS 文件
http://192.168.22.60:23080/MktSystem/page/index	最新的 Bootstrap 核心 JavaScript 文件
http://192.168.22.60:23080/MktSystem/page/index	FREEMARKER ERROR MESSAGE STARTS HERE
http://192.168.22.60:23080/MktSystem/page/index]]>
http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6	end of login_win
http://192.168.22.60:23080/MktSystem/page/mktInfo	end of ListCtrl
http://192.168.22.60:23080/MktSystem/page/mktInfo	end of ModelList

JavaScript 27

TOC

URL / 代码

http://192.168.22.60:23080/MktSystem/page/index

```
seajs.config({
  base: "/MktSystem/js/",
  alias: {
    'jquery': 'jquery/jquery/2.1.3/jquery',
    'jquery-ui': 'jquery/jquery/jquery-ui.min',
    'cookie': 'jquery/jquery-cookie-1.4.1/jquery.cookie',
    'dialog': 'jquery/dialog/6.0.4/dialog',
    'calendar': 'jquery/calendar/1.0/tinycal.debug.js',
    'angular': 'angular/1.1.5/angular',
    'tree': 'jquery/tree/3.5/ztree',
    'splitter': 'jquery/splitter/0.8.0/splitter',
    'meta': 'modules/base/meta/meta',
    'navi': 'modules/base/navi',
    'model': 'modules/base/model',
    'tools': 'modules/base/tools',
    'notice': 'modules/base/notice',
    'base': 'modules/base/base'
  },
  map: [
    [/^(.*\.?(?:css|js))(.*)$/i, '$1?20140219']
  ]
});
var __userKey="x9Oh1FBZaJbSP1CMKdWRmB";
var __cookieHeader="WAF_";
var __webRoot="/MktSystem";
```

http://192.168.22.60:23080/MktSystem/page/index

```
//">
```

http://192.168.22.60:23080/MktSystem/page/index

```
//>
```

<http://192.168.22.60:23080/MktSystem/page/index>

```
void(0);
```

<http://192.168.22.60:23080/MktSystem/js/angular/1.1.5/angular.js>

```
/*
  AngularJS v1.1.5
  (c) 2010-2012 Google, Inc. http://angularjs.org
  License: MIT
*/
(function(M,T,p){'use strict';function lc(){var b=M.angular;M.angular=mc;return b}function Xa(b)
{return b||typeof b.length!="number"?!1:typeof b.hasOwnProperty!="function"&typeof
b.constructor!="function"?!0:b instanceof R||ga&&b instanceof ga||Ea.call(b)!="[object Object]"||typeof
b.caller=="function"}function n(b,a,c){var d;if(b){if(H(b))for(d in
b)d!="prototype"&&d!="length"&&d!="name"&&b.hasOwnProperty(d)&&a.call(c,b[d],d);else
if(b.forEach&&b.forEach!=n)b.forEach(a,c);else if(Xa(b))for(d=
0;d<b.length;d++)a.call(c,b[d],d);else for(d in b)b.hasOwnProperty(d)&&a.call(c,b[d],d);return b}function
qb(b){var a=[],c;for(c in b)b.hasOwnProperty(c)&&a.push(c);return a.sort()}function nc(b,a,c){for(var
d=qb(b),e=0;e<d.length;e++)a.call(c,b[d[e]],d[e]);return d}function rb(b){return function(a,c)
{b(c,a)}}function Fa(){for(var b=ba.length,a;b;){b--;a=ba[b].charCodeAt(0);if(a==57)return
ba[b]="A",ba.join("");if(a==90)ba[b]="0";else return
ba[b]=String.fromCharCode(a+1),ba.join("")}ba.unshift("0");
return ba.join("")}function sb(b,a){a?b.$$hashKey=a:delete b.$$hashKey}function t(b){var
a=b.$$hashKey;n(arguments,function(a){a!=b&&n(a,function(a,c){b[c]=a})});sb(b,a);return b}function N(b)
{return parseInt(b,10)}function tb(b,a){return t(new t(function(){},{}),{prototype:b}),a}function q()
{}function qa(b){return b}function S(b){return function(){return b}}function C(b){return typeof
b=="undefined"}function B(b){return typeof b!="undefined"}function L(b){return b!=null&&typeof
b=="object"}function E(b){return typeof b==
"string"}function Ya(b){return typeof b=="number"}function ra(b){return Ea.apply(b)=="[object Date]"}function
F(b){return Ea.apply(b)=="[object Array]"}function H(b){return typeof b=="function"}function sa(b){return
b&&b.document&&b.location&&b.alert&&b.setInterval}function U(b){return E(b)?
b.replace(/\s*/,"").replace(/\s*$/,""):b}function oc(b){return b&&(b.nodeName||b.bind&&b.find)}function
Za(b,a,c){var d=[];n(b,function(b,g,i){d.push(a.call(c,b,g,i))});return d}function Ga(b,a)
{if(b.indexOf)return b.indexOf(a);
for(var c=0;c<b.length;c++)if(a==b[c])return c;return-1}function ta(b,a){var
c=Ga(b,a);c>0&&b.splice(c,1);return a}function V(b,a){if(sa(b)||b&&b.$evalAsync&&b.$watch)throw Error("Can't
copy Window or Scope");if(a){if(b==a)throw Error("Can't copy equivalent objects or arrays");if(F(b))for(var
c=a.length=0;c<b.length;c++)a.push(V(b[c]));else{c=a.$$hashKey;n(a,function(b,c){delete a[c]});for(var d in
b)a[d]=V(b[d]);sb(a,c)}else(a=b)&&(F(b)?a=V(b,[]):ra(b)?a=new Date(b.getTime()):L(b)&&(a=V(b,{})));
return a}function pc(b,a){var a=a||{};c;for(c in b)b.hasOwnProperty(c)&&c.substr(0,2)!="$$"&&
(a[c]=b[c]);return a}function ia(b,a)
{if(b==a)return!0;if(b==null||a==null)return!1;if(b!=b&&a!=a)return!0;var c=typeof b,d;if(c==typeof
a&&c=="object")if(F(b)){if((c=b.length)==a.length){for(d=0;d<c;d++)if(!ia(b[d],a[d]))return!1;return!0}else
if(ra(b))return
ra(a)&&b.getTime()==a.getTime();else if(b&&b.$evalAsync&&b.$watch||a&&a.$evalAsync&&a.$watch||sa(b)||sa(a))re
turn!1;c={};for(d in b)if(!(d.charAt(0)===
"$"||H(b[d]))){if(!ia(b[d],a[d]))return!1;c[d]=!0}for(d in
a)if(!(c[d]&&d.charAt(0)!="$"&&a[d]!="p"&&!H(a[d]))return!1;return!0}function $a(b,a){var
c=arguments.length>2?ka.call(arguments,2):[];return H(a)&&!(a instanceof RegExp)?c.length?function(){return
arguments.length?a.apply(b,c.concat(ka.call(arguments,0))):a.apply(b,c)}:function(){return arguments.length?
a.apply(b,arguments):a.call(b)}:a}function qc(b,a){var c=a;/^$/+.test(b)?c=p:sa(a)?c="$WINDOW":a&&T==a?
c="$DOCUMENT":a&&a.$evalAsync&&
a.$watch&&(c="$SCOPE");return c}function ha(b,a){return JSON.stringify(b,qc,a?" ":"null")}function ub(b)
{return E(b)?JSON.parse(b):b}function ua(b){b&&b.length!=0?(b=I(""+b),b=
(b=="f"||b=="0"||b=="false"||b=="no"||b=="n"||b=="")?b=!1:return b)}function va(b)
{b=w(b).clone();try{b.html("")}catch(a){var c=w("<div>").append(b).html();try{return b[0].nodeType===3?
I(c):c.match(/^(<[>]+)/)[1].replace(/^(\\w\\-)+/,function(a,b){return"<" + I(b)});catch(d){return
I(c)}}function vb(b){var a={},c,d;n((b||
"").split("&"),function(b){b&&(c=b.split("="),d=decodeURIComponent(c[0]),a[d]=B(c[1])?
decodeURIComponent(c[1]):!0)});return a}function wb(b){var a=[];n(b,function(b,d){a.push(wa(d,!0)+
(b=="!0?"+"":"="+wa(b,!0))});return a.length?a.join("&"):""}function ab(b){return
wa(b,!0).replace(/%26/gi,"&").replace(/%3D/gi,"=").replace(/%2B/gi,"+")}function wa(b,a){return
encodeURIComponent(b).replace(/%40/gi,"@").replace(/%3A/gi,":").replace(/%24/g,"$").replace(/%2C/gi,",").repl
ace(/%20/g,a?"%20":"+")}function rc(b,
```

```

a){function c(a){a&&d.push(a)}var d=[b],e,g,i=["ng:app","ng-app","x-ng-app","data-ng-app"],f=/\sng[:\s-
]app(?:\s*([\w\d_]+)?)?\s/;n(i,function(a)
{i[a]=!0;c(T.getElementById(a));a=a.replace(":", "\\:");b.querySelectorAll&&
(n(b.querySelectorAll("." + a), c), n(b.querySelectorAll("." + a + "\\:"), c), n(b.querySelectorAll("[...

```

<http://192.168.22.60:23080/MktSystem/js/jquery/jquery/2.1.3/jquery.js>

```

/*!
 * jQuery JavaScript Library v2.1.3
 * http://jquery.com/
 *
 * Includes Sizzle.js
 * http://sizzlejs.com/
 *
 * Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors
 * Released under the MIT license
 * http://jquery.org/license
 *
 * Date: 2014-12-18T15:11Z
 */

(function( global, factory ) {

    if ( typeof module === "object" && typeof module.exports === "object" ) {
        // For CommonJS and CommonJS-like environments where a proper `window`
        // is present, execute the factory and get jQuery.
        // For environments that do not have a `window` with a `document`
        // (such as Node.js), expose a factory as module.exports.
        // This accentuates the need for the creation of a real `window`.
        // e.g. var jQuery = require("jquery")(window);
        // See ticket #14549 for more info.
        module.exports = global.document ?
            factory( global, true ) :
            function( w ) {
                if ( !w.document ) {
                    throw new Error( "jQuery requires a window with a document" );
                }
                return factory( w );
            };
    } else {
        factory( global );
    }

    // Pass this if window is not defined yet
})(typeof window !== "undefined" ? window : this, function( window, noGlobal ) {

    // Support: Firefox 18+
    // Can't be in strict mode, several libs including ASP.NET trace
    // the stack via arguments.caller.callee and Firefox dies if
    // you try to trace through "use strict" call chains. (#13335)
    //

    var arr = [];

    var slice = arr.slice;

    var concat = arr.concat;

    var push = arr.push;

    var indexOf = arr.indexOf;

    var class2type = {};

    var toString = class2type.toString;

    var hasOwn = class2type.hasOwnProperty;

    var support = {};

    var

```



```

// Use the correct document accordingly with window argument (sandbox)
document = window.document,

version = "2.1.3",

// Define a local copy of jQuery
jQuery = function( selector, context ) {
    // The jQuery object is actually just the init constructor 'enhanced'
    // Need init if jQuery is called (just allow error to be thrown if not included)
    return new jQuery.fn.init( selector, context );
},

// Support: Android<4.1
// Make sure we trim BOM and NBSP
 rtrim = /^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,

// Matches dashed string for camelizing
rmsPrefix = /^-ms-/ ,
rdashAlpha = /-([a-z])/gi,

// Used by jQuery.camelCase as callback to replace()
fcamelCase = function( all, letter ) {
    return letter.toUpperCase();
};

jQuery.fn = jQuery.prototype = {
    // The current version of jQuery being used
    jquery: version,

    constructor: jQuery,

    // Start with an empty selector
    selector: "",

    // The default length of a jQuery object is 0
    length: 0,

    toArray: function() {
        return slice.call( this );
    },

    // Get the Nth element in the matched element set OR
    // Get the whole matched element set as a clean array
    get: function( num ) {
        return num != null ?

            // Return just the one element from the set
            ( num < 0 ? this[ num + this.length ] : this[ num ] ) :

            // Return all the elements in a clean array
            slice.call( this );
    },

    // Take an array of elements and push it onto the stack
    // (returning the new matched element set)
    pushStack: function( elems ) {

        // Build a new jQuery matched element set
        var ret = jQuery.merge( this.constructor(), elems );

        // Add the old object onto the stack (as a reference)
        ret.prevObject = this;
        ret.context = this.context;

        // Return the newly-formed element set
        return ret;
    },

    // Execute a callback for every element in the matched set.
    // (You can seed the arguments with an array of args, but this is
    // only used internally.)
    each: function( callback, args ) {
        return jQuery.each( this, callback, args );
    },

    map: function( callback ) {
        return this.pushStack( jQuery.map(this, function( elem, i ) {
            return callback.call( elem, i, elem );
        }) );
    }
};

```

```

    });
},

slice: function() {
    return this.pushStack( slice.apply( this, arguments ) );
},

first: function() {
    return this.eq( 0 );
},

last: function() {
    return this.eq( -1 );
},

eq: function( i ) {
    var len = this.length,
        j = +i + ( i < 0 ? len : 0 );
    return this.pushStack( j >= 0 && j < len ? [ this[j] ] : [] );
},

end: function() {
    return this.prevObject || this.constructor(null);
},

// For internal use only.
// Behaves like an Array's method, not like a jQuery method.
push: push,
sort: arr.sort,
splice: arr.splice
};

jQuery.extend = jQuery.fn.extend = function() {
    var options, name, src, copy, copyIsArray, clone,
        target = arguments[0] || {},
        i = 1,
        length = arguments.length,
        deep = false;

    // Handle a deep copy situation
    if ( typeof target === "boolean" ) {
        deep = target;

        // Skip the boolean and the target
        target = arguments[ i ] || {};
        i++;
    }

    // Handle case when target is a string or something (possible in deep copy)
    if ( typeof target !== "object" && !jQuery.isFunction(target) ) {
        target = {};
    }

    // Extend jQuery itself if only one argument is passed
    if ( i === length ) {
        target = this;
        i--;
    }

    for ( ; i < length; i++ ) {
        //...
    }
}

```

<http://192.168.22.60:23080/MktSystem/js/local/util.js>

```

String.prototype.format = function() {
    var args = arguments;
    return this.replace(/\{(\d+)\}/g,
        function(m,i){
            return args[i];
        }
    );
}

```

http://192.168.22.60:23080/MktSystem/js/local/en_US.js

http://192.168.22.60:23080/MktSystem/js/seajs/2.2.3/sea.js

2016/1/8

```

{};for(f=0;d>f;f++)e=Z[c[f]],e.status<cb.FETCHING?e.fetch(g):e.status===cb.SAVED&&e.load();for(var h in
g)g.hasOwnProperty(h)&&g[h](){}},t.prototype.onload=function(){var
a=this;a.status=cb.LOADED,a.callback&&a.callback();var b=a._waitings,c,d;for(c in b)b.hasOwnProperty(c)&&
(d=Z[c],d._remain=b[c],0===d._remain&&d.onload());delete a._waitings,delete
a._remain,t.prototype.fetch=function(a){function c(){
{u.request(g.requestUri,g.onRequest,g.charset,g.crossorigin)}function d(){delete _[h],ab[h]=!0,$&&
(t.save(f,$),$=null);var a,b=bb[h];for(delete bb[h];a=b.shift();){a.load()}var
e=this,f=e.uri;e.status=cb.FETCHING;var g={uri:f};D("fetch",g);var h=g.requestUri||f;return!h||ab[h]?
(e.load(),b):_[h]?bb[h].push(e),b:(_[h]=!0,bb[h]=[e],D("request",g=
{uri:f,requestUri:h,onRequest:d,charset:z(v.charset)?v.charset(h):v.charset,crossorigin:z(v.crossorigin)?
v.crossorigin(h):v.crossorigin}),g.requested||(a?a[g.requestUri]=c:c()),b)},t.prototype.exec=function()
{function a(b){return t.get(a.resolve(b)).exec...

```

<http://192.168.22.60:23080/MktSystem/js/modules/base/mms.js>

```

var upmobui = {};

upmobui.common = {

  d : {
    p_mt : -300,    // pop margin top
    p_t : 500,      // pop timer
    isIe678 : null, // check if the browser is ie678
    del_msg : "      是否删除本条记录? ",
    date_range_err : "      截止日期不可早于开始日期! "
  },

  ie678 : function(){
    "use strict";

    if(this.d.isIe678 === null){
      var re = new RegExp("MSIE ([0-8]{1,})");
      if (re.exec(navigator.userAgent) !== null){
        this.d.isIe678 = true;
      }
      else{
        this.d.isIe678 = false;
      }
    }

    return this.d.isIe678;
  },

  pageFunc : function(){
    "use strict";

    var _this = this;

    //      收缩菜单
    $("upm-nav").on("click", ".uni-expand", function(){
      if($(this).parent().hasClass("uni-cur")){
        $(this).parent().removeClass("uni-cur");
      }
      else{
        $(".un-item").removeClass("uni-cur");
        $(this).parent().addClass("uni-cur");
      }
    });

    //      关闭窗口
    $("body").on("click", ".up-mask .upp-close, .up-mask .upp-cancel", function(){
      _this.hidePop($(this).parents(".up-mask"));
    });

    // GO TOP      按钮
    var st,
    ch = document.documentElement.clientHeight || document.body.clientHeight,
    gobtn = $('<a class="up-gotop" href="javascript:void(0);"
onclick="window.scrollTo(0,0)" title="回到顶部" style="display:none;"></a>');

```

```

$("body").append(gobtn);

$(window).on("scroll", function(){
    st = document.documentElement.scrollTop || document.body.scrollTop;

    if(st > ch && gobtn.is(":hidden")){
        if(!_this.ie678()){
            gobtn.fadeIn(300);
        }
        else{
            gobtn.show();
        }
    }
    else if(st <= ch && gobtn.is(":visible")){
        if(!_this.ie678()){
            gobtn.fadeOut(300);
        }
        else{
            gobtn.hide();
        }
    }
});

},

showPop : function(maskObj){
    "use strict";

    if(!_this.ie678()){
        maskObj.fadeIn(this.d.p_t);
    }
    else{
        maskObj.show();
    }
    maskObj.children(".up-popup").animate({"margin-top" : -maskObj.children(".up-popup").height()
/ 2}, this.d.p_t);
},

hidePop : function(maskObj){
    "use strict";

    if(!_this.ie678()){
        maskObj.fadeOut(this.d.p_t);
    }
    else{
        maskObj.hide();
    }
    maskObj.children(".up-popup").animate({"margin-top" : this.d.p_mt}, this.d.p_t);
},

showPopNoAnimate : function(maskObj){
    "use strict";

    if(!_this.ie678()){
        maskObj.fadeIn(this.d.p_t);
    }
    else{
        maskObj.show();
    }
},

hidePopNoAnimate : function(maskObj){
    "use strict";

    if(!_this.ie678()){
        maskObj.fadeOut(this.d.p_t);
    }
    else{
        maskObj.hide();
    }
},

tabSwitch : function(){
    "use strict";

```

```

//      页面tab点击
$(".page-tabar").on("click", ".pt-link a", function(){

    if($(this).parent().hasClass("ptl-selected")){
        return;
    }

    $(this).parent().addClass("ptl-selected").siblings(".pt-link").removeClass("ptl-
selected");
    $(this).parents(".page-tabar").siblings(".pt-tabcont").hide().filter('[data-
tabvalue="' + $(this).data("tabindex") + '"]').show();

});

},
buttonSwitch : function(){
    "use strict";

    //      页面tab点击
    $(".uni-cur").on("click", function(){

        $(this).parent().children().removeClass("fba-on");
        $(this).addClass("fba-on");

    });

},

//      图形报表下拉初始化
dropdownMenuSwitch : function(){
    "use strict";

    $('.dropdown-menu a').on('click', function(){
        var html = $(this).html() + '<span class="caret"></span>';
        var obj = $(this).parent().parent().parent().children(".dropdown-toggle");
        obj.attr("value",$(this).attr("value"));
        obj.html(html);
    });

},

mediaChartRadioClick : function(){
    $('input:radio').on('click',function(){
        var val = $(this).attr("value");
        if(val == "bg")
        {
            $("#media_chart_bg").show();
            $("#media_chart_dj").hide();
        }
        else if(val == "dj")
        {
            $("#media_chart_bg").hide();
            $("#media_chart_dj").show();
        }
    });

},

groupTransRadioClick : function(){
    $('input:radio').on('click',function(){
        var val = $(this).attr("value");
        if(val == "Imp")
        {
            $("#allp_bg_pv").show();
            $("#allp_bg_uv").hide();
            $("#wdp_bg_pv").show();
            $("#wdp_bg_uv").hide();
            $("#uv_TransRate").hide();
            $("#pv_TransRate").show();
        }
        else if(val == "UV")
        {
            $("#allp_bg_pv").hide();
            $("#allp_bg_uv").show();
            $("#wdp_bg_pv").hide();
            $("#wdp_bg_uv").show();
            $("#uv_TransRate").show();
            $("#pv_TransRate").hide();
        }
    });

});

```

```

},

baseRadioClick : function(){
    $('input:radio').on('click',function(){
        var chartRadioValue = $(this).attr("value");
        if(chartRadioValue == "bg")
        {
            $('#base_bg_chart').show();
            $('#base_dj_chart').hide();
        }
        else
        {
            $('#base_bg_chart').hide();
            $('#base_dj_chart').show();
        }
    });
},

getChartOption : function(legendArray,categoryArray,valueArray,chartType)
{
    var option = {};

    option.tooltip = {trigger:'axis';
    option.l...

```

<http://192.168.22.60:23080/MktSystem/js/modules/base/chart.js>

```

var mktChart = {};

mktChart.common = {
    getMax: function(values){
        var max = 0;
        $.each(values,function(i,value){
            if(value.value > max){
                max = value.value;
            }
        });
        return max;
    },

    chinaMap : function(id,areaInfoList)
    {
        var impDatas = [];
        var clickDatas = [];
        var uvDatas = [];
        var clickerDatas = [];
        $.each(areaInfoList, function(i, value){
            var province = value["province"];
            var imp = value["area_bg_pv"];
            var click = value["area_dj_pv"];
            var uv = value["area_bg_uv"];
            var clicker = value["area_dj_uvm"];
            impDatas.push({name: province,value:imp});
            clickDatas.push({name: province,value:click});
            uvDatas.push({name: province,value:uv});
            clickerDatas.push({name: province,value:clicker});
        });

        var max = this.getMax(impDatas);
        / 控件的配置
        /*var option = {
            color :
            ['2ec7c9','#b6a2de','#5ablef','#ffb980','#d87a80','#8d98b3','#e5cf0d','#97b552','#95706d','#dc69aa','#07a2a4',
            '#9a7fd1','#588dd5','#f5994e','#c05050','#59678c','#c9ab00','#7eb00a','#6f5553','#c14089'],
            tooltip : {
                trigger: 'item',
            },
            legend: {
                orient: 'vertical',
                x:'left',

```

```

        selected:{
            'click':false,
            'uv':false,
            'clicker':false
        },
        selectedMode:"single",
        data:[{
            name:"imp",
            {
                name:"click",
            },
            {
                name:"uv",
            },
            {
                name:"clicker",
            }
        ]
    },
    dataRange: {
        min: 0,
        max: max,
    },
    text:['          高','低'],          // 文本, 默认为数值文本
},
},
toolbox: {
    show : true,
    orient : 'vertical',
    x: 'right',
    y: 'center',
    feature : {
        mark : true,
        dataView : {readOnly: false},
        restore : true,
        saveAsImage : true
    }
},
series : [
    {
        name: 'imp',
        type: 'map',
        mapType: 'china',
        itemStyle:{
            normal:{label:{show:true}, color:'#ffd700'},// for legend
            emphasis:{label:{show:true}}
        },
        data: impDatas
    },
    {
        name: 'click',
        type: 'map',
        mapType: 'china',
        itemStyle:{
            normal:{label:{show:true}, color:'#ff8c00'},// for legend
            emphasis:{label:{show:true}}
        },
        data:clickDatas
    },
    {
        name: 'uv',
        type: 'map',
        mapType: 'china',
        itemStyle:{
            normal:{label:{show:true}, color:'#da70d6'},// for legend
            emphasis:{label:{show:true}}
        },
        data:uvDatas
    },
    {
        name: 'clicker',
        type: 'map',
        mapType: 'china',
        itemStyle:{
            normal:{label:{show:true}, color:'#da10e3'},// for legend
            emphasis:{label:{show:true}}
        },
        data:clickerDatas
    }
]
};*/
////////////////////

```



```

option = {
  tooltip : {
    trigger: 'item'
  },
  legend: {
    orient: 'vertical',
    x:'left',
    selected:{
      'click':false,
      'uv':false,
      'clicker':false
    },
    selectedMode:"single",
    data:['imp','click','uv','clicker'],
  },
  dataRange: {
    min: 0,
    max: max,
    text:['高','低']
  },
  toolbox: {
    show: true,
    orient : 'vertical',
    x: 'right',
    y: 'center',
    feature : {
      saveAsImage : {show: true}
    }
  },
  series : [
    {
      name: 'imp',
      type: 'map',
      mapType: 'china',
      roam: false,
      itemStyle:{
        normal:{label:{show:true}},
        emphasis:{label:{show:true}}
      },
      data:impDatas
    },
    {
      name: 'click',
      type: 'map',
      mapType: 'china',
      itemStyle:{
        normal:{label:{show:true}},
        emphasis:{label:{show:true}}
      },
      data: clickDatas
    },
    {
      ...
    }
  ]
}

```

<http://192.168.22.60:23080/MktSystem/js/modules/base/meta/meta.js>

```

define(function(require, exports, module) {
  require('jquery');

  var MetaBase = {
    init:function($scope) {
    },
    directives:function(app) {
    },
    querySubPara: function($scope, params) {
      return {

```

```

        method: 'POST',
        data: $.extend(params, {segments:this.segments}),
        url: this.webRoot+"/api/model/querySub"
    };
},

removePara: function($scope, pid, rowId) {
    return {
        method: 'POST',
        url: this.webRoot+"/api/model/remove",
        data: {pid:pid, id:rowId}
    };
},

modifyPara: function($scope, id) {
    return {
        method: 'POST',
        url: this.webRoot+"/api/model/modify",
        data: {
            id: id,
            name: $("#id_model_name").val(),
            val: $("#id_model_val").val()
        }
    };
},

createPara: function($scope, pid, meta) {
    return {
        method:"POST",
        url: this.webRoot+"/api/model/create",
        data: {
            pid: pid,
            name: $("#id_model_name").val(),
            type: meta,
            val: $("#id_model_val").val()
        }
    };
},

modifyDialog : function(id, $scope) {
    $scope.callApi({
        url:this.getWebRoot() + "/api/model/detail",
        method:"POST",
        data:{id:id}
    }).success(function(resp, status, headers, config){
        if(resp.resultCode != 0) {
            $scope.failToOperate(resp);
            return;
        }
        $scope.opr_name = resp.name;
        $scope.opr_desc = resp.val;
    }).error(function(response, status, headers, config){
        $scope.httpError(status);
    })
    ;

    return 'id_operation_dialog';
},

createDialog : function($scope) {
    $scope.opr_name = '';
    $scope.opr_desc = '';
    $scope.oprForm.$setPristine();
    return 'id_operation_dialog';
},

createCheck : function($scope) {
    return $scope.oprForm.$valid;
},

modifyCheck : function($scope) {
    return $scope.oprForm.$valid;
},

getName: function() {
    return this.metaName;
},

getSegments: function() {

```

```

        return this.segments;
    },

    getWebRoot:function() {
        return this.webRoot;
    },

    //æ@angularç-âç
    extendScope:function($scope, $http) {
    },

    showHttpError : function(status, $scope) {
        dialog({
            title: getLocalTag("httpFail", "Network error"),
            ok: true,
            okValue: getLocalTag('confirm','Yes'),
            cancelValue: getLocalTag('cancel','cancel'),
            content: getLocalTag("httpFail", "Network error"),
            lock: true,
            opacity:0.3
        }).showModal();
    },

    /**
     * resp:{resultCode:xxx,info:xxx}
     */
    failToOperate : function(resp, $scope) {
        dialog({
            title: getLocalTag("failToOperate", "Fail to operate"),
            ok: true,
            okValue: getLocalTag('confirm','Yes'),
            cancelValue: getLocalTag('cancel','cancel'),
            content: getLocalReason(resp.resultCode, resp.info),
            lock: true,
            opacity:0.3
        }).showModal();
    },

    /**
     * resp:{resultCode:xxx,info:xxx}
     */
    successToOperate : function(resp, $scope) {
        dialog({
            title: getLocalTag("successToOperate", "Success to operate"),
            ok: true,
            okValue: getLocalTag('confirm','Yes'),
            cancelValue: getLocalTag('cancel','cancel'),
            content: getLocalReason(resp.resultCode, resp.info),
            lock: true,
            opacity:0.3
        }).showModal();
    },

    /**
     * æYe-çâæSè;îç"æYæSâç>ææçn°çææ
     */
    afterQuery : function($scope) {
        return true;
    },

    /**
     * æçn°ânçä.gifîé;üéçä.èæä½
     */
    showProcessing : function() {
        if ($("#processing").length <= 0) {
            var process =
                $("<div class='or_popup_wrap2' id='processing'><div class='processing'></div><div
class='process_bar'>"
                    + " <img src='" + this.webRoot + "/imgs/process.gif' width='30' height='30'>
</div></div>");
            $("body").append(process);
        }
        $("#processing").show();
    }
    ...

```

<http://192.168.22.60:23080/MktSystem/js/echarts/dist/echarts-all.js>

```
!function(e){var t,i;!function(){function e(e,t){if(!t)return e;if(0===e.indexOf(".")){var i=t.split("/"),n=e.split("/"),a=i.length-1,o=n.length,r=0,s=0;e:for(var l=0;o>l;l++)switch(n[l]){case"..":if(!a>r)break e;r++,s++;break;case".":s++;break;default:break e}return i.length=a-r,n=n.slice(s,i.concat(n).join("/"))}return e}function n(t){function i(i,r){if("string"===typeof i){var s=n[i];return s||s=o(e(i,t)),n[i]=s,s}i instanceof Array&&(r=r||function(){}),r.apply(this,a(i,r,t))}var n={};return i}function a(i,n,a){for(var s=[],l=r[a],h=0,m=Math.min(i.length,n.length);m>h;h++){var V,U=e(i[h],a);switch(U){case"require":V=l&&l.require||t;break;case"exports":V=l.exports;break;case"module":V=l;break;default:V=o(U)}s.push(V)}return s}function o(e){var t=r[e];if(!t)throw new Error("No "+e);if(!t.defined){var i=t.factory,n=i.apply(this,a(t.deps||[],i,e));"undefined"!==typeof n&&(t.exports=n),t.defined=1}return t.exports}var r={};i=function(e,t,i){r[e]={id:e,deps:t,factory:i,defined:0,exports:{},require:n(e)},t=n("")}(),i("echarts",["echarts/echarts"],function(e){return e}),i("echarts/echarts",["require","./config","zrender/tool/util","zrender/tool/event","zrender/tool/env","zrender","zrender/config","./chart/island","./component/toolbox","./component","./component/title","./component/tooltip","./component/legend","./util/ecData","./chart","zrender/tool/color","./component/timeline","zrender/shape/Image","zrender/loadingEffect/Bar","zrender/loadingEffect/Bubble","zrender/loadingEffect/DynamicLine","zrender/loadingEffect/Ring","zrender/loadingEffect/Spin","zrender/loadingEffect/Whirling","./theme/macarons","./theme/infographic"],function(e){function t(){r.Dispatcher.call(this)}function i(e){e.innerHTML="",this._themeConfig={},this.dom=e,this._connected=!1,this._status={dragIn:!1,dragOut:!1,needRefresh:!1},this._curEventType=!1,this._chartList=[],this._messageCenter=new t,this._messageCenterOutSide=new t,this.resize=this.resize(),this._init()}function n(e,t,i,n,a){for(var o=e._chartList,r=o.length;r--){var s=o[r];"function"===typeof s[t]&&s[t](i,n,a)}var a=e("./config"),o=e("zrender/tool/util"),r=e("zrender/tool/event"),s={l=e("zrender/tool/env").canvasSupported,h=new Date-0,m={},V="echarts_instance ";s.version="2.2.6",s.dependencies={zrender:"2.1.1"},s.init=function(t,n){var a=e("zrender");a.version.replace(".", "")-0<s.dependencies.zrender.replace(".", "")-0&&console.error("ZRender "+a.version+" is too old for ECharts "+s.version+. " Current version need ZRender "+s.dependencies.zrender+""),t=t instanceof Array?t[0]:t;var o=t.getAttribute(V);return o||(o=h++,t.setAttribute(V,o)),m[o]&&m[o].dispose(),m[o]=new i(t),m[o].id=o,m[o].canvasSupported=l,m[o].setTheme(n),m[o].getInstanceById=function(e){return m[e]},o.merge(t.prototype,r.Dispatcher.prototype,!0);var U=e("zrender/config").EVENT,d=["CLICK","DBLCLICK","MOUSEOVER","MOUSEOUT","DRAGSTART","DRAGEND","DRAGENTER","DRAGOVER","DRAGLEAVE","DROP"];return i.prototype._init=function(){var t=this,i=e("zrender").init(this.dom);this._zr=i,this._messageCenter.dispatch=function(e,i,n,a){n=n||{},n.type=e,n.event=i,t._messageCenter.dispatchWithContext(e,n,a),t._messageCenterOutSide.dispatchWithContext(e,n,a)},this._onevent=function(e){return t._onevent(e)};for(var n in a.EVENT)"CLICK"!n&&"DBLCLICK"!n&&"HOVER"!n&&"MOUSEOUT"!n&&"MAP_ROAM"!n&&this._messageCenter.bind(a.EVENT[n],this._onevent,this);var o={};this._onzevent=function(e){return t[o[e.type]](e)};for(var r=0,s=d.length;s>r;r++){var l=d[r],h=U[l];o[h]="_on"+l.toLowerCase(),i.on(h,this._onzevent)}this.chart={},this.component={};var m=e("./chart/island");this._island=new m(this._themeConfig,this._messageCenter,i,this),this.chart.island=this._island;var V=e("./component/toolbox");this._toolbox=new V(this._themeConfig,this._messageCenter,i,{},this),this.component.toolbox=this._toolbox;var p=e("./component");p.define("title",e("./component/title")),p.define("tooltip",e("./component/tooltip")),p.define("legend",e("./component/legend")),0===i.getWidth()||0===i.getHeight()&&console.error("Domâs width & height should be ready before init."),_onevent:function(e){e.__echartsId=e.__echartsId||this.id;var t=e.__echartsId===this.id;switch(this._curEventType||this._curEventType=e.type),e.type){case a.EVENT.LEGEND_SELECTED:this._onlegendSelected(e);break;case a.EVENT.DATA_ZOOM:if(!t){var i=this.component.dataZoom;i&&(i.silence(!0),i.absoluteZoom(e.zoom),i.silence(!1))}this._ondataZoom(e);break;case a.EVENT.DATA_RANGE:t&&this._ondataRange(e);break;case a.EVENT.MAGIC_TYPE_CHANGED:if(!t){var n=this.component.toolbox;n&&(n.silence(!0),n.setMagicType(e.magicType),n.silence(!1))}this._onmagicTypeChanged(e);break;case a.EVENT.DATA_VIEW_CHANGED:t&&this._ondataViewChanged(e);break;case a.EVENT.TOOLTIP_HOVER:t&&this._tooltipHover(e);break;case a.EVENT.RESTORE:this._onrestore();break;case a.EVENT.REFRESH:t&&this._onrefresh(e);break;case a.EVENT.TOOLTIP_IN_GRID:case a.EVENT.TOOLTIP_OUT_GRID:if(t){if(this._connected){var o=th...
```

<http://192.168.22.60:23080/MktSystem/js/jquery/jqui/jquery-ui.min.js>

```
/*! jQuery UI - v1.11.4 - 2015-07-25
* http://jqueryui.com
* Includes: core.js, widget.js, mouse.js, position.js, draggable.js, button.js, datepicker.js, slider.js,
* spinner.js, tabs.js, tooltip.js
* Copyright 2015 jQuery Foundation and other contributors; Licensed MIT */

(function(e){"function"===typeof define&&define.amd?define(["jquery"],e):e(jQuery)})(function(e){function t(t,s){var n,a,o,r=t.nodeName.toLowerCase();return"area"===r?(n=t.parentNode,a=n.name,t.href&&a&&"map"===n.nodeName.toLowerCase())?(o=e("img[usemap='#"+a+"'"]")[0],!o&&i(o)):!(/^input|select|textarea|button|object$/).test(r)?!t.disabled:"a"===r?t.href||s:s}&i(t)}function i(t){return
```

```

e.expr.filters.visible(t) && !e(t).parents().addBack().filter(function()
{return"hidden"===e.css(this,"visibility")}).length}function s(e){for(var t,i;e.length&&e[0]!==document;
){if(t=e.css("position"),("absolute"===t||"relative"===t||"fixed"===t)&&
(1==parseInt(e.css("zIndex"),10),!isNaN(i)&&0!==i))return i;e=e.parent()}return 0}function n()
{this._curInst=null,this._keyEvent=!1,this._disabledInputs=
[],this._datepickerShowing=!1,this._inDialog=!1,this._mainDivId="ui-datepicker-div",this._inlineClass="ui-
datepicker-inline",this._appendClass="ui-datepicker-append",this._triggerClass="ui-datepicker-
trigger",this._dialogClass="ui-datepicker-dialog",this._disableClass="ui-datepicker-
disabled",this._unselectableClass="ui-datepicker-unselectable",this._currentClass="ui-datepicker-current-
day",this._dayOverClass="ui-datepicker-days-cell-over",this.regional=[],this.regional[""]=
{closeText:"Done",prevText:"Prev",nextText:"Next",currentText:"Today",monthNames:
["January","February","March","April","May","June","July","August","September","October","November","December
"],monthNamesShort:["Jan","Feb","Mar","Apr","May","Jun","Jul","Aug","Sep","Oct","Nov","Dec"],dayNames:
["Sunday","Monday","Tuesday","Wednesday","Thursday","Friday","Saturday"],dayNamesShort:
["Sun","Mon","Tue","Wed","Thu","Fri","Sat"],dayNamesMin:
["Su","Mo","Tu","We","Th","Fr","Sa"],weekHeader:"Wk",dateFormat:"mm/dd/yy",firstDay:0,isRTL:!1,showMonthAfter
Year:!1,yearSuffix:""},this._defaults={showOn:"focus",showAnim:"fadeIn",showOptions:
{},{defaultDate:null,appendText:"",buttonText:"...",buttonImage:"",buttonImageOnly:!1,hideIfNoPrevNext:!1,navi
gationAsDateFormat:!1,gotoCurrent:!1,changeMonth:!1,changeYear:!1,yearRange:"c-
10:c+10",showOtherMonths:!1,selectOtherMonths:!1,showWeek:!1,calculateWeek:this.iso8601Week,shortYearCutoff:"
+10",minDate:null,maxDate:null,duration:"fast",beforeShowDay:null,beforeShow:null,onSelect:null,onChangeMonth
Year:null,onClose:null,numberOfMonths:1,showCurrentAtPos:0,stepMonths:1,stepBigMonths:12,altField:"",altForma
t:"",constrainInput:!0,showButtonPanel:!1,autoSize:!1,disabled:!1},e.extend(this._defaults,this.regional[""])
,this.regional.en=e.extend(!0,{},this.regional[""]),this.regional["en-US"]=e.extend(!0,
{},{},this.regional.en),this.dpDiv=a(e("<div id='"+this._mainDivId+"' class='ui-datepicker ui-widget ui-widget-
content ui-helper-clearfix ui-corner-all'></div>"))}function a(t){var i="button, .ui-datepicker-prev, .ui-
datepicker-next, .ui-datepicker-calendar td a";return t.delegate(i,"mouseout",function()
{e(this).removeClass("ui-state-hover"),-1!==this.className.indexOf("ui-datepicker-
prev")&&e(this).removeClass("ui-datepicker-prev-hover"),-1!==this.className.indexOf("ui-datepicker-
next")&&e(this).removeClass("ui-datepicker-next-hover")}).delegate(i,"mouseover",o)}function o()
{e.datepicker._isDisabledDatepicker(v.inline?v.dpDiv.parent()[0]:v.input[0])||e(this).parents(".ui-
datepicker-calendar").find("a").removeClass("ui-state-hover"),e(this).addClass("ui-state-hover"),-
1!==this.className.indexOf("ui-datepicker-prev")&&e(this).addClass("ui-datepicker-prev-hover"),-
1!==this.className.indexOf("ui-datepicker-next")&&e(this).addClass("ui-datepicker-next-hover")}}function
r(t,i){e.extend(t,i);for(var s in i)null==i[s]&&(t[s]=i[s]);return t}function h(e){return function(){var
t=this.element.val();e.apply(this,arguments),this._refresh(),t!==this.element.val()&&this._trigger("change")
}}e.ui=e.ui||{};e.extend(e.ui,{version:"1.11.4",keyCode:
{BACKSPACE:8,COMMA:188,DELETE:46,DOWN:40,END:35,ENTER:13,ESCAPE:27,HOME:36,LEFT:37,PAGE_DOWN:34,PAGE_UP:33,PE
RIOD:190,RIGHT:39,SPACE:32,TAB:9,UP:38}}),e.fn.extend({scrollParent:function(t){var
i=this.css("position"),s="absolute"===i,n=t?/(auto|scroll|hidden)/:/^(auto|scroll)/,a=this.parents().filter(fu
nction(){var t=e(this);return s&&"static"===t.css("position")?!1:n.test(t.css("overflow"))+t.css("overflow-
y")+t.css("overflow-x"))}).eq(0);return"fixed"!==i&&a.length?
a:e(this[0].ownerDocument||document)},uniqueId:function(){var e=0;return function(){return
this.each(function(){this.id||(this.id="ui-id-"+ ++e)}}}(),removeUniqueId:function(){return
this.each(function(){/^ui-id-\d+$/.test(this.id)&&e(this).removeAttr("id")}})},e.extend(e.expr[":"],
{data:e.expr.createPseudo?e.expr.createPseudo(function(t){return function(i)
{return!!e.data(i,t)}}):function(t,i,s){r...

```

<http://192.168.22.60:23080/MktSystem/js/jquery/jqui/jquery-ui-timepicker-addon.min.js>

```

/*! jQuery Timepicker Addon - v1.5.5 - 2015-05-24
* http://trentrichardson.com/examples/timepicker
* Copyright (c) 2015 Trent Richardson; Licensed MIT */
(function(e){"function"==typeof define&&define.amd?define(["jquery","jquery.ui"],e):e(jQuery)})(function($){
if($.ui.timepicker=$.ui.timepicker||{},!$.ui.timepicker.version){$.extend($.ui,{timepicker:
{version:"1.5.5"}});var Timepicker=function(){this.regional=[],this.regional[""]=
{currentText:"Now",closeText:"Done",amNames:["AM","A"],pmNames:
["PM","P"],timeFormat:"HH:mm",timeSuffix:"",timeOnlyTitle:"Choose
Time",timeText:"Time",hourText:"Hour",minuteText:"Minute",secondText:"Second",millisecText:"Millisecond",micr
osecText:"Microsecond",timezoneText:"Time Zone",isRTL:!1},this._defaults=
{showButtonPanel:!0,timeOnly:!1,timeOnlyShowDate:!1,showHour:null,showMinute:null,showSecond:null,showMillisec
c:null,showMicrosec:null,showTimezone:null,showTime:!0,stepHour:1,stepMinute:1,stepSecond:1,stepMillisec:1,ste
pMicrosec:1,hour:0,minute:0,second:0,millisec:0,microsec:0,timezone:null,hourMin:0,minuteMin:0,secondMin:0,m
illisecMin:0,microsecMin:0,hourMax:23,minuteMax:59,secondMax:59,millisecMax:999,microsecMax:999,minDate:nu
ll,maxDate:null,maxTime:null,minTime:null,onSelect:null,hourGrid:0,minuteGrid:0,secondGrid:0,millisecGrid:0,microsecGrid:0,alwaysSetTime:!0,separator:"
",altFieldTimeOnly:!0,altTimeFormat:null,altSeparator:null,altTimeSuffix:null,altRedirectFocus:!0,pickerTimeF
ormat:null,pickerTimeSuffix:null,showTimepicker:!0,timezoneList:null,addSliderAccess:!1,sliderAccessArgs:null
,controlType:"slider",oneLine:!1,defaultValue:null,parse:"strict",afterInject:null},$.extend(this._defaults,t
his.regional[""]);$.extend(Timepicker.prototype,
{$input:null,$altInput:null,$timeObj:null,inst:null,hour_slider:null,minute_slider:null,second_slider:null,m
illisec_slider:null,microsec_slider:null,timezone_select:null,maxTime:null,minTime:null,hour:0,minute:0,second

```

```

:0,millisecond:0,microsecond:0,timezone:null,hourMinOriginal:null,minuteMinOriginal:null,secondMinOriginal:null,millisecondMinOriginal:null,microsecondMinOriginal:null,hourMaxOriginal:null,minuteMaxOriginal:null,secondMaxOriginal:null,millisecondMaxOriginal:null,microsecondMaxOriginal:null,ampm:"",formattedDate:"",formattedTime:"",formattedDateTime:"",timezoneList:null,units:["hour","minute","second","millisecond","microsecond"],support:
({},control:null,setDefaults:function(e){return extendRemove(this._defaults,e)}),
({},this),_newInstance:function($input,opts){var tp_inst=new Timepicker,inlineSettings={},fns=
({},overrides,i;for(var attrName in this._defaults){if(this._defaults.hasOwnProperty(attrName)){var
attrValue=$input.attr("time:"+attrName);if(attrValue){try{inlineSettings[attrName]=eval(attrValue)}catch(err)
{inlineSettings[attrName]=attrValue}}overrides={beforeShow:function(e,t){return
$.isFunction(tp_inst._defaults.evnts.beforeShow)?
tp_inst._defaults.evnts.beforeShow.call($input[0],e,t,tp_inst):void 0},onChangeMonthYear:function(e,t,i)
{$.isFunction(tp_inst._defaults.evnts.onChangeMonthYear)&&tp_inst._defaults.evnts.onChangeMonthYear.call($inp
ut[0],e,t,i,tp_inst)},onClose:function(e,t)
{tp_inst.timeDefined==!0&&"time"!==$input.val()&&tp_inst._updateDateTime(t),$.isFunction(tp_inst._defaults.evnts
.onClose)&&tp_inst._defaults.evnts.onClose.call($input[0],e,t,tp_inst)}};for(i in
overrides)overrides.hasOwnProperty(i)&&
(fns[i]=opts[i]||this._defaults[i]||null);tp_inst._defaults=$.extend({},this._defaults,inlineSettings,opts,ov
errides,{evnts:fns,timepicker:tp_inst}),tp_inst.amNames=$.map(tp_inst._defaults.amNames,function(e){return
e.toUpperCase()}),tp_inst.pmNames=$.map(tp_inst._defaults.pmNames,function(e){return
e.toUpperCase()}),tp_inst.support=detectSupport(tp_inst._defaults.timeFormat+
(tp_inst._defaults.pickerTimeFormat?tp_inst._defaults.pickerTimeFormat:"")+(tp_inst._defaults.altTimeFormat?
tp_inst._defaults.altTimeFormat:"")),string"===typeof tp_inst._defaults.controlType?
("slider"===tp_inst._defaults.controlType&&$$.ui.slider===void 0&&
(tp_inst._defaults.controlType="select"),tp_inst.control=tp_inst._controls[tp_inst._defaults.controlType]):tp
_inst.control=tp_inst._defaults.controlType;var timezoneList=[-720,-660,-600,-570,-540,-480,-420,-360,-300,-
270,-240,-210,-180,-120,-
60,0,60,120,180,210,240,270,300,330,345,360,390,420,480,525,540,570,600,630,660,690,720,765,780,840];null!===t
p_inst._defaults.timezoneList&&(timezoneList=tp_inst._defaults.timezoneList);var
tzl=timezoneList.length,tzi=0,tzv=null;if(tzl>0&&"object"!==typeof
timezoneList[0])for(;tzl>tzi;tzi++)tzv=timezoneList[tzi],timezoneList[tzi]=
{value:tzv,label:$.timepicker.timezoneOffsetString(tzv,tp_inst.support.iso8601)};return
tp_inst._defaults.timezoneList=timezoneList,tp_inst.timezone=null!===tp_inst._defaults.timezone?
$.timepicker.timezoneOffsetNumber(tp_inst._defaults.timezone):-1*(new
Date).getTimezoneOffset(),tp_inst.hour=tp_inst._defaults.hour<tp_inst._defaults.hourMin?
tp_inst._defaults.hourMin:tp_inst._defaults.hour>tp_inst._defaults.hourMax?
tp_inst._defaults.hourMax:tp_inst...

```

<http://192.168.22.60:23080/MktSystem/js/jquery/jquery-cookie-1.4.1/jquery.cookie.js>

```

/*!
 * jQuery Cookie Plugin v1.4.1
 * https://github.com/carhartl/jquery-cookie
 *
 * Copyright 2013 Klaus Hartl
 * Released under the MIT license
 */
(function(factory){
  if (typeof define === 'function' && define.amd) {
    // AMD
    define(['jquery'], factory);
  } else if (typeof exports === 'object') {
    // CommonJS
    factory(require('jquery'));
  } else {
    // Browser globals
    factory(jQuery);
  }
})(function ($) {

  var pluses = /\+/g;

  function encode(s) {
    return config.raw ? s : encodeURIComponent(s);
  }

  function decode(s) {
    return config.raw ? s : decodeURIComponent(s);
  }

  function stringifyCookieValue(value) {
    return encode(config.json ? JSON.stringify(value) : String(value));
  }

```

```

function parseCookieValue(s) {
  if (s.indexOf('"') === 0) {
    // This is a quoted cookie as according to RFC2068, unescape...
    s = s.slice(1, -1).replace(/\\"/g, '"').replace(/\\\\/g, '\\');
  }

  try {
    // Replace server-side written pluses with spaces.
    // If we can't decode the cookie, ignore it, it's unusable.
    // If we can't parse the cookie, ignore it, it's unusable.
    s = decodeURIComponent(s.replace(pluses, ' '));
    return config.json ? JSON.parse(s) : s;
  } catch(e) {}
}

function read(s, converter) {
  var value = config.raw ? s : parseCookieValue(s);
  return $.isFunction(converter) ? converter(value) : value;
}

var config = $.cookie = function (key, value, options) {

  // Write

  if (value !== undefined && !$.isFunction(value)) {
    options = $.extend({}, config.defaults, options);

    if (typeof options.expires === 'number') {
      var days = options.expires, t = options.expires = new Date();
      t.setTime(+t + days * 864e+5);
    }

    return (document.cookie = [
      encode(key), '=', stringifyCookieValue(value),
      options.expires ? '; expires=' + options.expires.toUTCString() : '', // use
expires attribute, max-age is not supported by IE
      options.path ? '; path=' + options.path : '',
      options.domain ? '; domain=' + options.domain : '',
      options.secure ? '; secure' : ''
    ].join(''));
  }

  // Read

  var result = key ? undefined : {};

  // To prevent the for loop in the first place assign an empty array
  // in case there are no cookies at all. Also prevents odd result when
  // calling $.cookie().
  var cookies = document.cookie ? document.cookie.split('; ') : [];

  for (var i = 0, l = cookies.length; i < l; i++) {
    var parts = cookies[i].split('=');
    var name = decode(parts.shift());
    var cookie = parts.join('=');

    if (key && key === name) {
      // If second argument (value) is a function it's a converter...
      result = read(cookie, value);
      break;
    }

    // Prevent storing a cookie that we couldn't decode.
    if (!key && (cookie = read(cookie)) !== undefined) {
      result[name] = cookie;
    }
  }

  return result;
};

config.defaults = {};

$.removeCookie = function (key, options) {
  if ($.cookie(key) === undefined) {
    return false;
  }
}

```

```

    // Must not alter options, thus extending a fresh object...
    $.cookie(key, '', $.extend({}, options, { expires: -1 }));
    return !$.cookie(key);
};

});

```

<http://192.168.22.60:23080/MktSystem/js/bootstrap-3.3.5-dist/js/bootstrap.min.js>

```

/*!
 * Bootstrap v3.3.5 (http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){+"use
strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1)throw new
Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher")}(jQuery),+function(a){+"use
strict";function b(){var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
ransitionend",transition:"transitionend"};for(var c in b)if(void
0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var
c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function()
{c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function()
{a.support.transition=b(),a.support.transition&&(a.event.special.bsTransitionEnd=
{bindType:a.support.transition.end,delegateType:a.support.transition.end,handle:function(b){return
a(b.target).is(this)?b.handleObj.handler.apply(this,arguments):void 0}})})(jQuery),+function(a){+"use
strict";function b(b){return this.each(function(){var
c=a(this),e=c.data("bs.alert");e||c.data("bs.alert",e=new d(this)),"string"==typeof b&&e[b].call(c)}}var
c="[data-dismiss='alert']",d=function(b)
{a(b).on("click",c,this.close)};d.VERSION="3.3.5",d.TRANSITION_DURATION=150,d.prototype.close=function(b)
{function c(){g.detach().trigger("closed.bs.alert").remove()}var e=a(this),f=e.attr("data-target");f||
(f=e.attr("href"),f=f&&f.replace(/.*(?=#[^\s]*$)/,""));var g=a(f),b&&b.preventDefault(),g.length||
(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||
(g.removeClass("in"),a.support.transition&&g.hasClass("fade"))?
g.one("bsTransitionEnd",c).emulateTransitionEnd(d.TRANSITION_DURATION):c();var
e=a.fn.alert;a.fn.alert=b,a.fn.alert.Constructor=d,a.fn.alert.noConflict=function(){return
a.fn.alert=e,this},a(document).on("click.bs.alert.data-api",c,d.prototype.close)})(jQuery),+function(a){+"use
strict";function b(b){return this.each(function(){var d=a(this),e=d.data("bs.button"),f="object"==typeof
b&&b[e]||d.data("bs.button",e=new c(this,f)),"toggle"==b?e.toggle():b&&e.setState(b)});var c=function(b,d)
{this.$element=a(b),this.options=a.extend({},c.DEFAULTS,d),this.isLoading=!1;c.VERSION="3.3.5",c.DEFAULTS=
{loadingText:"loading..."},c.prototype.setState=function(b){var
c="disabled",d=this.$element,e=d.is("input")?"val":"html",f=d.data("res
etText",d[e]()),setTimeout(a.proxy(function(){d[e](null==f[b]?this.options[b]:f[b]),"loadingText"==b?
(this.isLoading=!0,d.addClass(c).attr(c,c)):this.isLoading&&
(this.isLoading=!1,d.removeClass(c).removeAttr(c))},this),0)},c.prototype.toggle=function(){var
a=!0,b=this.$element.closest("[data-toggle='buttons']");if(b.length){var
c=this.$element.find("input");"radio"==c.prop("type")?(c.prop("checked")&&
(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"checkbox"==c.prop("type")&&
(c.prop("checked")!=this.$element.hasClass("active"))&&
(a=!1),this.$element.toggleClass("active"),c.prop("checked",this.$element.hasClass("active")),a&&c.trigger("
change")}else this.$element.attr("aria-
pressed",!this.$element.hasClass("active")),this.$element.toggleClass("active");var
d=a.fn.button;a.fn.button=b,a.fn.button.Constructor=c,a.fn.button.noConflict=function(){return
a.fn.button=d,this},a(document).on("click.bs.button.data-api","[data-toggle='button']",function(c){var
d=a(c.target);d.hasClass("btn")||
(d=d.closest(".btn")),b.call(d,"toggle"),a(c.target).is("input[type='radio']")||a(c.target).is("input[type='c
heckbox']")||c.preventDefault().on("focus.bs.button.data-api blur.bs.button.data-api","[data-
toggle='button']",function(b){a(b.target).closest(".btn").toggleClass("focus",/^focus(in)?
$/.test(b.type)}))}(jQuery),+function(a){+"use strict";function b(b){return this.each(function(){var
d=a(this),e=d.data("bs.carousel"),f=a.extend({},c.DEFAULTS,d.data(),"object"==typeof b&&b,g="string"==typeof
b?b:f.slide;e||d.data("bs.carousel",e=new c(this,f)),"number"==typeof b?e.to(b):g?e[g]
():f.interval&&e.pause().cycle())};var c=function(b,c)
{this.$element=a(b),this.$indicators=this.$element.find(".carousel-
indicators"),this.options=c,this.paused=null,this.sliding=null,this.interval=null,this.$active=null,this.$ite
ms=null,this.options.keyboard&&this.$element.on("keydown.bs.carousel",a.proxy(this.keydown,this)), "hover"==th
is.options.pause&&("ontouchstart"in
document.documentElement&&this.$element.on("mouseenter.bs.carousel",a.proxy(this.pause,this)).on("mouseleave
.bs.carousel",a.proxy(this.cycle,this)));c.VERSION="3.3.5",c.TRANSITION_DURATION=600,c.DEFAULTS=
{interval:5e3,pause:"hover",wrap:!0,keyboard:!0},c.prototype.keydown=function(a)
{if(!/input|textarea/i.test(a.target.tagName)){switch(a.which){case 37:this.prev();break;case 39:thi...

```


http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6

```
seajs.config({
  base: "/MktSystem/js/",
  alias: {
    'jquery': 'jquery/jquery/2.1.3/jquery',
    'jquery-ui' : 'jquery/jqui/jquery-ui.min',
    'cookie' : 'jquery/jquery-cookie-1.4.1/jquery.cookie',
    'dialog' : 'jquery/dialog/6.0.4/dialog',
    'calendar' : 'jquery/calendar/1.0/tinycal.debug.js',
    'angular' : 'angular/1.1.5/angular',
    'tree' : 'jquery/tree/3.5/ztree',
    'splitter': 'jquery/splitter/0.8.0/splitter',
    'meta': 'modules/base/meta/meta',
    'navi' : 'modules/base/navi',
    'model': 'modules/base/model',
    'tools' : 'modules/base/tools',
    'notice' : 'modules/base/notice',
    'base' : 'modules/base/base'
  },

  map: [
    [/^(.*\.(?:css|js))(.*)$/i, '$1?20140219']
  ]
});
var __userKey="";
var __cookieHeader="WAF_";
var __webRoot="/MktSystem";
```

http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6

```
var __cookieHeader="WAF_";
var __webRoot="/MktSystem";
var __casClient=true;
if(true==__casClient)
{
  jQuery.ajax({
    type:"POST",
    url:__webRoot+"/api/user/login",
    dataType:"json",
    data: {
    },
    success: function(res){
      if(res.resultCode == 0) {
        showIndex(res.passport, res.__userKey);
      }
      else if(res.resultCode == 7001)
      {
        window.location.href = "https://biportal/BIPortal/noprivilege.jsp";
      }
      else
      {
        window.location.href = "https://biportal/BIPortal/login";
      }
    }
  });
}
else
{
  $("#loginDiv").show();
}
function loginAccountCheck()
{
  var account = $("#loginAccount").val();
  var regx = /^[5,40]$/;
  var flag = regx.test(account);
  if(flag)
  {
    $("#accountTip").hide();
  }
}
```

```

    }
    else
    {
        $("#accountTip").show();
    }
    return flag;
}
function loginPwdCheck()
{
    var pwd = $("#loginPwd").val();
    var regx = /^[6,40]$/;
    var flag = regx.test(pwd);
    if(flag)
    {
        $("#pwdTip").hide();
    }
    else
    {
        $("#pwdTip").show();
    }
    return flag;
}
function showIndex(passport, userKey) {
    window.location.href = __webRoot + "/page/index";
};
function showLogin() {
    window.location.href = __webRoot + "/page/login";
};
function refreshVerifyCode() {
    $("#verifyCode").val('')
    $('#ImageCheck').attr('src', __webRoot + "/page/verifyCode?t=" + (new Date().getTime().toString(36)));
};
function login() {
    if(!loginAccountCheck() || !loginPwdCheck())
    {
        return;
    }
    $.ajax({
        type : "POST",
        url : __webRoot + "/api/user/login",
        dataType : "json",
        data : {
            "account" : $("#loginAccount").val(),
            "password" : $("#loginPwd").val(),
            "verify" : $("#verifyCode").val(),
        },
        success : function (res)
        {
            if (res.resultCode != 0)
            {
                $("#loginInfo").html(getLocalReason(res.resultCode, res.info));
                refreshVerifyCode();
                return;
            } else
            {
                $("#loginInfo").html('');
                showIndex();
            }
        }
    });
};
};

```

http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6

loginAccountCheck()

http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6

```
loginPwdCheck()
```

http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6

```
refreshVerifyCode()
```

http://192.168.22.60:23080/MktSystem/page/index;jsessionid=FD4D8A3F19C87ED208A38B3CDE3511E6

```
login()
```

http://192.168.22.60:23080/MktSystem/page/mktInfo

```
seajs.use(["modules/base/model", "modules/base/meta/mktInfo"], function(model, MetaMktInfo) {  
  var meta = MetaMktInfo.instance("/MktSystem", 'mktInfo', ["mktinfoId", "name"]);  
  model.showList({  
    id: "13",  
    meta: meta,  
    webRoot: "/MktSystem",  
    from: 0,  
    perPage: 15  
  });  
});
```

http://192.168.22.60:23080/MktSystem/page/mktInfo

```
void(0)
```

http://192.168.22.60:23080/MktSystem/page/index

```
seajs.config({  
  base: "/MktSystem/js/",  
  alias: {  
    'jquery': 'jquery/jquery/2.1.3/jquery',  
    'jquery-ui': 'jquery/jqui/jquery-ui.min',  
    'cookie': 'jquery/jquery-cookie-1.4.1/jquery.cookie',  
    'dialog': 'jquery/dialog/6.0.4/dialog',  
    'calendar': 'jquery/calendar/1.0/tinycal.debug.js',  
    'angular': 'angular/1.1.5/angular',  
    'tree': 'jquery/tree/3.5/ztree',  
    'splitter': 'jquery/splitter/0.8.0/splitter',  
    'meta': 'modules/base/meta/meta',  
    'navi': 'modules/base/navi',  
    'model': 'modules/base/model',  
    'tools': 'modules/base/tools',  
    'notice': 'modules/base/notice',  
    'base': 'modules/base/base'  
  },  
  
  map: [  
    [/^(.*\.(?:css|js)) (.*)$/i, '$1?20140219']  
  ]  
})
```

```
});
var __userKey="4kuX-L8macLkENvRXy6uTC";
var __cookieHeader="WAF_";
var __webRoot="/MktSystem";
```

http://192.168.22.60:23080/MktSystem/page/index

```
seajs.use(["navi", "modules/base/user"], function(navi, user) {
    navi.showList("system");
});
```

cookie 11

TOC

名称	首先设置	域	安全
值	请求的 URL		到期
CASPRIVACY	https://biportal/BIPortal/login	biportal	False 1970/1/1 8:00:10
CASTGC	https://biportal/BIPortal/login	biportal	True
JSESSIONID	https://biportal/BIPortal/login?service=http://192.168.22.60:23080/MktSystem/page/index	biportal	False
JSESSIONID	http://192.168.22.60:23080/MktSystem/page/index?ticket=ST-2889-BaltdLYIBAN22CpnYRGy-BIPortal	192.168.22.60	False
FD4D8A3F19C87ED208A38B3CDE3511E6	http://192.168.22.60:23080/MktSystem/page/index		
WAF_mktinfoName			False
69	http://192.168.22.60:23080/MktSystem/page/index		
WAF_reportPlatform			False
-1	http://192.168.22.60:23080/MktSystem/page/index		
WAF_scopeld			False
13	http://192.168.22.60:23080/MktSystem/api/mktInfo/query		
WAF_scopeld			False
13	http://192.168.22.60:23080/MktSystem/api/mktDic/queryDicList		
WAF_scopeld			False
5	http://192.168.22.60:23080/MktSystem/page/index		
WAF_verifysession	http://192.168.22.60:23080/MktSystem/api/user/login	192.168.22.60	False 1970/1/1 8:00:10
WAF_verifysession			False
F8GA3cwNzZC	http://192.168.22.60:23080/MktSystem/api/user/login		