# i春秋网络安全公益赛 web easythinking thinkphp6.0 session任意创建文件、getshell

原创

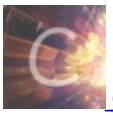
令狐东菱 于 2020-02-24 12:35:28 发布 

分类专栏： CTF



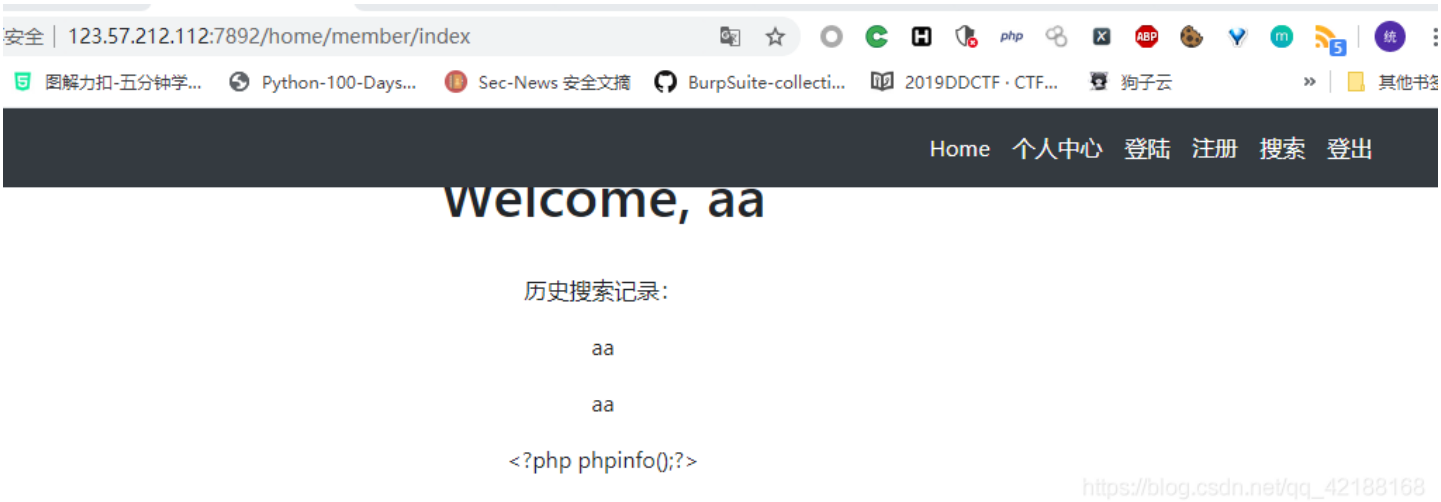
本文链接：https://blog.csdn.net/qq_42188168/article/details/104475375







首先进来看到url很熟悉，直接访问/user/member/index，发现爆错爆出了版本号





随后去网上搜索thinkphp 6.0漏洞，发现了最近的下面这篇文章

https://www.uedbox.com/post/65126/

# thinkphp6 session 任意文件创建漏洞POC

发表于 2020年02月01日 Vulndb

2020年1月13号，Thinkphp 6.0.2发布，在详情页指出修复了一处Session安全隐患。经分析，该漏洞允许攻击者在目标环境启用session的条件下创建任意文件以及删除任意文件，在特定情况下还可以getshell。

具体受影响版本为ThinkPHP6.0.0-6.0.1。

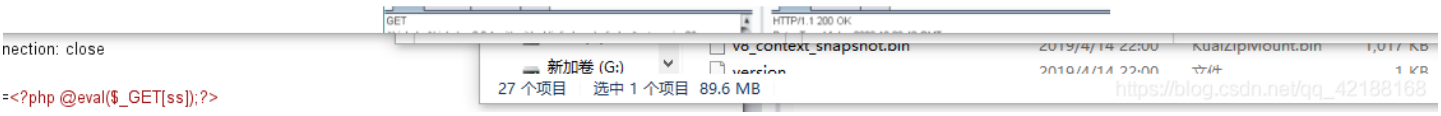
## 漏洞复现

在index控制器中添加如下action

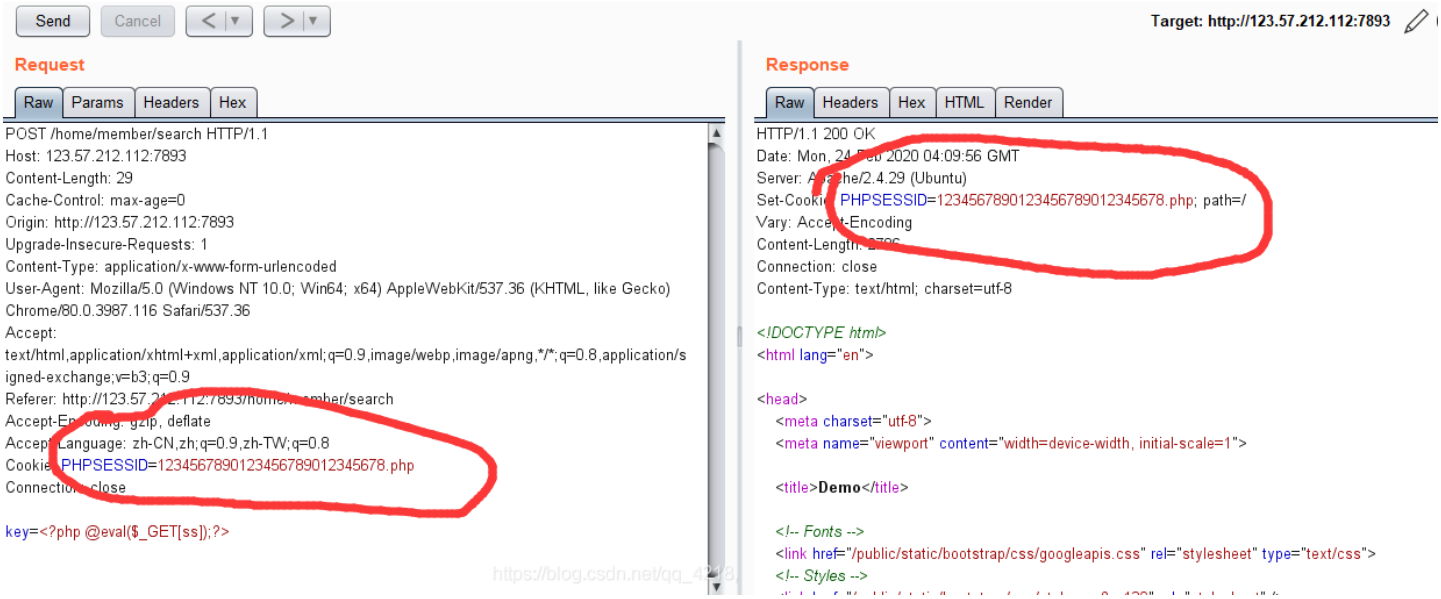
```
public function testsession2(){
    $username = Request::get('name');
    Session::set('username', $username);
    return 'hi';
}
```

用于获取name参数，并将之设置到session中。

访问url: http://127.0.0.1/tp6/public/index.php/index/testsession2?name=<?php%20phpinfo();?>




该漏洞可以在目标环境开启session的条件下任意创建文件，且在特定情况下可以getshell。
下面尝试了一下，大写的惊喜。




随后查看了phpinfo()、蚁剑进行连接,发现disable_function过滤了很多函数，直接上蚁剑的bypass插件绕过，在根目录下发现readflag，执行得到flag