前言

这周过年，基本没怎么做题，就看了一本xss的书和学了一点python。不能这么堕落了，等wp出来复现。

web

LazyDogR4U

Description
懒狗R4u把Flag藏起来了，但由于他是懒狗，所以flag藏的很不安全。
Challenge Address http://93c4f94f2e.lazy.r4u.top
首先，通过 hint，在地址后面加上 /www.zip 下载源码。又通过 hint 知道是变量覆盖。

```
if($_SESSION['username'] === 'admin'){
    echo "<h3 style='color: white'>admin将于今日获取自己忠实的flag</h3>";
    echo "<h3 style='color: white'>$flag</h3>";
}else{
    if($submit == "getflag"){
        echo "<h3 style='color: white'>{$_SESSION['username']}接近了问题的终点</h3>";
    }else{
        echo "<h3 style='color: white'>篡位者占领了神圣的页面</h3>";
    }
}
```


注意到 $_SESSION['username'] === 'admin' 时，会输出 $flag。查找资料后，知道是 $ 导致的变量覆盖漏洞。所以在地址栏上加上 ?_SESSSESSIONION[username]=admin，得到 flag。

misc

DNS

Description
A significant invention.
Challenge
Addresshttps://1.oss.hgame2021.vidar.club/dns_250e1c3c63209fd5546937be4f41cb39.pcapng
打开，用wireshark导出，发现一段代码。

```
<html>
<head>
</head>
<body>
<script>
        while(true){
            alert("Flag is here but not here")
        }
    </script>
<b>Do you know SPF?</b>
</body>
</html>
```


查资料，知道SPF协议本质是DNS，并且通过TXT记录。看到 alert(“Flag is here but not here”)，猜测flag在TXT记录里。在wireshark抓的包里找到http://flag.hgame2021.cf/。通过在cmd里输入nslookup -q=TXT http://flag.hgame2021.cf/ ，查询到flag。