## Vulnerability analysis

The search.php script accepts two inputs: a numerical one representing the issue number, and a string one representing the issue title. They cannot be both empty. The string input is not vulnerable to SQL injection since it is escaped. On the contrary, the numerical input can be exploited, resulting in a blind SQL injection.

We can test the vulnerability with Burp by sending the payload:

```
dydnum=0%2b1&dydtitle=
```

and checking that the result page is not abnormal, and it coincides with the page returned by the body:

```
dydnum=1&dydtitle=
```

This means that the 0+1 operation gets evaluated by the SQL server.