# YXcms 1.4.7 储存型xss

## 一、漏洞简介

## 二、漏洞影响

YXcms 1.4.7

## 三、复现过程

### 漏洞分析

前台的文件源码protected/apps/default/controller/columnController.php

public function index()  
{  
 $ename=in($\_GET['col']);  
 if(empty($ename)) throw new Exception('栏目名不能为空~', 404);  
 $sortinfo=model('sort')->find("ename='{$ename}'",'id,name,ename,path,url,type,deep,method,tplist,keywords,description,extendid');  
 $path=$sortinfo['path'].','.$sortinfo['id'];  
 $deep=$sortinfo['deep']+1;  
 $this->col=$ename;  
 switch ($sortinfo['type']) {  
 case 1://文章  
 $this->newslist($sortinfo,$path,$deep);  
 break;  
 case 2://图集  
 $this->photolist($sortinfo,$path,$deep);  
 break;  
 case 3://单页  
 $this->page($sortinfo,$path,$deep);  
 break;  
 case 4://应用  
  
 break;  
 case 5://自定义  
  
 break;  
 case 6://表单  
 $this->extend($sortinfo,$path,$deep);  
 break;  
 default:  
 throw new Exception('未知的栏目类型~', 404);  
 break;  
 }  
}

后台的文件源码protected/apps/admin/controller/extendfieldController.php

public function mesedit()  
{  
 $tableid=intval($\_GET['tabid']);  
 if(!$this->checkConPower('extend',$tableid)) $this->error('您没有权限管理此独立表内容~');  
 $id=intval($\_GET['id']);//信息id  
 if(empty($tableid) || empty($id) ) $this->error('参数错误~');  
 $tableinfo = model('extend')->select("id='{$tableid}' OR pid='{$tableid}'",'id,tableinfo,name,type,defvalue','pid,norder DESC');  
 if(empty($tableinfo)) $this->error('自定义表不存在~');  
 if (!$this->isPost()) {  
 $info=model('extend')->Extfind($tableinfo[0]['tableinfo'],"id='{$id}'");  
 $this->info=$info;  
 $this->tableid=$tableid;  
 $this->id=$id;  
 $this->tableinfo=$tableinfo;  
 $this->display();  
 }else{  
 for($i=1;$i<count($tableinfo);$i++){  
 if(is\_array($\_POST[$tableinfo[$i]['tableinfo']]))  
 $data[$tableinfo[$i]['tableinfo']]=implode(',',$\_POST[$tableinfo[$i]['tableinfo']]);  
 else  
 $data[$tableinfo[$i]['tableinfo']]=html\_in($\_POST[$tableinfo[$i]['tableinfo']]);  
 }  
 if(model('extend')->Extup($tableinfo[0]['tableinfo'],"id='{$id}'",$data)) $this->success('修改成功~',url('extendfield/meslist',array('id'=>$tableid)));  
 else $this->error('信息修改失败~');  
 }  
}

中间没什么过滤

### 复现

http://0-sec.org/index.php?r=default/column/index&col=guestbook

payload：

<svg/onload=alert(1)>



然后登陆后台，查看审核



点击编辑

image