

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 268 收藏 1

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

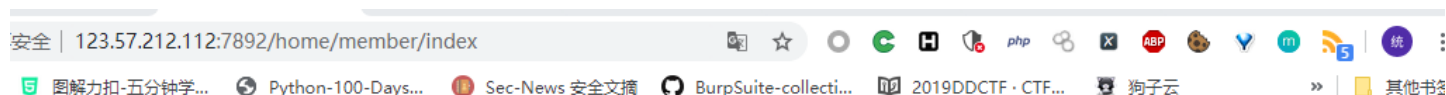


[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

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



Home 个人中心 登陆 注册 搜索 登出

Welcome, aa

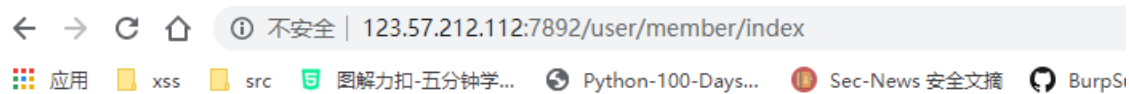
历史搜索记录:

aa

aa

<?php phpinfo();?>

https://blog.csdn.net/qq_42188168



控制器不存在: app\home\controller\User

[ThinkPHP V6.0.0 { 十年磨一剑-为API开发设计的高性能框架 } - 官方手册](#)

https://blog.csdn.net/qq_42188168

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/>



您阻止了广告, 我们绝不会做任何打扰您正常浏览的广告。请考虑停用广告拦截器或将 uedbox.com 加入白名单来支持我们发展下去, 感谢!

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。

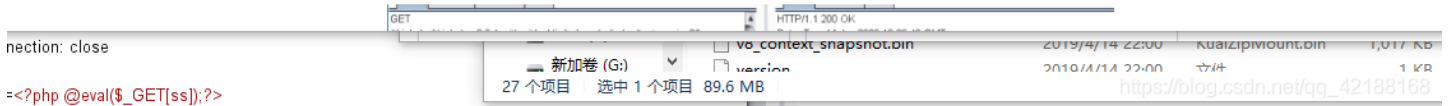
漏洞复现

在index控制器中添加如下action

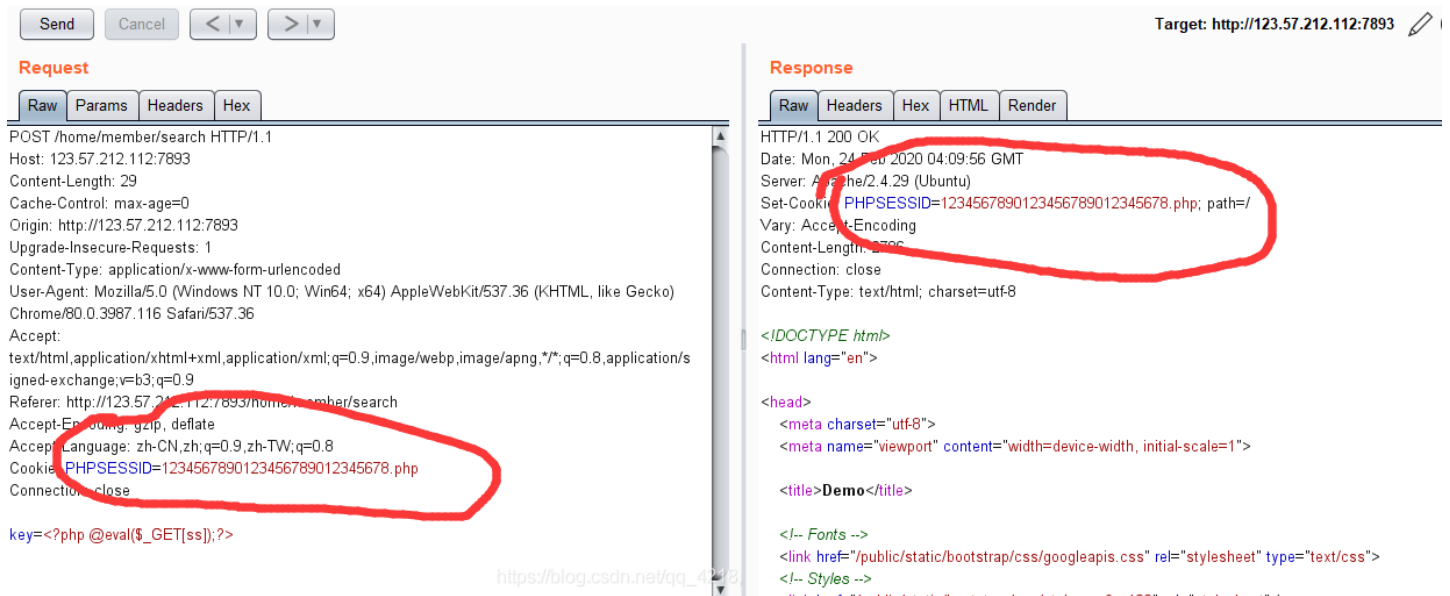
```
1 public function testsession2(){
2     $username = Request::get('name');
3     Session::set('username', $username);
4     return 'hi!';
5 }
```

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





[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)