XSS in multiple-results.php

86 views

Seongil Wi
to ICEcoder

Apr 23, 2021, 3:16:17 AM

Hi,

Our research team in KAIST WSP Lab found a reflected vulnerability in ICEcoder 8.0.

- Description: A reflected XSS vulnerability was identified in the multipe-results.php page due to insufficient sanitization of the _GET['replace'] variable. As a result, arbitrary Javascript code can get executed.

- Steps to reproduce the report

1. Login to the website

2. Go to the link: http://[server]/icecoder/lib/multiple-results.php?csrf=[CSRF or Session Token]&replace=123%27)%3Cscript%3Ealert(1);%3C/script%3E

3. Boom!