



# CVE-2023-1485

Published on: Not Yet Published

Last Modified on: 03/23/2023 02:21:00 PM UTC

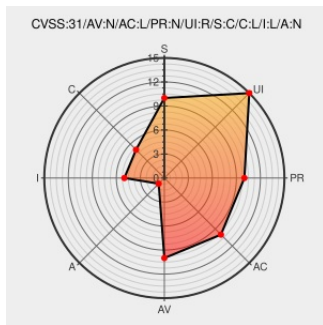
## CVE-2023-1485

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Young Entrepreneur E-negosyo System](#) from [Young Entrepreneur E-negosyo System Project](#) contain the following vulnerability:

A vulnerability classified as problematic has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. This affects an unknown part of the file `/bsenordering/index.php` of the component GET Parameter Handler. The manipulation of the argument category with the input `<script>alert(222)</script>` leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223371.

CVE-2023-1485 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **SourceCodester - Young Entrepreneur E-Negosyo System** version = 1.0

CVSS3 Score: **6.1 - MEDIUM**

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

## CVE References

Description	Tags	Link
bug_report/XSS-1.md at main · 2714925725/bug_report · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/2714925725/bug_report/blob/main/XSS-1.md">github.com/2714925725/bug_report/blob/main/XSS-1.md</a>
Login required	<a href="#">vuldb.com</a> <a href="#">text/html</a> <b>Inactive Link</b> <b>Not Archived</b>	MISC <a href="https://vuldb.com/?id.223371">vuldb.com/?id.223371</a>

Login required

[vuldb.com](#)

[text/html](#)

Inactive Link Not Archived

MISC vuldb.com/?ctiid.223371

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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE


### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Young Entrepreneur E-negosyo System Project</a>	<a href="#">Young Entrepreneur E-negosyo System</a>	1.0	All	All	All

```
cpe:2.3:a:young_entrepreneur_e-negosyo_system_project:young_entrepreneur_e-negosyo_system:1.0:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	<a href="#">CVE-2023-1485</a>	2023-03-18 22:38:23

[← 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](#)