

盘企LCMS的代码审计 『CNVD-2021-28469』

一 前言

前不久逛 cnvd 的时候看到一款小众 CMS, 大型 CMS 咱也审计不出啥漏洞呀, 复盘了下上面的漏洞, 仔细看了下, 又发现了一些其他的问题, 小众 cms 可以跟一下具体的流程, 了解下漏洞发生的原因, 用来练手还是可以的。

二 反射型 XSS 漏洞

其实像这样小众的 CMS 出现 XSS 漏洞是比较常见的, 而他出现 XSS 的地方也算是经常遇到的地方, 报错时直接把输入的信息在没有任何安全措施的情况下进行了原样输出从而触发了 XSS 漏洞。

拿到该 CMS 的第一步首先简单看下看下该 CMS 的 URL 路由情况, 方便定位相关函数

```
$t = @$_GET['t'] ? $_GET['t'] : "sys";
$n = @$_GET['n'] ? $_GET['n'] : "index";
$c = @$_GET['c'] ? $_GET['c'] : "index";
$a = @$_GET['a'] ? $_GET['a'] : "index";
define("L_TYPE", $t);
define("L_NAME", $n);
define("L_CLASS", $c);
define("L_MODULE", "admin");
define("L_ACTION", "do{$a}");
require_once '../core/route.php';
```

包含了 / core/route.php 函数, 跟进去看一下

```
define('PATH_UPLOAD', PATH_WEB . "upload/");
define('PATH_CORE', PATH_WEB . "core/");
define('PATH_CORE_CLASS', PATH_WEB . "core/class/");
define('PATH_CORE_FUNC', PATH_WEB . "core/function/");
define('PATH_CORE_PLUGIN', PATH_WEB . "core/plugin/");
define('PATH_APP_NOW', PATH_APP . L_TYPE . '/' . L_NAME . '/');
define('PATH_APP_OWN', PATH_APP . L_TYPE . '/' . L_NAME . '/' . L_MODULE . '/');
define('PHP_FILE', basename(__FILE__));
define('PHP_SELF', htmlentities($_SERVER['PHP_SELF']) == "" ? $_SERVER['SCRIPT_NAME'] : htmlentities($_SERVER['PHP_SELF']));
define('SYS_TIME', time());
define('HTTP_HOST', isset($_SERVER['HTTP_HOST']) ? $_SERVER['HTTP_HOST'] : $_SERVER['SERVER_NAME']);
define('HTTP_PORT', $_SERVER["SERVER_PORT"]);
define('HTTP_TOP', $_SERVER['HTTP_REFERER']);
define('HTTP_QUERY', $_SERVER['REQUEST_URI']);
define('SERVER_IP', $_SERVER['SERVER_ADDR']);
define('PAGE_START', microtime(true));
require_once PATH_CORE_FUNC . 'common.func.php';
require_once PATH_CORE_CLASS . 'lcms.class.php';
if ((!L_NAME || !L_CLASS || !L_ACTION) && !preg_match('/^[A-Za-z0-9_]+$', L_TYPE . L_NAME . L_MODULE
```

```

L_CLASS . L_ACTION)) {
    LCMS::X(403, "拒绝访问");
}
require_once PATH_CORE_CLASS . 'load.class.php';
define('CLIENT_IP', LCMS::IP());
load::module();

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628165242-333b7040-d7ee-1.png>)

定义了一些常量，在最后调用了 load 类中的 module 函数，该函数位于 \core\class\load.class.php 中

```

public static function module($path = '', $modulename = '', $action = '')
{
    if (!$path) {
        if (!$path) {
            $path = PATH_APP_OWN;
        }
        if (!$modulename) {
            $modulename = L_CLASS;
        }
        if (!$action) {
            $action = L_ACTION;
        }
        if (!$action) {
            $action = 'doindex';
        }
    }
    return self::_load_class($path, $modulename, $action);
}

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628165410-67c2ba62-d7ee-1.png>)

然后调用相关函数，该函数会查看传入的文件是否存在

```

private static function _load_class($path, $classname, $action = '')
{
    $classname = str_replace('.class.php', '', $classname);
    $is_myclass = 0;
    if (!@self::$mclass[$classname]) {
        if (is_file($path . $classname . '.class.php')) {
            require_once $path . $classname . '.class.php';
        } else {
            LCMS::X(404, str_replace(PATH_WEB, '', $path) . $classname . '.class.php 文件不存在');
        }
    }
}

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628165518-900c6c20-d7ee-1.png>)

如果文件不存在会将错误信息传入类 LCMS 的 X 函数，该函数位于 \core\class\lcms.class.php 中，该函数会调用 template 函数生成模板进行错误的输出

```
/**
 * @输出错误提示页面
 * @param {*}
 * @return {*}
 */
public static function X($errcode, $errmsg, $go = "")
{
    if ($_SERVER['CONTENT_TYPE'] == "application/json" || (isset($_SERVER["HTTP_X_REQUESTED_WITH"]) &&
    strtolower($_SERVER["HTTP_X_REQUESTED_WITH"]) == "xmlhttprequest")) {
        ajaxout(0, $errmsg ? "拒绝访问！");
    } else {
        global $_L;
        $X["code"] = $errcode ? 403;
        $X["msg"] = $errmsg ? "拒绝访问！";
        require self::template(PATH_PUBLIC . "ui/admin/X");
    }
    exit;
}
```

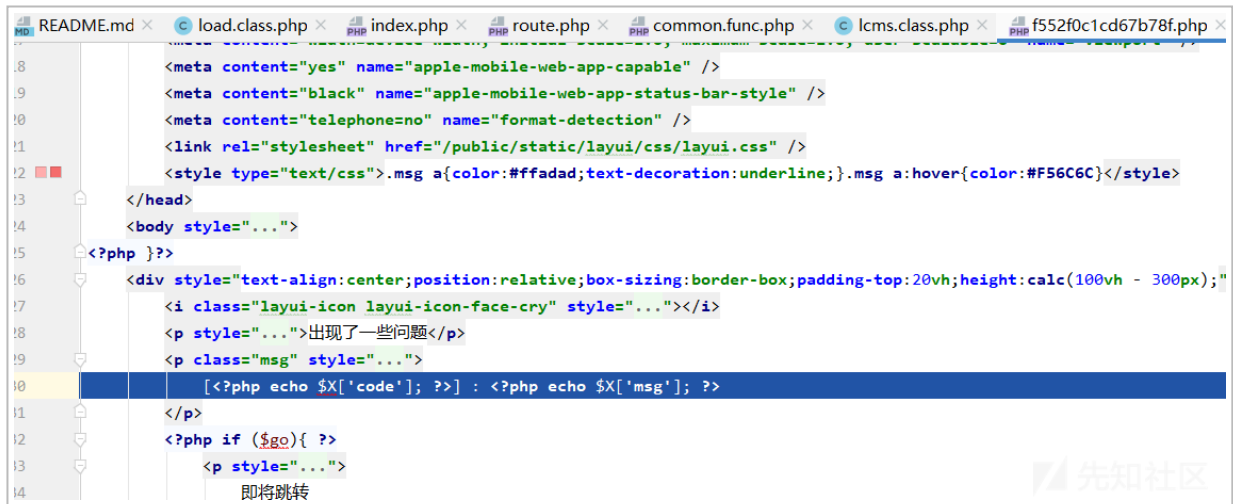
(<https://xzfile.aliyuncs.com/media/upload/picture/20210628165622-b67864fe-d7ee-1.png>)

然后生成报错信息模板

```
public static function template($path, $ui = "")
{
    global $_L;
    $dir = explode( delimiter: '/', $path);
    $postion = $dir[0];
    $fpath = substr(stristr($path, needle: '/'), start: 1);
    if ($postion == 'own') {
        $uipath = $ui ? "{$ui}/" : "";
        $file = PATH_APP_OWN . "tpl/{$uipath}{$fpath}.html";
        $fpath = str_replace( search: PATH_WEB, replace: "", $file);
    } elseif ($postion == 'ui') {
        $file = PATH_PUBLIC . "ui/" . L_MODULE . "/{$fpath}.html";
        $fpath = str_replace( search: PATH_WEB, replace: "", $file);
    } else {
        $file = "{$path}.html";
        $fpath = str_replace( search: PATH_WEB, replace: "", $file);
    }
    is_file($file) || LCMS::X( errcode: 404, errmsg: "{$fpath} 文件未找到");
    $cname = substr(md5($fpath), start: 8, length: 16);
    $cache = PATH_CACHE . "tpl/{$cname}.php";
    if (filemtime($file) > filemtime($cache)) {
        $html = file_get_contents($file);
        preg_match_all( pattern: "/{{(.*)}}/i", $html, &matches: $match);
        preg_match_all( pattern: "/<(.*)(&#x2F|'|>(&#x2F;)/i", $html, &matches: $tags);
        // 新版模板标签处理
    }
}
```

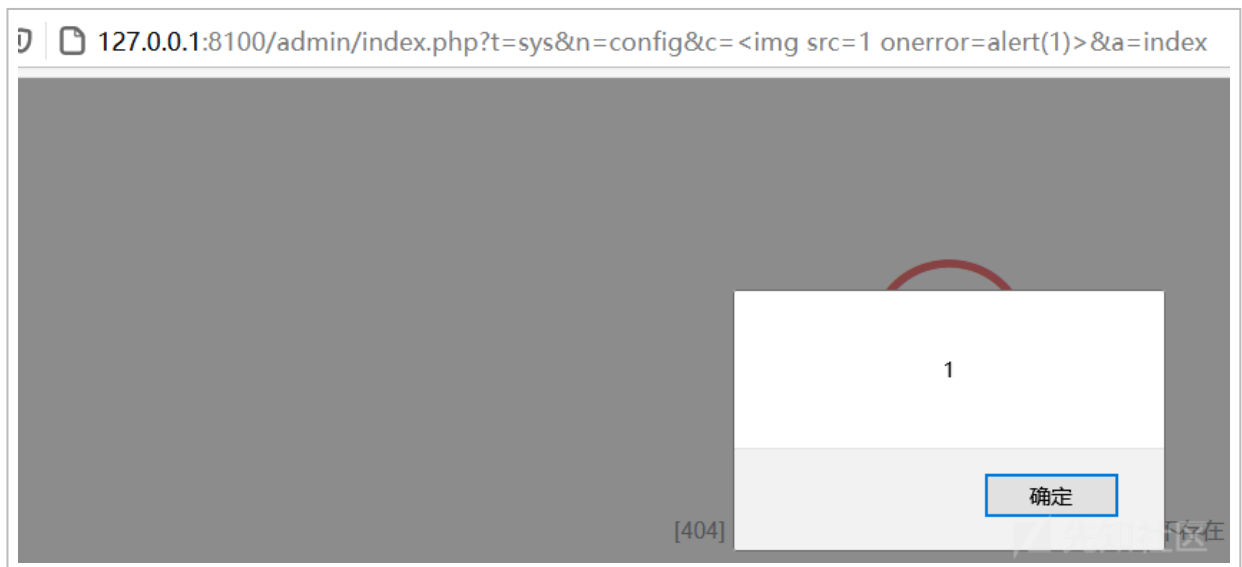
(<https://xzfile.aliyuncs.com/media/upload/picture/20210628165838-077090a2-d7ef-1.png>)

在进行输出的时候并没有看到对错误进行的任何过滤行为，直接进行了输出，触发了反



```
8 <meta content="yes" name="apple-mobile-web-app-capable" />
9 <meta content="black" name="apple-mobile-web-app-status-bar-style" />
10 <meta content="telephone=no" name="format-detection" />
11 <link rel="stylesheet" href="/public/static/layui/css/layui.css" />
12 <style type="text/css">.msg a{color:#ffadad;text-decoration:underline;}.msg a:hover{color:#F56C6C}</style>
13 </head>
14 <body style="...">
15 <?php ?>
16 <div style="text-align:center;position:relative;box-sizing:border-box;padding-top:20vh;height:calc(100vh - 300px);"
17 <i class="layui-icon layui-icon-face-cry" style="..."></i>
18 <p style="...">出现了一些问题</p>
19 <p class="msg" style="...">
20 [<?php echo $X['code']; ?>] : [<?php echo $X['msg']; ?>]
21 </p>
22 <?php if ($go){ ?>
23 <p style="...">
24 即将跳转
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628165925-2358e6b6-d7ef-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20210628165950-326e2ac6-d7ef-1.png>)

基本上涉及到的这种错误输出都没有过滤，都存在反射型 xss 漏洞

三 存储型 XSS 漏洞

在通过 Seay 代码审计工具自动扫描的时候发现了该 CMS 获取客户端 IP 的方式存在漏洞，可以进行伪造，并且后台记录了登录成功的 IP，但是只会记住登录成功的用户的 IP，所以只能通过拿下一个低权限的账号的时候才有可能触发该存储 XSS。

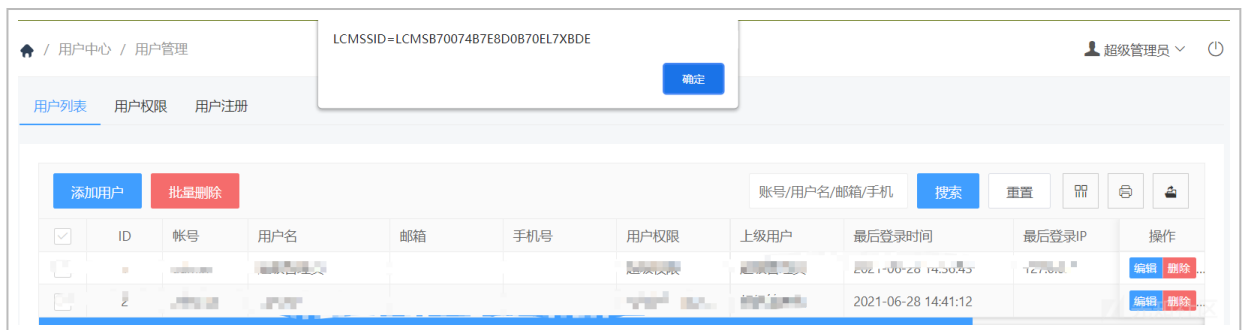
注册一个低权限的账号，然后在登录的时候进行客户端 IP 伪造，发现可以触发存储型

XSS.

```
POST /admin/index.php?n=login&a=check HTTP/1.1
Host: 192.168.5.155:8100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 81
Origin: http://192.168.5.155:8100
Connection: close
Referer: http://192.168.5.155:8100/admin/index.php?rootid=0&n=login&go=http%3A%2F%2F192.168.5.155%3A8100%2Fadmin%2F&name=admin&pass=admin&code=6032
Cookie: LCMSCID=5367CA4FFABFF867SJLJLE; LCMSID=LCMS5367CA4FFABFF867SJLJLE
X-Forwarded-For: <img src=1 onerror=alert(document.cookie)> IP伪造
go=http%3A%2F%2F192.168.5.155%3A8100%2Fadmin%2F&name=admin&pass=admin&code=6032
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628171734-ac8c0272-d7f1-1.png>)

管理员登录系统, 点击用户中心—用户管理处即可触发储存型 XSS 漏洞



(<https://xzfile.aliyuncs.com/media/upload/picture/20210628171755-b8a7947c-d7f1-1.png>)

定位到 IP 伪造的相关函数, 函数位于 \ app\sys\login\admin\index.class.php 中, 获取客户端的 IP 然后进行数据库的更新

```
if ($admininfo['status'] == '1') {
    if ($admininfo['lasttime'] > "0000-00-00 00:00:00" && $admininfo['lasttime'] < datenow()) {
        ajaxout(0, "此账户已到期");
    } else {
        $admininfo['parameter'] = sql2arr($admininfo['parameter']);
        unset($admininfo['pass']);
        $logintime = datenow();
        $admininfo['logintime'] = $logintime;
        SESSION::set("LCMSADMIN", $admininfo);
        sql_update(["admin", ["logintime" => $logintime, "ip" => CLIENT_IP], "id = " . $admininfo['id']]");
        ajaxout(1, "登录成功", $_L['form']['go'] ? $_L['form']['go'] : $_L['url']['admin']);
    }
}
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628171830-cdd70d32-d7f1-1.png>)

d7f1-1.png)

而 CLIENT_IP，根据全局变量可知为 LCMS::IP()，跟进到相关函数，函数位于 \

core\class\lcms.class.php 中，根据函数可知攻击者可以在客户端伪造 IP

```
public static function IP()
{
    $iplib = ["HTTP_ALI_CDN_REAL_IP", "HTTP_TRUE_CLIENT_IP",
    "HTTP_X_REAL_FORWARDED_FOR", "HTTP_X_CONNECTING_IP", "HTTP_CF_CONNECTING_IP",
    "HTTP_X_FORWARD_FOR", "HTTP_X_REAL_IP", "HTTP_X_FORWARDED_FOR", "REMOTE_ADDR"];
    foreach ($iplib as $val) {
        if (isset($_SERVER[$val]) && $_SERVER[$val] && strcasecmp($_SERVER[$val],
        "unknown")) {
            $ips = explode(' ', $_SERVER[$val]);
            $ip = $ips[0];
            break;
        }
    }
    return $ip;
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210628171909-e539265e-d7f1-1.png)

最后将从客户端获取到的 IP 更新到了数据库中

email	mobile type	balance	addtime	lasttime	logintime	parameter ip	lcms
(Null)	(Null)	lcms	0.00	2019-01-01 00:00:00	(Null)	2021-06-28 188.8.8.8	0
(Null)	(Null)	1247	0.00	2021-06-28 14:39:11	2021-07-10 2021-06-28	(Null) <img src=1 onerror=alert(docu	0

(https://xzfile.aliyuncs.com/media/upload/picture/20210628171939-f7182dca-d7f1-1.png)

当我们点击用户中心的时候，查看调用的函数 \ app\sys\user\admin\admin.class.php

```
$account = sql_counter(["admin"]);
require LCMS::template( path: "own/admin-list");
}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210628172001-0421e4c0-d7f2-1.png)

从数据库中取数据然后进行模板的渲染输出，触发 XSS 漏洞

四 任意文件删除

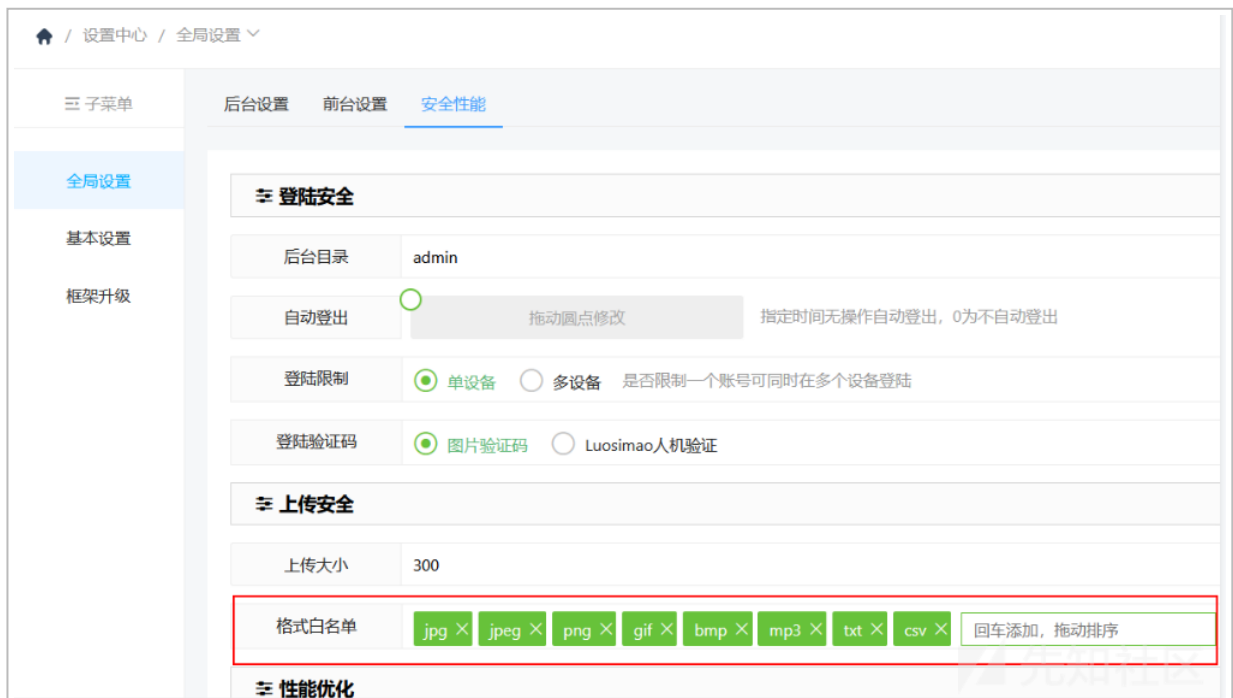
在删除备份 SQL 文件的时候

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628172506-b9d3cd06-d7f2-1.png>)

五 任意文件上传

很少看到有这么干的 CMS 了, 看到的时候还是有些吃惊, 有人说这是正常功能, 看了写这个 CMS 的上传他的本意应该还是上传非执行性脚本的意思, 初衷并不是希望你上传 php 文件。

在设置中心—> 安全性能—> 格式白名单添加 php

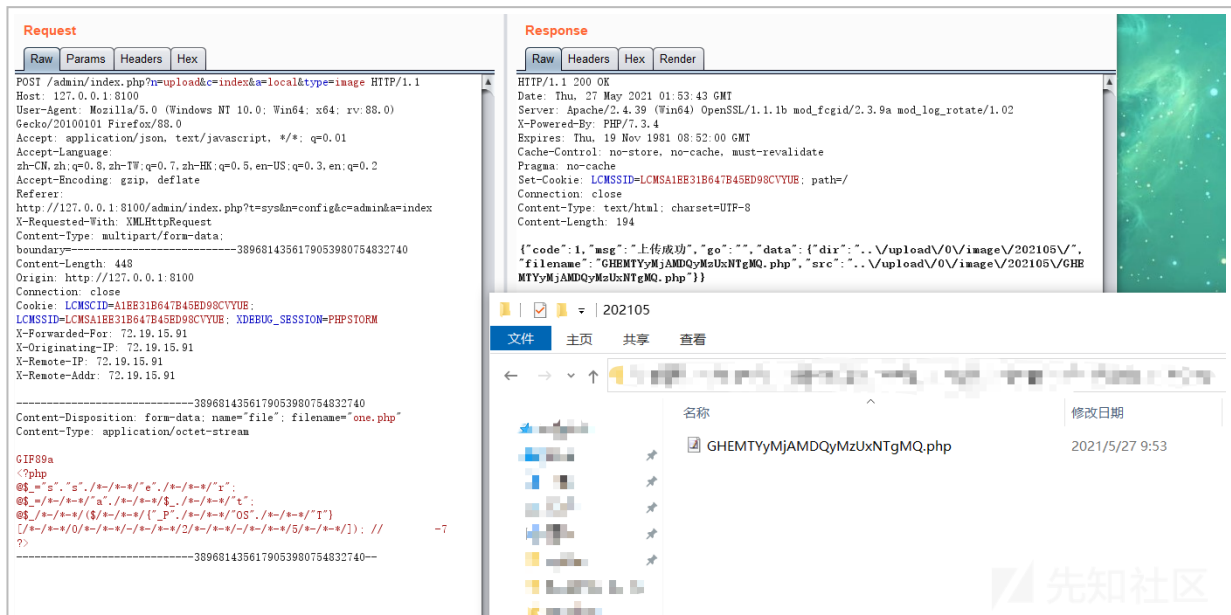


(<https://xzfile.aliyuncs.com/media/upload/picture/20210629100102-db22f85c-d87d-1.png>)

然后在设置中心—> 后台设置—> 后台 LOGO 直接上传 php 文件即可



(<https://xzfile.aliyuncs.com/media/upload/picture/20210629100119-e5451860-d87d-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20210628173029-7a27292c-d7f3-1.png>)

上传函数位于 \core\class\upload.class.php 中，只要 php 是允许的后缀名即可实现文件上传 getshell

```

// 如果文件地址是本地上传
$file = $para ? $para : $_FILES['file'];
if ($file['error'] != 0) {
    return self::out(0, "上传失败 CODE:{$file['error']}");
}

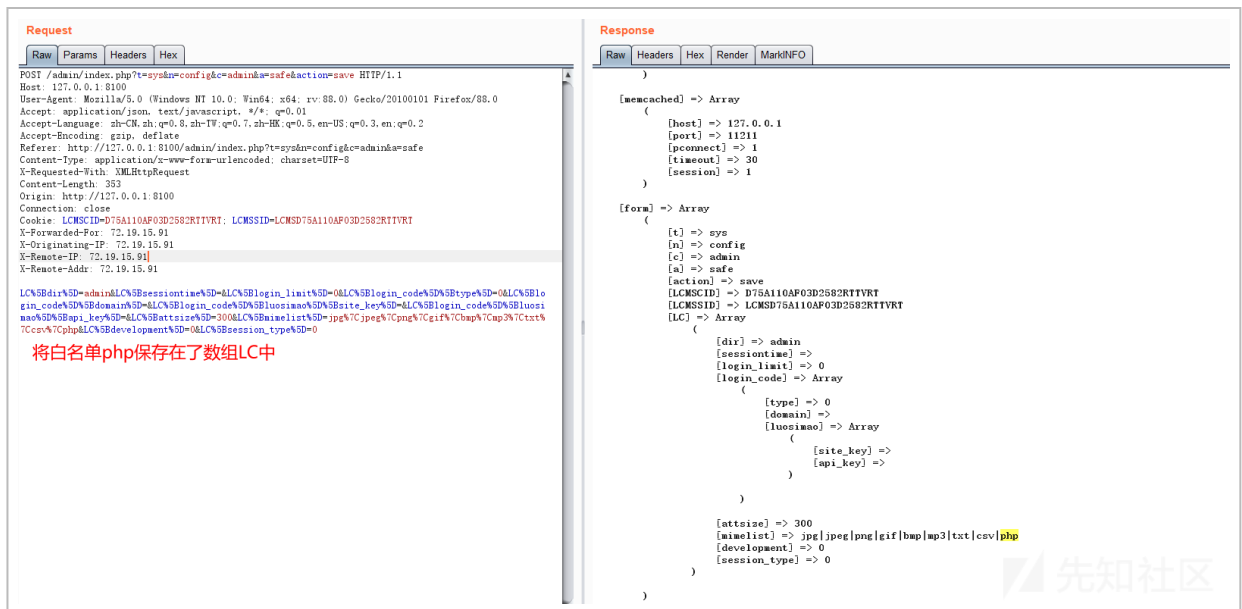
$mime = substr($file['name'], strpos($file['name'], ".") + 1);
$size = round($file['size'] / 1024); // 获取文件后缀名

if ($size > $_L['config']['admin']['attsize']) {
    // 如果文件大小超过上传限制
    $return = self::out(0, "文件大小超过($_L['config']['admin']['attsize'])KB");
} else {
    // 文件后缀名和系统允许的后缀名进行匹配
    if (strpos($_L['config']['admin']['mimelist'], $mime) !== false) {
        $name = randstr(3, "let") . preg_replace("/[0-9]/", "", str_replace(["+", "-", "=", "/"], "", base64_encode(strval(time()) . microseconds())) . ".$mime");
        if (is_url($para) && file_put_contents("{$_dir}{$name}", $file)) {
            $return = self::out(1, "上传成功", path_relative($_dir, $name));
        } elseif (move_uploaded_file($file['tmp_name'], "{$_dir}{$name}")) {
            $return = self::out(1, "上传成功", path_relative($_dir, $name));
        } else {
            $return = self::out(0, "上传失败");
        }
    }
}

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210628173133-a04ab1e6-d7f3-1.png>)

打印下保存的文件白名单



(<https://xzfile.aliyuncs.com/media/upload/picture/20210628173158-af629054-d7f3-1.png>)

跟进下相关函数，位于 app\sys\config\admin\admin.class.php 中的 dosafe 函数，该函数会将用户添加的白名单保存在全局变量中，在校验白名单时从全局变量中取值导致触发任意文件上传漏洞

```
public function dosafe()
{
    global $_L;
    switch ($_L['form']['action']) {
        case 'save':
            if ($_L['form']['LC']['dir'] != $_L['config']['admin']['dir']) {
                if (!getdirpower(PATH_WEB)) {
                    unset($_L['form']['LC']['dir']);
                    ajaxout(1, "根目录没有写权限", "reload");
                } else {
                    $change = true;
                }
            }
            LCMS::config([
                "do" => "save",
                "type" => "sys",
                "cate" => "admin",
                "lcms" => true,
            ]);
    }
}
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210629095538-1a2eb546-d87d-1.png>)

```
["layui" => "title", "title" => "上传安全"],
["layui" => "input", "title" => "上传大小",
    "name" => "LC[attnsize]",
    "value" => $config['attnsize'],
    "tips" => "限制上传文件的大小, 单位KB",
    "verify" => "required"],
["layui" => "tags", "title" => "格式白名单",
    "name" => "LC[mimelist]",
    "value" => $config['mimelist'],
    "tips" => "允许上传白名单里的文件格式",
    "verify" => "required"],
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210629095559-264d5a30-d87d-1.png>)

六 SQL 注入漏洞

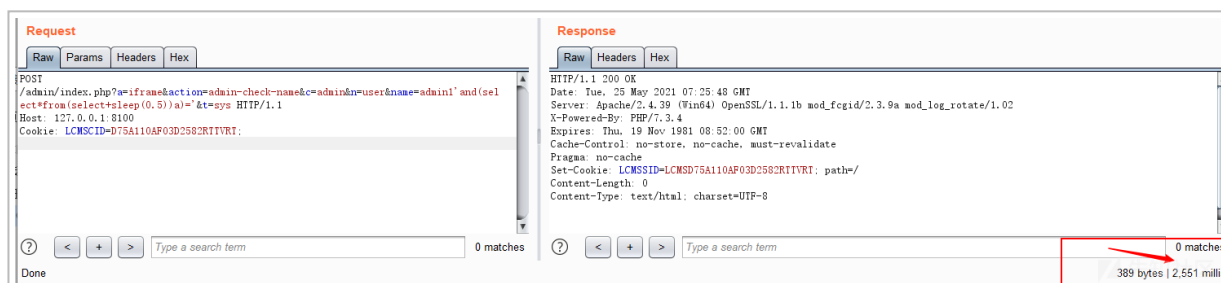
这个 CMS 应该是全部都没有进行安全检测的，基本上和数据库交互的地方都存在 SQL 注入吧，举一个例子吧，多了都是同类。

在用户管理—> 添加用户处



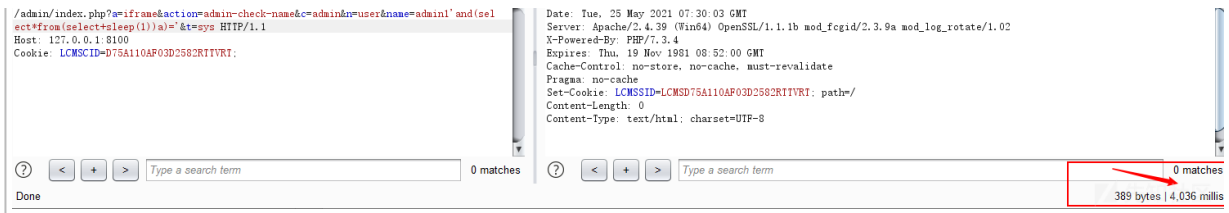
(<https://xzfile.aliyuncs.com/media/upload/picture/20210629100320-2d98e754-d87e-1.png>)

payload: admin1'and(select*from(select+sleep(1))a)='



(<https://xzfile.aliyuncs.com/media/upload/picture/20210629100456-6666e874-d87e-1.png>)





(<https://xzfile.aliyuncs.com/media/upload/picture/20210629100508-6de99452-d87e-1.png>)

通过更改 sleep 时间可以看到 sleep 函数生效了, 执行时间相差了大概 1 倍, 通过查看 SQL 语句执行记录可知, sleep 函数被拼接到了 sql 语句中, 并执行了 sql 语句

Date	SQL
2021-05-25 15:32:50...	SHOW WARNINGS
2021-05-25 15:32:50...	SELECT @@session.autocommit
2021-05-25 15:32:50...	SET NAMES utf8
2021-05-25 15:32:50...	SET character_set_results = NULL
2021-05-25 15:32:50...	SET global general_log=on
2021-05-25 15:32:50...	SET GLOBAL log_output='table'
2021-05-25 15:32:54...	SHOW TABLES
2021-05-25 15:32:54...	SELECT * FROM lcms_config WHERE name = 'config' AND type = 'sys' AND cate = 'admin' AND lcms = '0'
2021-05-25 15:32:54...	SELECT * FROM lcms_config WHERE name = 'config' AND type = 'sys' AND cate = 'web' AND lcms = '0'
2021-05-25 15:32:54...	SELECT * FROM lcms_admin WHERE id = '1'
2021-05-25 15:32:54...	SELECT * FROM lcms_config WHERE name = 'config' AND type = 'sys' AND cate = 'plugin' AND lcms = '0'
2021-05-25 15:32:54...	SELECT * FROM lcms_config WHERE name = 'config' AND type = 'sys' AND cate = 'plugin' AND lcms = '0'
2021-05-25 15:32:54...	SELECT * FROM lcms_admin WHERE name = 'admin' and(select*from(select sleep(1))a)=' OR email = 'admin' and(select*from(select sleep(1))a
2021-05-25 15:32:59...	SHOW WARNINGS
2021-05-25 15:32:59...	SELECT @@session.autocommit
2021-05-25 15:32:59...	SET NAMES utf8
2021-05-25 15:32:59...	SET character_set_results = NULL

(<https://xzfile.aliyuncs.com/media/upload/picture/20210629101332-9a3da146-d87f-1.png>)

根据 url 跟进到漏洞函数, 函数位于 \app\sys\user\admin\admin.class.php 中的 doiframe。具体代码如下, 在没有经过过滤的情况下直接获取了数据

```

case 'admin-check-name':|
    $admininfo = sql_get(["admin", "name = ':name' OR email = ':name' OR
mobile = ':name'", "id DESC", [
    ":name" => $_L['form']['name'],
    ]]);
    if ($admininfo) {
        ajaxout(0, "账号已存在");
    }

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210629101837-5003c708-d880-1.png>)

`$_L` 是全局的变量, 包含系统所有的变量数据, 打印下可以看到输出了网站的所有参数, 可以看到 `$_L` 包含了系统所有的变量数据

```

global $_L;
$secure = $_L['config']['admin']['https'] ? "https://" : ($_SERVER['HTTPS'] === 1 || $_SERVER['HTTPS'] === 'on') ? "https://" : "http://";
$url_site = $secure . HTTP_HOST . "/";
$url_now = $secure . HTTP_HOST . HTTP_QUERY;
$url_admin = $url_site . ($_L['config']['admin']['dir'] ? "admin" : "admin") . "/";
$_L['url'] = [
    "secure" => $secure,
    "site" => $url_site,
    "now" => $url_now,
    "admin" => $url_admin,
    "public" => "{$url_site}public/",
    "static" => "{$url_site}public/static/",
    "upload" => "{$url_site}upload/",
    "cache" => "{$url_site}cache/",
    "app" => "{$url_site}app/",
    "qrcode" => "{$url_site}app/index.php?n=system&c=qr&text=",
    "own" => "{$url_admin}index.php?",
    "own_path" => "{$url_site}app/" . L_TYPE . "/" . L_NAME . "/",
    "own_form" => "{$url_admin}index.php?t=" . L_TYPE . "&n=" . L_NAME . "&c=" . L_CLASS . "&a=",
];

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210629102800-9fcf4144-d881-1.png>)

```

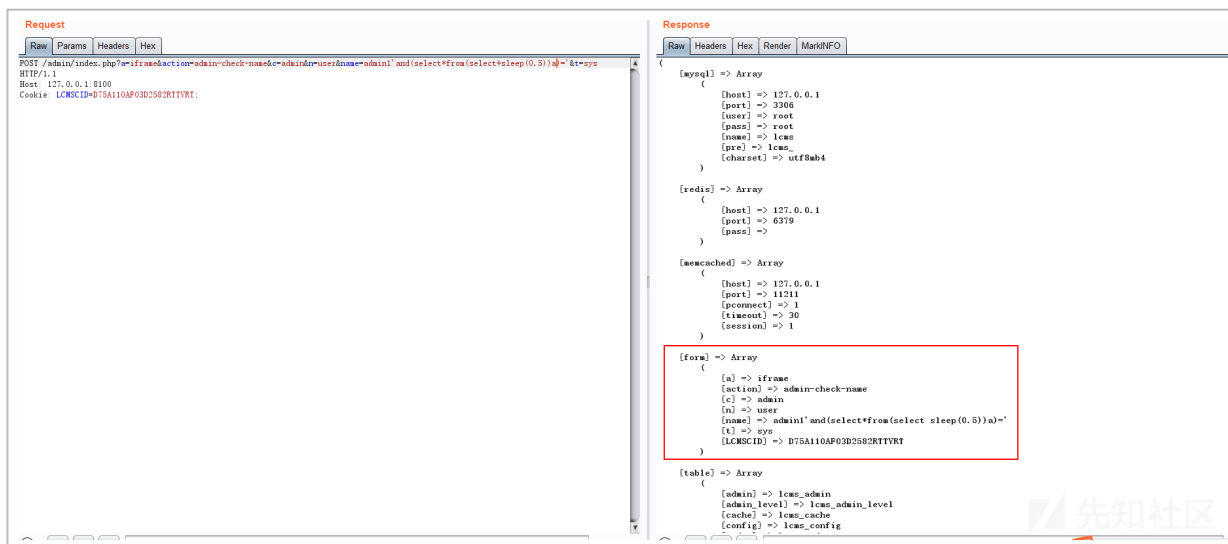
protected function load_common_config()
{
    global $_L;
    $_L['config']['admin'] = LCMS::config([
        "name" => "config",
        "type" => "sys",
        "cate" => "admin",
        "lcms" => true,
    ]);
    $_L['config']['web'] = LCMS::config([
        "name" => "config",
        "type" => "sys",
        "cate" => "web",
        "lcms" => true,
    ]);
    if ($_L['config']['admin']['development']) {
        $_L['config']['ver'] = "9999." . time();
        ob_start();
    } else {
        $version = PATH_CORE . "version";
    }
}

```

```
if (is_file($version)) {
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210629102830-b1aa40ee-d881-1.png>)

name 值为拼接了恶意 sql 语句的内容, 该值直接拼接到了 SQL 语句中去执行从而触发了 sql 注入漏洞



(<https://xzfile.aliyuncs.com/media/upload/picture/20210629103225-3d5c2e40-d882-1.png>)

七 总结

也没啥亮点吧, 很平常的 cms 流程跟踪一下就得了, 如有师傅需要 cms 可以留下联系邮箱。