ctfshow萌新红包题writeup

原创

秋风瑟瑟... 于 2020-02-20 16:52:28 发布 3154 收藏 1

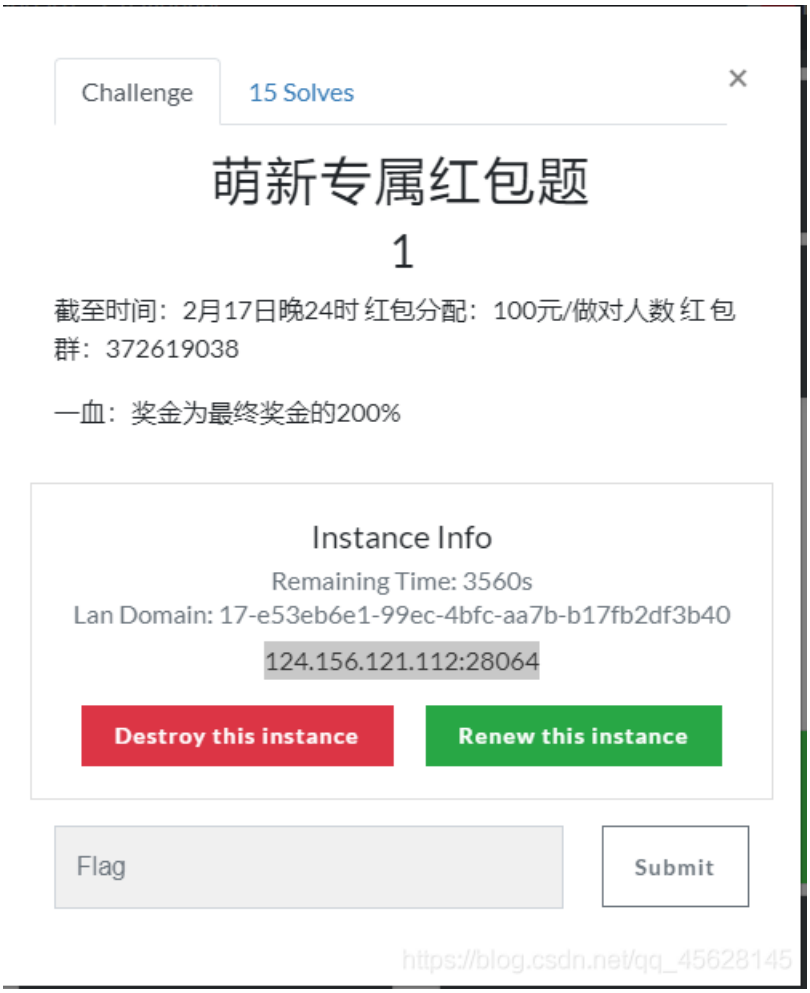
文章标签： web 安全

本文链接：https://blog.csdn.net/qq_45628145/article/details/104412419

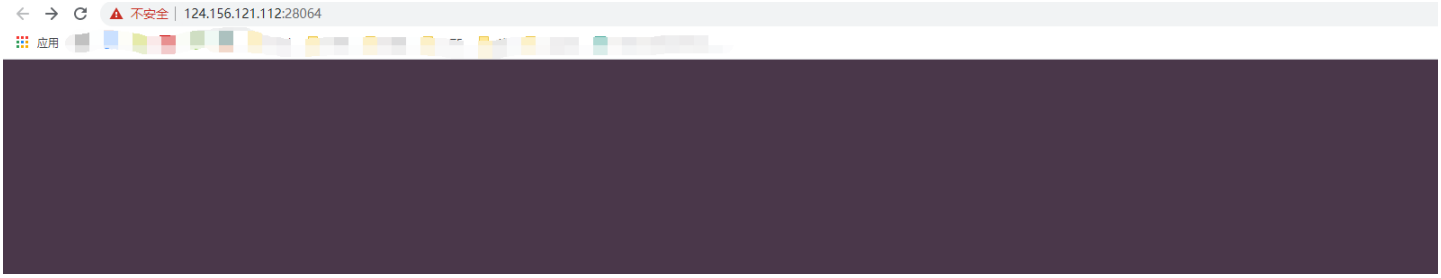
ctfshow萌新专属红包题writeup

题目来源：https://ctf.show/

这一题是ctfshow平台上面2月17日更新的一个萌新红包题，当天在官方交流群内知道晚上会有一个萌新红包题之后，就有点期待了（小萌新也想拿一次红包，嘿嘿），下面来看看这个题目吧。



进入题目之后，是一个ctfshow萌新登录页面。

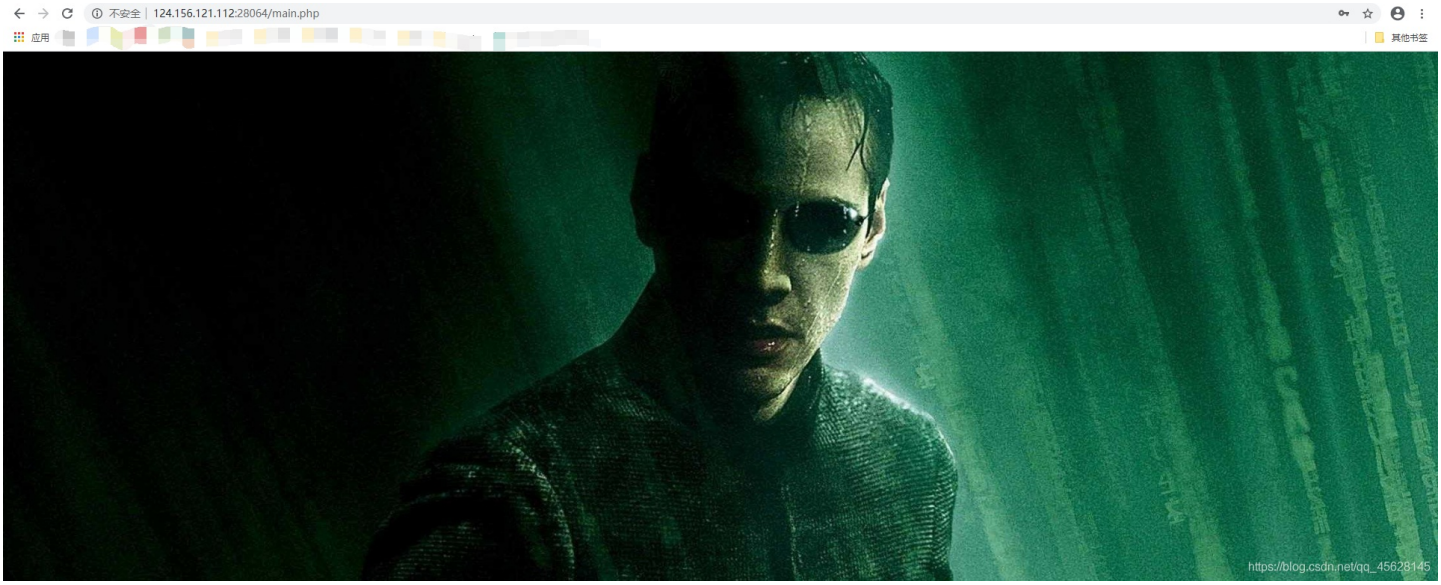


首先，老规矩，先看源码。一顿操作之后，没有任何发现。群主在官方交流群里面先后给过几个提示，**开始第一个提示是这个题目是萌新难度，不难**。于是我就去尝试弱口令登陆了。

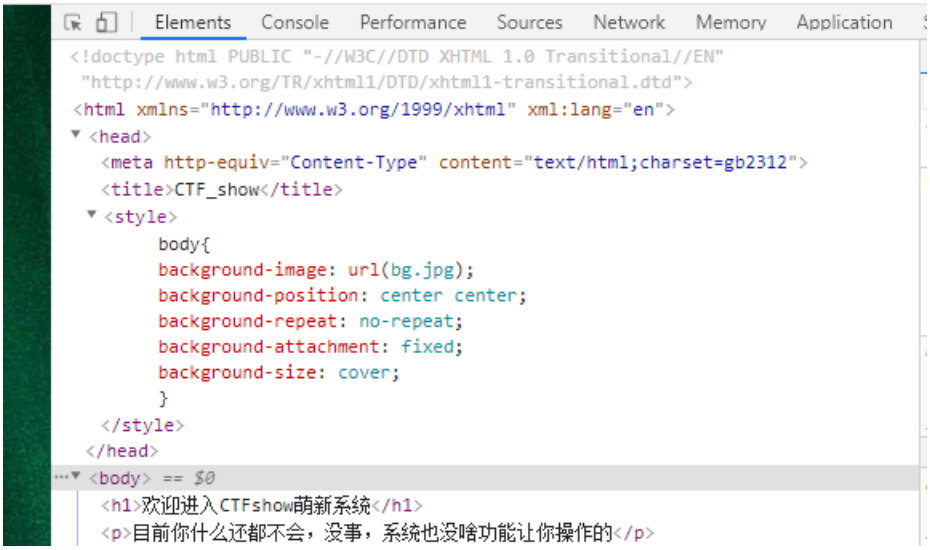
我最开始是尝试用户名admin进行登录，我输入的密码并没有登录进去，后来想爆破，但是群主说不能爆破，于是继续尝试，还是没有找到密码。过了一会儿，我尝试用自己ctfshow平台的账号登录，也没有用，尝试用自己的账号用弱口令登录，也还是没有用。

然后又过了一会儿， 我去看了看这个登陆页面的响应头，看下里面会不会藏一些东西，但是并没有任何发现。因为过了挺久的，还没有人做出来，于是群主放出第二个提示，**用户名admin，密码admin888**，并且在放提示之前说可能这个提示一放出来，就会有人秒了。

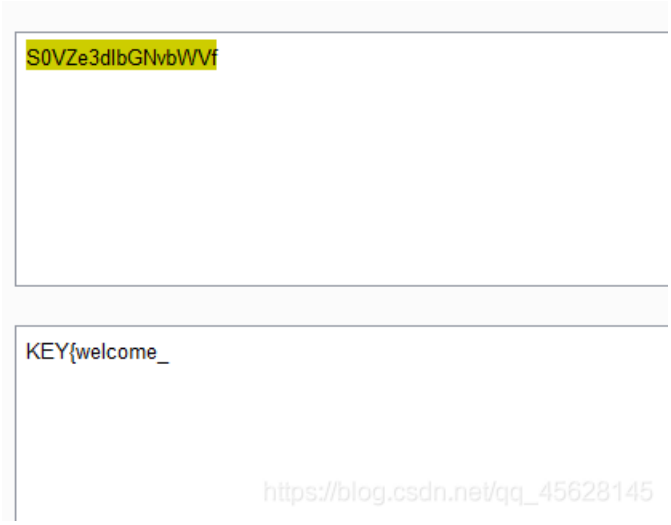
在获得这个提示之后，我就去登录了，果然登陆进去了。登陆进去之后是这样的一个页面。



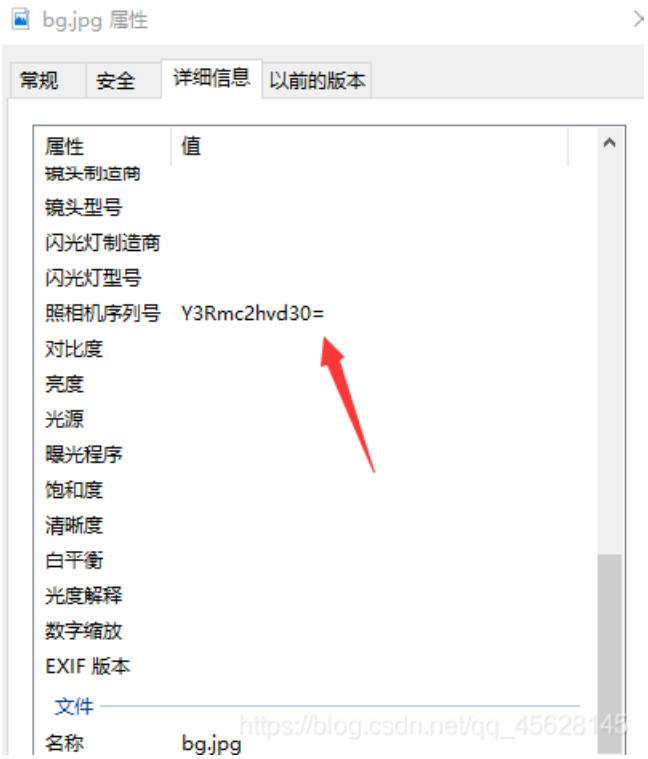
在登陆进来之后，是一个这样的界面，于是查看源码，发现了一段base64字符串。



对其进行解码之后，是这样的一个字符串。



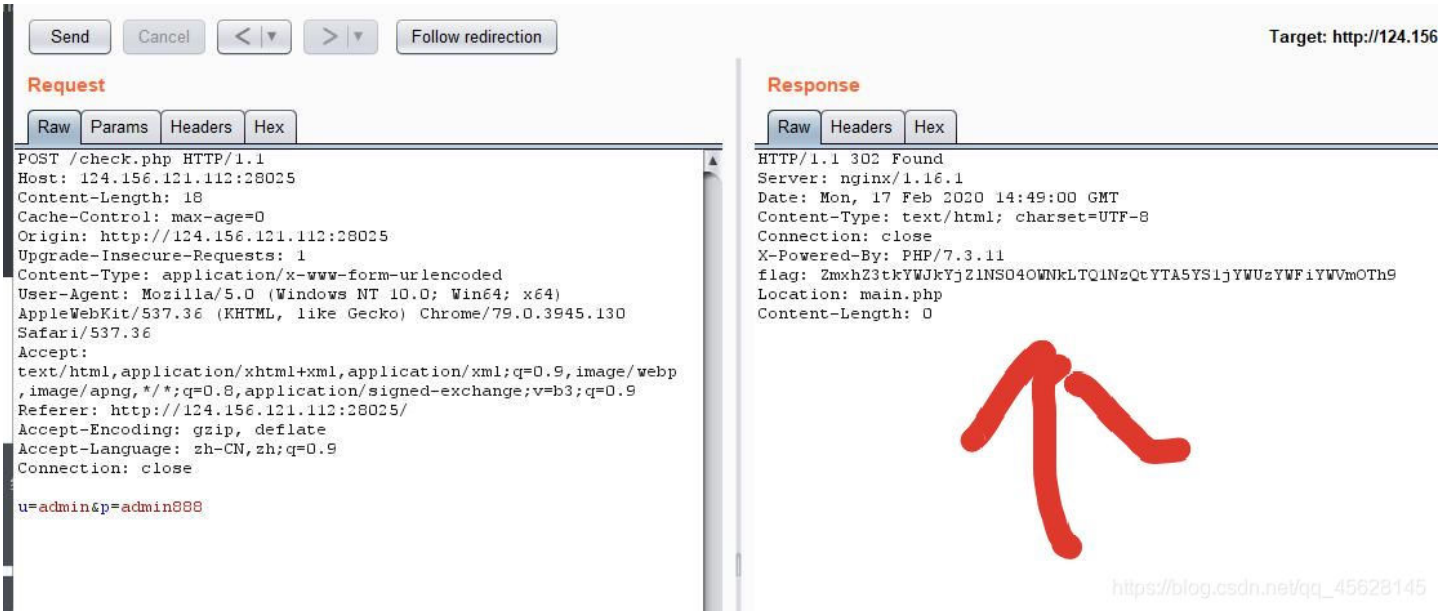
当时觉得这个就是一半的flag，于是继续寻找另一半的base64。我先看的是响应头，看看剩下的一半base64在不在里面，但是没有任何操作。想了一会儿，把这个背景图片下载了下来，猜可能在图片里面。我先是把图片拖进winhex，查看头尾，看看有没有base64，没有发现，然后搜索里面有没有‘base64’或者‘base’这个字符串，想找到另一半base64，但是没有发现。于是关掉之后，查看图片信息，发现里面有一段base64，终于找到了。



对其解码，得到flag。

KEY{welcome_ctfshow}

然后去提交，发现提交错误，这是一个假的flag！！！
然后呢我又根据前面的KEY是大写，将里面的英文改成大写，进行提交，还是错误。又接着尝试了一半大写一半小写，还有一堆操作，全部提交失败。
然后我根据这个KEY，尝试以用户名admin和我的平台用户名，这个假flag为密码，各种改变密码的样式，进行登录，但没成功，甚至拿welcome作为用户名，ctfshow密码登录，也还是没有用。（心灰意冷.jpg）
当时没有找到任何有效信息，尝试玄学一下看看，抓个包，没想到抓出东西了。我再次以admin，admin888登录的时候，发现有东西了。

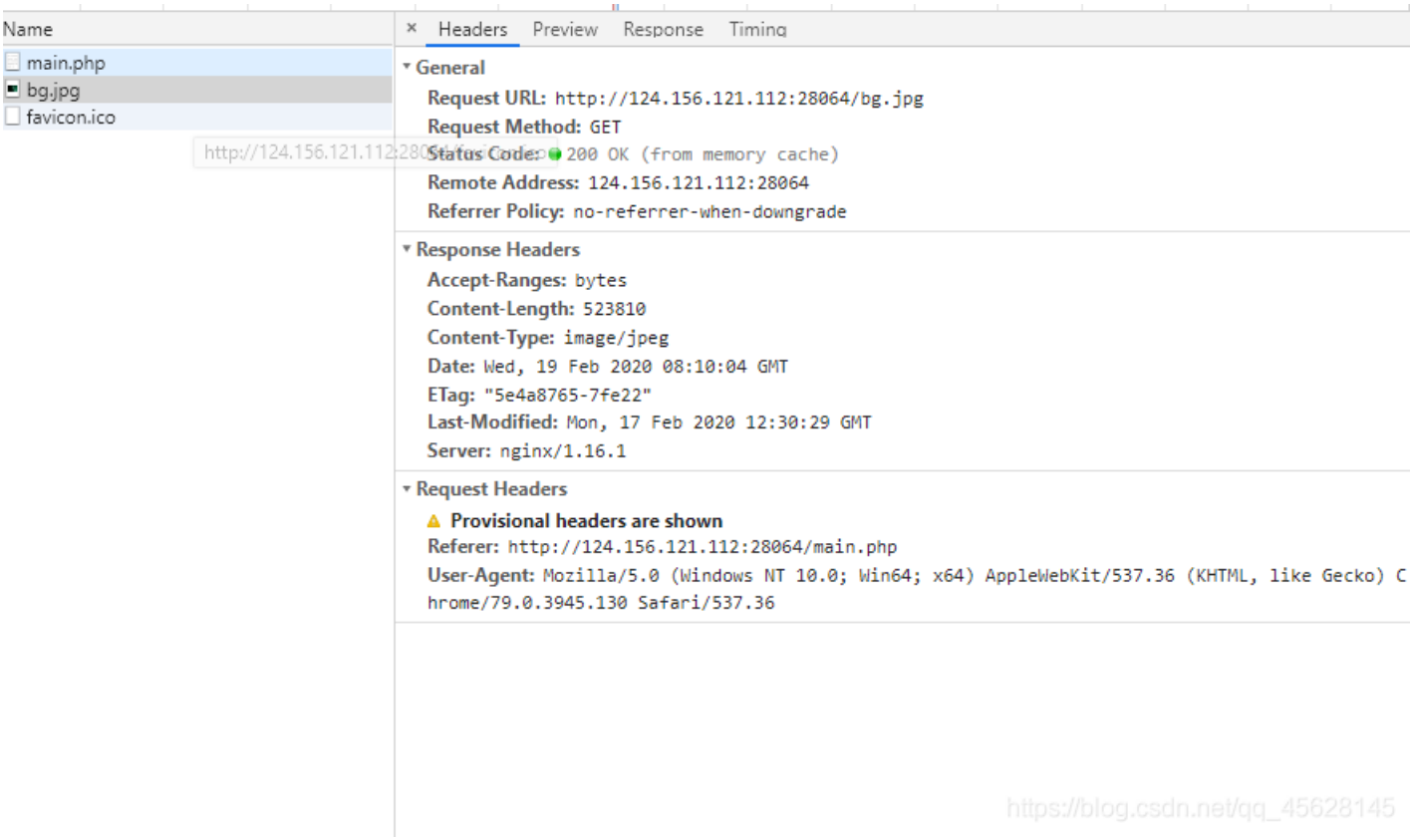


然后对其进行base64解码，得到flag。

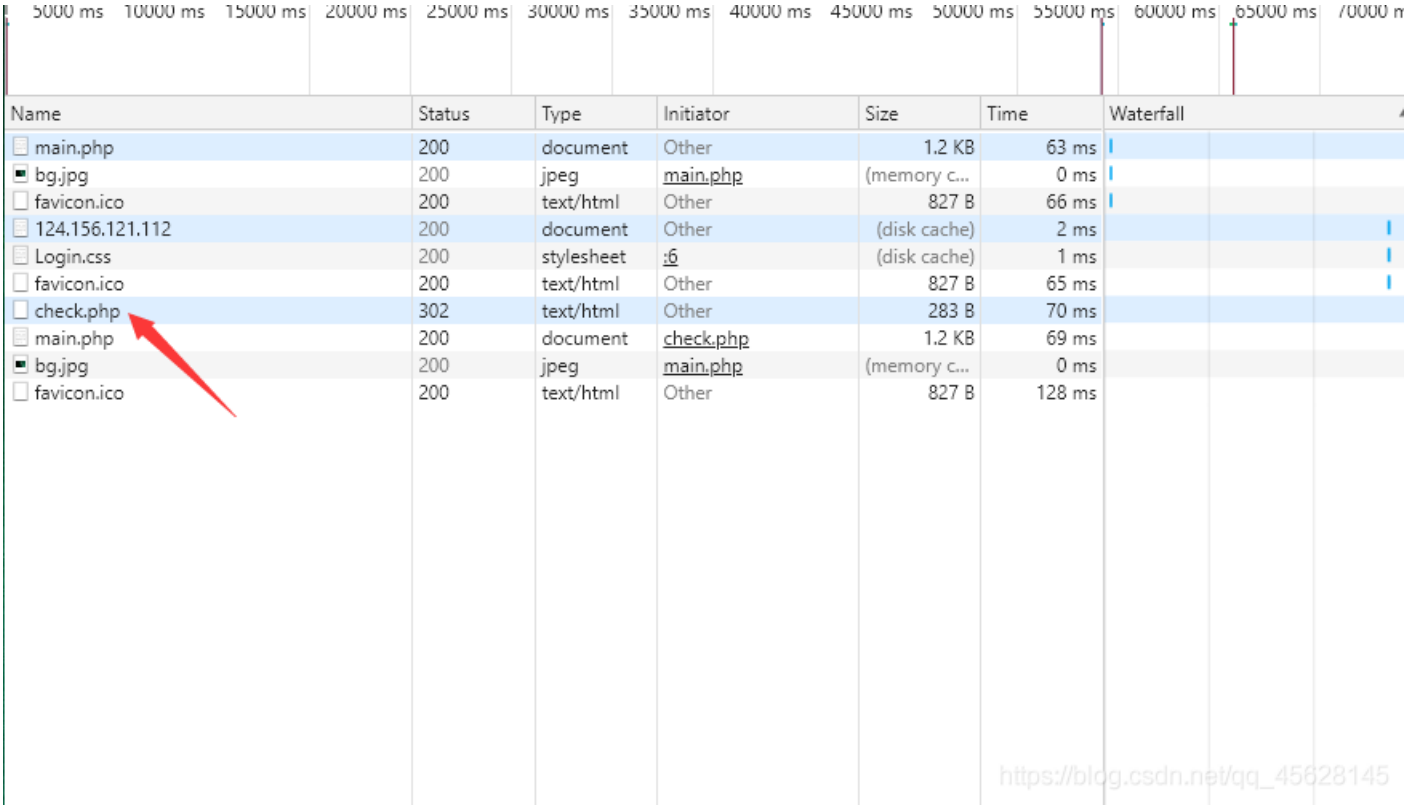
ZmxhZ3tkYWJkYjZlNS04OWNkLTQ1NzQtYTA5YS1jYWUzYWFiYWVmOTh9Cg==

flag{dabdb6e5-89cd-4574-a09a-cae3aabaef98}

提交，正确，终于做出来了。
这个响应头呢是登陆的时候，check.php回复的，登陆进去之后在浏览器里面没看见，开始在浏览器的的network里面当时也没有看到它的回复，可能是因为我登陆进去刷新了一下页面导致的。



然后我又登陆了一次，登陆进去没有刷新，就看到了。



总结：这真的是一个萌新题！！！怪不得群主说放出提示可能就被秒了！！！弱口令登陆的密码admin888来源于动易默认密码。