XDCMS 1.0 csrf 漏洞

一、漏洞简介

二、漏洞影响

XDCMS 1.0

三、复现过程

CSRF 漏洞常存在于涉及权限控制的地方，像管理后台、会员中心、论坛帖子、资料修改、交易管理等。

通常可检查相应代码处是否存在检测 token 或 referer，如果没有 token/referer 直接请求该页面进行判断

漏洞存在于用户资料修改页面，URL：`index.php?m=member&f=edit`，同 SQL 注入 2 漏洞点相同

直接修改 Cookie 中 `member_userid` 字段，成功将其他用户信息修改