



SEP 10, 2022 | WEB | RESEARCH

CVE-2021-36568



Kirito
HACKER

Description

After the creation of a course it is possible to add into the resources database, with text input, where in the "Field name" and "Field description" are vulnerable to Cross-Site Scripting Stored (XSS)

Proof of Concept (POC)

To exploit the vulnerability it is necessary that an user gets access to the course and click into the option "Search"

The affected fields are: "Field name" and "Field description" , both text input.

Attacker

0:00 / 0:36

Victim

0:00 / 0:17

Affected Versions

3.9.7

3.10.4

3.11

References

CVE: CVE-2021-36568

Classification

Type: Cross-Site Scripting

OWASP TOP 10: [A03:2021-Injection](#)

CWE: [CWE-79 Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)

Researchers/Hackers

Thiago Martins, Leandro Inacio, Matheus Oliveira e Lucas Gomes

Support us

Hacking Force is a community focused on spreading knowledge about technology and cyber security, offering a way for people to rise. We are grateful for being supported by people with the same point of view. If you identify with it, then consider joining us.

contact@hackingforce.com.br

PRINCIPAL SPONSORS

nowGY

Blog Hacking Force © 2022

