Catfish-4.5.7利用TP框架漏洞-配合XSRF到Getshell

phpoop / 2017-09-13 06:35:00 / 浏览数 5192 安全技术 漏洞分析 顶(0) 踩(0)

0x01 用户评论处xss

查看了这个框架，可以确定没有注入了，全站基本都是基于缓存进行交互的，因此想着能不能通过xss，首先可以确定的是这个cms使用的是框架thinkphp5，了解到是TP框架的话想找xss的先 看配置文件

文件：application\config.php
参数：default_filter

最后找到一处未过滤的地方

文件：application/index/controller/Index.php
方法：pinglun()

过滤函数

文件：application\index\controller\Common.php
方法：filterJs()

可以看到只是简单的过滤<script>很简单就可以绕过
自己在此cms注册一个账号然后随便点击一篇文章

从这里我们已经可以确定后台评论未过滤完全导致可以xss，我们前面说了这个站点使用TP5做的而且大部分的功能都是与缓存进行交互的！！！那么配合我前段时间发的文章

0x02 Getshell

这里放上我在先知社区的一篇文章方便大家看后面的内容有大概的一个了解：

文章名称：Thinkphp5.0.10-3.2.3缓存函数设计缺陷可导致getshell
文章链接：https://xianzhi.aliyun.com/forum/read/1973.html

看完我上面的文章大家应该有个大概的感念了

经过确认此cms也并没有添加 csrf_token 那么我们就可以使用下面的思路

思路：

前台评论出插入xss代码->诱骗后台管理员访问网站-内容管理-评论管理-自动执行xss代码->通过csrf插入一条新文章->通过csrf清除缓存->在通过js访问前端任意页面生

大概的想法就是这样做了。

后台创建文章方法

地址：application\admin\controller\Index.php
方法：write();

这个方法没有什么可以讲的只是后面的组合漏洞要使用到他

后台清除缓存方法

地址：application\admin\controller\Index.php
方法：clearcache()

这个方法没有什么可以讲的只是后面的组合漏洞要使用到他

例子：

1、准备好脚本

2、利用前面的xss漏洞，配合这个脚本形成xsrf漏洞

这样我们在前端的事情就完事了。接着我们模拟后台管理员进入后台的操作

模拟的后端管理员操作：

漏洞原理与流程：

1、后台创建文章方法

地址：application\admin\controller\Index.php
方法：write();

这个方法没有什么可以讲只是单纯的从前端获取数据然后写入数据库罢了

2、后台清除缓存方法

地址：application\admin\controller\Index.php
方法：clearcache()

这个方法没有什么可以讲的。只是单纯的删除缓存数据

3、访问前端重新生成缓存

地址： application\index\controller\Index.php
方法：index()

缓存的名字由来

缓存的名字组成就是比较简单的了。

这上面几幅图就是缓存的名字了什么意思呢？很简单

首先是从index目录里面的index模块下面的index方法

调用了一个方法`$template = $this->receive('index'); = index`

然后是ndex目录里面的Common模块里面的receive 方法

获取了变量`$source`值 = `index`

获取了变量`$page` 值 =`1`

`Cache::set('hunhe_'.$source.$page,$hunhe,3600);`缓存方法

最后就是

`MD5(hunhe_index1) = 9040ab6906a15768edcd9e5b1d57fcda`

0x 03 后记：

使用此方法的话，尝试一下在url中输入

http://www.xxxxxxx.com/runtime
http://www.xxxxxxx.com/runtime/cache
http://www.xxxxxxx.com/runtime/cache/8d6ab84ca2af9fccd4e4048694176ebf.php

按顺序输入如果前两个访问得到的结果是403 最后的结果不是403或是404
而是返回正常的页面，那么说明站点的缓存目录是可以访问的，这个时候可以使用此漏洞。配合XSS+CSRF获取Getshel

点击收藏 | 0 关注 | 1

上一篇：Use DNS Rebinding... 下一篇：iOS代码加密的几种方式

1. 8 条回复

phpoop 2017-09-13 09:24:38

我晚上重新更新一下图片，现在和马赛克一样。

0 回复Ta

anivia 2017-09-13 15:12:01

看不懂、、

0 回复Ta

hades 2017-09-13 15:44:19

后期会出一套代码审计的初级文章把
成长总是有过程的

0 回复Ta


wyldlmu 2017-09-14 00:52:59

表哥，排版有点迷糊

0 回复Ta


hades 2017-09-14 01:33:19

你确定？？？

0 回复Ta

phpoop 2017-09-14 16:42:44

例如是哪里看不懂呢？

0 回复Ta


lucifaer 2017-09-15 01:36:27

好文，之前就看到过师傅的那篇文章，一直在找利用TP5缓存getshell的例子，可惜没找到。
这次的挖掘思路非常的清晰，学习了

0 回复Ta

 hades 2017-09-15 01:55:08

先低调~别怼了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板