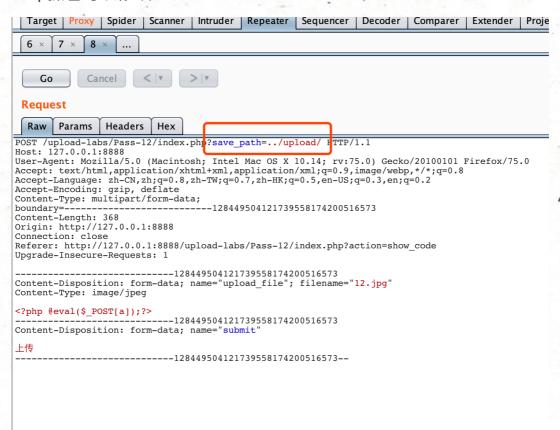
根据源代码,要将文件保存到get请求指定的路径下,并且对文件名随机化处理',因此我们可以在get请求中使用%00阶段,使其在随机化处理文件名之前就截断(因此不能在文件名中使用截断,只能在路径部分截断,因为文件名很容易被随机化处理)

这个get请求是由那个按钮发出的



## burp抓包可以修改



将?save\_path改为../upload/12.php%00,就可以将上传的jpg文件保存为php文件了。

但是经尝试上传失败,上网查了下,原来利用%00截断,php版本必须是小与5.3.4的,并且php.ini中的magic\_quotes\_gpc = Off,如果为On则%00会被转义字符

下载的MAMP没有5.3以下版本的,不过已经知道怎么做了,这一关算过了