Day 5 - Postcard | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:11:37 发布 222 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。

Day 5 - Postcard

你能从下列代码中发现安全漏洞吗？

```
class Mailer {
    private function sanitize($email) {
        if (!filter_var($email, FILTER_VALIDATE_EMAIL)) {
            return '';
        }

        return escapeshellarg($email);
    }

    public function send($data) {
        if (!isset($data['to'])) {
            $data['to'] = 'none@vsplate.com';
        } else {
            $data['to'] = $this->sanitize($data['to']);
        }

        if (!isset($data['from'])) {
            $data['from'] = 'none@vsplate.com';
        } else {
            $data['from'] = $this->sanitize($data['from']);
        }

        if (!isset($data['subject'])) {
            $data['subject'] = 'No Subject';
        }

        if (!isset($data['message'])) {
            $data['message'] = '';
        }

        mail($data['to'], $data['subject'], $data['message'],
             '', "-f" . $data['from']);
    }
}

$mailer = new Mailer();
$mailer->send($_POST);
```

这个漏洞其实就是`mail()`函数的漏洞，我们同样需要通过`mail()`中的第五个参数以`-X`的方式写入webshell。但是中途进行了两次过滤，分别是`filter_var($email, FILTER_VALIDATE_EMAIL)`和`escapeshellarg($email)`。我们接下来分别分析这两个过滤函数。