CVE-2020-6637 (https://cinzinga.com/CVE-2020-6637/)

2 minute read

OpenSIS v7.3 is vulnerable to unauthenticated SQL injection via the 'username' field, this allows for remote database compromise as well as authentication bypass. The following is a brief write-up of the identification, exploitation, and reporting of CVE-2020-6637 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6637).

The Software

Wikipedia (https://en.wikipedia.org/wiki/OpenSIS) describes OpenSIS as the following:

> *OpenSIS is one of several free and open source student information system available to K-12 and higher education institutions. The solution has been in development for several years and appears to have much of the functionality that long time commercial versions have.*

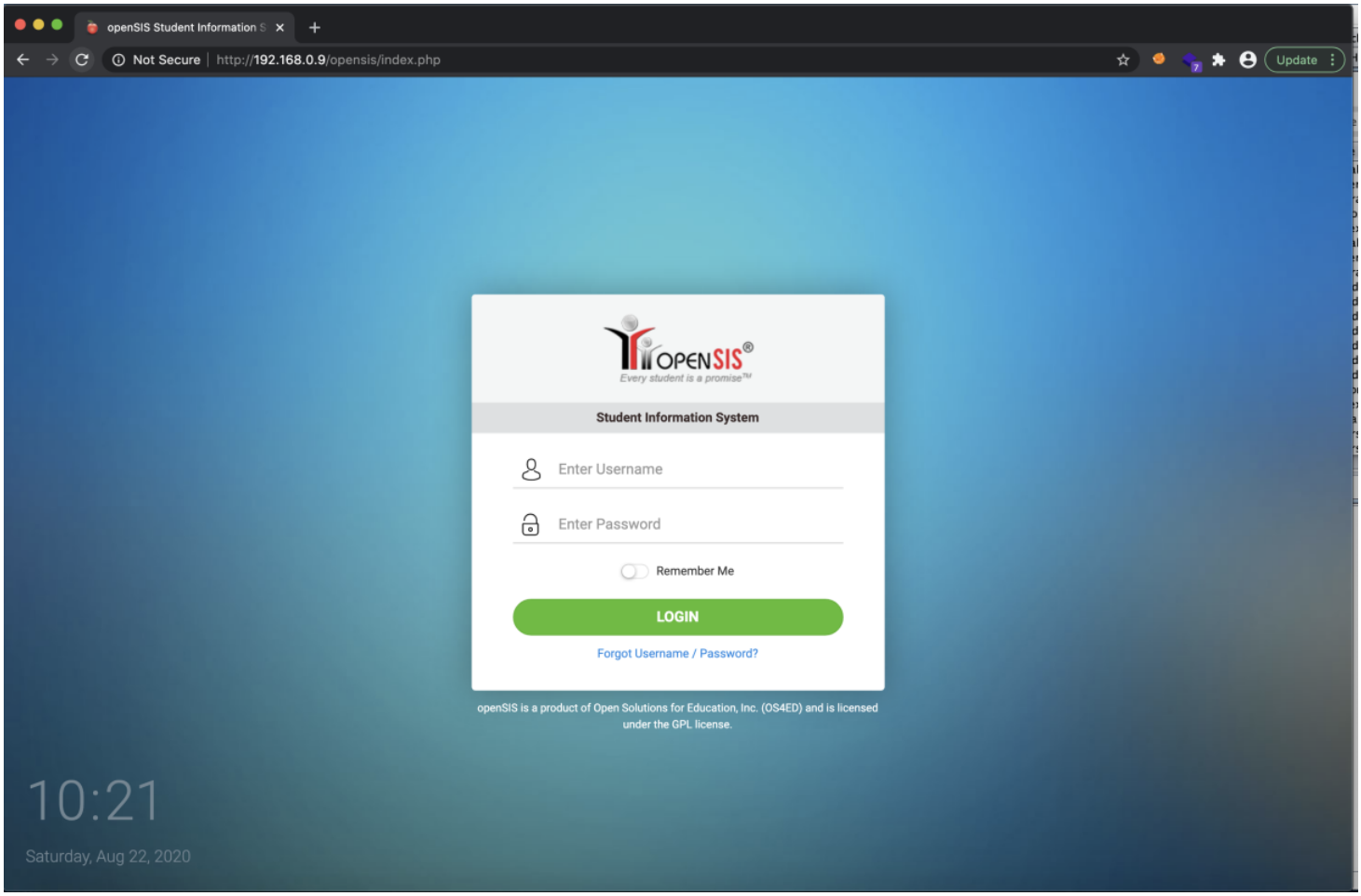
The community edition of the software can be obtained here (https://sourceforge.net/projects/opensis-ce/).

Selecting software to review for vulnerabilities can be very hit or miss. There are a handful of reasons I decided to look into this software:

1. Written in PHP with a SQL database. This is often a recipe for vulnerabilities.
2. History of vulnerabilities on Exploit-DB (https://www.exploit-db.com/search?q=opensis), if bugs existed in the past, more will likely exist in the future.
3. This software is a school information system. That means it protects a lot of juicy PII and the impact of any bugs is greatly magnified.

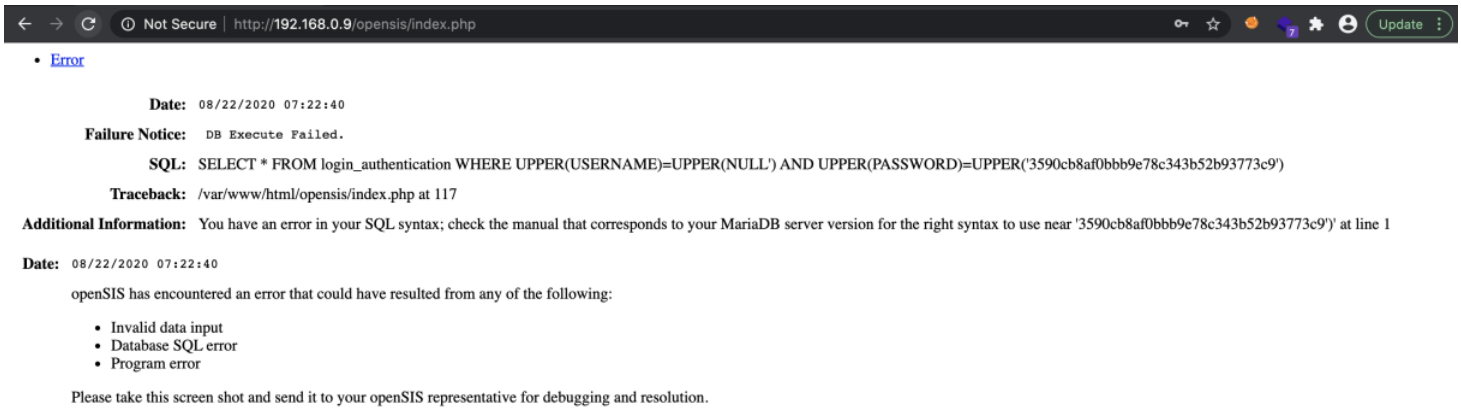
The Bug

After installing OpenSIS locally, one will be greeted with the following login screen.



Checking for SQL injection on the login page is perhaps one of the quickest and easiest check one can perform when analyzing a web application. It takes just a few seconds to drop a `'` in the username password fields and pray for that `Error in your SQL Synax` message.

Lo and behold...



Not only does the web application tell us we have an error in our SQL syntax, it also provides an incredibly detailed error message that includes the whole SQL query. At this point, one could fire up SQLMap and exploit this error based SQL injection; however, let's first look at the error message and code further.

Line 117 of index.php is show below.

```
$login_uniform = DBGet(DBQuery('SELECT * FROM login_authentication WHERE UPPER(USERNAME)=UPPER(\'' . $username . '\') AND UPPER(PASSWORD)=UPPER(\'' . $password . '\')'));
```

Placing a SQL query directly in PHP code is never a recommended practice. In the photo above, it is clear where our `'` is reflected in the SQL string.

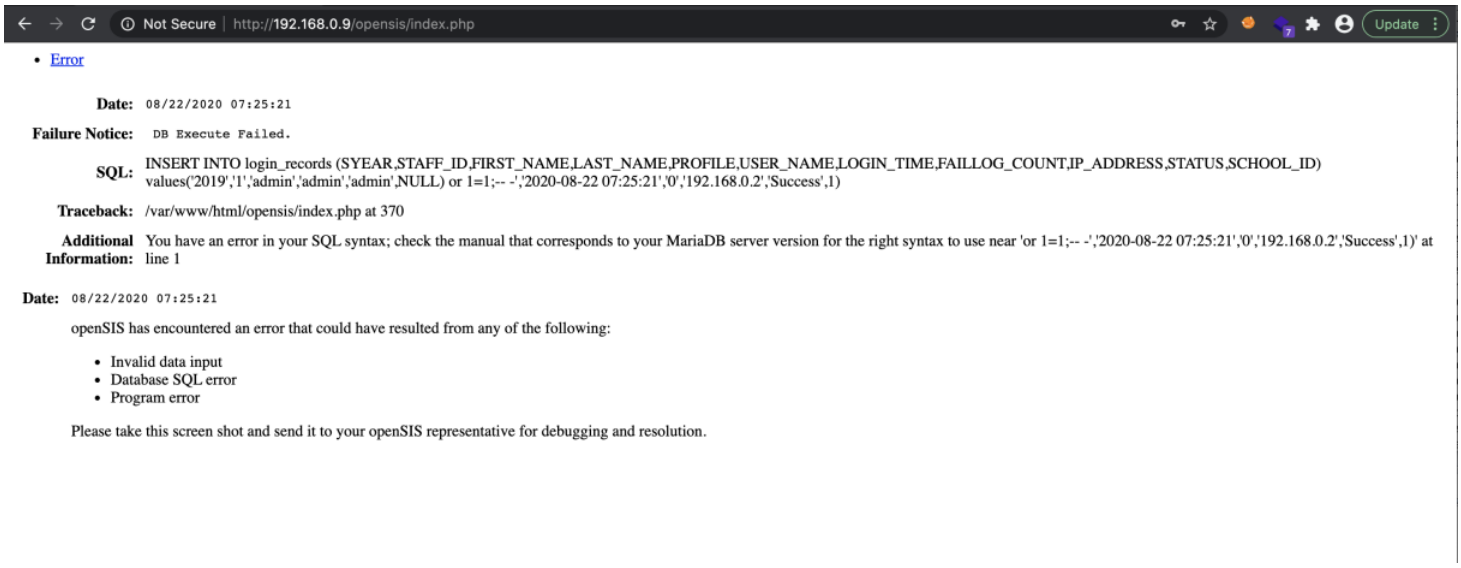
Payload: `'`
SQL Query:

```
SELECT * FROM login_authentication WHERE UPPER(USERNAME)=UPPER(NULL') AND UPPER(PASSWORD)=.....
```

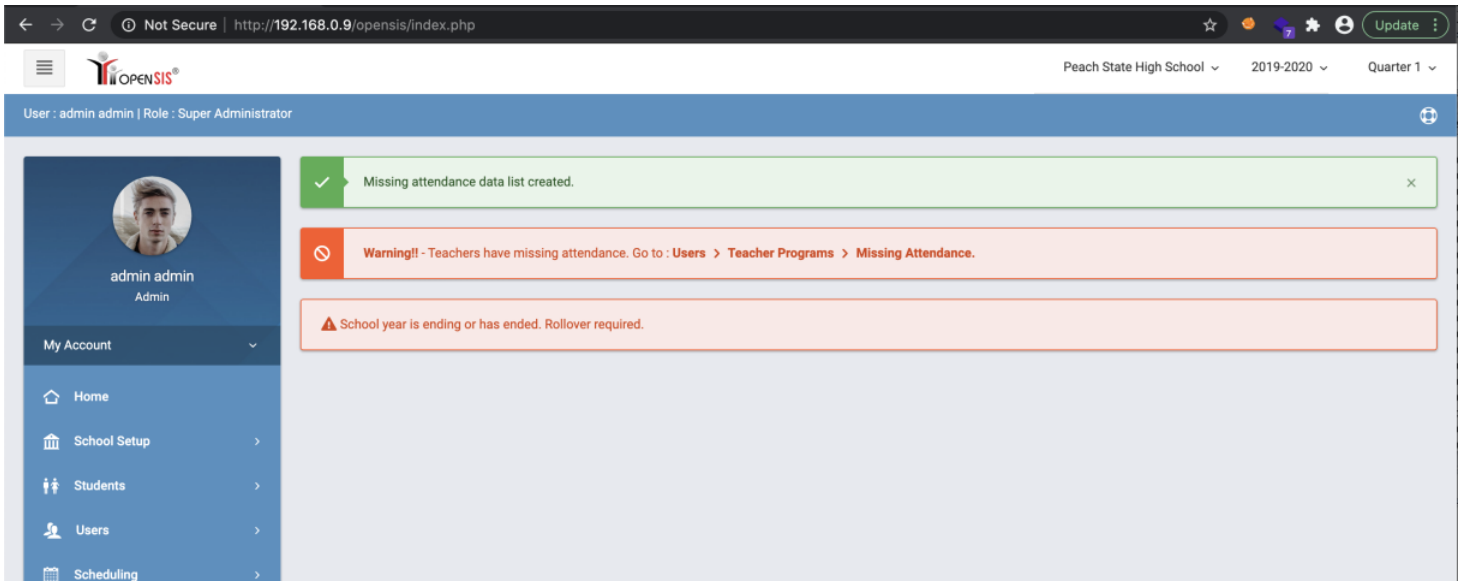
Thus by changing our payload slightly we may be able to utilize tautology to cause this query to return `true`.

Payload: `') or 1=1;-- -`
SQL Query:

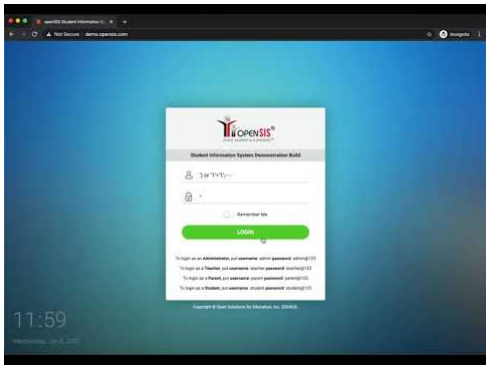
```
SELECT * FROM login_authentication WHERE UPPER(USERNAME)=UPPER(NULL') or 1=1;-- -) AND UPPER(PASSWORD)=.....
```



Interestingly enough, this returned an `INSERT` SQL statement, but upon refreshing the page, one would be logged in as the administrator.



A video POC is shown below against the OpenSIS demo site.



(https://www.youtube.com/watch?v=IDc_3kwse5Q)

(Note: after contacting OpenSIS I was given explicit permission to demonstrate this vulnerability against their demo site)

Timeline

7 January 2020 - Bug discovered and reported to OpenSIS.
8 January 2020 - Response recieved and video POC requested.
8 January 2020 - CVE reserved.
13 January 2020 - Issue patched.
16 January 2020 - Code pushed to SourceForge.
23 August 2020 - Sufficient time has passed, CVE publicly disclosured via blog post.

Conclusion

While using this simple SQL tautology no longer bypasses authentication, the newest version of OpenSIS still throws a verbose SQL syntax error if a ' is submitted upon login. Thus, database compromise still may be possible with the assistance of SQLMap. Preliminary Google Dork-ing reveals the existance of many school using OpenSIS with each being (potentially) vulnerable to unauthenticated SQL injection.

"openSIS is a product of Open Solutions for Education, Inc. (OS4Ed)."

All News Images Maps Videos More Settings Tools

About 270 results (0.48 seconds)

[redacted]com

openSIS Student Information System

Login. Forgot Username / Password? **openSIS is a product of Open Solutions for Education, Inc. (OS4ED)** and is licensed under the GPL license.

Tags: Exploit-Dev Penetration Testing

Updated: August 23, 2020