Whale蓝鲸CTF—Web writeup

原创

Senimo_ 于 2019-08-14 19:23:17 发布 475 收藏 1
分类专栏： 各CTF平台 Writeup 文章标签： 蓝鲸CTF WhaleCTF writeup web

本文链接：https://blog.csdn.net/weixin_44037296/article/details/99438503

Whale蓝鲸CTF—Web writeup

Whale蓝鲸CTF链接

SQL注入

无法打开页面，暂时无法做。

Find me

分值：50
请找到我
解题链接

查看**网页源码**即可得到flag：

```
<!--flag:{This_is_s0_simpl3}-->
```

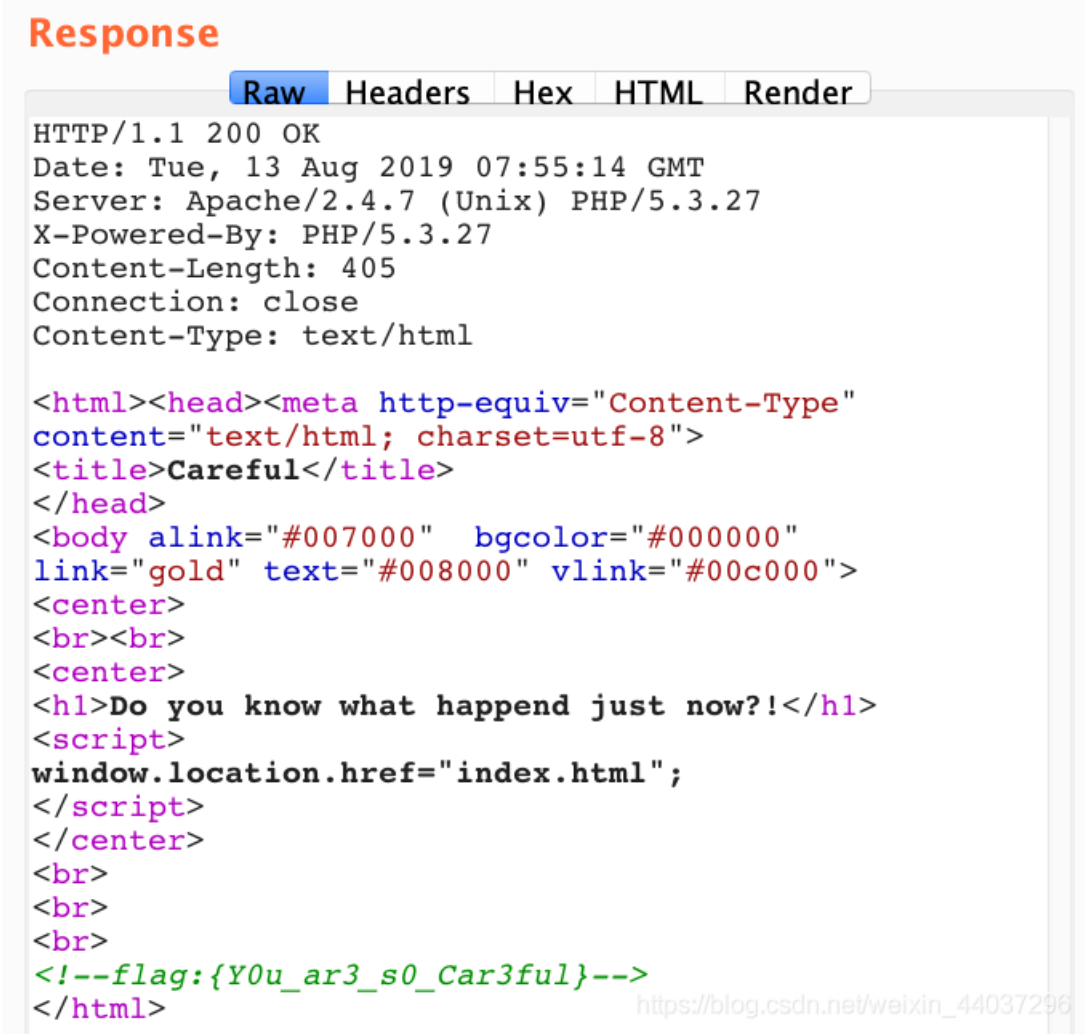
http呀

分值：50

从你眼前溜过去了~

解题链接

根据提示**从你眼前溜过去**，使用**Burp Suite**抓取数据包，**Send to Repeater**后发送数据包，在**Response**得到**flag**：



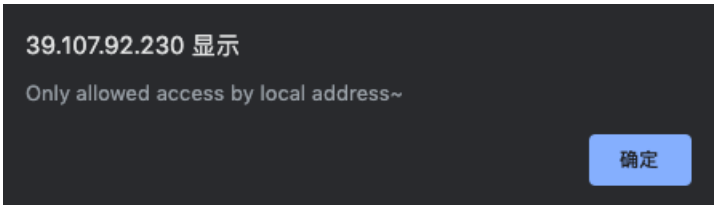
本地登陆

分值：100

只允许本机登录哦！

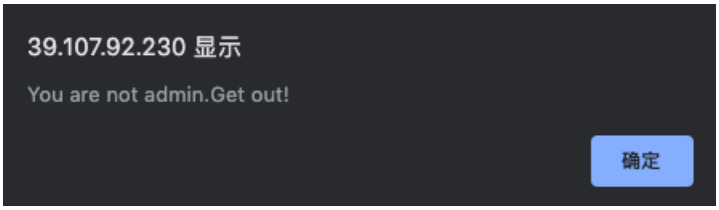
解题链接

进入页面后提示弹窗：

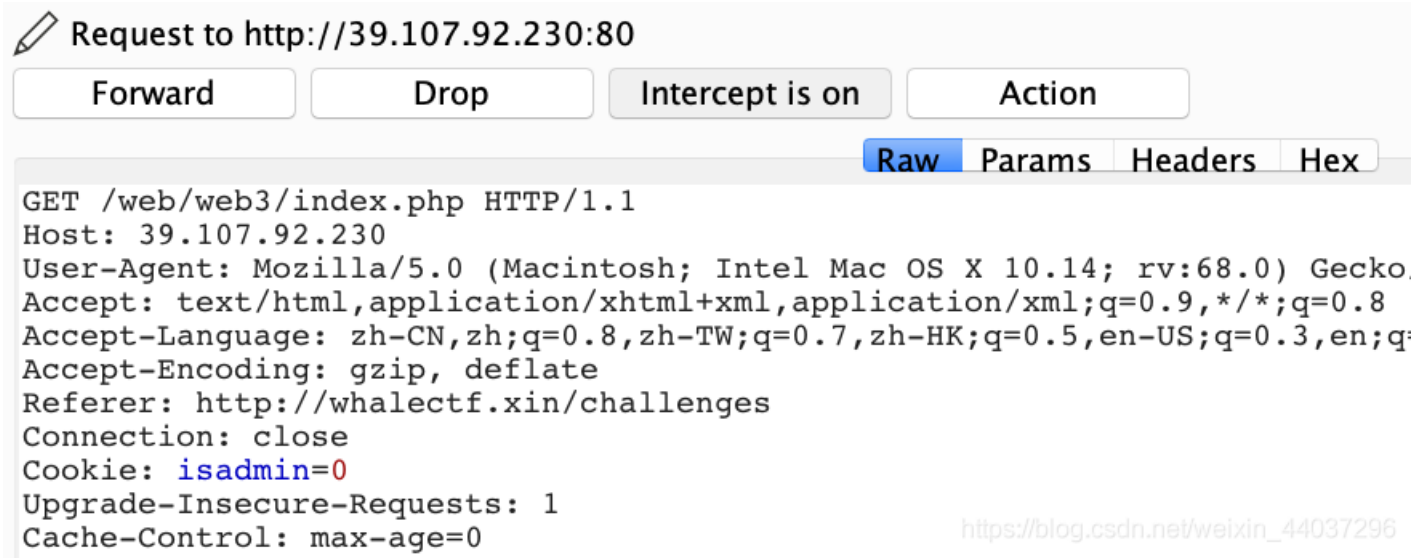


在**Google Chrome插件ModHeader**添加`X-Forwarded-For:127.0.0.1`，得到新的提示

进入页面后显示：



使用**Burp Suite**抓取数据包：



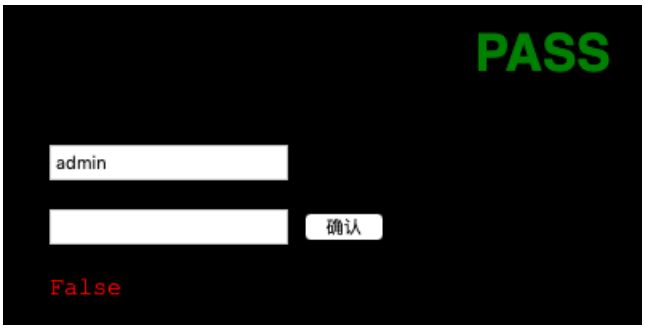
将**Cookie**中的`siadmin=0`修改为`isadmin=1`，发送数据包，获得**flag**：`flag:{Why_ar3_y0u_s0_dia0}`

密码泄露

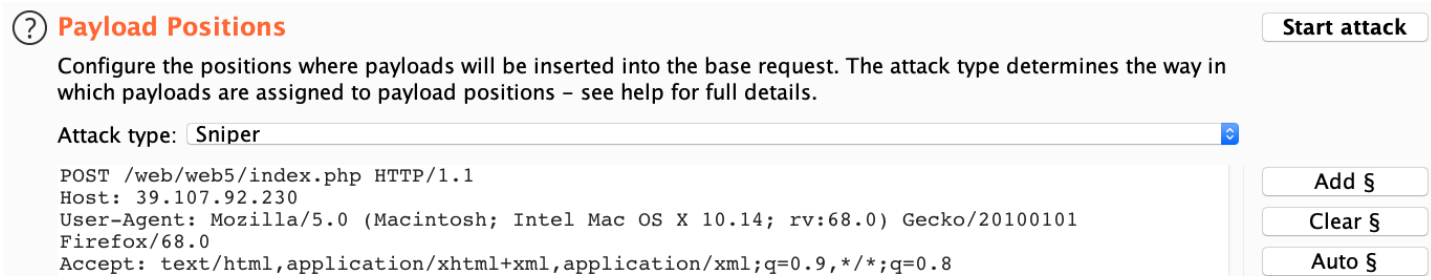
分值：100

不小心把密码泄露出来了！

解题链接



提示需要登陆，查看**网页源码**，得到提示`<!--password.txt-->`，访问该页面，下载密码字典，使用**Burp Suite**抓取数据包，**Send to Intruder**，修改变量：

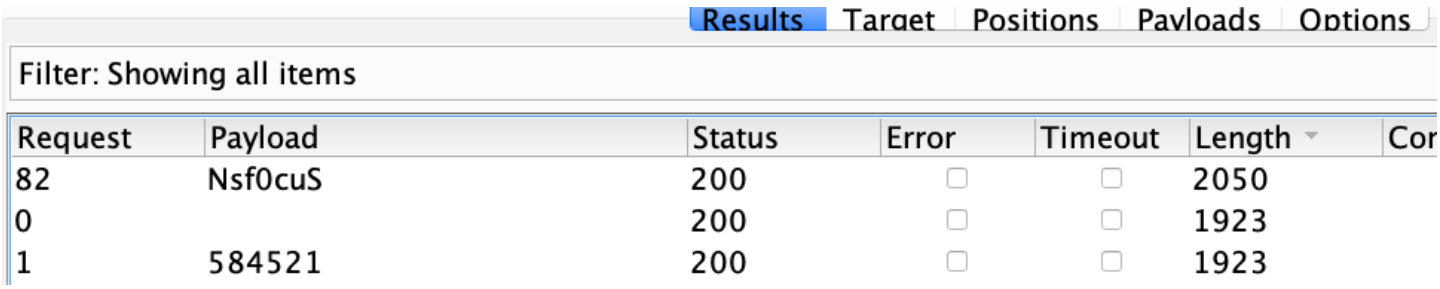


```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Connection: close
Referer: http://39.107.92.230/web/web5/index.php
Upgrade-Insecure-Requests: 1

username=admin&password=$admin$
```

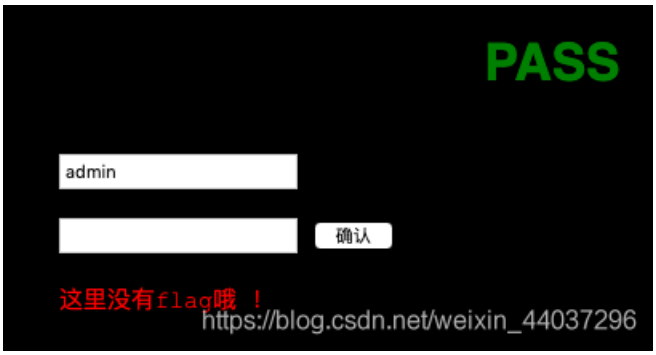
Refresh

将密码字典粘贴到**Payload Options**，**Start attack**，根据长度得出密码：`Nsf0cuS`




```
<input type="password" name="password" maxlength="5" value="" ></input>
```

将**<input>**标签中的**maxlength**属性的限制去掉后登陆：



使用使用**Burp Suite**抓取登陆时的数据包，在**Response**中得到新的提示`newpag`：

```
Date: Wed, 14 Aug 2019 07:03:07 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie:
newpage=MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMGI5ZDgzYjk
ucGhw; expires=Wed, 14-Aug-2019 07:04:07 GMT
Content-Length: 1753
Connection: close
Content-Type: text/html
```


在线Base64解码，得到`290bca70c7dae93db6644fa00b9d83b9.php`，访问新页面：

小黑留言板

小黑最近刚学会php就写了个留言板让大家使用,可是这个留言板有漏洞，导致大黑们可以通过某些手段以小黑的身份留言

大黑们，你们准备好了吗?

留言者	留言内容

尝试留言：

留言者	留言内容
guest	111

显示留言者为**guest**，使用**Burp suite**抓取数据包：

Request to http://39.107.92.230:80

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

```
POST /web/web5/290bca70c7dae93db6644fa00b9d83b9.php?act=add HTTP/1.1
Host: 39.107.92.230
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Connection: close
Referer: http://39.107.92.230/web/web5/290bca70c7dae93db6644fa00b9d83b9.php?act=add
Upgrade-Insecure-Requests: 1

content=1111&userlevel=guest&Submit=%E7%95%99%E8%A8%80
```

Send to Repeater后添加**Cookie**参数`Login=1`，将`guest`修改为`root`，发送数据包后在**Response**中的到**URL编码的flag**：`Flag=flag%7BC0ngratulati0n%7D`，解码后提交。