CVE-2022-29603: High-Severity SQL Injection Vulnerability in UniverSIS

By Stavros Mekesis on April 24, 2022

CVE-ID: CVE-2022-29603
Affected Products: UniverSIS-API versions prior to commit 39e47d7f
Class: Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’) (CWE-89)
Discovered by: Stavros Mekesis

Vulnerability Details

An SQL Injection vulnerability exists in UniverSIS-API versions prior to commit 39e47d7f via the `$select` parameter in multiple API endpoints due to improper validation of user-supplied input to the `$select` parameter. A remote authenticated attacker could send specially crafted SQL statements to a vulnerable UniverSIS API endpoint (e.g. `/api/students/me/messages/`) using the `$select` parameter, which could allow the attacker to view, add, modify or delete information in the back-end database.

Proof of Concept

SQL injection can be detected manually by submitting the single quote character (’) and looking for errors or other anomalies (see Fig. 1).

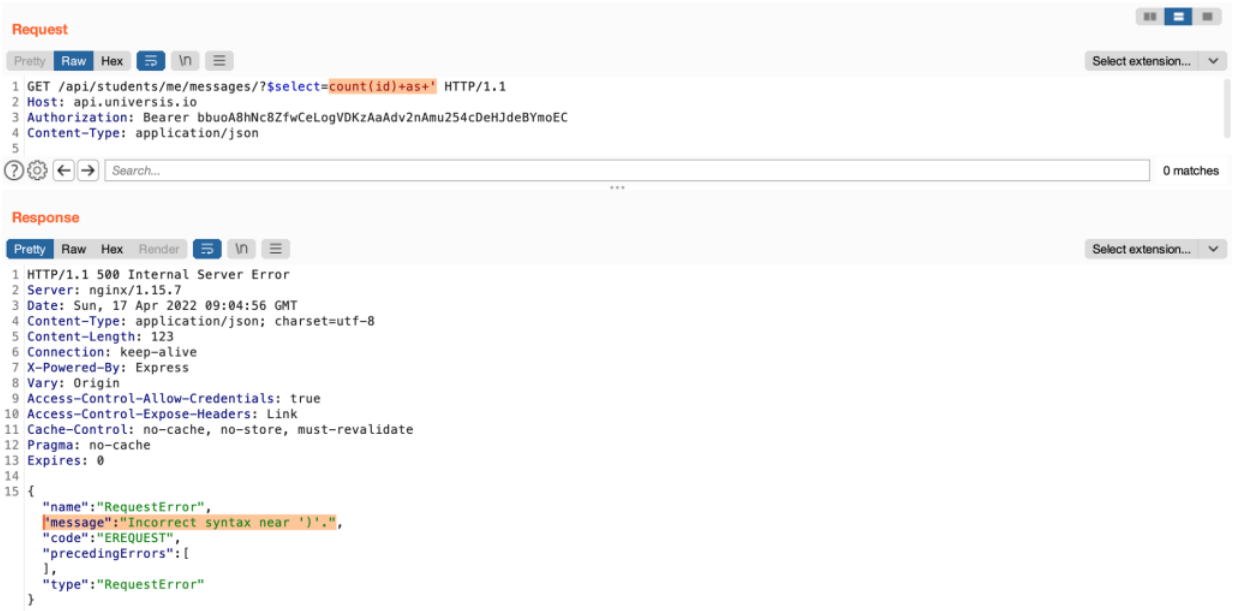

Fig. 1. Verifying that the $select parameter is vulnerable to SQL Injection.

A remote authenticated attacker can leverage the SQL injection vulnerability to retrieve data from other tables within the database. For example, the following request will cause the application to return all IDs, given names, family names, father's names, mother's names, Social Security numbers, home addresses, home phones, and mobile phones from the `PersonData` table (see Fig. 2).

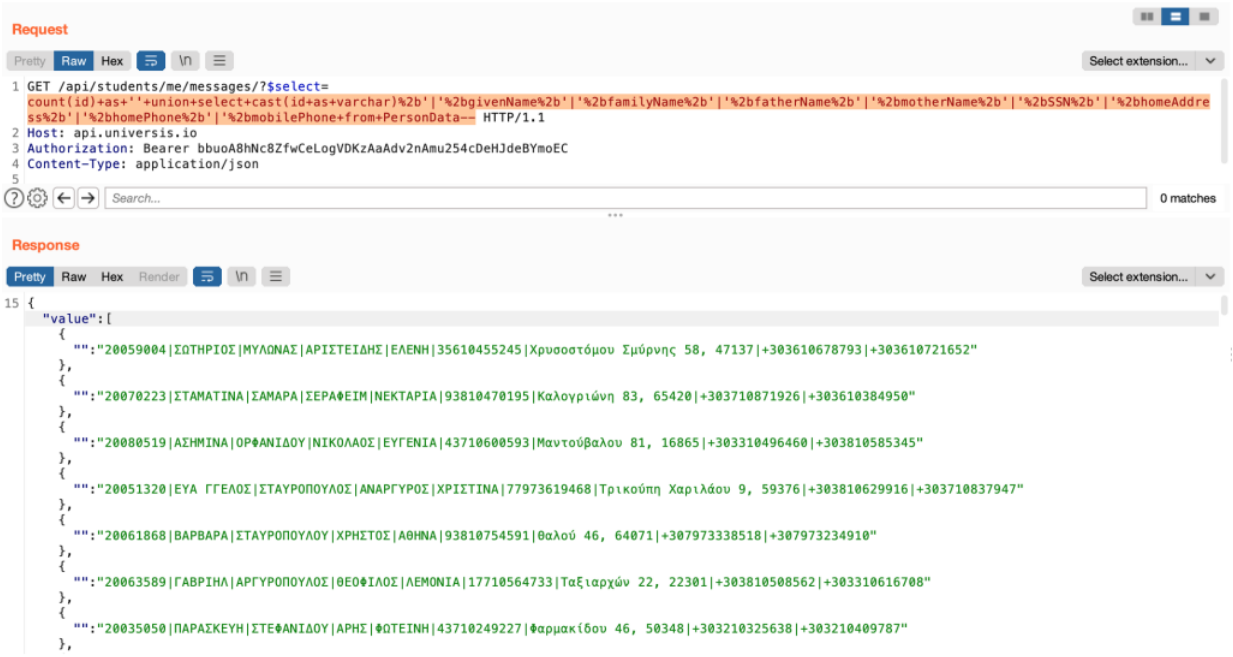

Fig. 2. Retrieving sensitive personal data from the PersonData table. NOTE: The 'demo' application uses dummy data.

Also, the attacker can leverage the SQL injection vulnerability to modify information in the back-end database. For example, the following request will cause the application to change the thesis grade for Μιχαλόπουλος Αντώνιος (student7@example.com) to “10” (see Fig. 3–5).

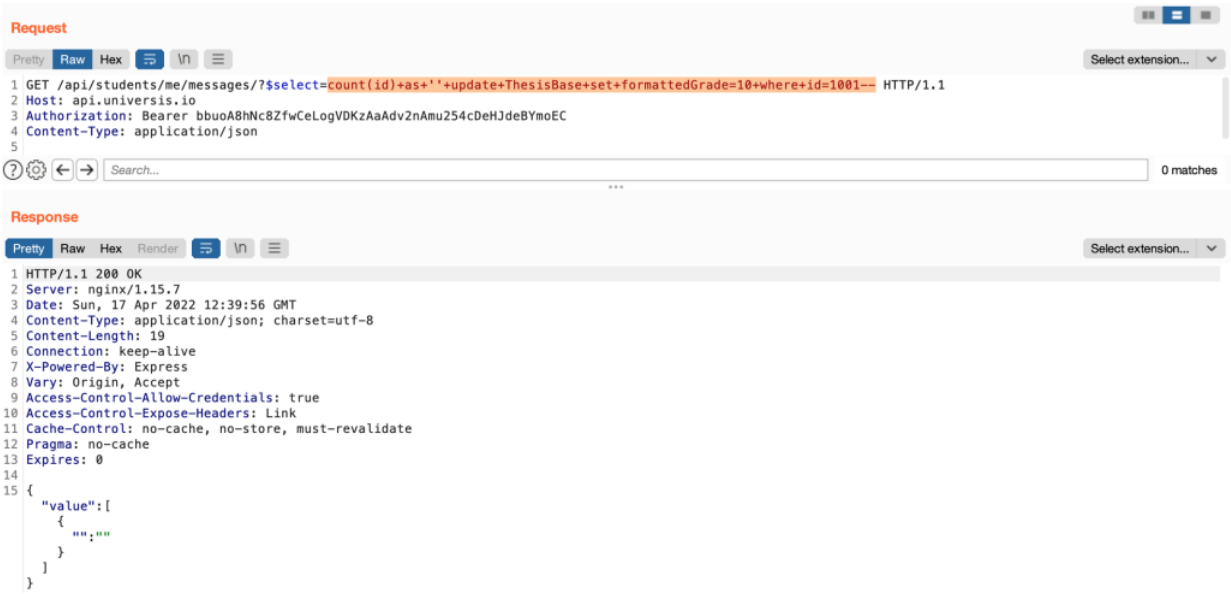

Fig. 3. Changing the thesis grade for Μιχαλόπουλος Αντώνιος (student7@example.com) to "10".

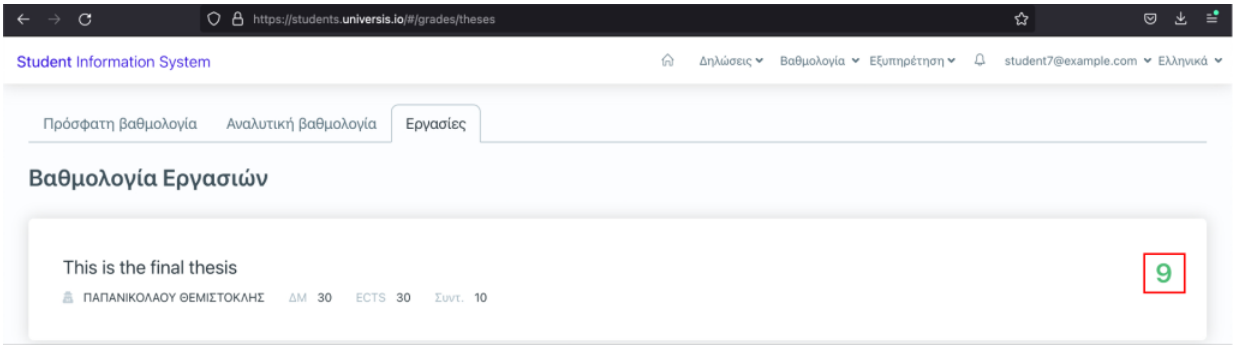

Fig. 4. The thesis grade before the SQL Injection attack.

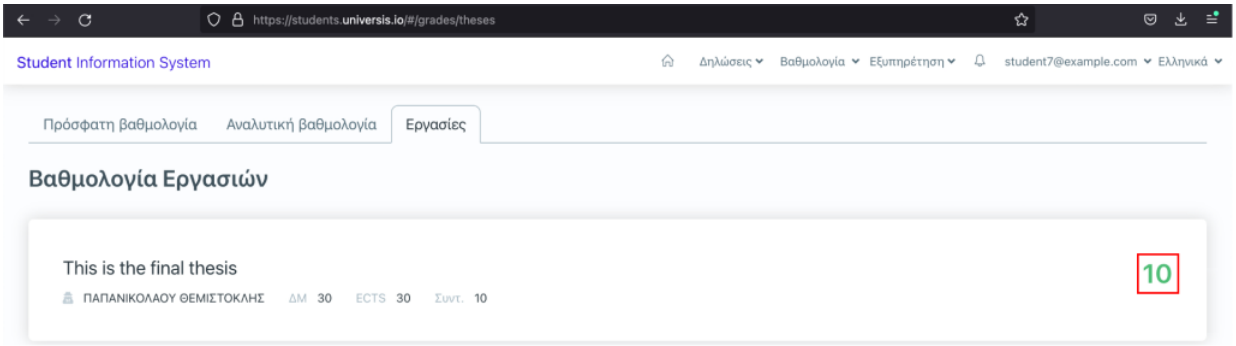

Fig. 5. The thesis grade after the SQL Injection attack.

Remediation

UniverSIS has released a patch for this vulnerability on GitLab. Please apply the patch as soon as possible.

Responsible Disclosure Timeline

Vendor Contact: April 17, 2022
Vendor Fix Released: April 18, 2022
Public Advisory: April 24, 2022
CVE Allocation: April 25, 2022

In the News

“Student grades stored in Greek education platform UniverSIS could be manipulated via SQLi.” The Daily Swig (PortSwigger).

Previous
CVE-2022-28924: Sensitive Information Disclosure Vulnerability in UniverSIS

Next
Interview: Student grades stored in Greek education platform UniverSIS could be manipulated via SQLi