

SCM Manager XSS漏洞 (CVE-2023-33829)

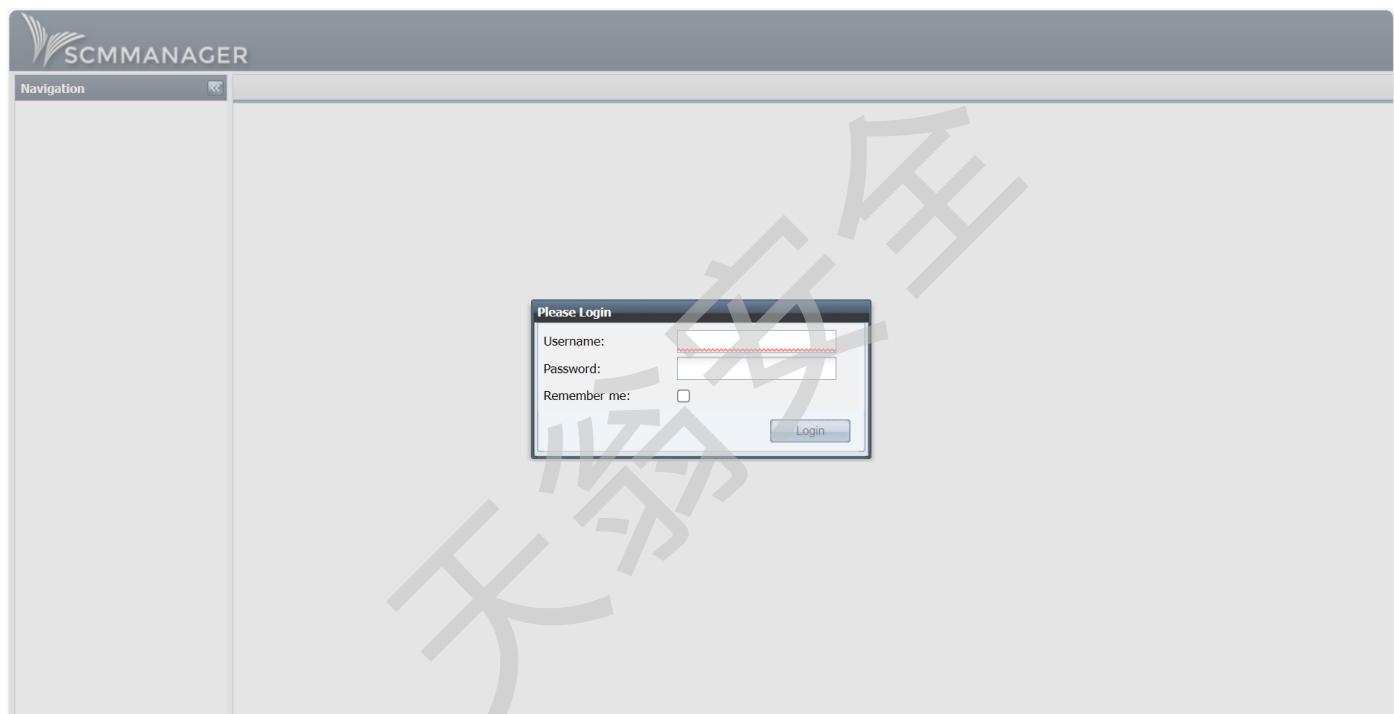
SCM-Manager 是一款开源的版本库管理软件，同时支持 subversion、mercurial、git 的版本库管理。安装简单，功能较强，提供用户、用户组的权限管理，有丰富的插件支持。由于在MIT的许可下是开源的，因此它允许被用于商业用途，而且其代码可以在GitHub上获取到。

测试环境 (目前仅支持AMD64, 不支持ARM)

执行如下命令启动一个SCM-Manager 1.60：

```
docker compose up -d
```

环境运行后，访问 `http://your-ip:8080` 即可查看SCM-Manager主页，默认账密 `scmadmin/scmadmin`



漏洞复现

修改脚本中IP：

运行脚本：

```
python CVE-2023-33829.py
```

```
访问http://172.16.31.147:8080/scm/即可触发XSS。登录用户名密码为：scmadmin/scmadmin
PS D:\BaiduSyncdisk\000ctf\github\VulhubExpand\SCM-Manager\CVE-2023-33829> █
```

登录输入用户名密码触发XSS:

The screenshot shows a web browser window for the SCMMANAGER application. The URL in the address bar is 172.16.31.147:8080/scm/#repositoryPanel;2YU9WfGQe2. A modal dialog box is displayed in the center, titled '172.16.31.147:8080 显示' (Display) with the identifier 'VulhubExpand-0.8923383209669913'. The dialog contains a single button labeled '确定' (Confirm). The main content area of the page shows a 'Repositories' table with columns: Name, Contact, Description, Creation date, and Url. A 'Loading...' message is visible in the center of the table area. At the bottom of the page, there is a 'Repository Form' section with the placeholder text 'Add or select an Repository'.