在进行一次企业src的挖掘过程中，我四处寻找可以突破限制的点，有一句话说的很好，突破原有的限制就算漏洞，只不过危害有大有小。

在找到一个站点之后，我就开始找突破点，结果发现他这里提示我，不能创建作品超过两个以上，于是我就开始着手尝试绕过。

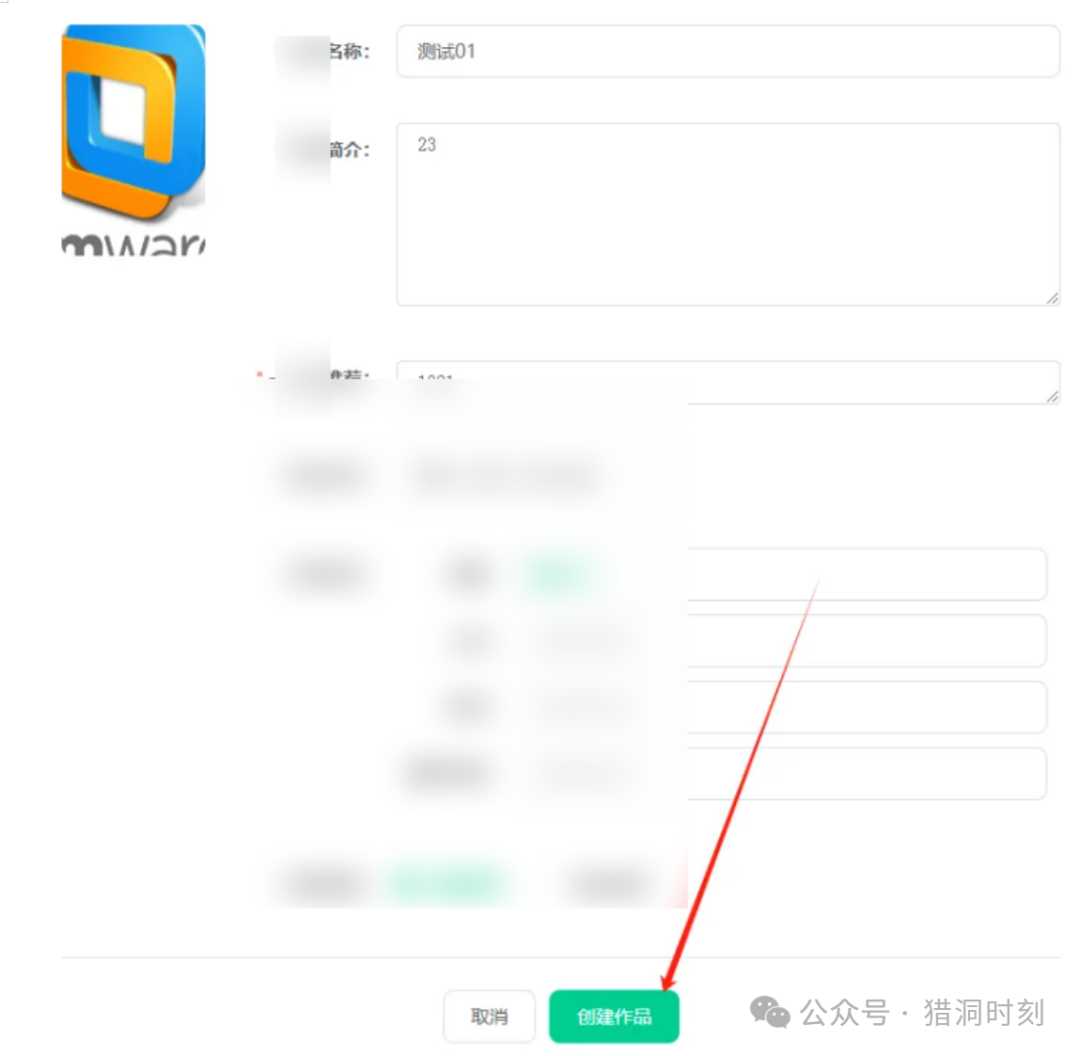


经过测试发现，他这个每次创建作品之前，都会进行校验一次，检验已创建作品的数量，如果超过两个，就会拒绝创建作品。于是分析出下面的绕过方法：

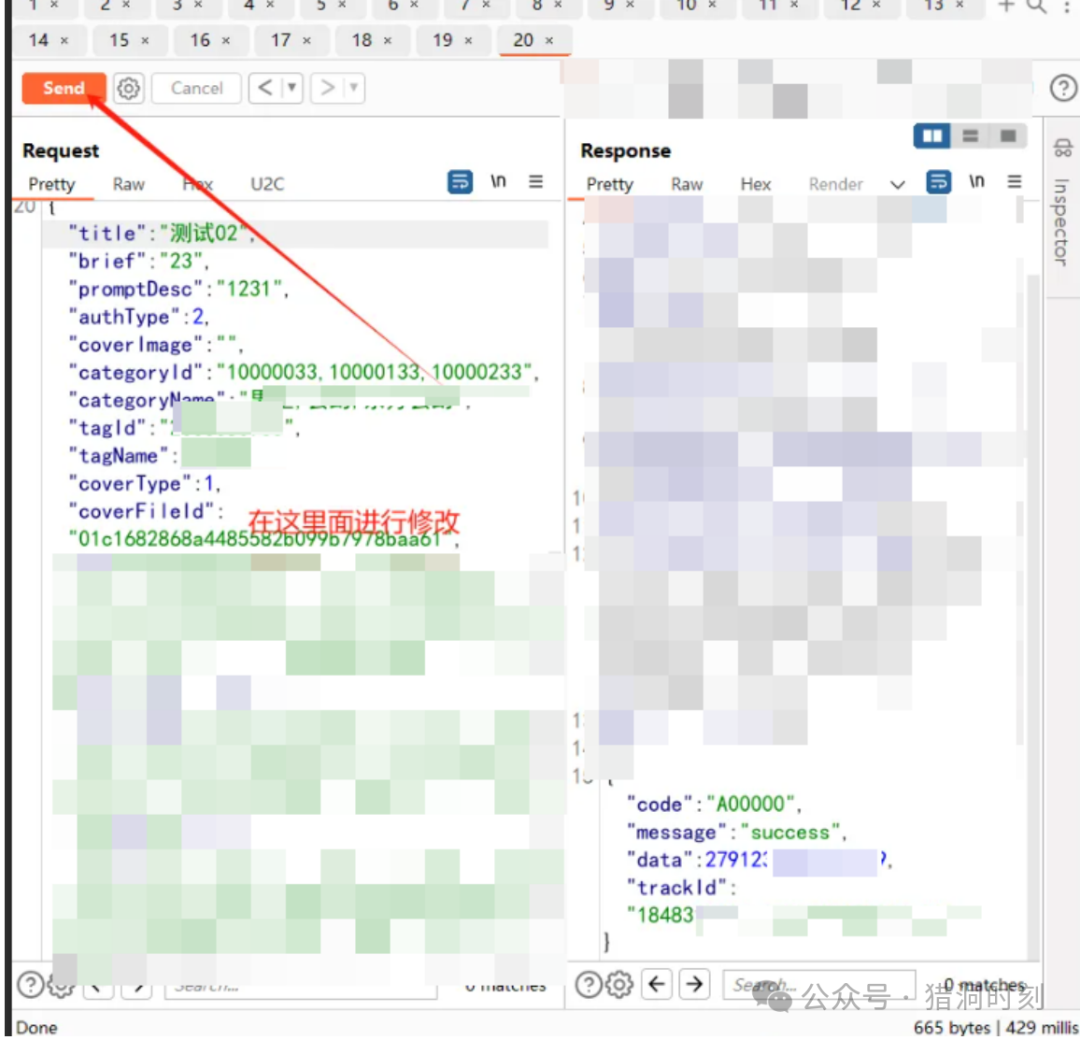


他这个鉴权方法，无论是前端的校验还是后端的校验，都能很简单的绕过，除非开发者在发送创建数据的时候进行验证数量，才能防止被绕过。

下面进行创建作品然后进行抓包。



然后在数据包中进行修改即可，就能达到绕过限制，修改后直接send发包，从而无限创建作品，绕过限制。



下面可以看出来，创建了多个作品，成功绕过了原本的限制。

