[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

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。

```
</head>
<script>
    $.ajax({
    url: "api/admin",
    type: "get",
    success:function (data) {
        //console.log(data);
        if (data.code == 200){
            // 如果有值：前端跳转
            var input = document.getElementById("flag1");
            input.value = String(data.data);
        } else {
            // 如果没值
            $('#flag1').html("接口异常，请稍后再试~");
        }
    }
})
</script>
<script>
$.ajax({
    url: "api/ctf/2",
    type: "get",
    success:function (data) {
        //console.log(data);
        if (data.code == 200){
            // 如果有值：前端跳转
            $('#flag2').html("flag2: " + data.data);
        } else {
            // 如果没值
            $('#flag2').html("需要使用bilibili Security Browser浏览器访问~");
        }
    }
```


JSON 原始数据 头

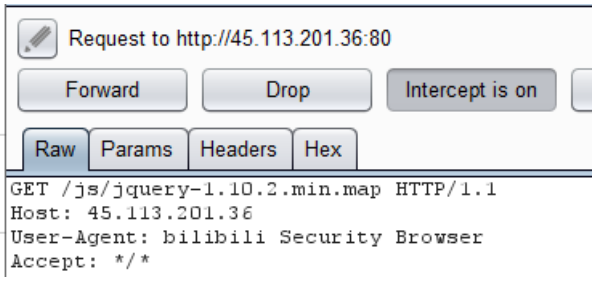
保存 复制 全部折叠 全部展开 过滤 JSON

```
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

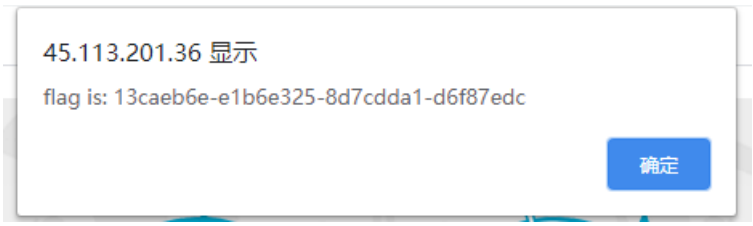
直接访问页面提示需要使用bilibili Security Browser浏览器访问，加上题目的hint，非常传统的一道ctf题，应该是要改写UserAgent来访问。

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



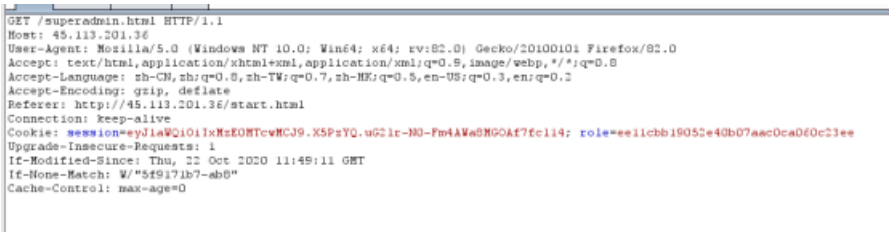
0x03 密码是啥？

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。



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。

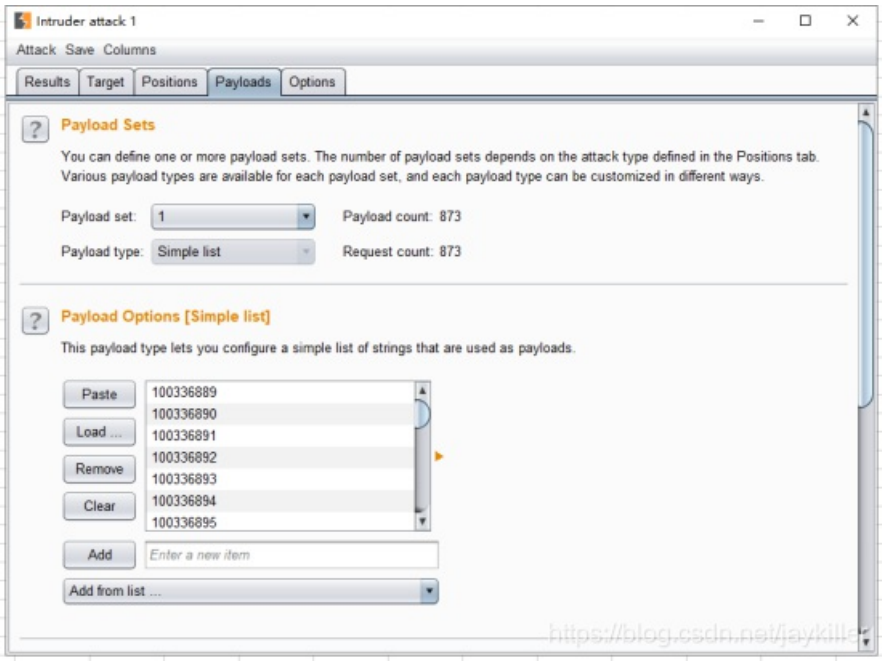
这里没有你想要的答案~

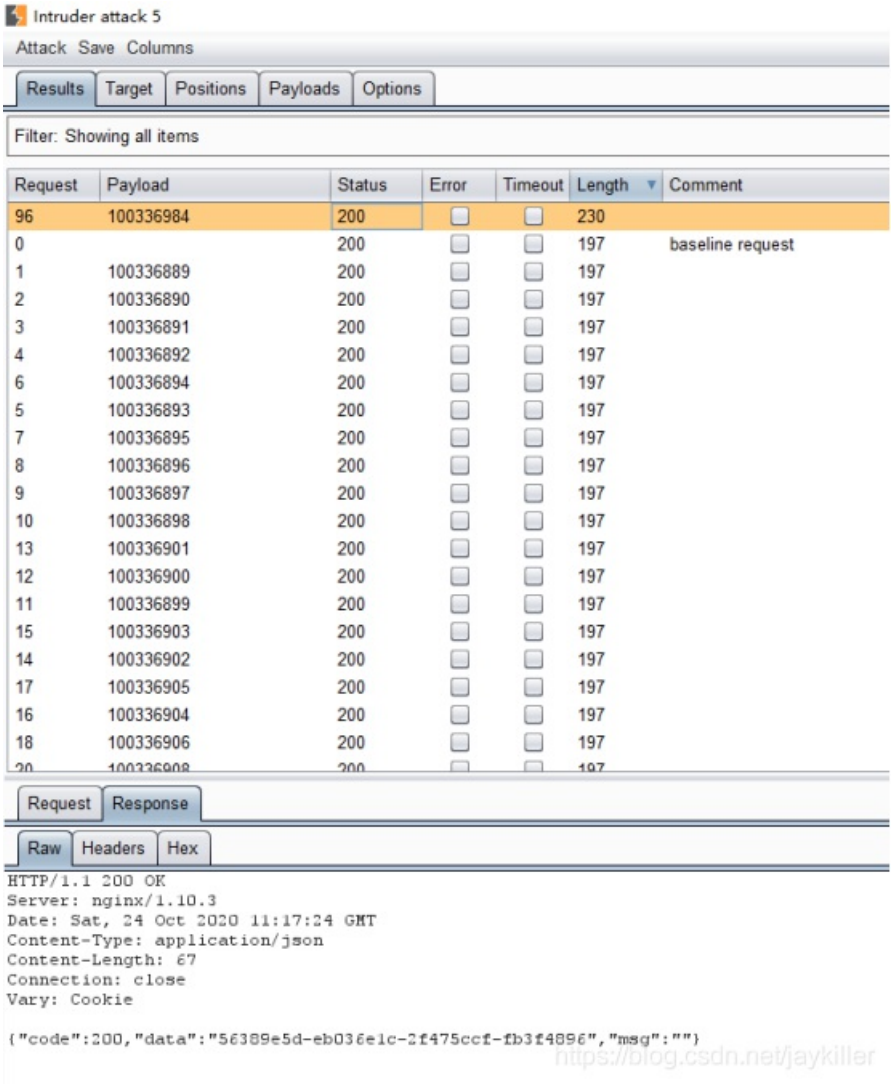

```
$(function () {

    (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~")
            }
        }
    })
});
```


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。

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 ▾

@in interesting-1024 Add files via upload

1 contributor

22 lines (17 sloc) | 382 Bytes

```php
<?php

//filename end.php

$bilibili = "bilibili1024havefun";

$str = intval($_GET['id']);
$reg = preg_match('/\d/is', $_GET['id']);

if(!is_numeric($_GET['id']) and $reg !== 1 and $str === 1){
        $content = file_get_contents($_GET['url']);

        //文件路径猜解
        if (false){
                echo "还差一点点啦~";
        }else{
                echo $flag;
        }
}else{
        echo "你想要的不在这儿~";
}
?>
```


构造路径，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。

用记事本打开，搜索flag，可以找到flag10的值。

((□ 賬{flag10:2ebd3b08-47ffc478-b49a5f9d-f6099d65}}

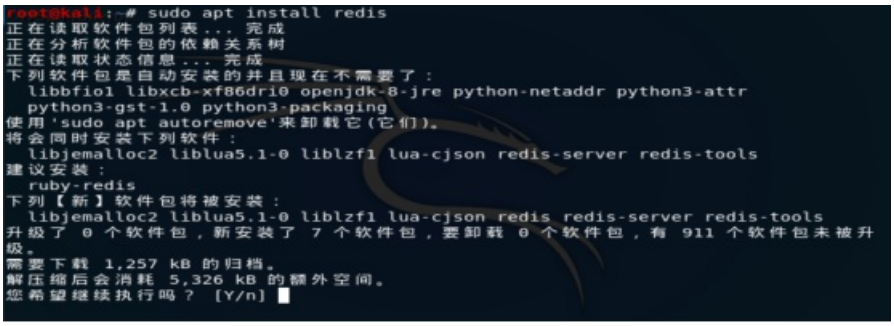
第8题

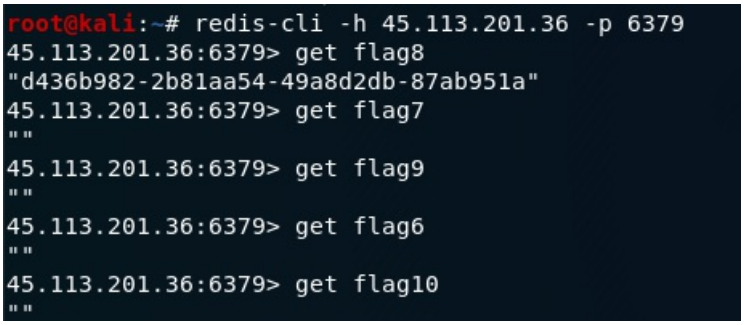
nmap扫一下，因为靶机一直被扫，要看运气，多试几次。大概率会出现只扫出来80端口的情况。

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。

用6379的redis，kali中没有，现下一个。

sudo apt install redis





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。