BUUCTF [MRCTF2020] PYWebsite

原创

Senimo_ 于 2021-01-05 23:08:58 发布 178 收藏 3

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF MRCTF2020 PYWebsite writeup CTF

[MRCTF2020]PYWebsite

考点：

1. X-Forwarded-For

启动环境：

提示需要购买flag，首先对题目进行信息收集，查看网页源码时，发现：

```
<script>

   function enc(code){
     hash = hex_md5(code);
     return hash;
   }
   function validate(){
     var code = document.getElementById("vcode").value;
     if (code != ""){
       if(hex_md5(code) == "0cd4da0223c0b280829dc3ea458d655c"){
         alert("您通过了验证！");
         window.location = "./flag.php"
       }else{
         alert("你的授权码不正确！");
       }
     }else{
       alert("请输入授权码");
     }

   }

 </script>
```

通过验证后将跳转到`flag.php`页面，访问`flag.php`页面：

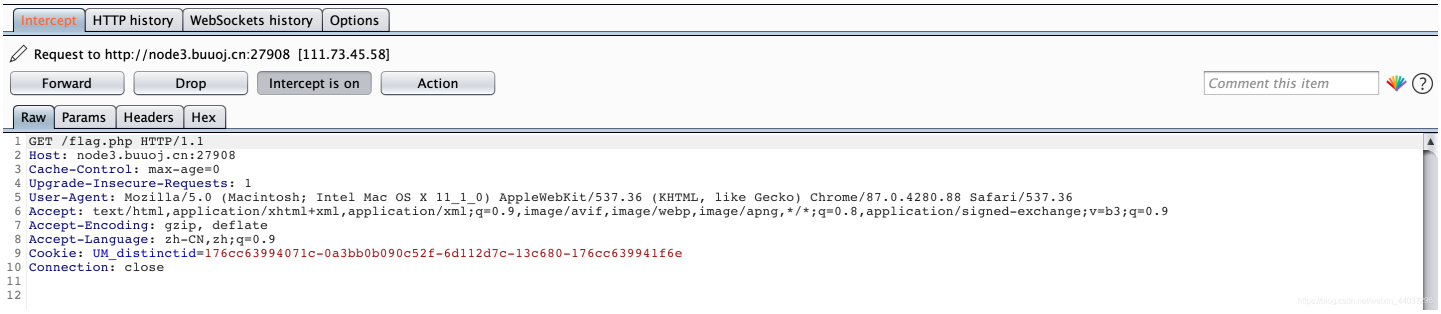
拜托，我也是学过半小时网络安全的，你骗不了我！

我已经把购买者的IP保存了，显然你没有购买

验证逻辑是在后端的，除了购买者和我自己，没有人可以看到flag

还不快去买

提示在后端验证了IP，还提示了需要购买者或自己IP，猜测可能是对`X-Forward-For`做了验证，使用**BurpSuite**抓取数据包：



在请求信息中添加：`X-Forwarded-For: 127.0.0.1`，发送数据包，得到flag：