Day 2 - Twig | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:08:50 发布
文章标签： 代码审计

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 2 - Twig

你能从下列代码中发现安全漏洞吗？

```
// composer require "twig/twig"
require 'vendor/autoload.php';

class Template {
    private $twig;

    public function __construct() {
        $indexTemplate = '<img ' .
            'src="https://loremflickr.com/320/240">' .
            '<a href="{{link|escape}}">Next slide »</a>';

        // Default twig setup, simulate loading
        // index.html file from disk
        $loader = new Twig\Loader\ArrayLoader([
            'index.html' => $indexTemplate
        ]);
        $this->twig = new Twig\Environment($loader);
    }

    public function getNexSlideUrl() {
        $nextSlide = $_GET['nextSlide'];
        return filter_var($nextSlide, FILTER_VALIDATE_URL);
    }

    public function render() {
        echo $this->twig->render(
            'index.html',
            ['link' => $this->getNexSlideUrl()]
        );
    }
}

(new Template())->render();
```

在 26 行存在XSS漏洞。该题首先使用 `filter_var()` 函数来判断了传入参数是否合法的URL（第22行），然后再次使用模板引擎 `Twig` 自带的方法来转义URL（第10行）