SEP 10, 2022 | WEB | RESEARCH

CVE-2021-36568

Kirito

HACKER

Description

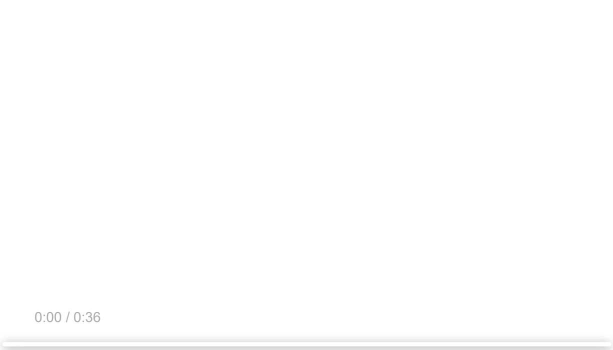
After the creation of a course it is possible to add into the resources database, with text input, where in the "Field name" and "Field description" are vulnerable to Cross-Site Scripting Stored (XSS)

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



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