

ACTF新生赛 EASYHTTP

原创

[person by 小鸟](#) 于 2020-03-17 11:19:54 发布 449 收藏

分类专栏: [笔记](#)

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/SopRomeo/article/details/104917042>

版权



[笔记 专栏收录该内容](#)

31 篇文章 1 订阅

订阅专栏

最近自闭了, 找了ACTF新生赛的源码自己复现做了一下

服务器IP:

服务器操作系统:

PHP版本:

端口:

Submit

重置

```
array(4) {
  [0]=>
  string(15) "192.168.230.133"
  [1]=>
  string(6) "Debian"
  [2]=>
  string(47) "Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45"
  [3]=>
  string(2) "80"
}
```

<https://blog.csdn.net/SopRomeo>

看到下面输出了服务器对应的信息，将这些信息依次填上去

GET请求

hello参数的值: 一入安全深似海

POST请求

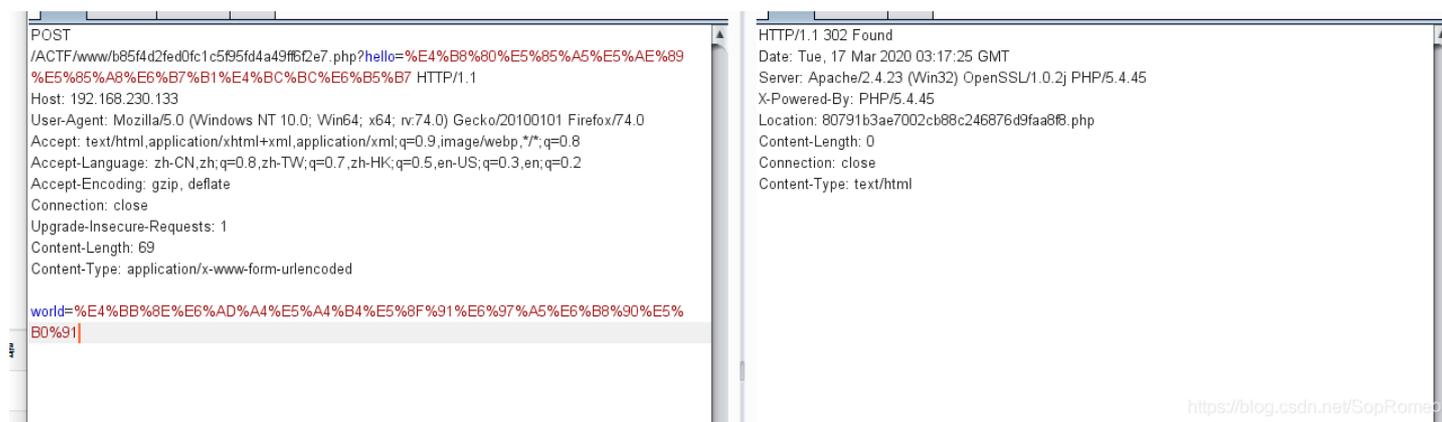
world参数的值: 从此头发日渐少

<https://blog.csdn.net/SopRomeo>

192.168.230.133/ACTF/www/b85f4d2fed0fc1c5f95fd4a49ff6f2e7.php

GET,POST, 注意url地址:

地址换了, 放burp去上传GET,POST.(传中文需进行url编码)



<https://blog.csdn.net/SopRomeo>

发现换了个php代码, 复制到proxy放行,

重新抓包 伪造ip地址即可得到flag