

网络信息安全攻防学习平台-脚本关 writeup

原创

4ct10n 于 2016-09-17 00:33:58 发布 22986 收藏 5

分类专栏: [WEB漏洞 write-up](#) 文章标签: [信息安全](#) [脚本](#) [hackinglab](#) [writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_31481187/article/details/52559718

版权



[WEB漏洞](#) 同时被 2 个专栏收录

23 篇文章 2 订阅

订阅专栏



[write-up](#)

22 篇文章 2 订阅

订阅专栏

1.key又又找不到了

直接burpsuit截断

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
39	http://lab1.xseclab.com	GET	/xss1_30ac8668cd453e7e387c76b132...	<input type="checkbox"/>	<input type="checkbox"/>	200	278	HTML	php	
40	http://lab1.xseclab.com	GET	/xss1_30ac8668cd453e7e387c76b132...	<input type="checkbox"/>	<input type="checkbox"/>			HTML	php	
41	http://s1-im-notify.csdn.net	GET	/socket.io/1/xhr-polling/fcwxKjzGUeQ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
42	http://i.g-fox.cn	GET	/notification/0.7/rules_sincefx4.json	<input type="checkbox"/>	<input type="checkbox"/>			script	json	

```
GET /xss1_30ac8668cd453e7e387c76b132b140bb/search_key.php HTTP/1.1
Host: lab1.xseclab.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://lab1.xseclab.com/xss1_30ac8668cd453e7e387c76b132b140bb/index.php
```

出flag

key is : yougotit_script_now

2.快速口算

这道题比较有意思

在两秒钟之内回答他的算术题

思路：直接编写python脚本访问网站，获取html计算算式，得出答案，post传参，注意要建立长连接。

代码如下：

```
# -*- coding:utf-8 -*-
import requests, re
url = 'http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php'
s = requests.session()
c = s.get(url).content
print c
r = re.findall(r'[\d]{2,}',c)
r=int(r[0])*int(r[1])+int(r[2])*(int(r[3])+int(r[4]))
c1 = s.post(url, data={'v':r}).content
print c1.decode('utf-8')

print eval('8743*89513+1985*(8743+89513)')
```

这里有一篇python request 的快速入门

编写的代码如下：

```
# -*- coding:utf-8 -*-
import requests, re
url = 'http://lab1.xseclab.com/xss2_0d557e6d2a4ac08b749b61473a075be1/index.php'
s = requests.session()
c = s.get(url).content
print c
r = re.findall(r'[\d]{2,}',c)
r=int(r[0])*int(r[1])+int(r[2])*(int(r[3])+int(r[4]))
c1 = s.post(url, data={'v':r}).content
print c1.decode('utf-8')

print eval('8743*89513+1985*(8743+89513)')
...
decode的作用是将其他编码的字符串转换成unicode编码，
如str1.decode('gb2312')，表示将gb2312编码的字符串转换成unicode编码。
encode的作用是将unicode编码转换成其他编码的字符串，
如str2.encode('gb2312')，表示将unicode编码的字符串转换成gb2312编码。
...
```

在这补充一句正则表达式python用法：

```
import re #导入re模块
r = re.findall(r'[\d]{2,}',c) #匹配所有会连的
r=int(r[0])*int(r[1])+int(r[2])*(int(r[3])+int(r[4]))
```

运行脚本即可得flag

key is 123iohHKHJ%^&*(jkh

3.这个题目是空的

什么是空的:

0,null,none,no等等试一下就出来了

结果为null

4.怎么就是不弹出key呢?

查看页面源码:

```
把前面几个函数去掉
function alert(a){
    return false;
}
document.write=function(){
    return false;
}
function prompt(a){
    return false;
}
```

重新打开即可

5.逗比验证码第一期

有验证码就不能爆破吗?答案是能

burpsuit intruder爆破一下出来

6.逗比验证码第二期

将vcode=;即vcode不赋值

7.逗比的验证码第三期 (SESSION)

解法同6

8.微笑一下就能过关了

这是道好题

看页面源码:

```
<label for="SMILE">请使用微笑过关<a href="?view-source">源代码</a></label>
<input type="text" name="T_T" placeholder="where is your smile" required>
```

打开连接出来源代码

```
http://lab1.xsecrlab.com/base13_ead1b12e47ec7cc5390303831b779d47/index.php?view-source
```

代码如下:

```

<?php
    header("Content-type: text/html; charset=utf-8");
    if (isset($_GET['view-source'])) {
        show_source(__FILE__);
        exit();
    }

    include('flag.php');

    $smile = 1;

    if (!isset($_GET['^_^'])) $smile = 0;
    if (preg_match ( '/\./', $_GET['^_^'])) $smile = 0;
    if (preg_match ( '/%/', $_GET['^_^'])) $smile = 0;
    if (preg_match ( '/[0-9]/', $_GET['^_^'])) $smile = 0;
    if (preg_match ( '/http/', $_GET['^_^']) ) $smile = 0;
    if (preg_match ( '/https/', $_GET['^_^']) ) $smile = 0;
    if (preg_match ( '/ftp/', $_GET['^_^'])) $smile = 0;
    if (preg_match ( '/telnet/', $_GET['^_^'])) $smile = 0;
    if (preg_match ( '/_/', $_SERVER['QUERY_STRING'])) $smile = 0;
    if ($smile) {
        if (@file_exists ($_GET['^_^'])) $smile = 0;
    }
    if ($smile) {
        $smile = @file_get_contents ($_GET['^_^']);
        if ($smile === "(•'-'•)") die($flag);
    }
?>

```

出现了各种绕过。

1. 必须有^_^参数
2. 参数中不能有.%
3. 键名中不能有_(与1矛盾)
4. ^_^必须是文件
5. 文件不再本地存在

这题学到了新知识，data协议

data://text/plain;charset:unicode,(•'-'•)

就可构造出文本

对于3绕过的方法是在URL中_和.等价所以参数为^_^

得出flag

hkjasfhsa*&IUHKUH