

New issue

[Jump to bottom](#)

There is stored XSS in version 1.5.6 which can lead to stealing sensitive information of logged-in users #24

Open youki992 opened this issue on Jun 11 · 1 comment

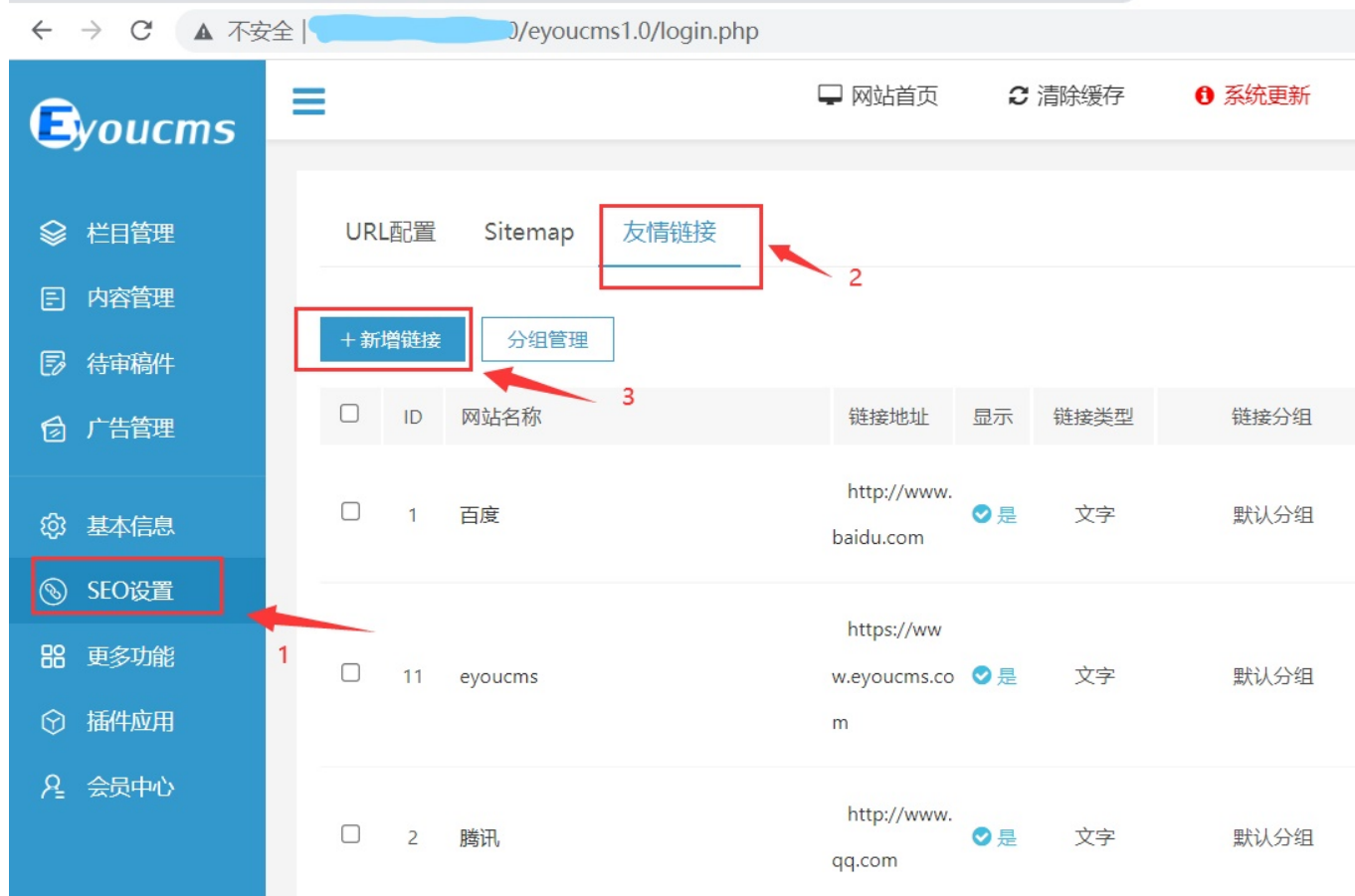
youki992 commented on Jun 11

Software Link : <https://github.com/eyoucms/eyoucms>

Website : <http://www.eyoucms.com/>

Vulnerable version 1.5.6 download address : <https://www.eyoucms.com/plus/down.php>

After the installation is complete, log in as admin, open the page

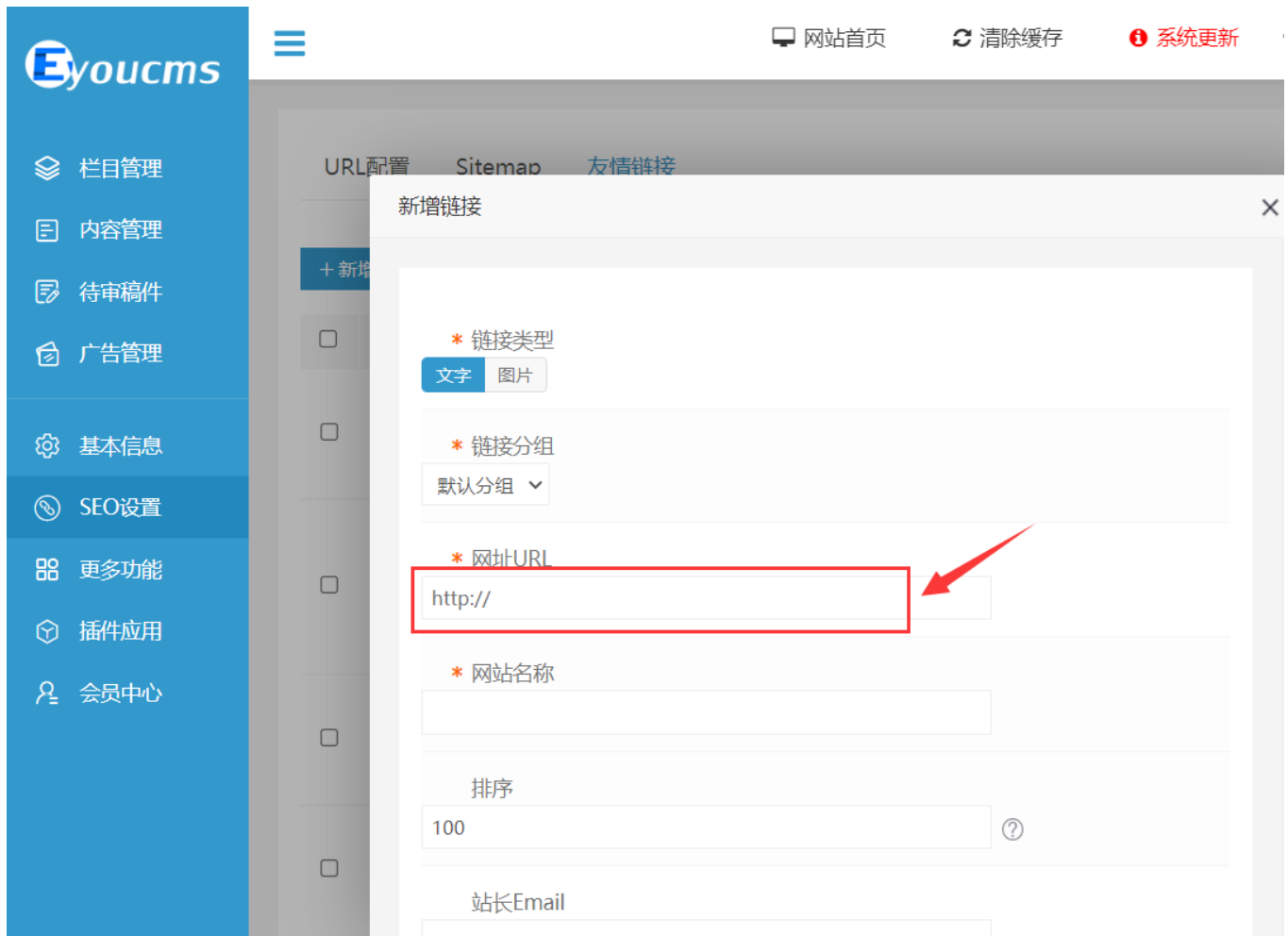


URL配置 Sitemap 友情链接

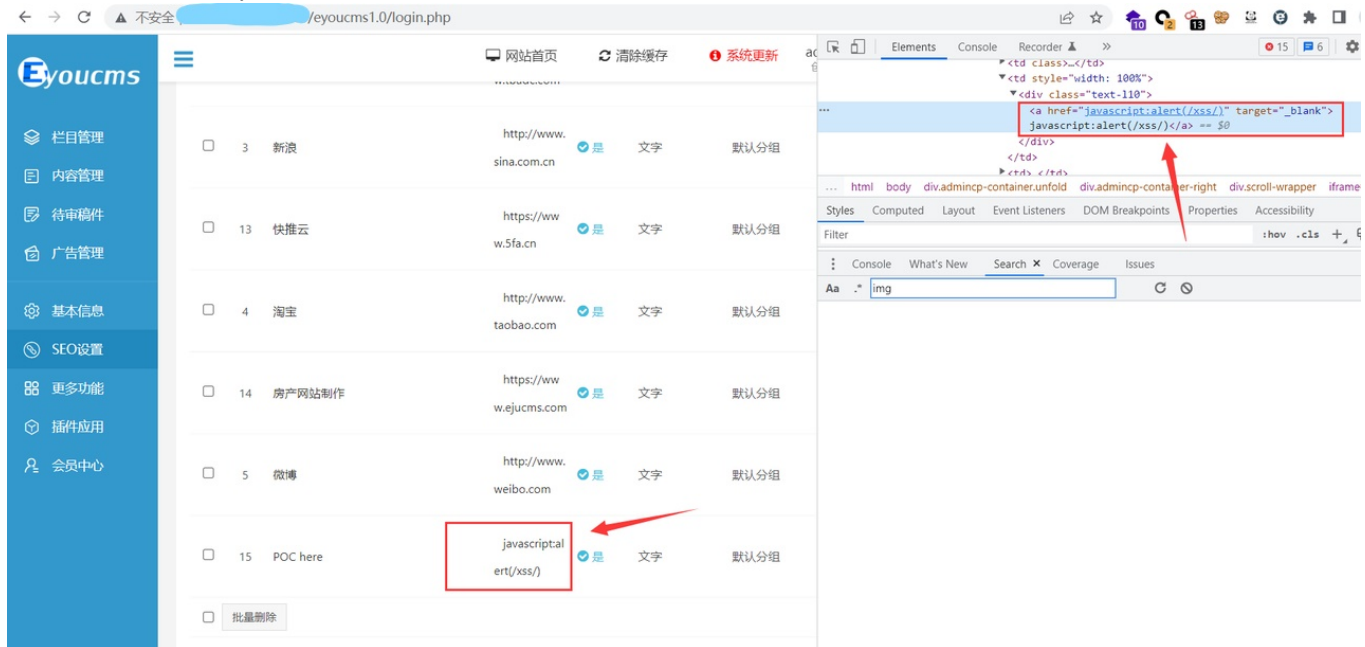
+ 新增链接 分组管理

<input type="checkbox"/>	ID	网站名称	链接地址	显示	链接类型	链接分组
<input type="checkbox"/>	1	百度	http://www.baidu.com	<input checked="" type="checkbox"/> 是	文字	默认分组
<input type="checkbox"/>	11	eyoucms	https://www.eyoucms.com	<input checked="" type="checkbox"/> 是	文字	默认分组
<input type="checkbox"/>	2	腾讯	http://www.qq.com	<input checked="" type="checkbox"/> 是	文字	默认分组

Here you can fill in malicious JavaScript code to cause stored xss



Malicious code is spliced into the href link



Causes stored XSS to steal sensitive information of logged-in users



POC :

```
javascript:alert(/XSS/)
```

youki992 commented on Jun 24

Author

use [CVE-2022-33122](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

