## 一、漏洞摘要

漏洞名称: S-CMS企业建站系统PHP版v3.0后台存在CSRF可添加管理员权限的账号

上报日期: 2019-02-22  
漏洞发现者: qn（[137535957@qq.cn](mailto:137535957@qq.cn)）

产品首页: <https://www.s-cms.cn>

软件链接: https://cdn.shanling.top/file/1.com.php.zip

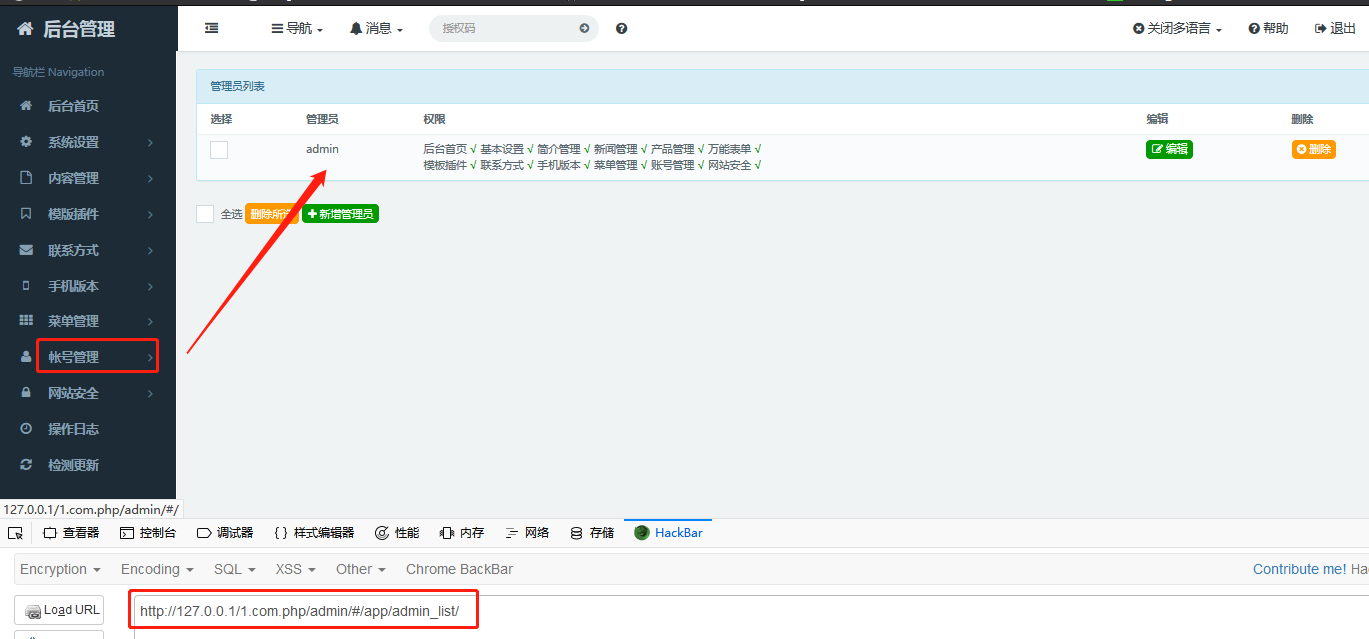
版本: PHP v3.0

## 二、漏洞概述

恶意攻击者可以精心伪造一个html页面诱骗已登录的管理用户点击，从而更改管理员账户密码。

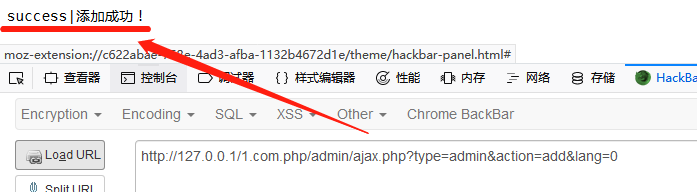
## 三、漏洞演示

首先下载源码，本次实验在windows上用phpstudy进行搭建。

首先以管理员身份登录后台

可有看到管理员只有一个admin

在桌面生成1.html，添加一个test1用户，exp如下：

保存退出之后，点击访问：

然后在到我们的后台查看管理员列表

test1用户已添加