



CVE-2022-0210

Published on: 01/18/2022 12:00:00 AM UTC

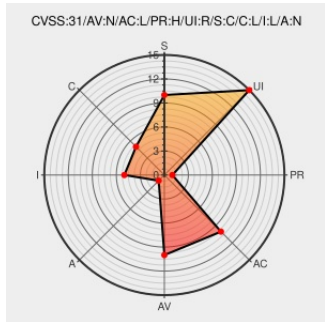
Last Modified on: 01/25/2022 05:00:00 PM UTC

CVE-2022-0210

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Random Banner](#) from [Buffercode](#) contain the following vulnerability:

The Random Banner WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient escaping via the category parameter found in the `~/include/models/model.php` file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 4.1.4. This affects multi-site installations

where `unfiltered_html` is disabled for administrators, and sites where `unfiltered_html` is disabled.

CVE-2022-0210 has been assigned by security@wordfence.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Random Banner - Random Banner version <= 4.1.4**

CVSS3 Score: **4.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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
2022/Random Banner Xss.md at main · BigTiger2020/2022 · GitHub	github.com text/html	<input type="checkbox"/> MISC github.com/BigTiger2020/2022/blob/main/Random%20Banner%20Xss.md
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	<input type="checkbox"/> MISC plugins.trac.wordpress.org/browser/random-banner/tags/4.1.4/include/models/model.php#L132
Vulnerability Advisories - Wordfence	www.wordfence.com text/html	<input type="checkbox"/> MISC www.wordfence.com/vulnerability-advisories/#CVE-2022-0210

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Buffercode	Random Banner	All	All	All	All
cpe:2.3:a:buffercode:random_banner:*:*:*:*:wordpress:*:*:						

Discovery Credit

Big Tiger

Social Mentions

Source	Title	Posted (UTC)
<input type="checkbox"/> @CVEreport	CVE-2022-0210 : The Random Banner WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient... twitter.com/i/web/status/1...	2022-01-18 17:12:47
<input type="checkbox"/> @LinInfoSec	Php - CVE-2022-0210: wordfence.com/vulnerability-...	2022-01-18 21:01:21

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 |

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](#)