

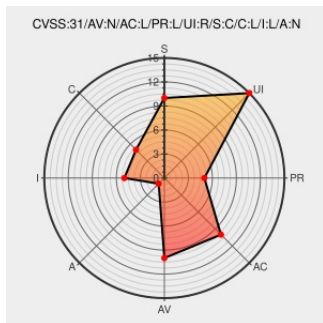


CVE-2021-42664

Published on: 11/05/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 03:32:00 AM UTC

CVE-2021-42664

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Engineers Online Portal](#) from [Engineers Online Portal Project](#) contain the following vulnerability:

A Stored Cross Site Scripting (XSS) Vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the (1) Quiz title and (2) quiz description parameters to add_quiz.php. An attacker can leverage this vulnerability in order to run javascript commands on the web server surfers behalf, which can lead to cookie stealing and more.

CVE-2021-42664 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
GitHub - TheHackingRabbi/CVE-2021-42664: CVE-2021-42664 - Stored Cross-Site Scripting vulnerability in the Engineers online portal system.	github.com text/html	MISC github.com/TheHackingRabbi/CVE-2021-42664

Engineers Online Portal 1.0 SQL Injection ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/164618/Engineers-Online-Portal-1.0-SQL-Injection.html
Engineers Online Portal 1.0 - 'multiple' Stored Cross-Site Scripting (XSS) - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	 MISC www.exploit-db.com/exploits/50451
Engineers Online Portal in PHP Free Source Code & Tutorials	www.sourcecodester.com text/html	 MISC www.sourcecodester.com/php/13115/engineers-online-portal-php.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2021-42664 - Stored Cross-Site Scripting vulnerability in the Engineers online portal system.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Engineers Online Portal Project	Engineers Online Portal	1.0	All	All	All
cpe:2.3:a:engineers_online_portal_project:engineers_online_portal:1.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-42664 : A Stored Cross Site Scripting #XSS Vulneraibility exists in Sourcecodester Engineers Online Port... twitter.com/i/web/status/1...	2021-11-05 13:09:16

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)