**Pass-01-前端js检查**

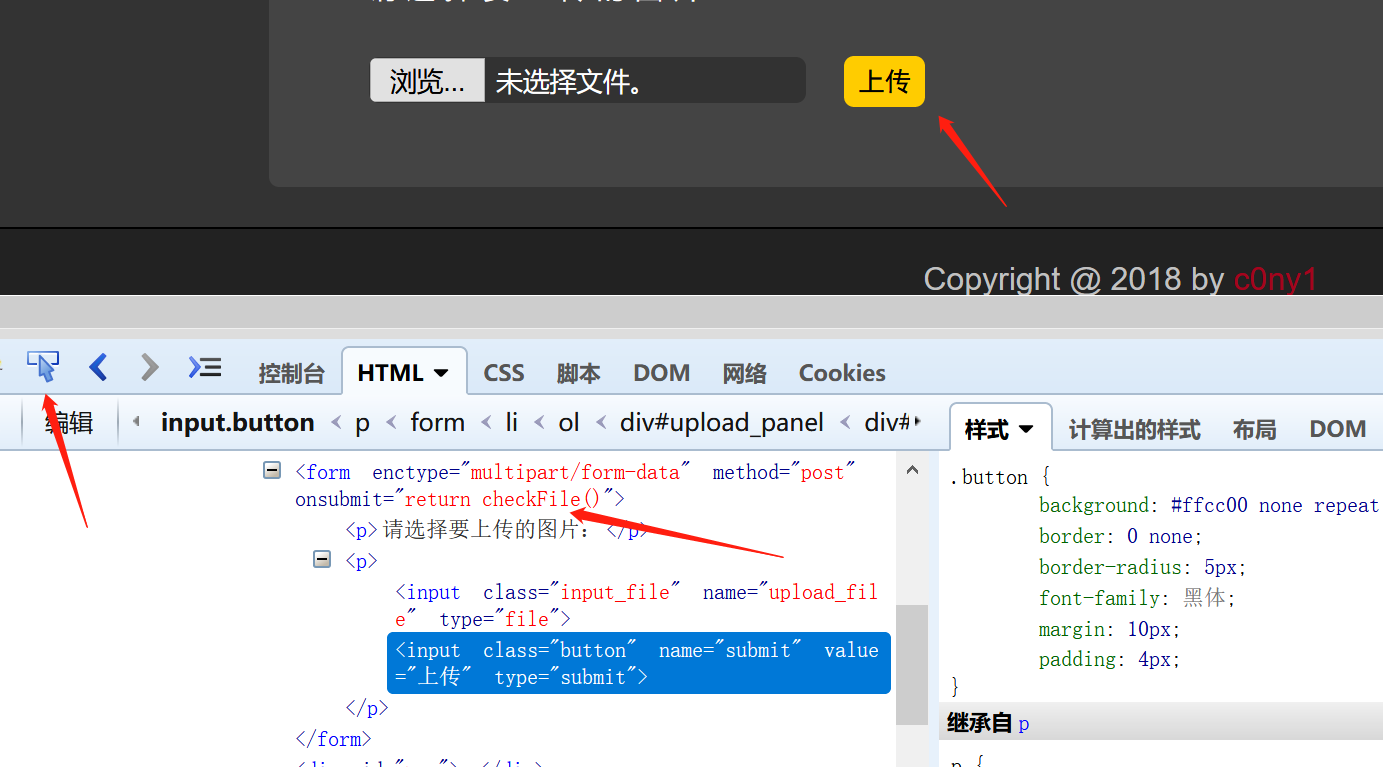
**探测验证点**

1. 首先打开burp和浏览器
2. 上传1.php文件进行观察
3. 这里发现，http请求都没通过burp就弹出了不允许上传的提示框，这表明验证点在前端，而不在服务端

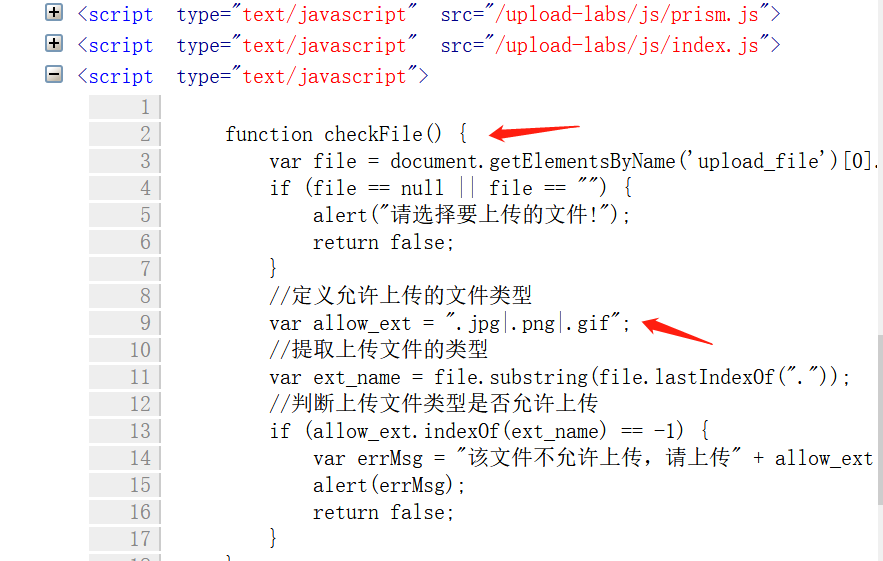


**代码分析**

判断了验证点在前端之后，就可以查看具体js判断代码。于是按F12,找到判断代码。

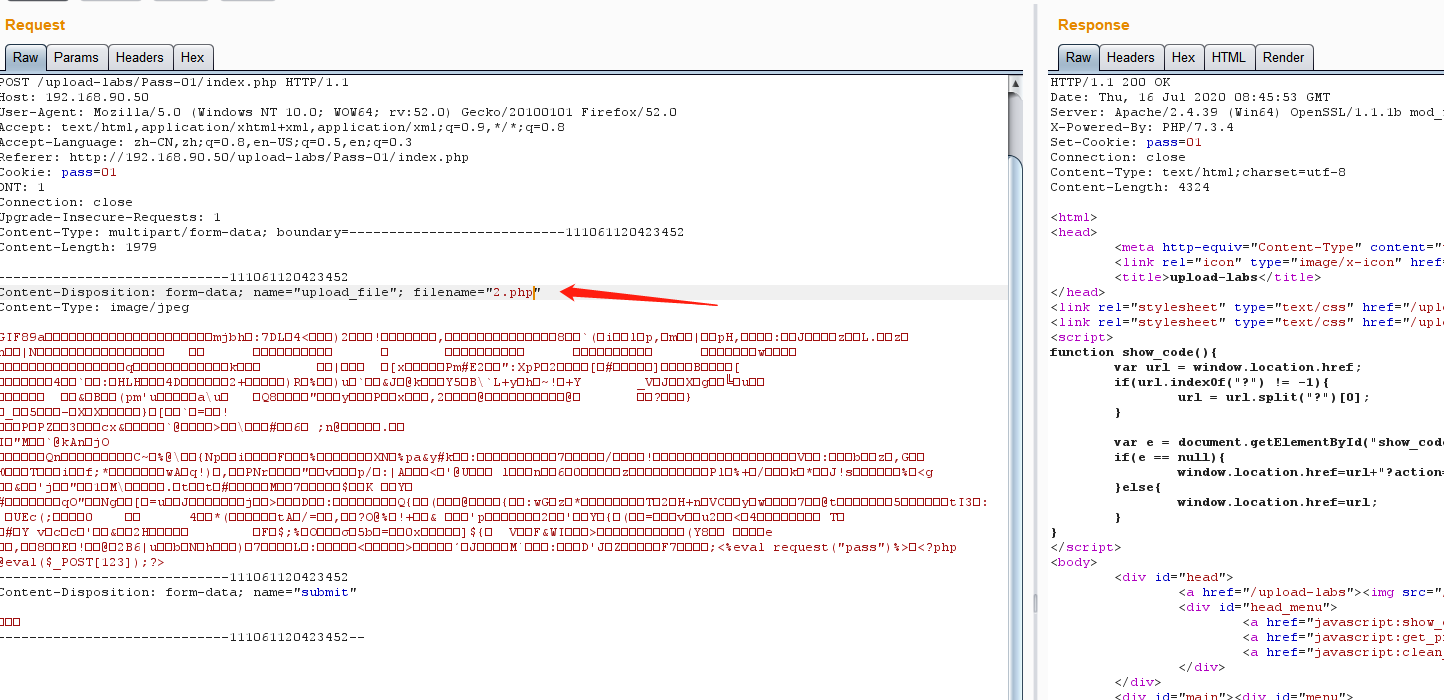


这里很明显是checkFile()这个函数，我们找一下这个函数



**绕过方法**

对于前端js验证的绕过方法较为简单，我们可以将要上传的php文件改后缀名为jpg|png|gif,绕过js验证后，再用burp更改上传请求。或者浏览器禁用js后进行上传。



验证