Day 6 - Frost Pattern | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:12:23 发布 247 收藏

RIPSTECH PRESENTS PHP SECURITY CALENDAR 是由 RIPS 团队出品的PHP代码安全审计挑战系列题目，RIPSTECH PRESENTS PHP SECURITY CALENDAR 2017 共包含24道题目（Day 1 ~ 24），每道题目将包含一个较新颖的知识点供大家学习。

VULNSPY 提供在线实验环境让您可以在线进行模拟渗透测试，在线体验 RIPSTECH PRESENTS PHP SECURITY CALENDAR。

在线实验环境和Writeup: http://www.vulnspy.com/cn-ripstech-presents-php-security-calendar-2017/

查看更多内容，点击右上角 `START TO HACK` 可以快速访问在线实验环境。

你能从下列代码中发现安全漏洞吗？

```
class TokenStorage {
    public function performAction($action, $data) {
        switch ($action) {
            case 'create':
                $this->createToken($data);
                break;
            case 'delete':
                $this->clearToken($data);
                break;
            default:
                throw new Exception('Unknown action');
        }
    }

    public function createToken($seed) {
        $token = md5($seed);
        file_put_contents('/tmp/tokens/' . $token, '...data');
    }

    public function clearToken($token) {
        $file = preg_replace("/[^a-z.-_]/", "", $token);
        unlink('/tmp/tokens/' . $file);
    }
}

$storage = new TokenStorage();
$storage->performAction($_GET['action'], $_GET['data']);
```

本题的问题是在于`clearToken()`中的正则表达式`[^a-z.-_]`。按照代码的本意是，是将非`a-z`、`.`、`-`、`_`全部替换为空。这样`../../../`目录穿越的方式就无法使用了，因为`/`会被替换为空。