SQL Injection was found in the /lms/search_class.php of the kashipara E-learning Management System project v1.0 , Allows remote attackers to execute arbitrary SQL command to get unauthorized database access via the school_year parameter in a POST HTTP request.

- **Official Website URL**

  https://www.kashipara.com/project/php/13138/e-learning-management-system-php-project-source-code

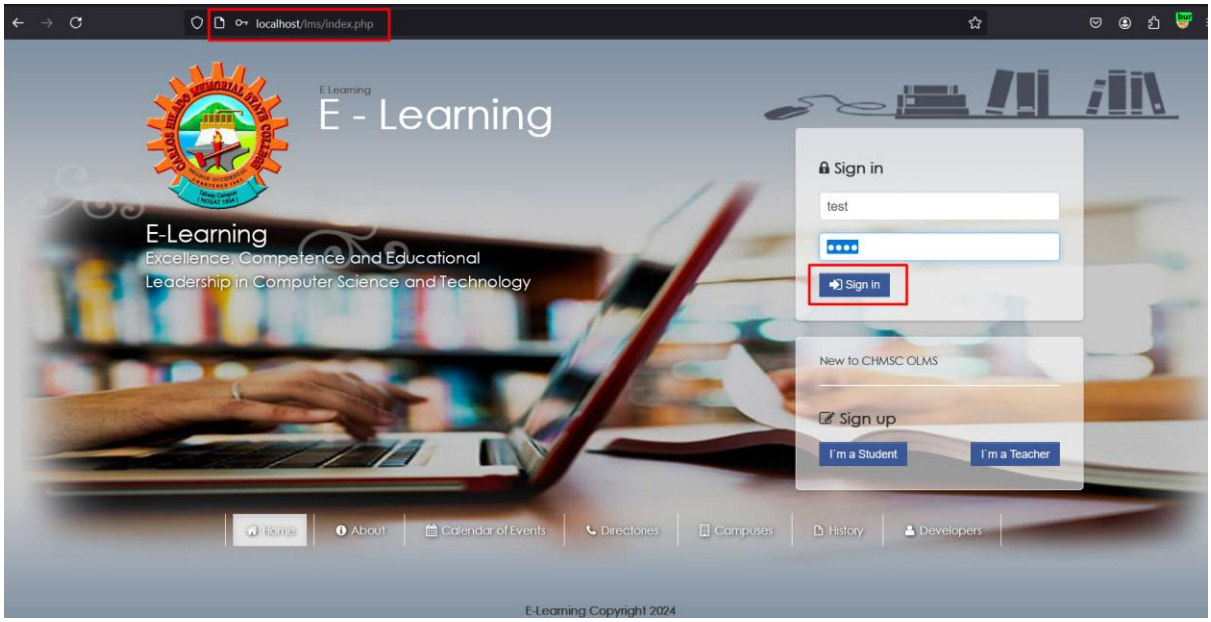
- **Affected Product Name**

  E-learning Management System project in PHP with source code and document

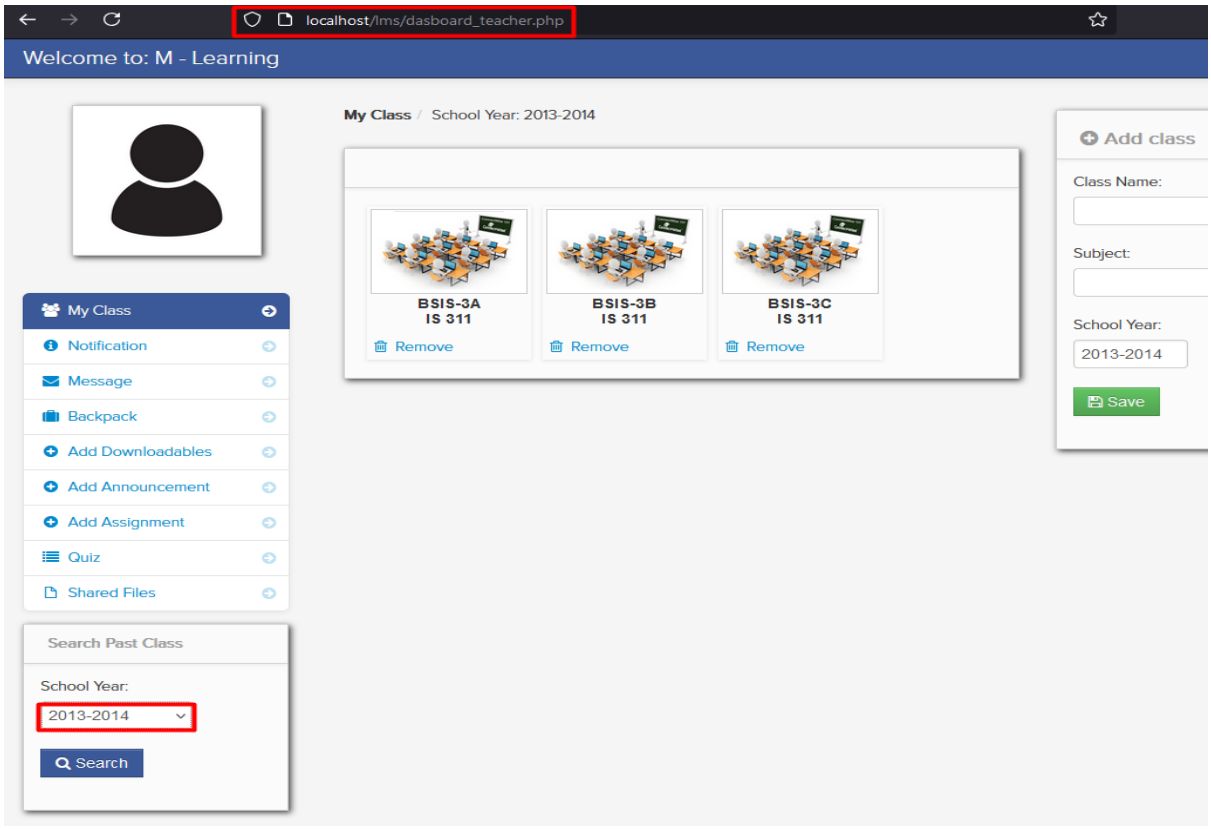
Affected Vendor	kashipara
Affected Code File	/lms/search_class.php
Affected Parameter	school_year
Method	POST
Type	boolean-based blind, time-based blind, UNION query
Version	V1.0

Steps to Reproduce:

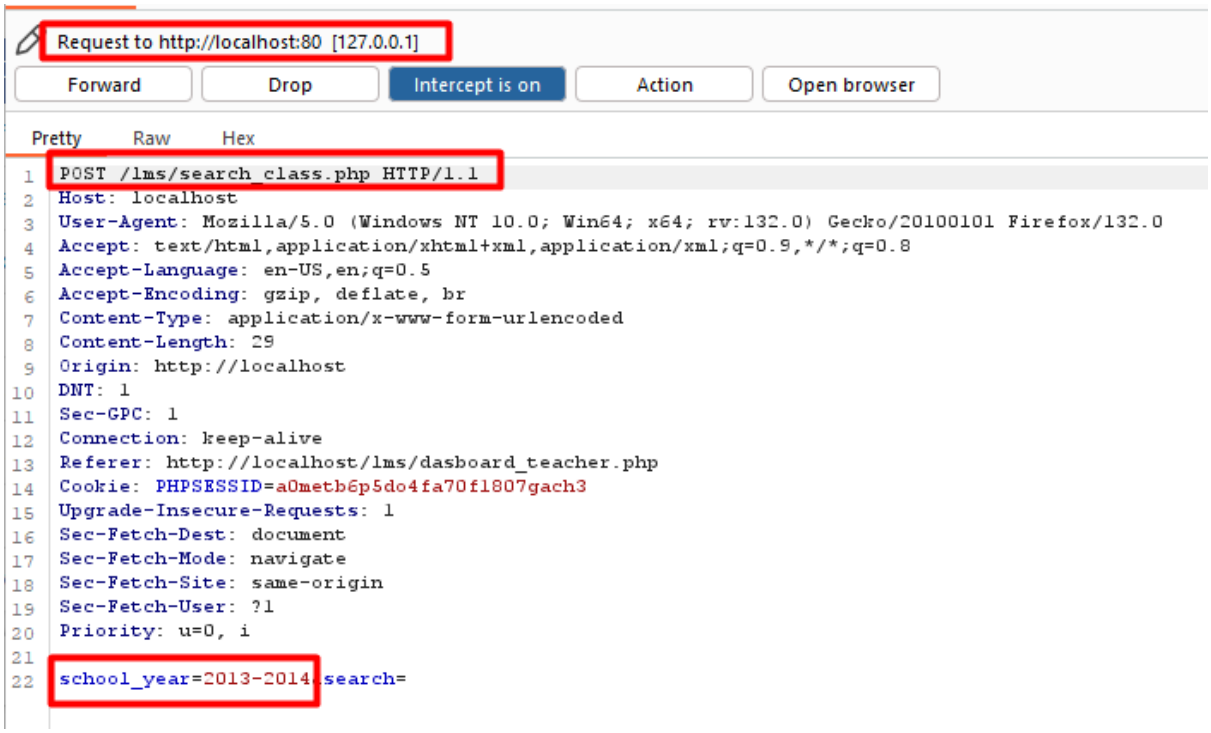
Step 1: Visit to login page and login with teacher credential.



Step 2: Navigate the 'School Year' search box and select year from list.

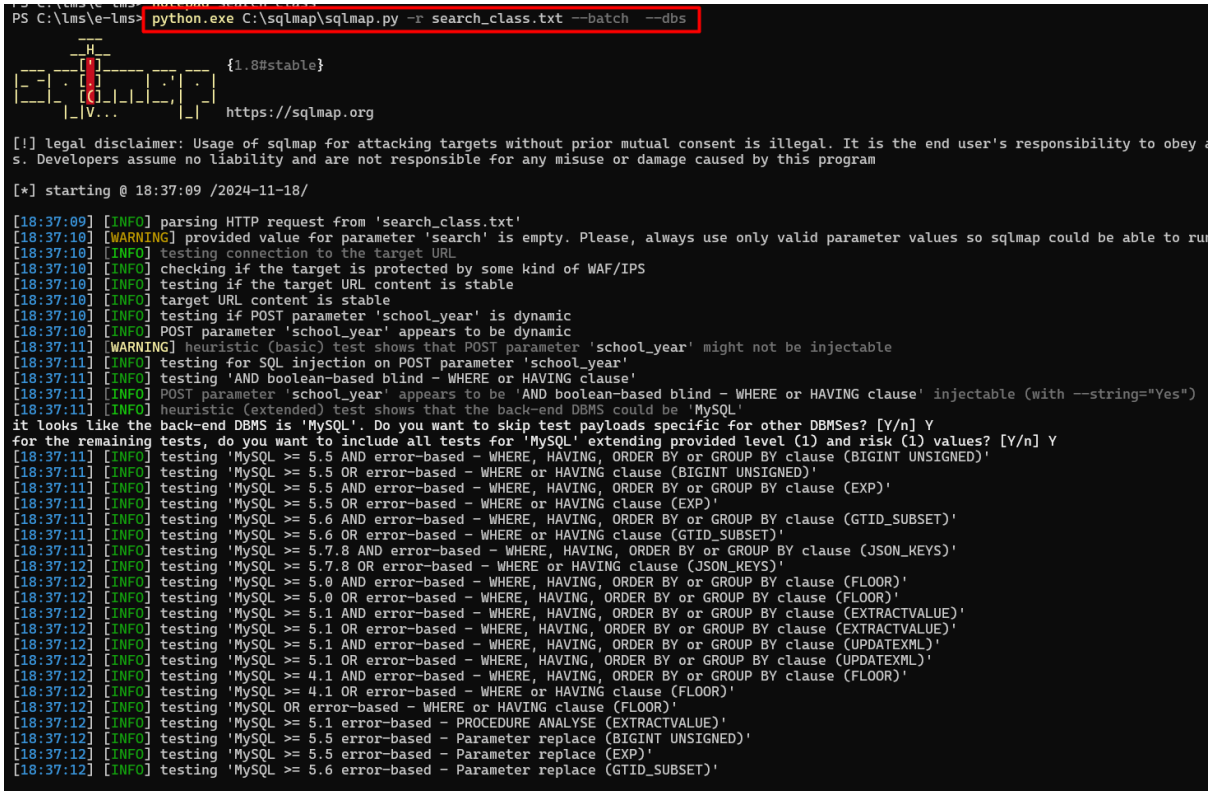


Step 3: Now enable intercept in bupsuite and click on 'Search' button. Save the burpsuite request in a file.

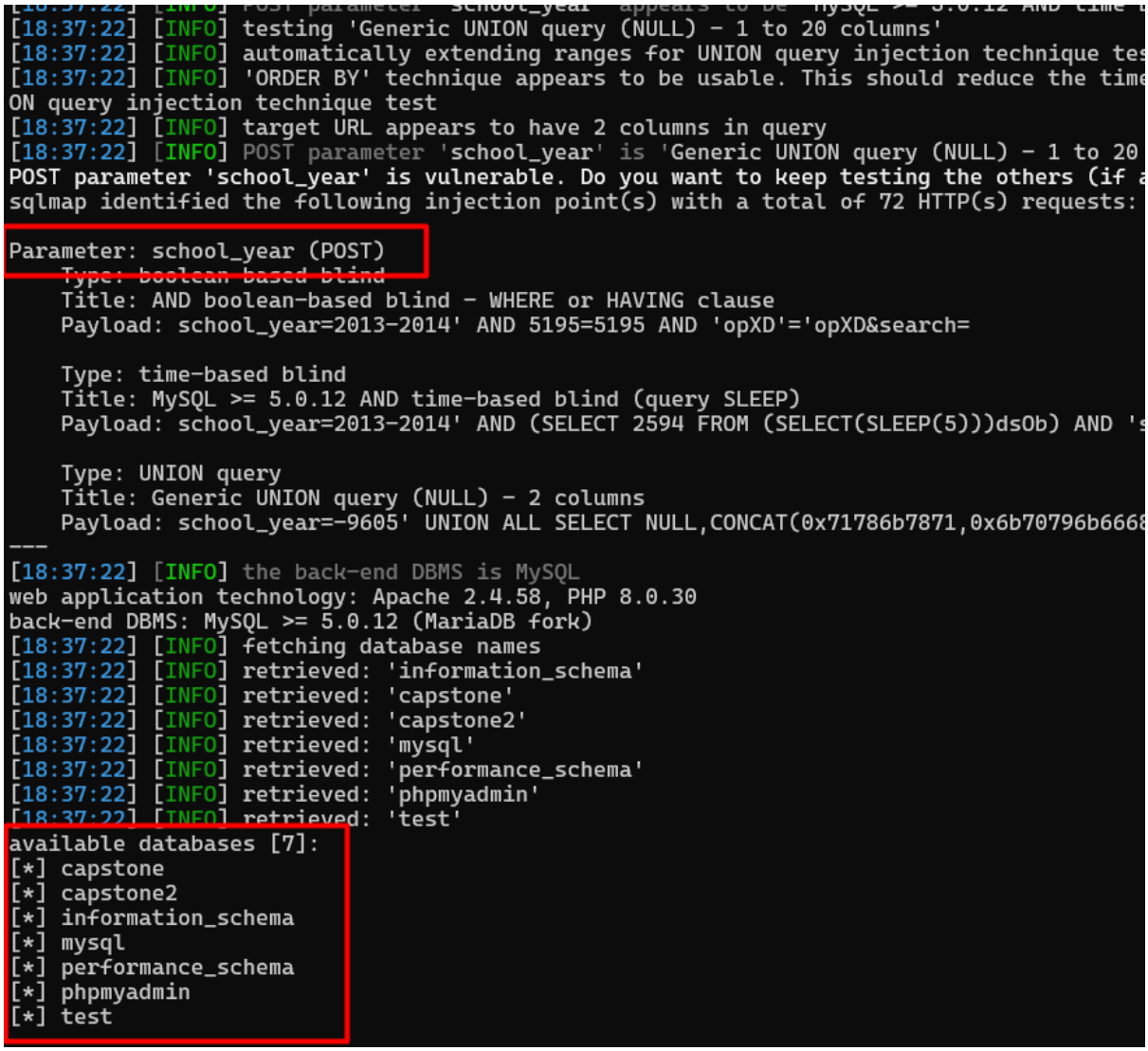


Step 4: Now run the sqlmap command against request saved in file.

- python.exe C:\sqlmap\sqlmap.py -r search_class.txt --batch --dbs



Step 5: Now notice that 'school_year' parameter is detected vulnerable and all database is successfully retrieved.



Mitigation/recommendations

- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
- https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection