DOI:10.19695/j.cnki.cn12-1369.2016.02.087

JWT认证技术及其在WEB中的应用

范展源 罗福强
(四川大学锦城学院 四川成都 611731)

摘要:本文介绍了JWT认证技术的概念、组成结构及原理,并将之与传统认证技术比较,从而说明JWT认证技术的优势所在。同时,通过在最新单页WEB技术Laravel5和AngularJS上集成JWT,展示了该认证技术的应用方法。JWT的加密方法,以及如何在令牌过期时刷新令牌等更多细节问题,是本文今后的研究方向。

关键词:JWT令牌 Laravel5 AngularJS 单页应用
中图分类号:TP391 **文献标识码**:A **文章编号**:1007-9416(2016)02-0114-01

随着单页应用、移动应用和RESTful API服务架构的发展,开发人员编写服务器后台代码的方式也发生了变化。通过使用AngularJS等前端技术,开发人员在服务端只需要为前端应用提供数据API。这样,服务器后台可以更多关注业务逻辑和数据存取,而将界面展示任务交给前端或移动端。这种变化促进了现代应用认证技术的新发展。

1 JWT认证技术

1.1 什么是JWT

JWT,是一种基于JSON格式,用于WEB应用环境下各方之间传递声明信息的开放标准。JWT令牌具有紧凑性和URL安全性,它的典型应用场景是在网络中传递认证用户的身份信息。

1.2 JWT的结构

JWT令牌包括头信息、有效载荷和加密签名三个部分。如图1所示,头信息和有效载以JSON格式封装并用base64编码,它们之间以'.'字符连接。签名部分是前两个部分通过强加密算法加密的结果,通过'.'字符连接在令牌的末端。

1.3 JWT的技术优势

在讨论JWT技术前,先了解下传统认证系统的工作原理。

(1)浏览器将用户输入的用户名及密码提交给服务器;

(2)服务器接收登录请求后,验证用户合法性并创建保存一个session,在响应中返回包含这个session 的cookie给浏览器;

(3)在访问应用中受限制资源时通过cookie提供session信息;

(4)如果session有效,允许用户访问受限制资源。

传统认证系统有以下不足:

无法跨域请求:通过AJAX从另一个域名请求资源很可能会失败,因为HTTP协议规定在跨域访问时默认不能携带cookie。

扩展性差:服务器需要为每个账户创建并存储session,而由于跨域访问限制,这种基于session的认证系统难以扩展成应用服务器与session存储分离的分布式系统。

不适用移动设备:在移动应用上使用session或cookie行不通。

JWT的认证原理如下:

(1)浏览器或移动终端将用户输入的用户名及密码提交给认证服务器;

(2)认证服务器在验证用户有效性后,创建一个JWT访问令牌并返回给客户端;

(3)在访问应用服务器中受限制的服务器资源时客户端总是携带这个访问令牌;

(4)应用服务器验证令牌的有效性,如果验证通过,则允许用户访问受限制的资源。

图1 JWT令牌格式

JWT认证系统的优势在于:

易于扩展:令牌中包含了认证用户的所有信息,无需在服务端存储session。因此可以在希望实现负载均衡的分布式系统中使用。

可复用:可在不同的服务器、操作系统平台或不同的域名下,复用同一令牌进行用户认证,甚至在不同应用之间,也可以复用同一令牌。

安全性:因为不需要使用cookies,所以不用担心跨域请求欺骗攻击。但如果令牌中有敏感信息,仍应该用JWE标准对令牌加密。

高效率:只需对令牌签名字段进行认证,而不需要每次请求都查询并反序列化session。

2 Laravel5集成JWT

Laravel5是目前国际上最流行的PHP框架,这里以Laravel5作为服务器后台。由社区开发者分享的tymon/jwt-auth包是一个基于Laravel5的JWT认证实现,可以使用这个包来扩展服务端的认证功能。

3 AngularJS集成JWT

JWT令牌一般放在HTTP的认证头部。为了将JWT令牌注入到HTTP认证头部,需要拦截应用的每个HTTP请求。下面的代码在拦截到HTTP请求时,从本地存储服务中获取在登录时存储的令牌,并将该令牌加到请求的HTTP认证头部。

```
$httpProvider.interceptors.push(['$q', '$location',
'$localStorage',
function ($q, $location, $localStorage) {
return {
'request': function (config) {
if ($localStorage.token) {
config.headers.Authorization = 'Bearer ' + $localStorage.
token;
}
return config;
}
};
}]);
```

4 结语

基于令牌的认证机制使得构建解耦合的系统成为可能。这些令牌可以产生给任何浏览器或设备使用,或者在任何使用相同签名密钥的服务器上被解析验证。

本文通过在Laravel5和AngularJS中集成JWT的例子,说明了JWT的基本用法,也展示了JWT令牌的优势。JWE加密方法,及如何在过期时刷新令牌等更多细节问题,是本文今后的研究方向。

参考文献

[1]Wikipedia.JSON Web Token [EB/OL].https://en.wikipedia.org/wiki/JSON_Web_Token.
[2]Martin Bean.Laravel 5 Essentials[M].Packt Publishing.2015.
[3]董英茹.简谈AngularJS在下一代Web开发中的应用[J].软件工程师,2015年5月:29~30.

收稿日期:2015-12-25
作者简介:范展源(1986—),男,汉,重庆人,助教,硕士,研究方向:web应用、物联网。