

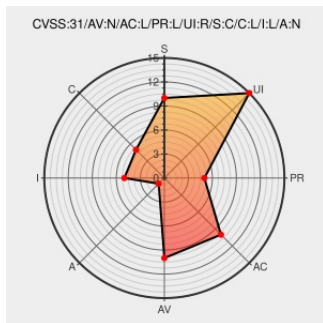


CVE-2022-37150

Published on: Not Yet Published

Last Modified on: 08/27/2022 01:28:00 AM UTC

CVE-2022-37150

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

Certain versions of [Online Diagnostic Lab Management System](#) from [Online Diagnostic Lab Management System Project](#) contain the following vulnerability:

An issue was discovered in Online Diagnostic Lab Management System 1.0. There is a stored XSS vulnerability via firstname, address, middlename, lastname , gender, email, contact parameters.

CVE-2022-37150 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

CVE References

Description	Tags	Link
Online Diagnostic Lab Management System in PHP with Free Source Code Free Source Code Projects and Tutorials	www.sourcecodester.com text/html	MISC www.sourcecodester.com/php/15129/online-diagnostic-lab-management-system-php-free-source-code.html
GitHub - Fjowel/CVE-2022-37150: Online Diagnostic Lab Management System Stored XSS	github.com text/html	MISC github.com/Fjowel/CVE-2022-37150

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

Online Diagnostic Lab Management System Stored XSS

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Online Diagnostic Lab Management System Project	Online Diagnostic Lab Management System	1.0	All	All	All
cpe:2.3:a:online_diagnostic_lab_management_system_project:online_diagnostic_lab_management_system:1.0:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-37150 : An issue was discovered in Online Diagnostic Lab Management System 1.0. There is a stored #XSS vul... twitter.com/i/web/status/1...	2022-08-26 13:07:05
 @LinInfoSec	Php - CVE-2022-37150: github.com/Fjowel/CVE-202...	2022-08-26 15:00:06
 @threatmeter	CVE-2022-37150 An issue was discovered in Online Diagnostic Lab Management System 1.0. There is a stored XSS vulner... twitter.com/i/web/status/1...	2022-08-26 23:25:59
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-37150 - An issue was discovered in Online Diagnostic Lab Management System 1.... twitter.com/i/web/status/1...	2022-08-27 02:12:15
 @threatmeter	CVE-2022-37150 An issue was discovered in Online Diagnostic Lab Management System 1.0. There is a stored XSS vulner... twitter.com/i/web/status/1...	2022-08-28 07:09:52
 /r/netcve	CVE-2022-37150	2022-08-26 13:38:46

[← 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](#)