jsjbcyber Update bug_p History

1 contributor

35 lines (32 sloc) | 1.52 KB

```
Build environment with PHP5.
--------------------------------
affected source code file: /admin/templates/template_manage.php
--------------------------------
affected source code:

  ......
        <?php
            //$arr = $array_file[];
            //foreach ($array_file as $key => $value){
            $filename = $_GET["filename"];
            $foldername = $_GET["foldername"];
            //echo "$filename:".$filename."<br>";
            //echo "$foldername:".$foldername."<br>";
            $act = $_GET["act"];
            $file_content = stripslashes($_POST["file_content"]);
            //echo stripslashes($file_content);
            //die();
            if($act == "tmod"){
              file_put_contents(ROOT.$templatedir.$filename,$file_content);
              echo "<script>alert('修改成功!');window.location='template_manage.php';</script>";
            }
            //die();
            $temp_manage->setdirvar($dir,$templatedir,$filename,$foldername);
        ?>
  ......


--------------------------------
affected executable:
```

```
After Signing in to the background in advance. Then we can visit the following URL: http://xx.xx
Also, we use POST-method to post data "file_content=<?php phpinfo();?>";
Then, we can find that the file we wrote in the /template directory under the root directory - t
we visit http://xx.xx.com/template/test.php and get the phpinfo informations.

So, we can also write a shell file for controlling the system.
```