New issue

Jump to bottom

UCMs v1.6.0 arbitrary file upload #1

Open **cc-225** opened this issue on Jul 4 · 0 comments

cc-225 commented on Jul 4 Owner

UCMS_v1.6.0 Arbitrary file upload vulnerability

Vulnerability type:

V 1.6.0

Recurrence environment:

Windows 10

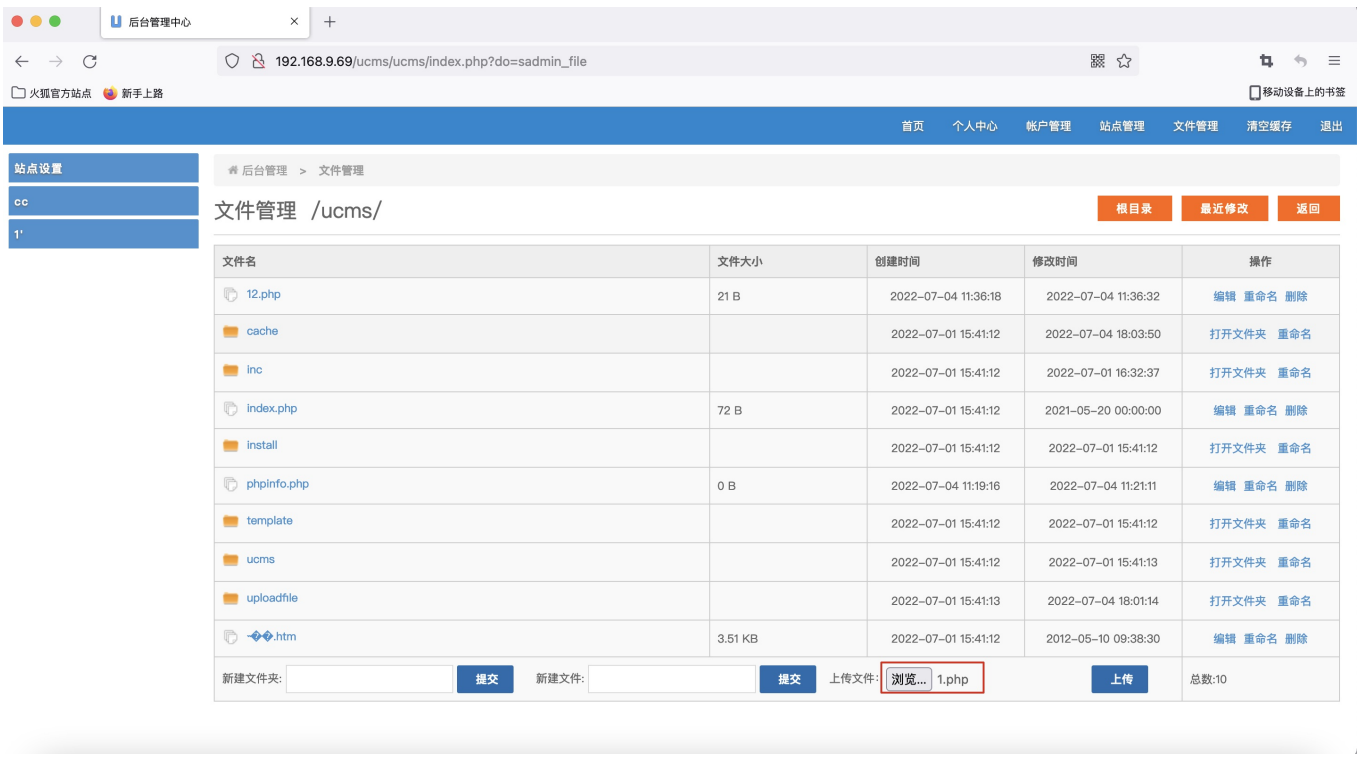
phpstudy

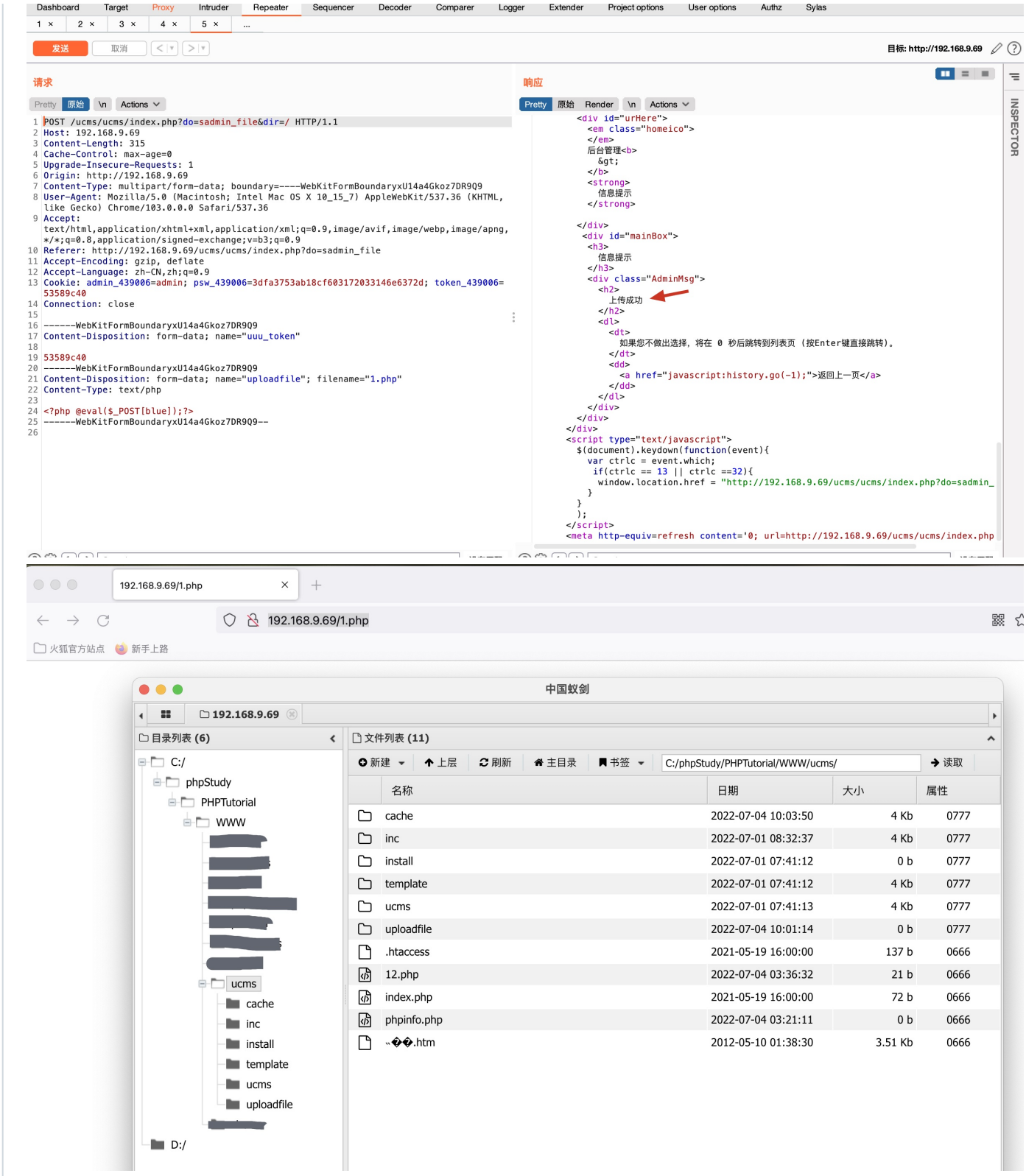
Vulnerability description:

The vulnerability lies in /ucms-v1.6/ucms/sadmin/file PHP file, the file suffix on is not verified, so any file can be uploaded

Loophole recurrence:

```php
if(isset($_FILES['uploadfile'])) {
    checktoken();
    if(!isset($_SERVER["HTTP_REFERER"])) {
        die('error');
    }
    if(stripos($_GET['dir'],'..')===false) {}else {die('error file');}
    if(is_uploaded_file($_FILES['uploadfile']['tmp_name'])){
        $filaname=$alldir.$_FILES["uploadfile"]["name"];
        if(@move_uploaded_file($_FILES['uploadfile']['tmp_name'],$filaname)) {
            adminmsg($refererurl,'上传成功',0);
        }else {
            adminmsg($refererurl,'上传失败,无法写入文件,请确认目录权限',1);
        }
        exit();
```





Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant