

# BugkuCTF Web部分的几道题

原创

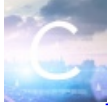
[Sandra\\_93](#) 于 2018-10-22 19:55:51 发布 349 收藏

分类专栏: [BugkuCTF CTF](#)

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/Sandra\\_93/article/details/83210672](https://blog.csdn.net/Sandra_93/article/details/83210672)

版权



[BugkuCTF](#) 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



[CTF](#)

9 篇文章 0 订阅

订阅专栏

## Web4

**url解码:** url编码, 由%和数字构成

将代码用url进行解码,

```
var p1 = 'function checkSubmit(){
var a=document.getElementById("password");
if("undefined"!==typeof a){
if("67d709b2b";
var p2 = 'aa648cf6e87a7114f1'==a.value)
return!0;
alert("Error");
a.focus();
return!1
}
}document.getElementById("levelQuest").onsubmit=checkSubmit;';
eval(unescape(p1) + unescape('54aa2' + p2));
```

**unescape() 函数:**可对通过 escape() 编码的字符串进行解码。该函数的工作原理是这样的: 通过找到形式为 %xx 和 %uxxxx 的字符序列 (x 表示十六进制的数字), 用 Unicode 字符 \u00xx 和 \uxxxx 替换这样的字符序列进行解码。

**eval()函数:**eval() 函数可计算某个字符串, 并执行其中的的 JavaScript 代码。

```
eval("2+3")    返回5
```

所以就是拼接, 拼成这个输进去

67d709b2b54aa2aa648cf6e87a7114f1, 得到writeup

## 输入密码查看flag

五位数字密码, 直接到burp suite里

抓包, 发送到Intruder, 设置payloads type为numbers,

到options里设置个多线程就好

## 点击一百万次

查看源代码，还真要一百万次才能蹦出flag,

```
if(clicks >= 1000000){
    var form = $('<form action="" method="post">' +
        '<input type="text" name="clicks" value="' + clicks + '"' hidden/>' +
        '</form>');
    $('body').append(form);
    form.submit();
}
```

好吧，方式post,使用插件Hackbar,在第一个框里粘贴地址，勾上Enable Post data,又出现一个框，写上：

```
clicks=1000000000, (随便多少，大于一百万就ok)
```

这是用post方式传进去一个参数，

web基础\$\_POST也是这种做法

## 各种绕过

看代码，要uname不等于passwd,但是sha1又要相等，那就数组呀

按要求，uname是get方式，passwd是post方式，

那就url里补充

```
?uname[]=1&id=margin
```

post方式传送 passwd[]=1