09.表单伪造和 CSRF 保护

学习要点：

1.表单伪造

本节课我们来开始学习表单伪造和 CSRF 保护的功能。

一. 表单伪造

1. 之前一直用的 GET 请求方式，而表单可以实现 POST 方式，我们来实验下：
2. 先在 TaskController 创建两个方法，一个表单页，一个接受表单数据路由；

```
public function form()
{
    return view('form');
}

//表单页
Route::get('task/form', 'TaskController@form');

//接受表单数据
Route::any('task/getform', function () {
    return \Illuminate\Support\Facades\Request::method();
});
```

3. 表单页以 post 发送，路由也使用 post 接受，以下表单提交会出现 419 错误；

```
<form action="/task/getform" method="post">
    用户名：<input type="text" name="user">
    <button type="submit">提交</button>
</form>
```

4. 这是为了避免被跨站请求伪造攻击，框架提供了 CSRF 令牌保护，请求时验证；

```
<input type="hidden" name="_token" value="{{csrf_token()}}">
```

5. 表单可以实现 POST 提交方式，那其它提交方式该如何实现呢？可以采用伪造技术；

```
<input type="hidden" name="_method" value="PUT">
```

6. 对于 CSRF 令牌保护和表单伪造提交方式，也支持快捷方式的声明，如下：

```
@csrf
@method('PUT')
```

7. 如果我们想让某些 URL 关闭 csrf 验证，可以设置 csrf 白名单；
8. 白名单具体设置位置在：中间件目录下的 VerifyCsrfToken.php 文件；
9. 当然，不建议直接注释掉这个验证 csrf 功能的中间件；

```
protected $except = [
    //
    'api/*',
];
```