bugku上聪明的PHP

原创

该用户正摸鱼 已于 2022-02-17 17:34:57 修改 1019 收藏 1
分类专栏： bugku题目wp 文章标签： php 开发语言 后端
于 2022-02-14 15:36:39 首次发布
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/weixin_58111246/article/details/122924785
版权


bugku题目wp 专栏收录该内容
11 篇文章 1 订阅
订阅专栏

1：打开环境，翻译看看意思，随便传一个参数如图，随意传参获取到smarty提示，有可能是模板注入

CSDN @该用户正摸鱼

2：审计一下代码，preg_match后面就是代表这些被过滤了，环境地质+./template.html就是假的答案，就想到了抓包看看

还是看了别人的才知道个东西叫模板注入，要验证一下是不是模板注入，像这样，114.67.175.224:18407/?flag.txt?a={4*4}里面的4*4随便你，后面代码后面会多出一个像这样的 flag_txt?a 16

3:构造payload

补充

php命令执行函数有

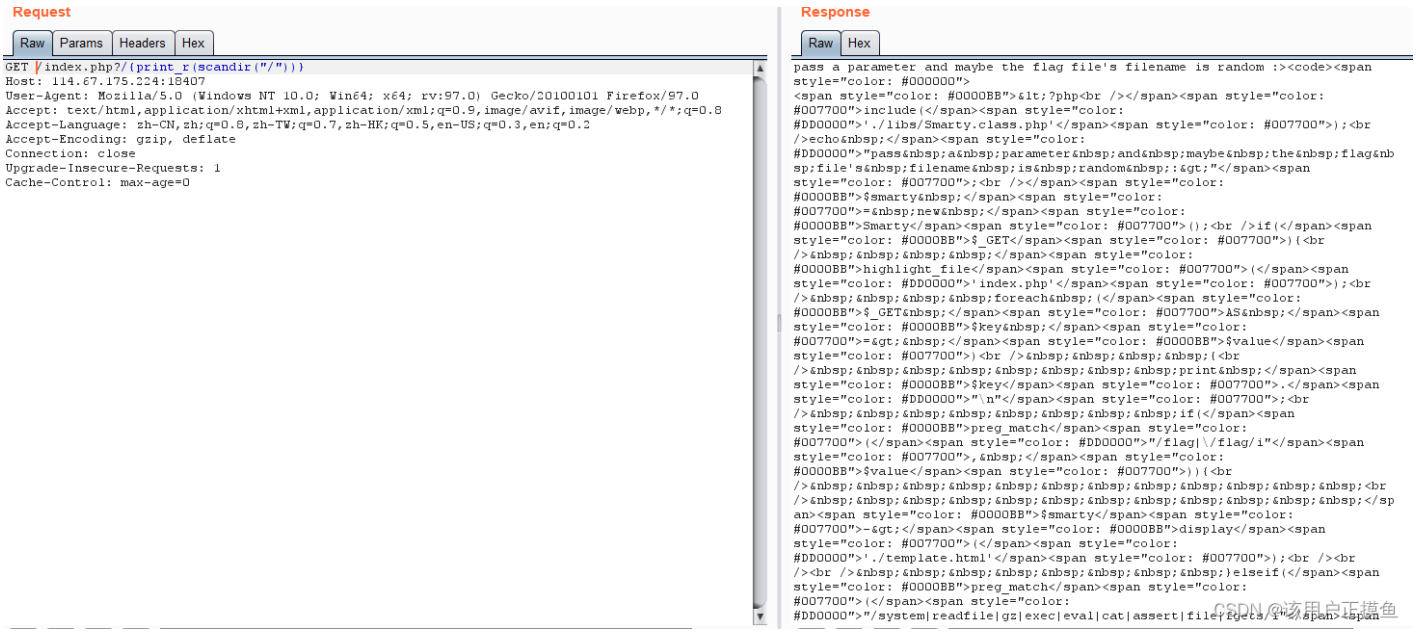
https://www.php.net/exec

exec – 执行一个外部程序
passthru – 执行外部程序并且显示原始输出
proc_close – 关闭由 proc_open 打开的进程并且返回进程退出码
proc_open – 执行一个命令，并且打开用来输入/输出的文件指针。
popen – 打开一个指向进程的管道，该进程由派生给定的 command 命令执行而产生。
proc_terminate – 杀除由 proc_open 打开的进程
shell_exec – 通过 shell 环境执行命令，并且将完整的输出以字符串的方式返回。
system – 执行外部程序，并且显示输出
scandir 列出指定路径中的文件和目录
eval – 把字符串作为PHP代码执行
assert --函数直接将传入的参数当成PHP代码执行
linux查看文件的命令

cat tac more less head tail nl static-sh paste od bzmore bzless
php文件读取函数

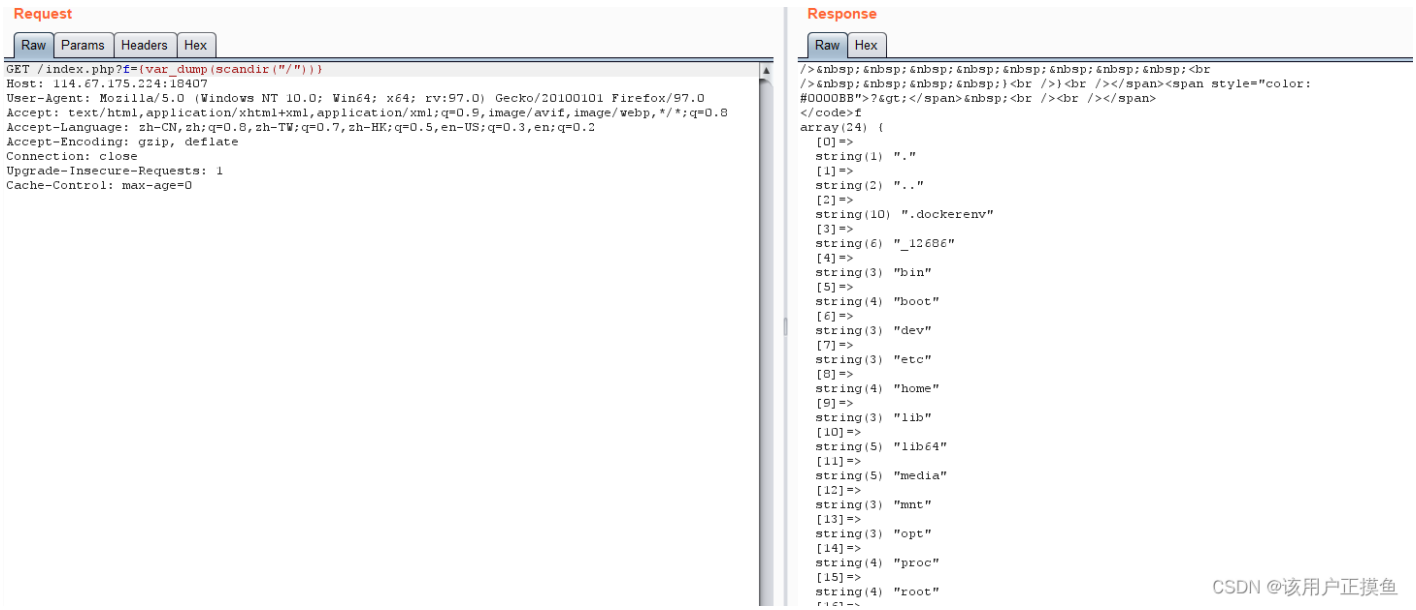
printr() fread() fgets() vardump()

用scandir函数去查找关于flag的文件，还有获取flag文件内容：/index.php?f={print_r(scandir("/"))}



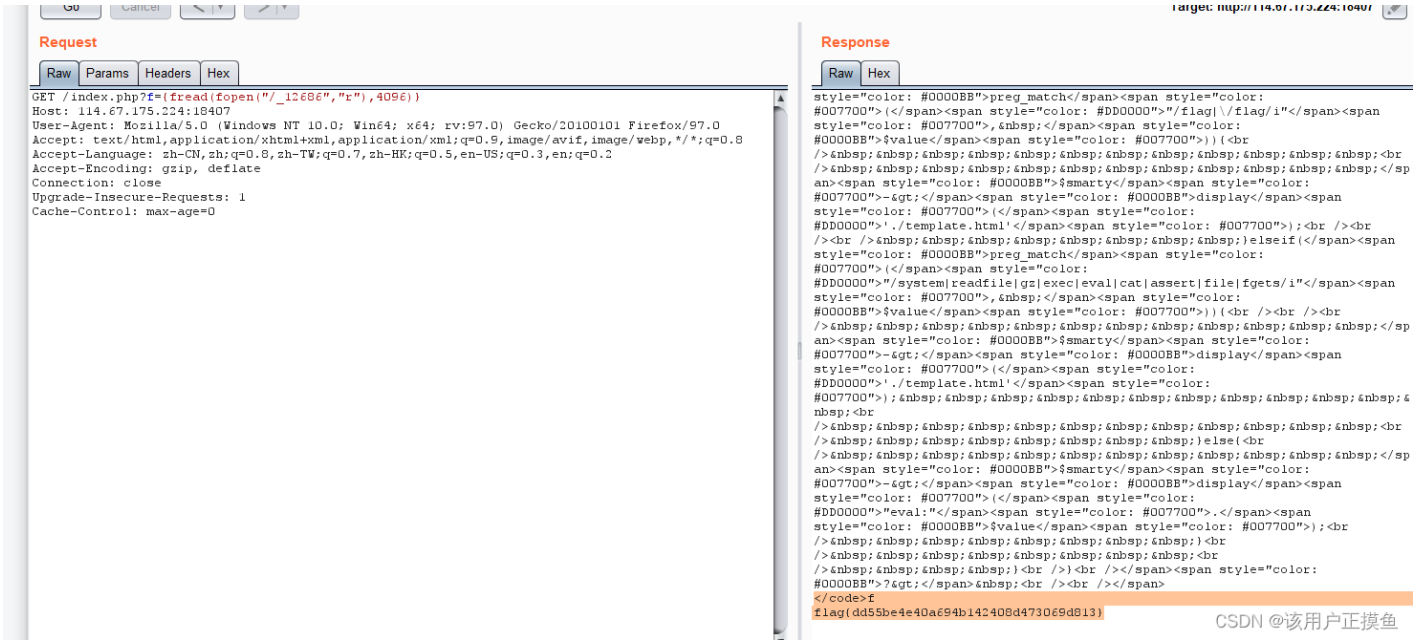
/index.php?f={var_dump(scandir("/"))}，发现重要东西，_12686这个文件夹名字就不一样了，先搞它

CSDN @该用户正摸鱼



在后面粘贴上，/index.php?f={fread(fopen("/_12686","r"),4096)}

4096是啥，我也不晓得



得到flag

4：呃呃呃4096是什么，速度？看到博客的，知道的，qql告诉我吧

PHP中的文件系统函数第三部分_瑾的日常-CSDN博客

还有一个大佬的博客，我就是看了·他的payload我才做出来

bugku CTF 聪明的php WriteUp - 知乎 (zhihu.com)