Day 9 - Rabbit | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:14:55 发布 227 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 9 - Rabbit

你能从下列代码中发现安全漏洞吗？

```
class LanguageManager
{
    public function loadLanguage()
    {
        $lang = $this->getBrowserLanguage();
        $sanitizedLang = $this->sanitizeLanguage($lang);
        require_once("/lang/$sanitizedLang");
    }

    private function getBrowserLanguage()
    {
        $lang = $_SERVER['HTTP_ACCEPT_LANGUAGE'] ?? 'en';
        return $lang;
    }

    private function sanitizeLanguage($language)
    {
        return str_replace('../', '', $language);
    }
}

(new LanguageManager())->loadLanguage();
```

这个题目是一个比较明显的任意文件包含的漏洞，主要的漏洞是出在`str_replace('../', '', $language)`。这个包含只是单次替换而不是循环替换，所以这种替换就很容易被绕过。
如`..././`、`....//`。其次`$_SERVER['HTTP_ACCEPT_LANGUAGE']`这个变量是客户端可控的。