gnuboard xss漏洞

漏洞简介

Gnuboard是韩国Sir公司开发一套PHP+Mysql CMS程序。 本身数据结构简单，可扩展性能强，程序运行代码与皮肤文件分离，可扩展数据字段多，可以进行多种功能转变，简单安装就可以作为BBS告示板使用，也可以下载皮肤插件变成 综合网站，地方信息，购物，人才市场，物品交易网站。gnuboard 5.3 header头过滤不严导致xss漏洞。

##漏洞分析## `/adm/admin.tail.php`文件第17行存在漏洞。

```
<footer id="ft">
    <p>
        Copyright &copy; <?php echo $_SERVER['HTTP_HOST']; ?>. All rights
reserved. <?php echo $print_version; ?><br>
        <a href="#">상단으로</a>
    </p>
</footer>
```

`<?php echo $_SERVER['HTTP_HOST']; ?>` 中HTTP_HOST没有任何过滤直接echo输出 导致xss漏洞。 ##漏洞复现## 访问管理员后台，抓包吧 HOST 改成 xss payload 即可触发xss漏洞。