

AngularJS 使用\$sce控制代码安全检查

由于浏览器都有同源加载策略，不能加载不同域下的文件、也不能使用不合要求的协议比如file进行访问。
在angularJs中为了避免安全漏洞，一些ng-src或者ng-include都会进行安全校验，因此常常会遇到一个iframe中的ng-src无法使用。

什么是SCE

SCE，即strict contextual escaping,我的理解是 严格的上下文隔离 ...翻译的可能不准确，但是通过字面理解，应该是angularjs严格的控制上下文访问。

由于angular默认是开启SCE的，因此也就是说默认会决绝一些不安全的行为，比如你使用了某个第三方的脚本或者库、加载了一段html等等。

这样做确实是安全了，避免一些跨站XSS，但是有时候我们自己想要加载特定的文件，这时候怎么办呢？

此时可以通过\$sce服务把一些地址变成安全的、授权的链接...简单地说，就像告诉门卫，这个陌生人其实是我的好朋友，很值得信赖，不必拦截它！

常用的方法有：

```
$sce.trustAs (type,name);
$sce.trustAsHtml (value);
$sce.trustAsUrl (value);
$sce.trustAsResourceUrl (value);
$sce.trustAsJs (value);
```

其中后面的几个都是基于第一个api使用的，比如trsutAsUri其实调用的是trsutAs(\$sce.URL,"xxx");

其中type可选的值为：

```
$sce.HTML
$sce.CSS
$sce.URL //a标签中的href , img标签中的src
$sce.RESOURCE_URL //ng-include,src或者ngSrc ,比如iframe或者Object
$sce.JS
```

来自官网的例子：ng-bind-html

```
<!DOCTYPE html>
<html>
<head>
  <title></title>
  <script src="http://apps.bdimg.com/libs/angular.js/1.2.16/angular.min.js"></script>
</head>
<body ng-app="mySceApp">
  <div ng-controller="AppController">
    <i ng-bind-html="explicitlyTrustedHtml" id="explicitlyTrustedHtml"></i>
  </div>
  <script type="text/javascript">
    angular.module('mySceApp',[])
    .controller('AppController', ['$scope', '$sce',
      function($scope, $sce) {
        $scope.explicitlyTrustedHtml = $sce.trustAsHtml(
          '<span onmouseover="this.textContent="Explicitly trusted HTML bypasses ' +
            'sanitization."">Hover over this text.</span>');
      }]);
  </script>
</body>
</html>
```

实际工作中的例子：ng-src链接

```
<!DOCTYPE html>
<html>
<head>
  <title></title>
  <script src="http://apps.bdimg.com/libs/angular.js/1.2.16/angular.min.js"></script>
</head>
```

公告



大连地区，如果有代理记账咨询纳税可以私信联系！

昵称：xingoo
园龄：5年5个月
粉丝：2913
关注：71
+加关注

<	2018年3月						>
日	一	二	三	四	五	六	
25	26	27	28	1	2	3	
4	5	6	7	8	9	10	
11	12	13	14	15	16	17	
18	19	20	21	22	23	24	
25	26	27	28	29	30	31	
1	2	3	4	5	6	7	

最新随笔

1. Mac下IDE无法读取环境变量问题

2. Spark DataFrame写入HBase的常用方式

3. 极大似然估计的理解与应用

4. 推荐系统那点事儿

5. Spark机器学习——模型选择与参数调优之交叉验证

6. Spark Client启动原理探索

7. Spark源码分析 之 Driver和Excutor是怎么跑起来的?(2.2.0版本)

8. 《恶意》—— 读后总结

9. 基于Dubbo的http自动测试工具分享

10. Spark监控官方文档学习笔记

随笔分类(815)

AngularJS(26)

Elasticsearch(53)

Hadoop(17)

```
</div>
<script type="text/javascript">
    angular.module('mySceApp', [])
    .controller('AppController', ['$scope', '$sce', function($scope, $sce) {
        $scope.trustSrc = $sce.trustAs($sce.RESOURCE_URL, "http://fanyi.youdao.com/");
        // $scope.trustSrc = $sce.trustAsResourceUrl("http://fanyi.youdao.com/");//等同于这个方法
    }]);
</script>
</body>
</html>
```

参考

- 【1】[angular源码分析：angular中入境检查官\\$sce](#)
- 【2】[野兽的 Angular 学习 -- \\$sce和sceDelegate](#)
- 【3】[\\$sce官方手册](#)

作者：xingoo
Github：<https://github.com/xinghalo>
本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。

分类： AngularJS

标签： AngularJS, angular, \$sce, ng-src, ng-bind-html, sce

好文要顶 关注我 收藏该文



 xingoo
关注 - 71
粉丝 - 2913
[+加关注](#)

« 上一篇：我的2015，我的2016
» 下一篇：Nodejs-内存控制

posted @ 2016-01-04 22:53 xingoo 阅读(11632) 评论(0) 编辑 收藏

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 [登录](#) 或 [注册](#)，[访问网站首页](#)。

Java(146)
JavaScript(71)
Kafka(3)
linux(29)
Logstash(16)
Mac说(2)
MongoDB(2)
Oozie(12)
Oracle(44)
Python(2)
Redis(1)
Ruby(8)
Scala(8)
Spark(25)
Spring(25)
Sqoop(3)
TensorFlow(1)
程序人生(120)
缓存系统(6)
机器学习(13)
全栈折腾(11)
软件考试(1)
设计模式(23)
数据仓库(9)
数学理论(2)
算法(85)
网络(20)
杂谈(21)
杂项文章(18)

