基本信息

漏洞类型：源码泄露漏洞

漏洞等级：高危

厂商信息：此处需要手动搜索

漏洞简述

漏洞描述

整个网站的源代码文件泄露，包括大量的敏感数据，数据库连接数据 等。

产生原因

在运行git init初始化代码库的时候，会在当前目录下面产生一个.git的隐藏文件，用来记录代码的变更记录等等。在发布代码的时候，把.git这个目录没有删除，直接发布了。使用这个文件，可以用来恢复源代码。

漏洞危害

攻击者就可以利用下载git文件夹 , 可以利用其中储存的版本控制信息 , 完全恢复网站后台的代码和目录结构 , 当然 , 一般网站都会涉及到数据库操作 , 而一般来说 , 需要链接数据库就需要用户名/密码/端口/库名等信息 , 而这些信息肯定会在网站后台的源码里面又体现 , 因此这种情况是极其危险的 , 还有 , 一旦服务器开放了数据库的远程连接功能 , 攻击者就可以利用从源码中找到的数据库用户名和密码对远程数据库进行登陆 , 危险性不言而喻

漏洞详情

网站漏洞报表

漏洞地址:http://static.www.gfan.net.cn/.git/config

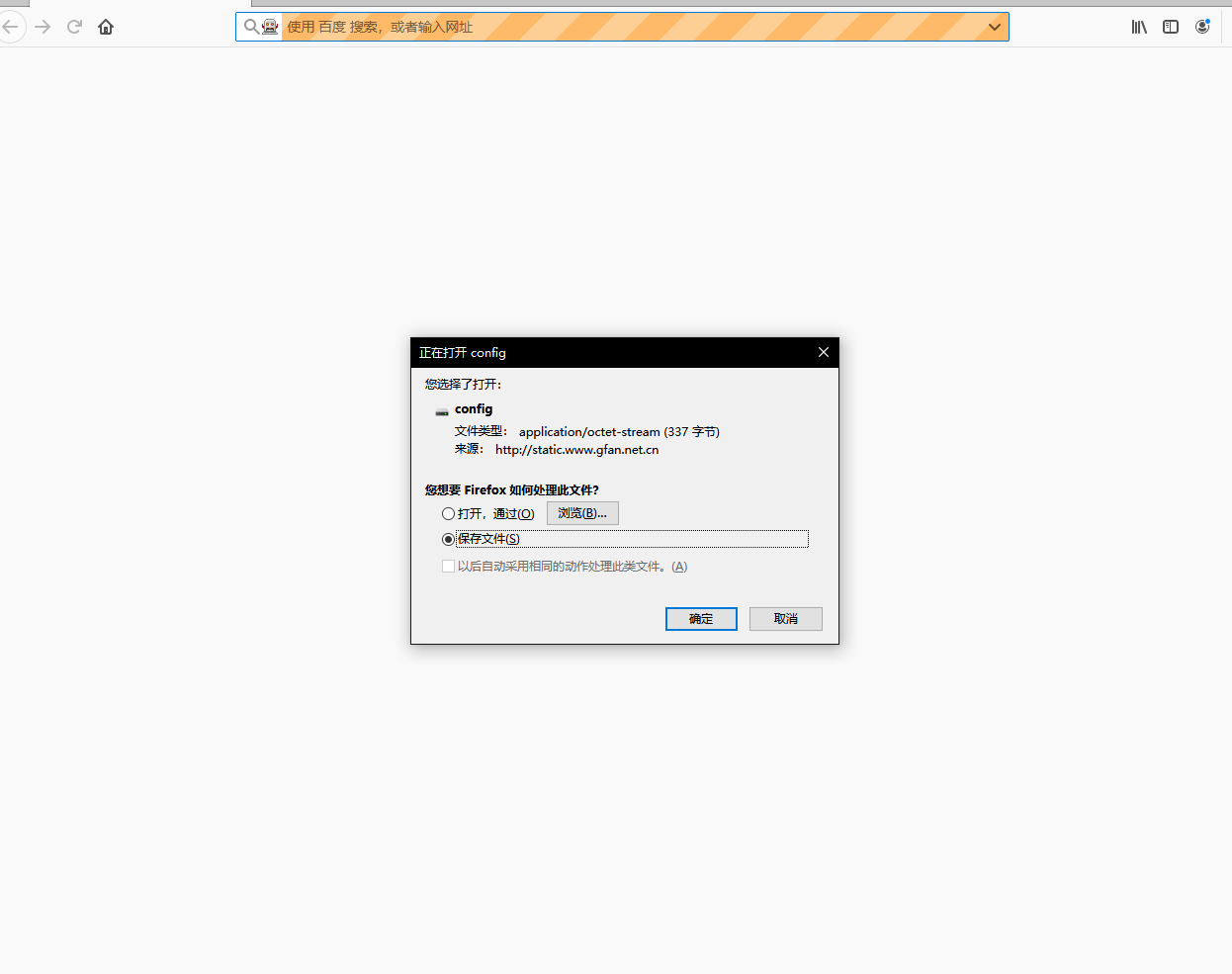
网站信息报表

网站漏洞复现(使用Firefox浏览器)

下载链接

http://static.www.gfan.net.cn/.git/config

返回结果



源码恢复检测工具

xxxxxx这里手动插图xxxxxxxxxx

复现完成，验证存在源码泄露漏洞

修复建议

根源上进行修复

1、对.git目录的访问权限进行控制  
 2、在每次pull之后删除.git文件夹