asfi
Follow
Dec 8, 2020 · 1 min read · Listen

Exploit for CVE-2020–29258— Reflected Cross-site scripting (XSS) vulnerability

Exploit Title: Online Examination System 1.0 — Reflected Cross-Site Scripting
Date: 21/Nov/2020
Exploit Author: Asfiya Shaikh
Vendor Homepage: https://www.sourcecodester.com/php/14358/online-examination-system.html
Version: 1.0
Tested on: Windows 7

Description — Cross-site scripting (XSS) vulnerability in Online Examination System 1.0 via the w parameter to index.php.
Affected Component — http://192.168.0.175/OnlineExaminationSystem/index.php?w=<Vulnerable_Parameter>
Payload — <script>alert(1)</script>

Impact — Reflected Cross Site Scripting is relatively complex to exploit as the malicious payload has to be send as a part of URL and user should be tricked to visit that URL. However, it has the same impact as that of a persistent XSS. XSS can be used to hijack victim's session and thereby gaining complete access to his/her user account. Additionally, it can be used to redirect victim to a malicious website which may contain browser exploits or a phishing page.

Reference — https://www.sitepoint.com/php-security-cross-site-scripting-attacks-xss/
https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

Cve
Penetration Testing