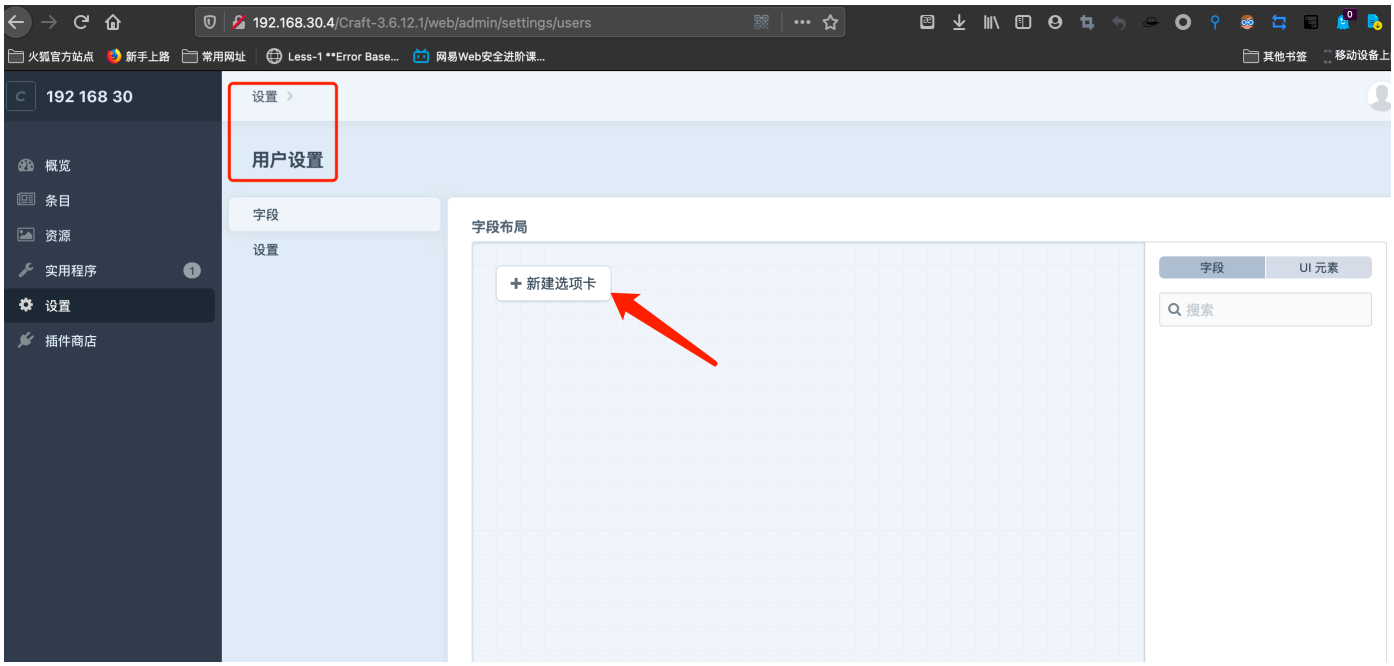
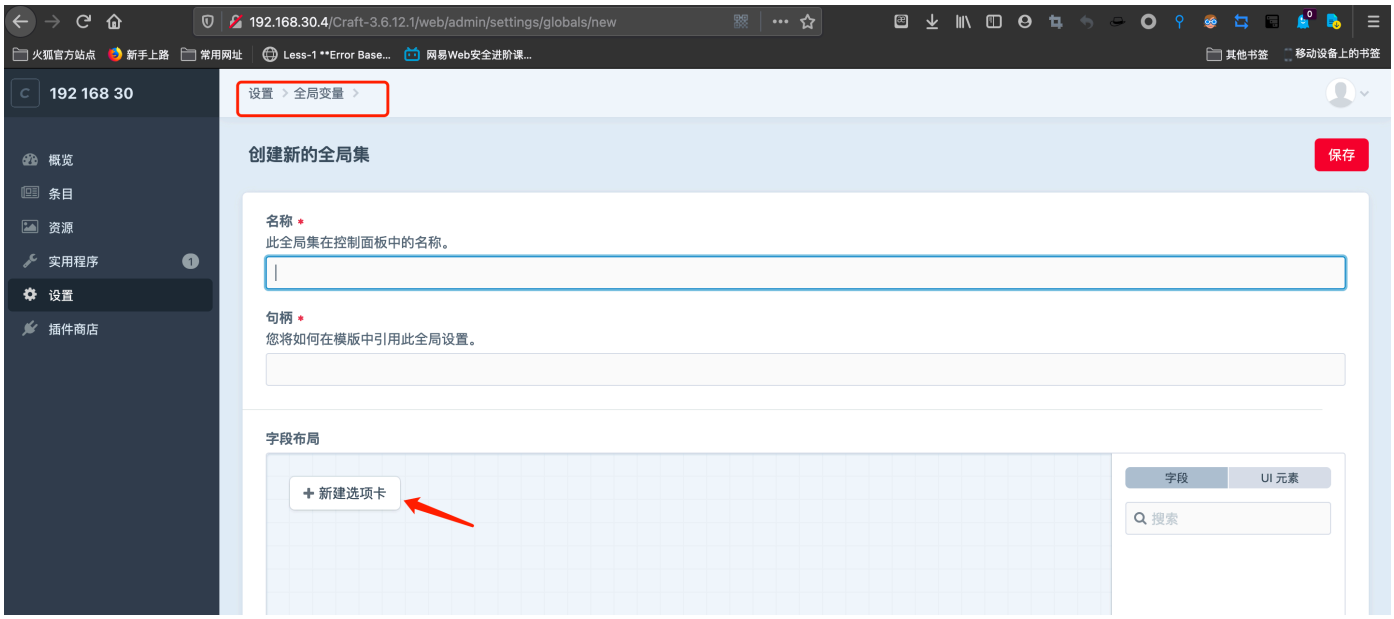
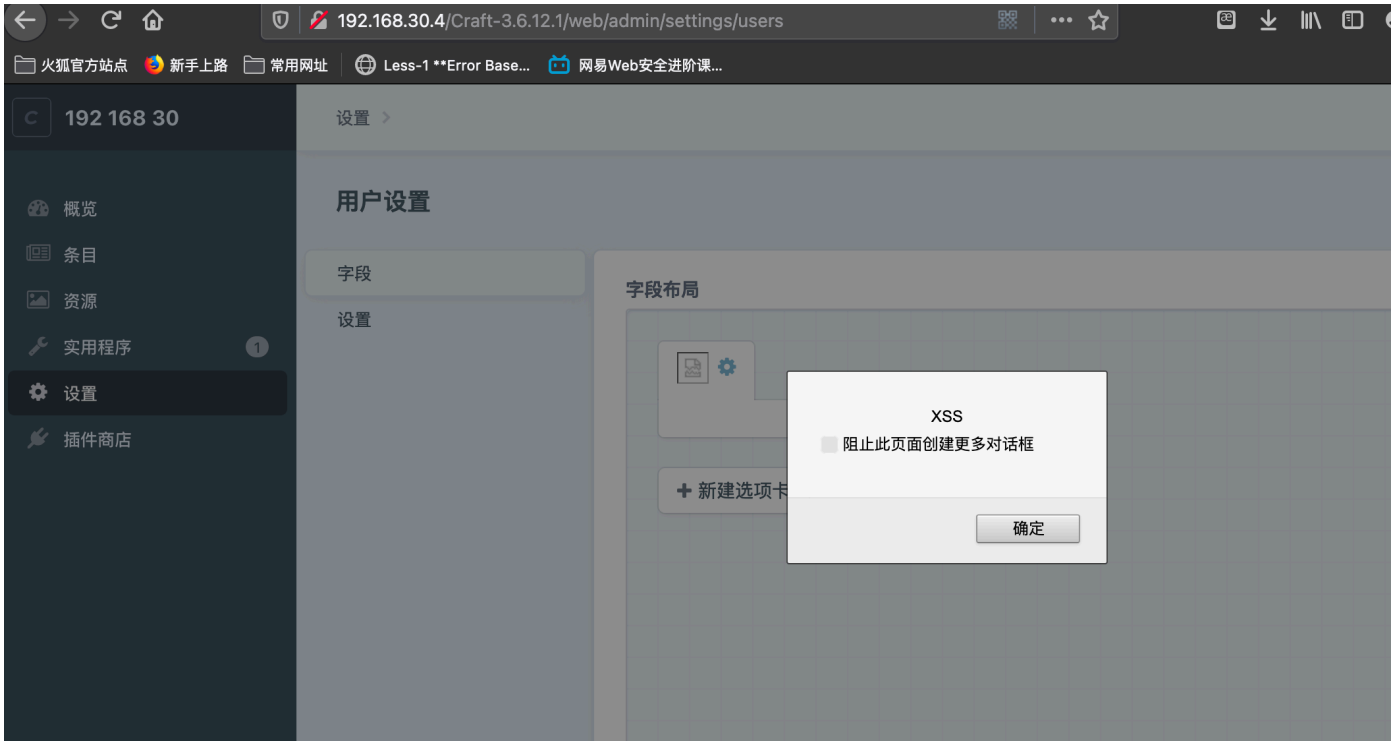
Craft-3.6.12 Stored XSS vulnerabilities

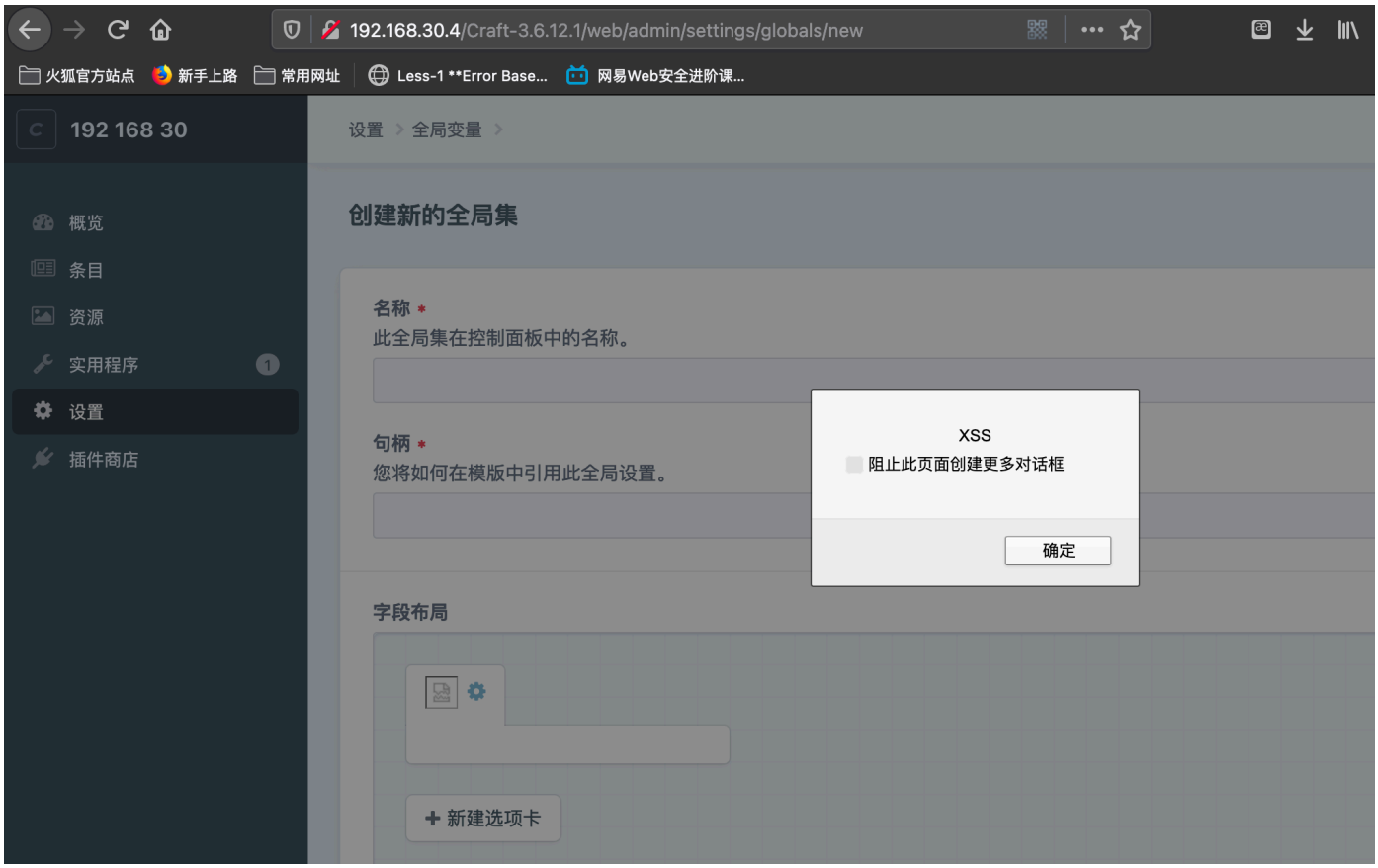
在用户，全局变量,分类等有字段布局设置的都存在存储型XSS

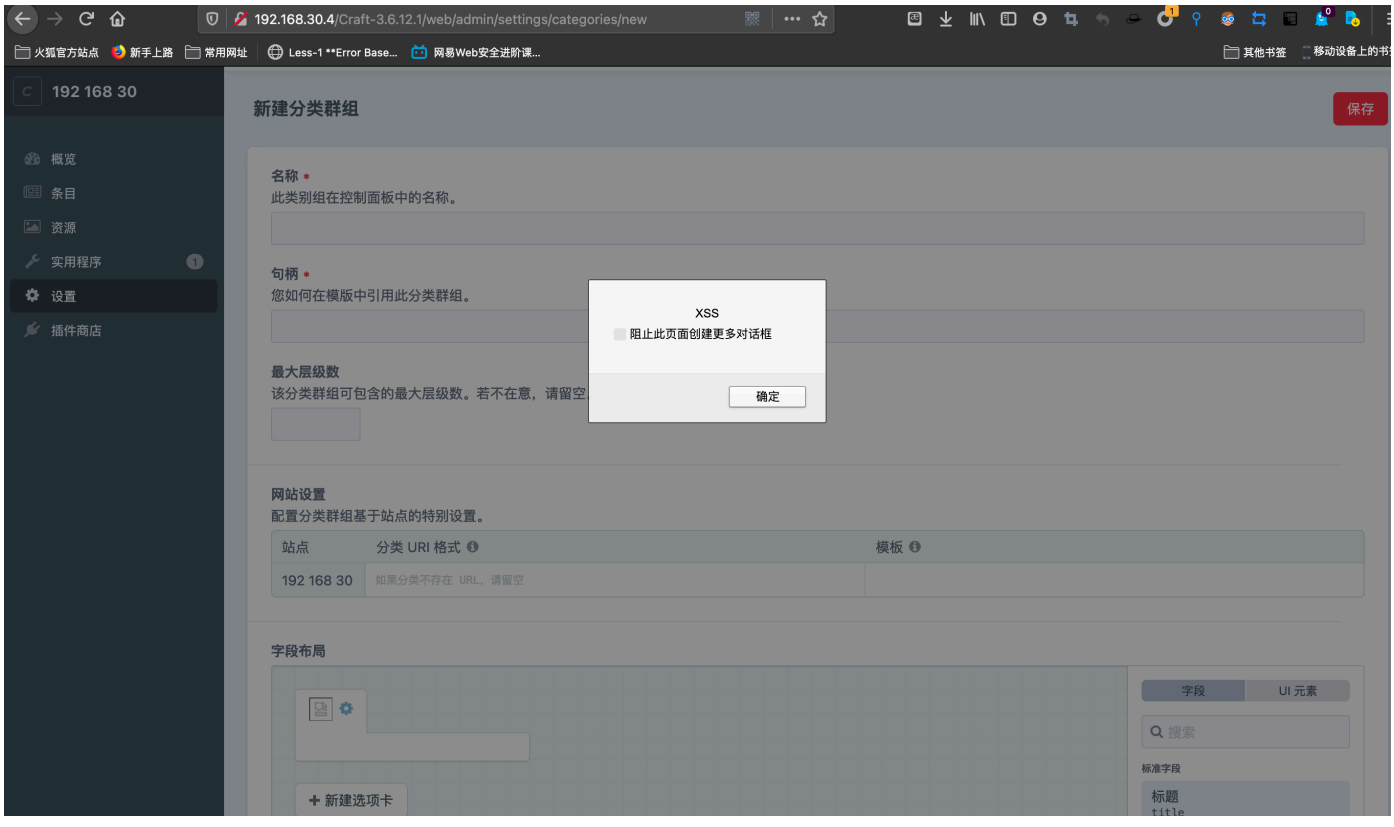




Payload:<img src=x onerror=alert('XSS');>







官方确认漏洞并更新发布了新版本

Brad Bell (Pixel & Tonic)
Apr 30, 2021, 2:36 PM PDT

Hi Himawari,

This has been fixed in this commit and will be included in the next release (likely next week sometime):
https://github.com/craftcms/cms/commit/f9378aa154b5f9b64bed3d59cce0c4a8184bf5e6

-Brad

Brad Bell (Pixel & Tonic)
Apr 30, 2021, 1:51 PM PDT

Hi Himawari,

I can confirm these on the latest Craft release. Will get them patched and let you know when it's released... thanks for the report!

-Brad

Shenzihao
Apr 30, 2021, 1:49 AM PDT

Submitted on: 2021-04-30 01:49:25

- What can we help you with?: Security disclosure
- Name: himawari
- Email: shenzihao@yunzhisec.com
- How can we help?: Security Question

  Hello
  Craft-3.6.12.1 XSS exists in the background, The path is background➡️settings➡️user settings➡️fields➡️create a new tab, the content is not verified when entering the user name, so there will be XSS vulnerabilities
  In the settings, resources, global variables, categories, all have XSS vulnerabilities
  payload:<img src=x onerror=alert('XSS');>
  https://user-images.githubusercontent.com/41565767/116662413-5506e280-a9c8-11eb-8704-3b8a5b5f2678.png